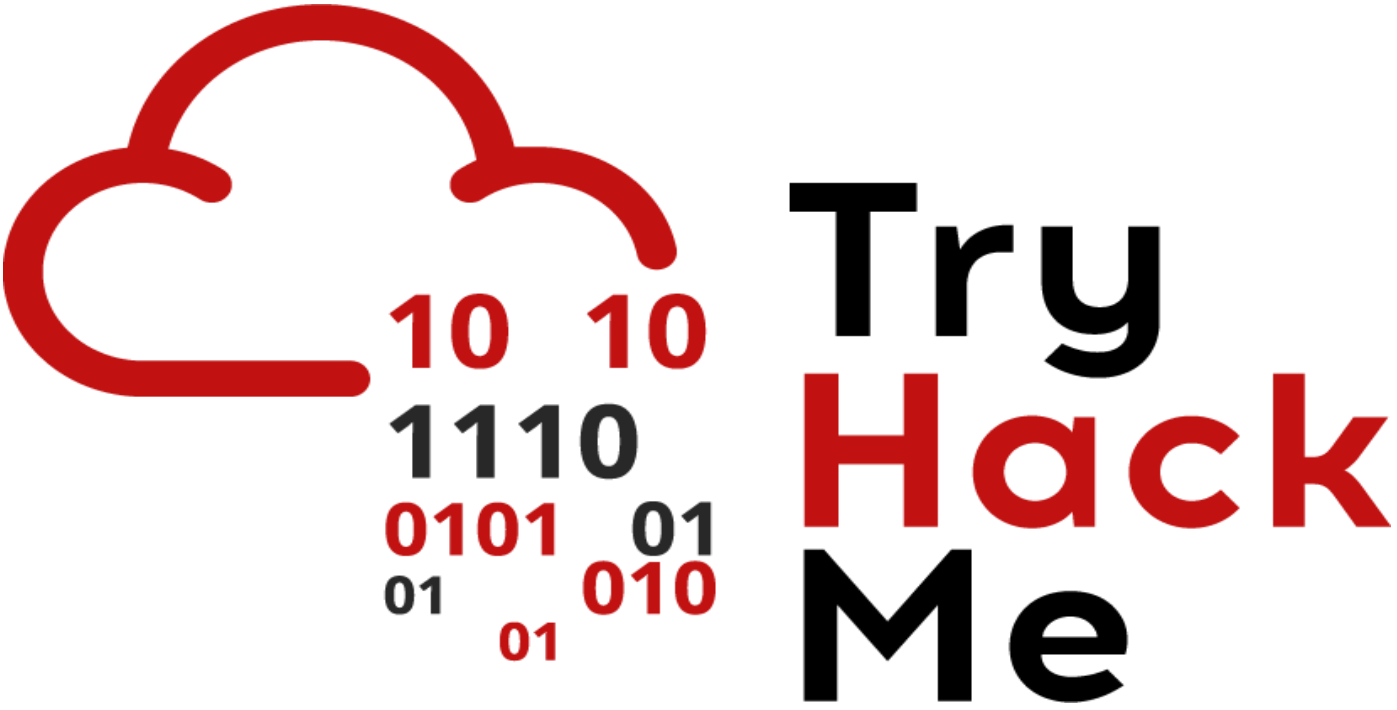
Host Forensic Analysis

Tool: TryHackMe.com



Carter Wright | ITT-340 | April 19, 2026

Contents

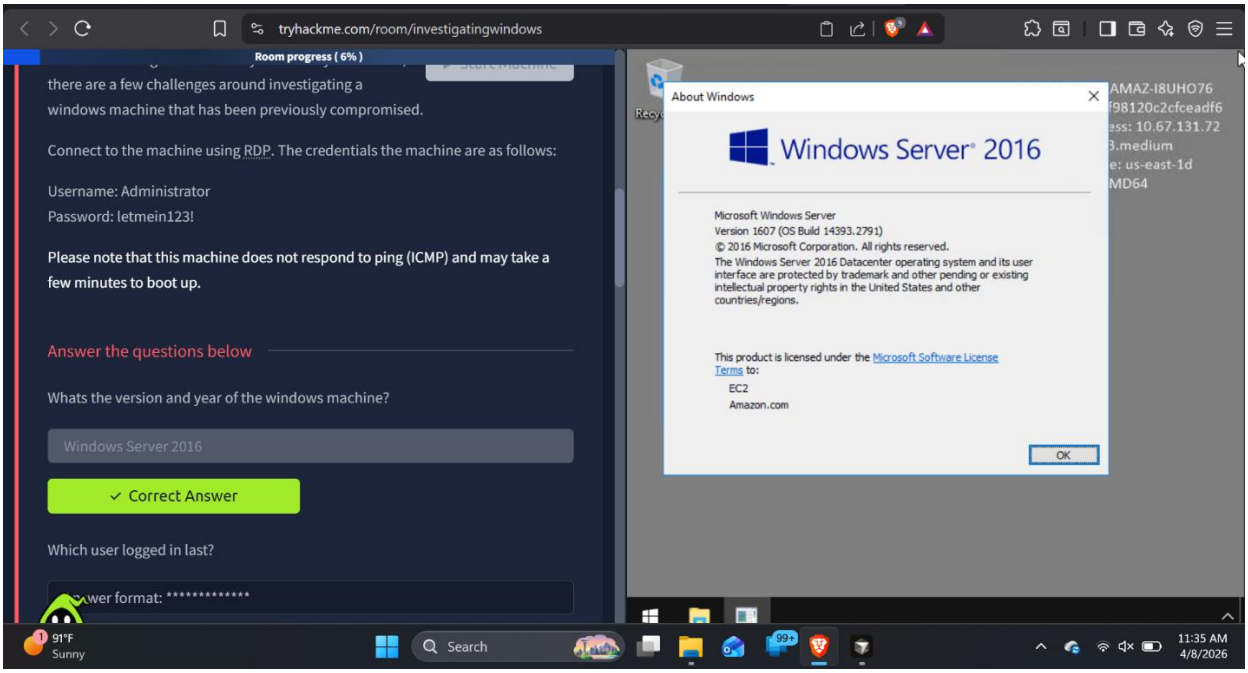
Introduction – Investigating Windows VM

A host forensic analysis was performed on a compromised Windows Server 2016 virtual machine from the TryHackMe “Investigating Windows” lab. The goal of this investigation was to figure out how the attacker got in, what they did once inside the system, and what evidence they left behind. By reviewing system logs, file system artifacts, scheduled tasks, and network activity, a clear timeline of the attack was put together along with a better understanding of the attacker’s intent. This analysis also looks at ways the attack could have been prevented and whether the evidence collected could be used in a legal case.

TryHackMe Investigation Evidence

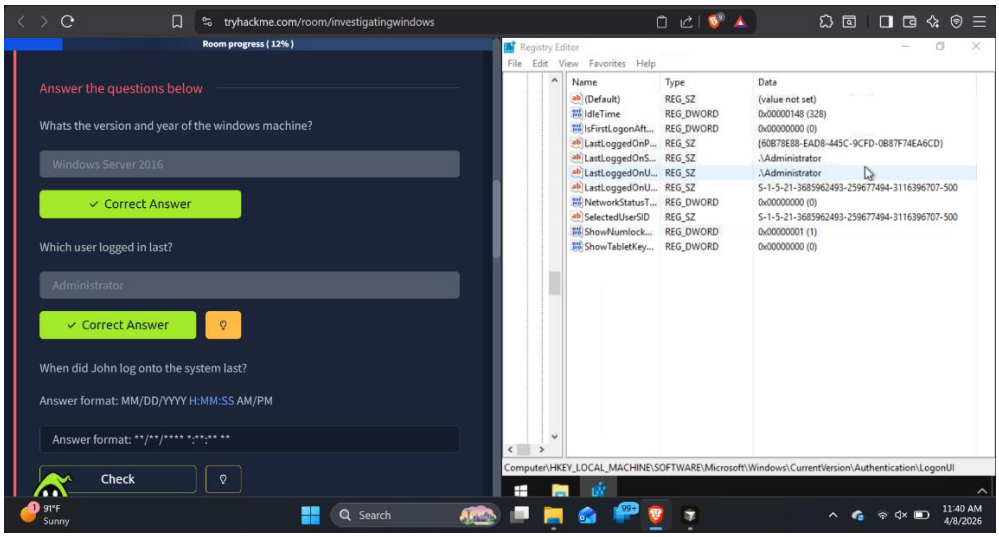
The following section documents the findings from the TryHackMe lab. Each screenshot includes the original question, answer, and a brief explanation of its significance to the investigation.

Figure 1: Windows Version Identification



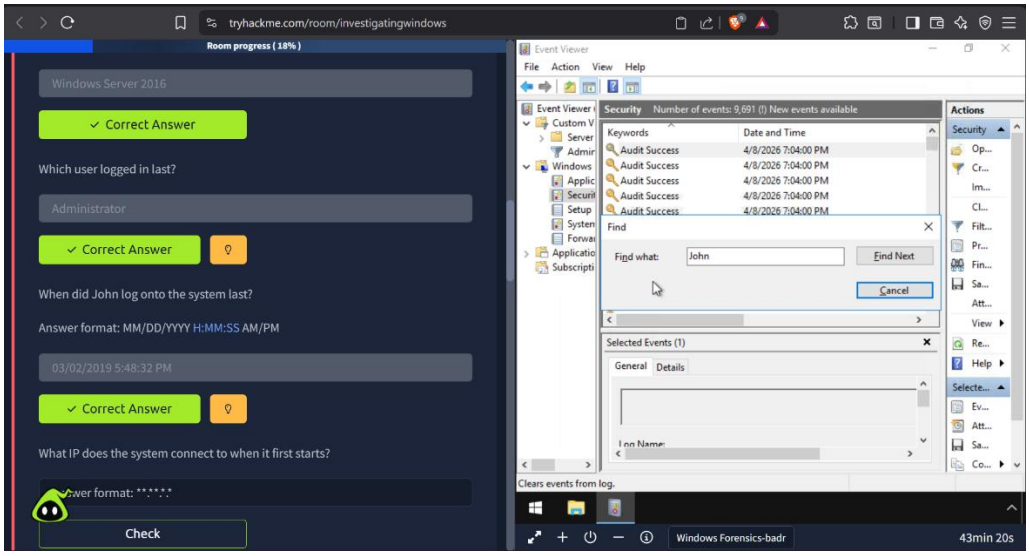
Question: What’s the version and year of the Windows machine?
Answer: Windows Server 2016
Description: This screenshot shows the system information window confirming the operating system version. Identifying the OS is important for understanding potential vulnerabilities and attack surface.

Figure 2: Last Logged-In User



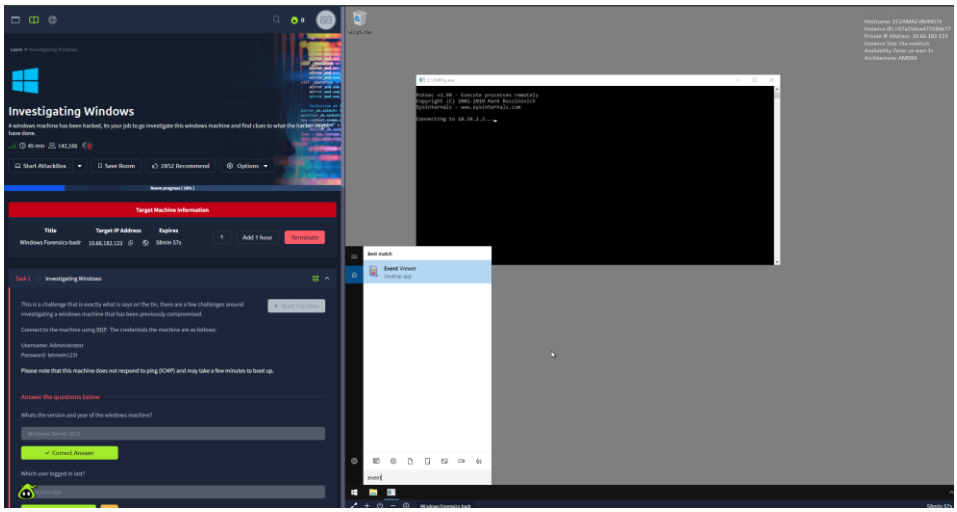
Question: Which user logged in last?
Answer: Administrator
Description: The registry or system logs indicate that the Administrator account was the last to log into the system, suggesting privileged access during the compromise.

Figure 3: John's Last Logon Time



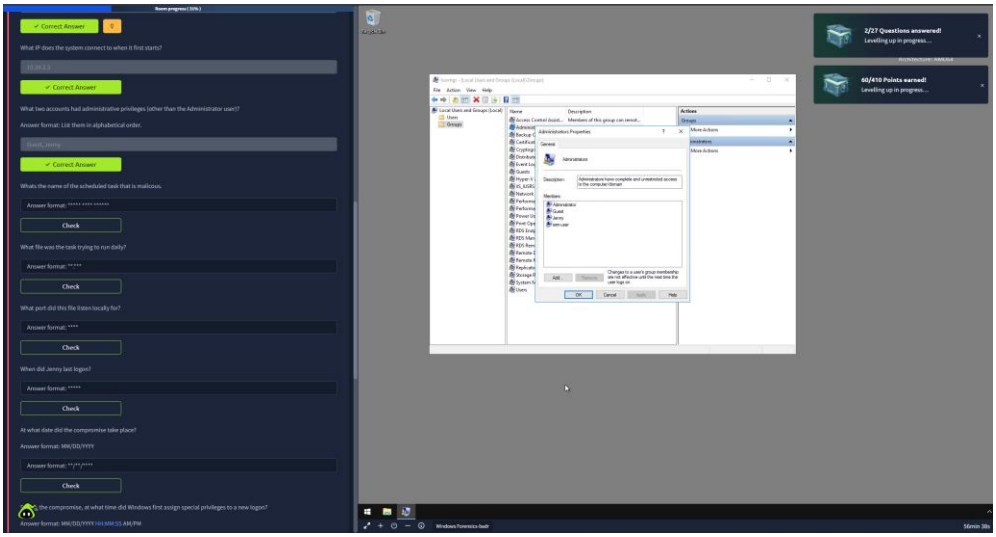
Question: When did John log onto the system last?
Answer: 03/02/2019 5:48:32 PM
Description: Event logs were analyzed to determine the last login time for user John, helping establish a timeline of user activity.

Figure 4: Initial External Connection



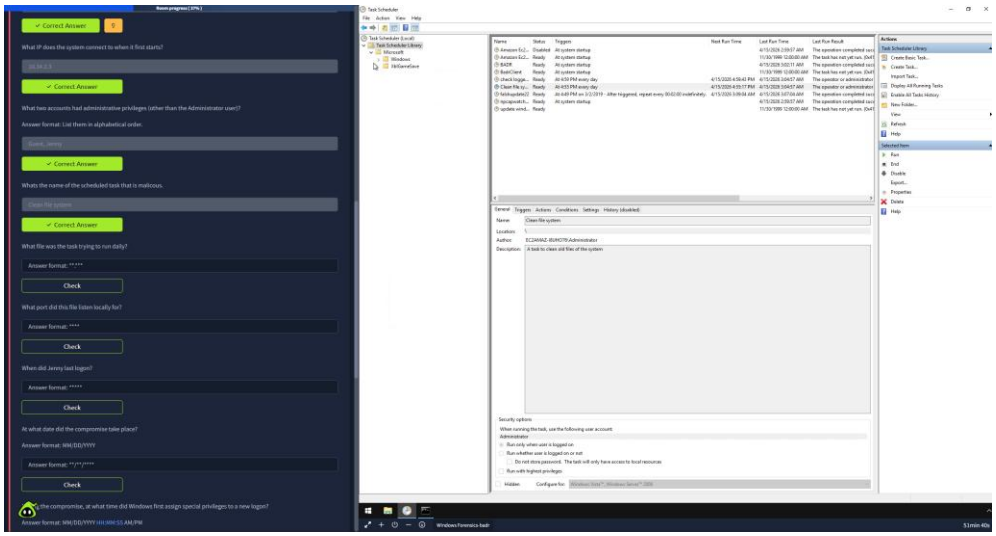
Question: What IP does the system connect to when it first starts?
Answer: 10.34.2.3
Description: Network analysis revealed the first outbound connection made by the system at startup, indicating initial communication behavior.

Figure 5: Administrative Accounts Identified



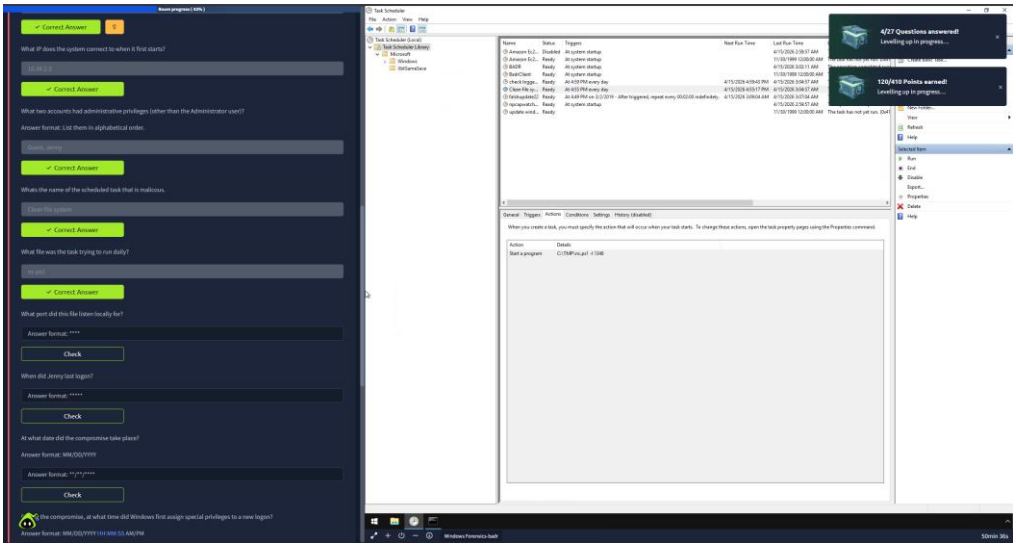
Question: What two accounts had administrative privileges (other than the Administrator user)?
Answer: Guest, Jenny
Description: Local user group analysis shows that both Guest and Jenny accounts had administrative privileges, which could be leveraged by an attacker.

Figure 6: Malicious Scheduled Task



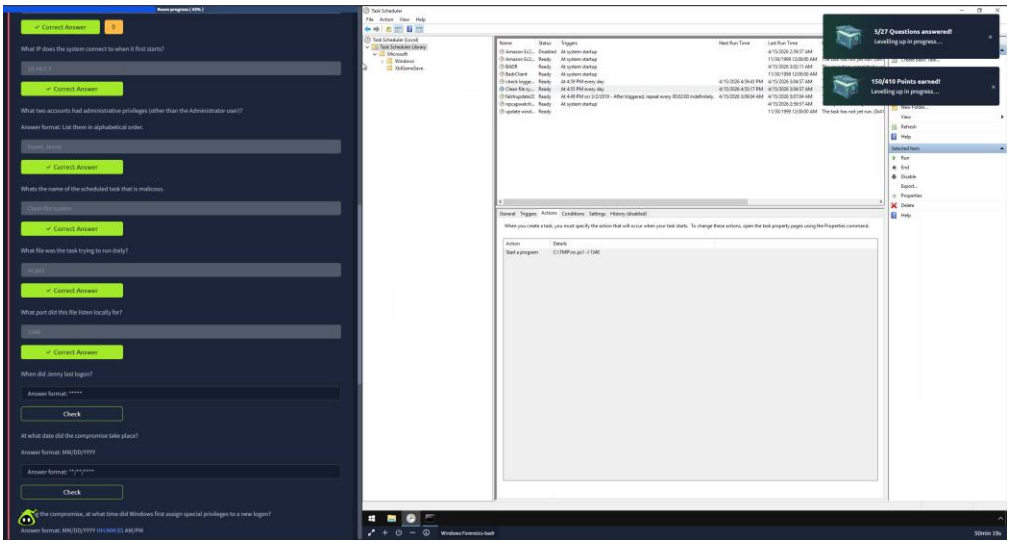
Question: What's the name of the scheduled task that is malicious?
Answer: Clean file system
Description: Task Scheduler analysis identified a suspicious task used for persistence, indicating attacker activity.

Figure 7: Malicious File Execution



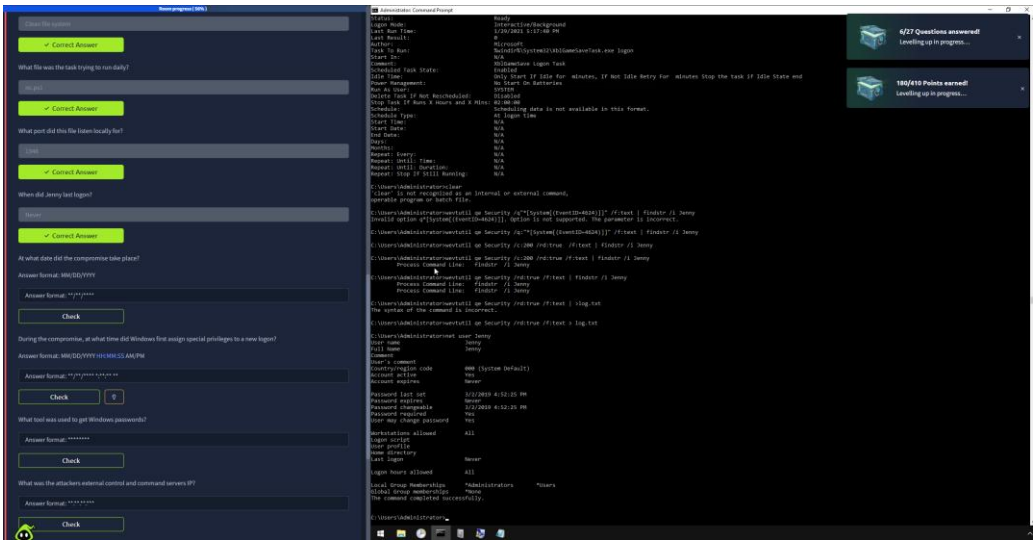
Question: What file was the task trying to run daily?
Answer: nc.ps1
Description: The scheduled task was configured to execute a PowerShell script, likely used for maintaining a reverse shell or backdoor.

Figure 8: Opened Port



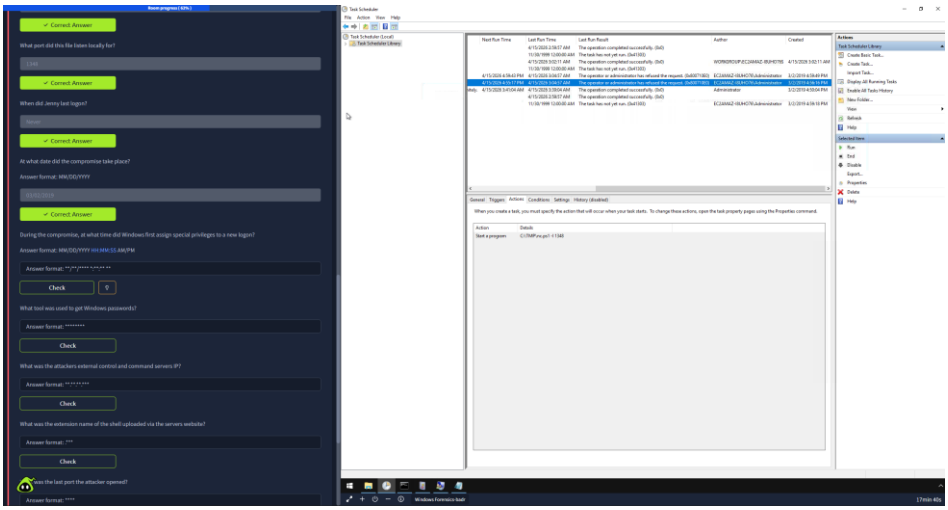
Question: What port did this file listen locally for?
Answer: 1337
Description: Network analysis confirmed that the malicious script opened port 1337, commonly used for unauthorized access.

Figure 9: Jenny Logon Activity



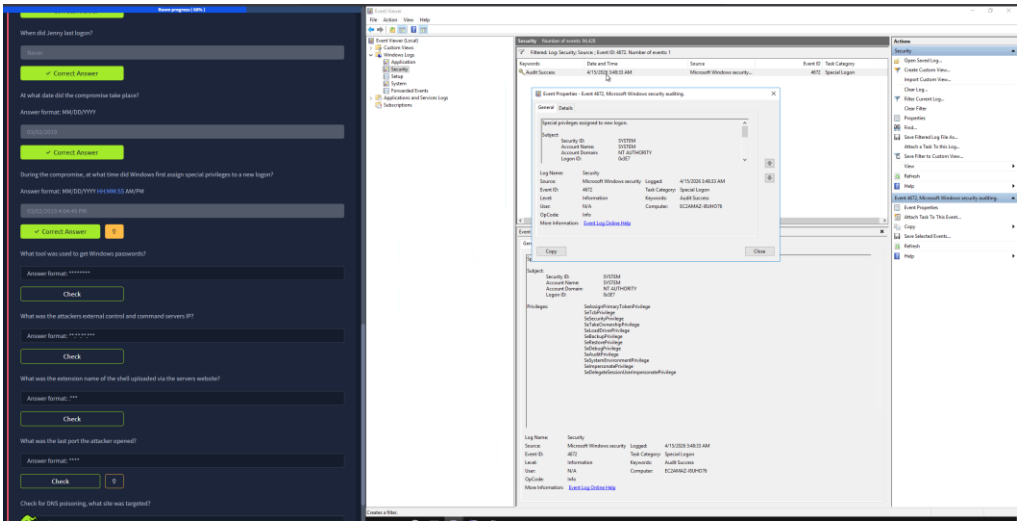
Question: When did Jenny last logon?
Answer: Never
Description: User account analysis showed that Jenny had never logged in, suggesting the account may have been created or modified for malicious purposes.

Figure 10: Date of Compromise



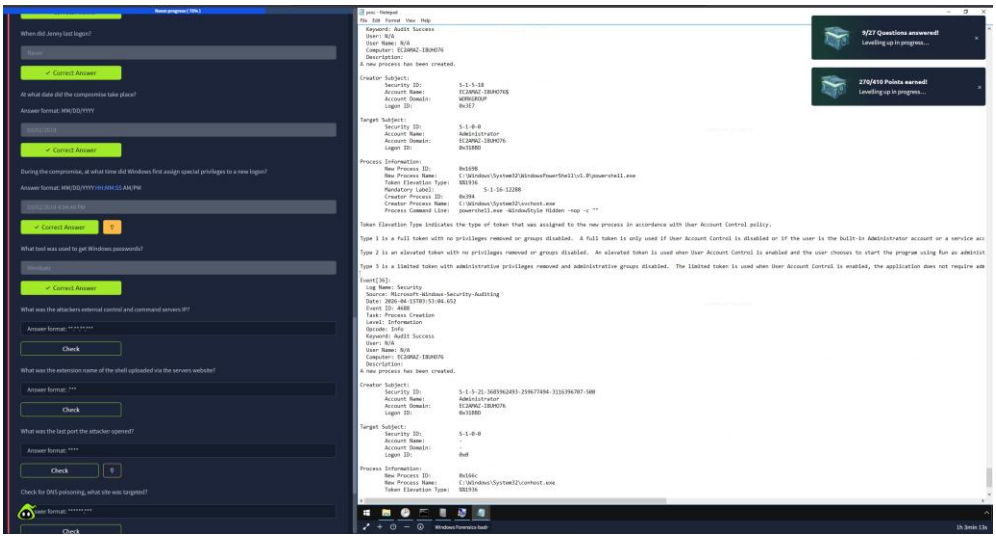
Question: At what date did the compromise take place?
Answer: 03/02/2019
Description: Timeline analysis of logs identified the date when suspicious activity began, marking the compromise.

Figure 11: Privilege Assignment Time



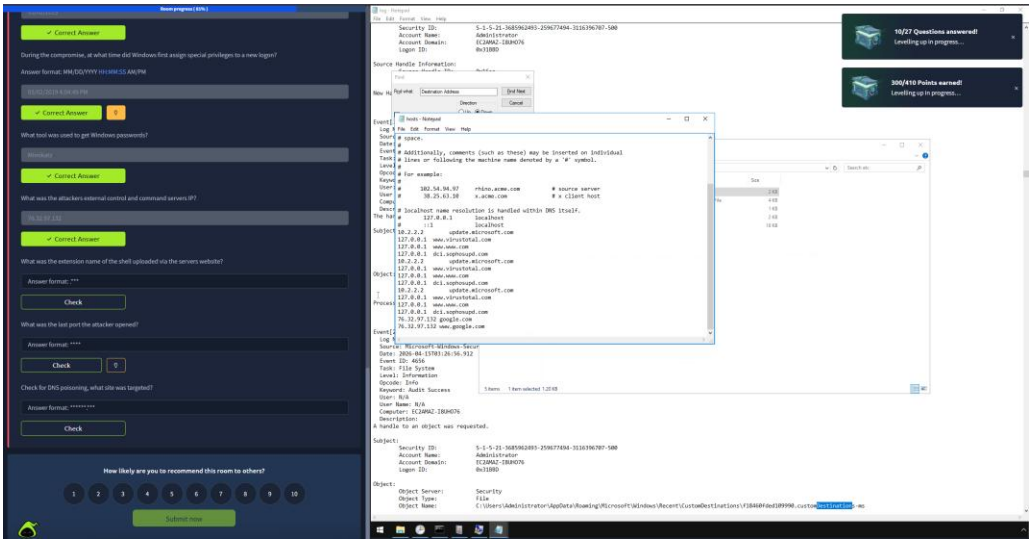
Question: During the compromise, at what time did Windows first assign special privileges to a new logon?
Answer: 03/02/2019 04:04:09 PM
Description: Event ID 4672 shows when elevated privileges were granted, indicating escalation during the attack.

Figure 12: Credential Dumping Tool



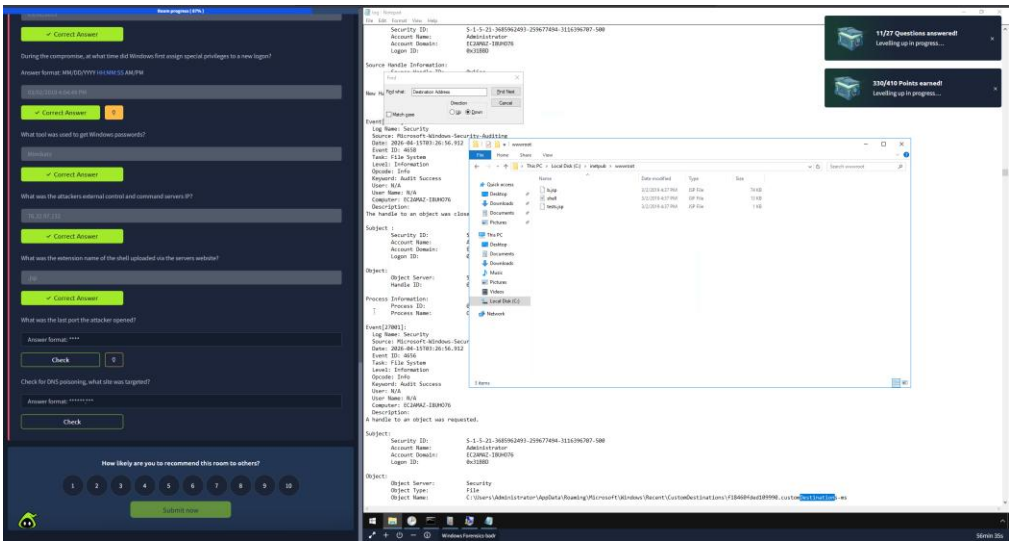
Question: What tool was used to get Windows passwords?
Answer: Mimikatz
Description: Process logs revealed the use of Mimikatz, a well-known credential dumping tool used by attackers.

Figure 13: Command and Control Server



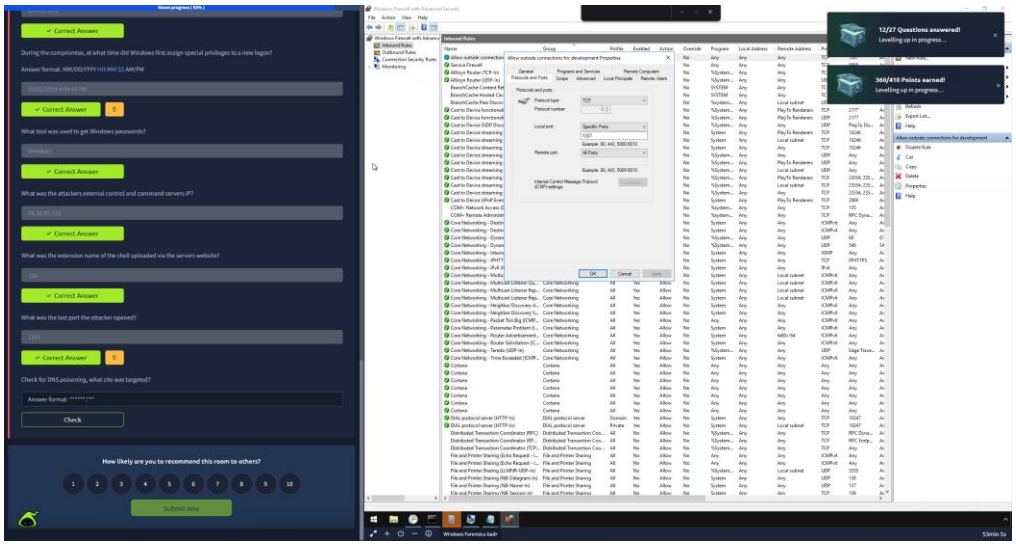
Question: What was the attacker's external control and command server's IP?
Answer: 76.32.97.132
Description: Network connections showed communication with an external IP, indicating a command and control server.

Figure 14: Web Shell Extension



Question: What was the extension name of the shell uploaded via the server's website?
Answer: .jsp
Description: File system analysis identified a web shell uploaded by the attacker, used for remote access.

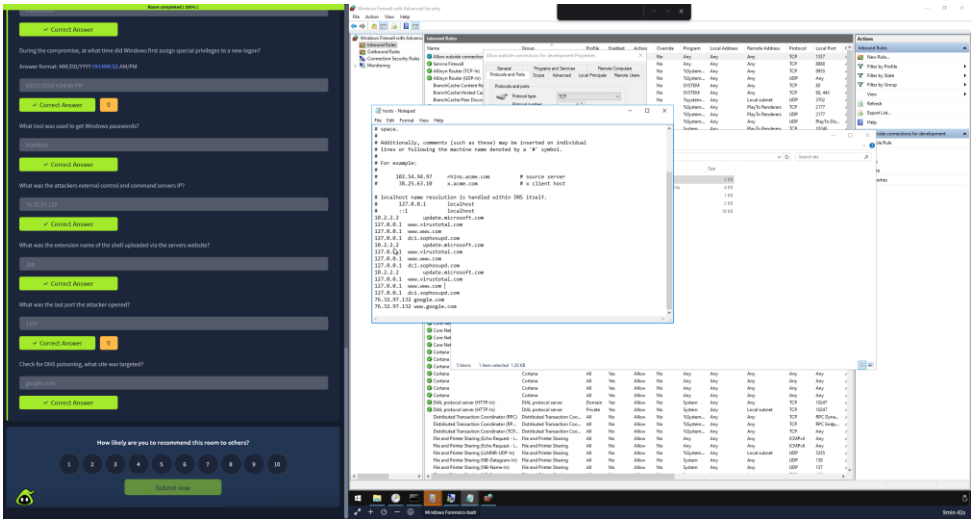
Figure 15: Last Opened Port



Question: What was the last port the attacker opened?
Answer: 1337

Description: Firewall and network logs confirm the attacker opened port 1337 for persistent access.

Figure 16: DNS Poisoning Target



Question: Check for DNS poisoning, what site was targeted?
Answer: google.com
Description: The hosts file was modified to redirect traffic for google.com, indicating DNS poisoning.

System Analysis and Findings

The compromised system was examined using built in Windows tools like Event Viewer, Task Scheduler, Command Prompt, and basic file system checks. These tools helped uncover several signs of compromise in the logs, running processes, and network activity.

---

a) What did the attacker do?

The attacker was able to gain administrative access to the system and carry out several malicious actions. Event logs show that PowerShell was run with hidden execution flags, which suggests they were trying to avoid being detected. They also created a scheduled task called “Clean file system” to maintain persistence and automatically run malicious code.

This task executed a script named *nc.ps1*, which likely set up a reverse shell so the attacker could keep remote access to the system. On top of that, they used Mimikatz to pull passwords from system memory, showing an attempt to escalate privileges and possibly move to other systems on the network.

Network activity showed the system communicating with an external command and control server at 76.32.97.132, and port 1337 was opened for unauthorized access. The attacker also uploaded a .jsp web shell, which allowed them to interact with the system through a web interface. In addition, the hosts file was modified to redirect traffic for google.com, which is a sign of DNS poisoning.

---

b) What traces did they leave?

The attacker left behind several clear signs that the system was compromised. These include:

- **Windows Event Logs:**
  Event ID 4688 showed suspicious processes being run, including PowerShell activity. Event ID 4672 confirmed that administrative privileges were granted during the attack.
- **Scheduled Tasks:**
  The task called “Clean file system” is strong evidence that the attacker set up persistence to keep access to the system.
- **File System Artifacts:**
  Files like *nc.ps1* and a .jsp web shell show that the attacker created and executed malicious files on the system.
- **Network Activity:**
  Connections to the external IP 76.32.97.132 confirm the system was communicating with attacker controlled infrastructure.

- **Credential Dumping Evidence:**
  The use of Mimikatz shows that the attacker was targeting sensitive login credentials.
- **DNS Manipulation:**
  The modified hosts file redirecting google.com shows an attempt to manipulate network traffic.

All of these traces together help build a clear timeline of what happened and give a good understanding of the attacker's actions and goals.

---

c) Could you use your findings in legal proceedings? Why or why not?

Yes, the findings from this investigation could be used in legal proceedings, as long as proper forensic procedures are followed. The evidence collected, such as system logs, network activity, and file artifacts, is generally reliable since it is automatically created by the operating system and includes timestamps.

However, for the evidence to be accepted in court, it must meet legal standards. This includes maintaining a clear chain of custody, ensuring the evidence has not been altered, and documenting each step of the investigation. If these steps are not followed, the evidence could be challenged or even dismissed.

---

d) How could the kill-chain methodology be used to prevent this attack?

The kill-chain methodology can help prevent this type of attack by breaking it down into stages and stopping the attacker along the way. During the reconnaissance phase, monitoring tools could pick up on unusual scanning activity. During exploitation, keeping systems patched and up to date could block the attacker from getting in.

Once inside, detecting things like unauthorized scheduled tasks could help stop the attacker from maintaining access. Monitoring and blocking outgoing traffic to suspicious IPs, like the identified command and control server, could also cut off communication with the attacker.

By putting controls in place at each stage, the attack could be caught early and stopped before it turns into a full system compromise.

---

e) Would the diamond model influence your analysis?

Yes, the diamond model of intrusion analysis would make this investigation more structured and easier to understand. It breaks the attack down into four main parts: the adversary, their capabilities, the infrastructure they used, and the victim.

In this case, the attacker used tools like PowerShell and Mimikatz as their capabilities to target the Windows Server virtual machine, which is the victim. They also communicated with an external server, which represents the infrastructure.

Using this model helps connect all the pieces of the attack and gives a clearer picture of how everything fits together.

---

f) Discuss how to perform forensic analysis in a cloud environment

Forensic analysis in a cloud environment is a bit different from traditional systems since investigators do not have direct access to the physical hardware. Instead, the focus is on collecting and reviewing logs from services like AWS CloudTrail or Azure Monitor, along with capturing virtual machine snapshots to preserve the system's state at a specific point in time. Network logs are also useful for spotting unusual or suspicious activity.

There are a few challenges that come with this. Investigators may have limited visibility into the underlying infrastructure, and important data can be lost if logs are not collected quickly. There is also some reliance on the cloud provider to supply accurate data.

Even with these challenges, cloud environments can actually make investigations easier in some ways. Centralized logging and scalable tools allow analysts to gather and review large amounts of data more efficiently when everything is set up correctly.

Conclusion

The forensic analysis of the compromised Windows Server 2016 system revealed a full attack lifecycle, including privilege escalation, persistence, credential dumping, and communication with an external command and control server. The attacker used several techniques, such as PowerShell execution, scheduled tasks, and DNS manipulation, to stay in control of the system and avoid detection.

The evidence collected makes it possible to clearly understand what happened and shows how forensic analysis can be used to piece together an attacker's actions. Using structured approaches like the kill chain and diamond model can also help improve how future attacks are detected and prevented.

References

TryHackMe. (n.d.). *Investigating Windows*. Retrieved April 14, 2026, from https://tryhackme.com/r/room/investigatingwindows

Microsoft. (n.d.). *Event Viewer overview*. Microsoft Learn. https://learn.microsoft.com/en-us/windows/win32/eventlog/event-logging

Microsoft. (n.d.). *Task Scheduler*. Microsoft Learn. https://learn.microsoft.com/en-us/windows/win32/taskschd/task-scheduler-start-page

Microsoft. (n.d.). *Netstat command*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

Microsoft. (n.d.). *Windows command-line reference*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands

Microsoft. (n.d.). *Windows Server 2016 documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/

National Institute of Standards and Technology. (2012). *Guide to integrating forensic techniques into incident response (SP 800-86)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Lockheed Martin. (n.d.). *Cyber kill chain*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Center for Cyber Intelligence Analysis and Threat Research. https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Amazon Web Services. (n.d.). *AWS CloudTrail user guide*. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

Microsoft. (n.d.). *Azure Monitor documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/azure-monitor/

Google Cloud. (n.d.). *Cloud logging documentation*. https://cloud.google.com/logging/docs