Student:	Email:
Bradley Adams	badams10@my.athens.edu

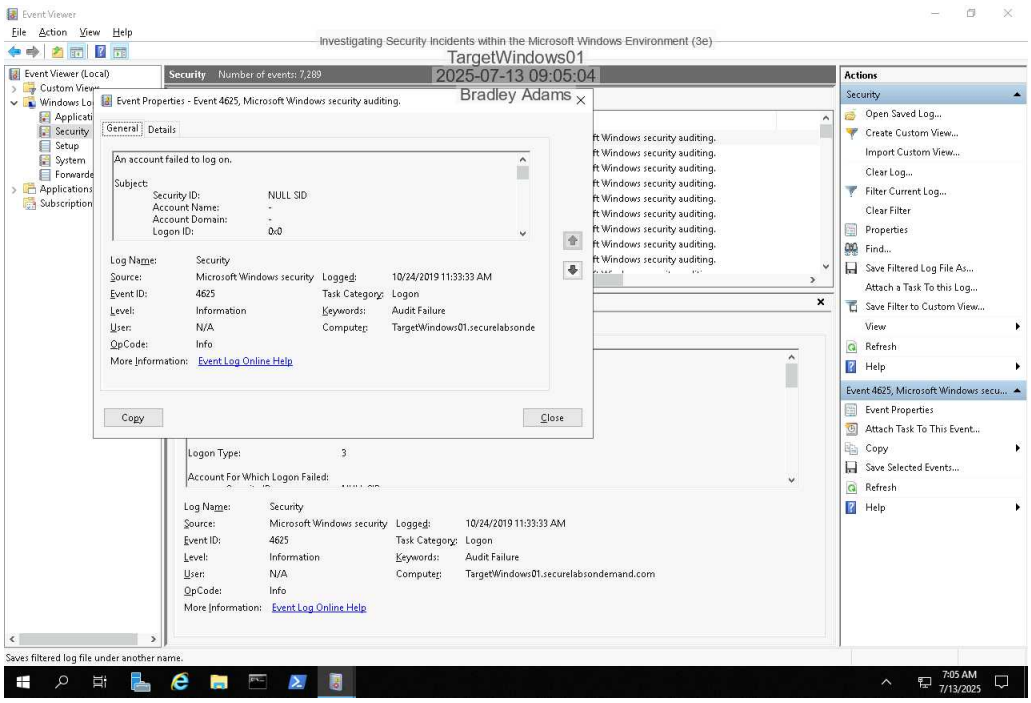
Time on Task:	Progress:
7 hours, 57 minutes	100%

Report Generated: Sunday, July 13, 2025 at 2:48 PM

Section 1: Hands-On Demonstration

Part 1: Use the Event Viewer to Detect Failed Log-in Attempts

10. **Make a screen capture** showing the **Security Event Properties dialog box on TargetWindows01**.

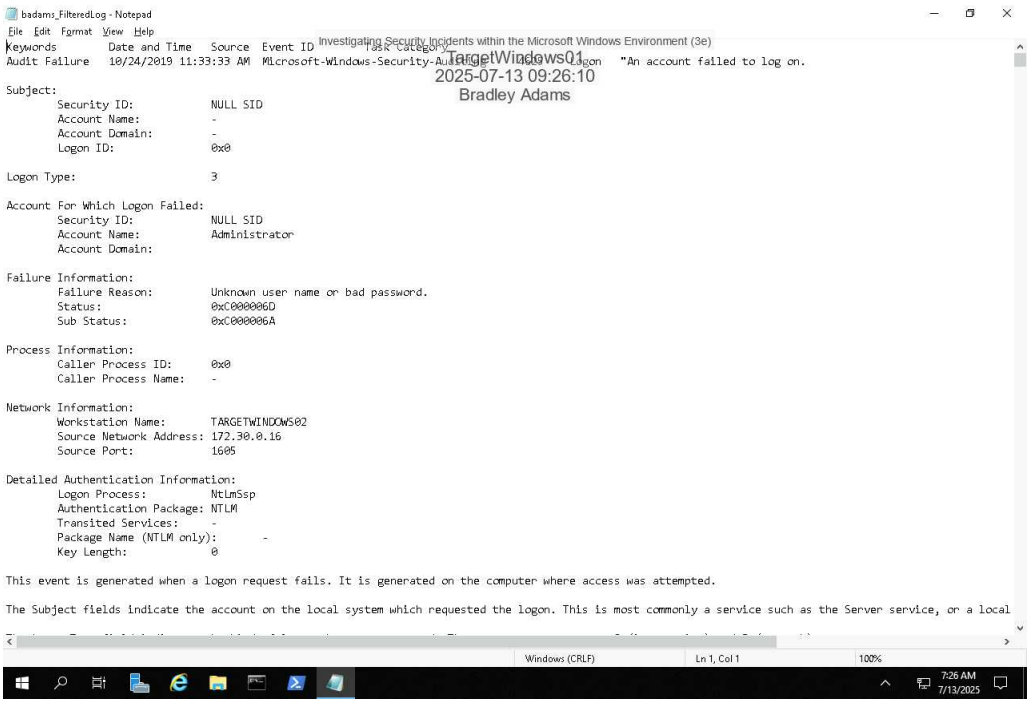


16. **Summarize** the logon errors and **recommend** ways to respond to them.

The logs show repeated failed login attempts with more than a hundred instances logged within a single second. The failed logins targeted the Administrator account and used NTLM authentication over a network logon (logon type 3), originating from the IP address 172.30.0.16 and the workstation named TARGETWINDOWS02. The failure codes 0xC000006D and 0xC000006A indicate that the attempts failed due to incorrect passwords. This activity suggests a brute-force attack. The NULL SID and 0x0 process ID further indicate that these requests were unauthenticated and remote.

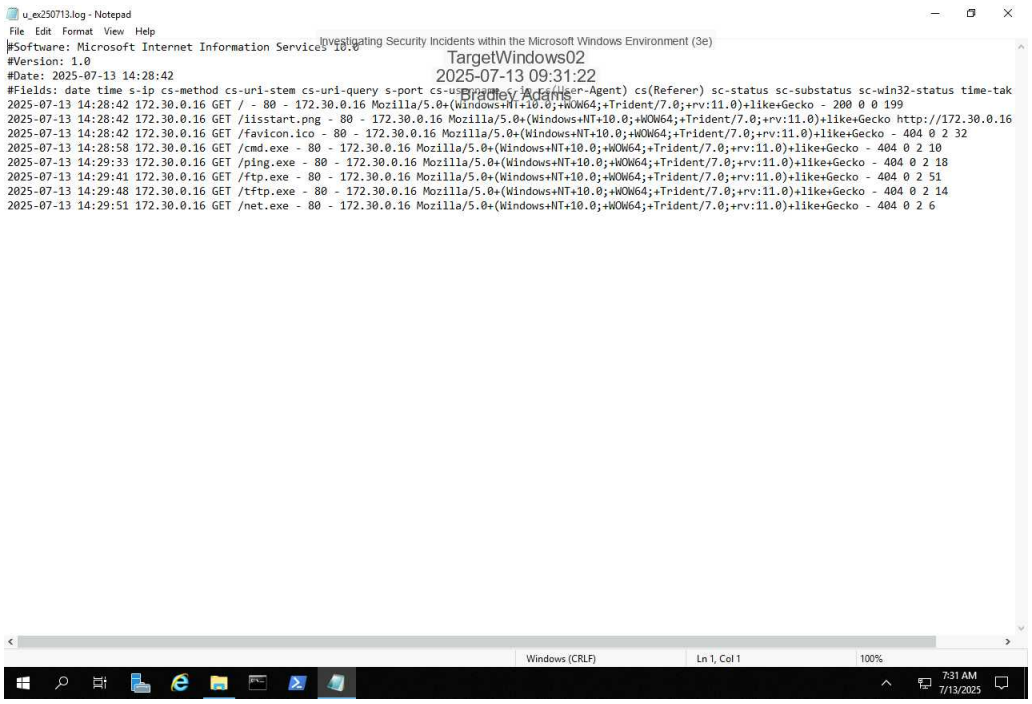
Response should include blocking the offending IP address, disabling or renaming the default Administrator account, and enabling account lockout policies to block further brute-force attempts. The organization should improve the policy for authentication by limiting NTLM use, enforcing stronger passwords, enabling MFA, and monitoring logs using a SIEM.

20. **Make a screen capture** showing the **filtered log file in Notepad**.



Part 2: Identify Errors in IIS Logs

9. **Make a screen capture** showing the **IIS errors**.



10. **Summarize** the IIS errors and **recommend** ways to respond to them.

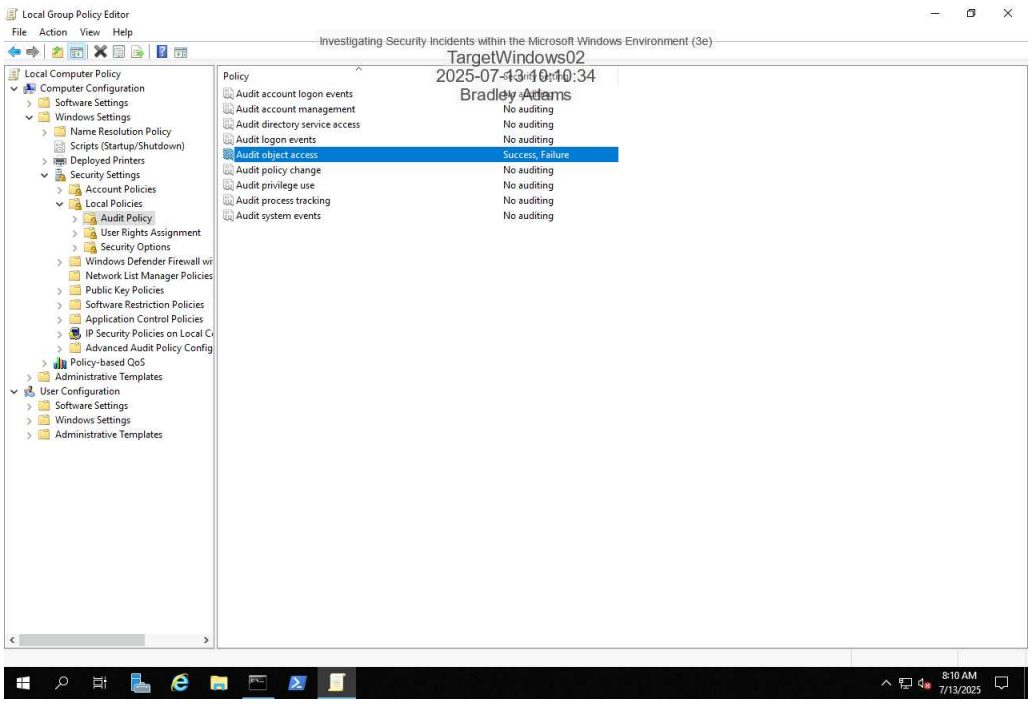
    Refer to your textbook or research the errors on the internet, if necessary.

The IIS log shows requests coming from the same source IP address, 172.30.0.16. The requests occur over a short period. The initial requests are standard access to the root page, a .png image file, and a .ico file. Starting at 14:28:58, the client requested executable files: cmd.exe, ping.exe, tftp.exe, and net.exe. This activity suggests that the attacker is probing for remote command execution or exploiting misconfigurations that might allow file access or code execution via the web server.

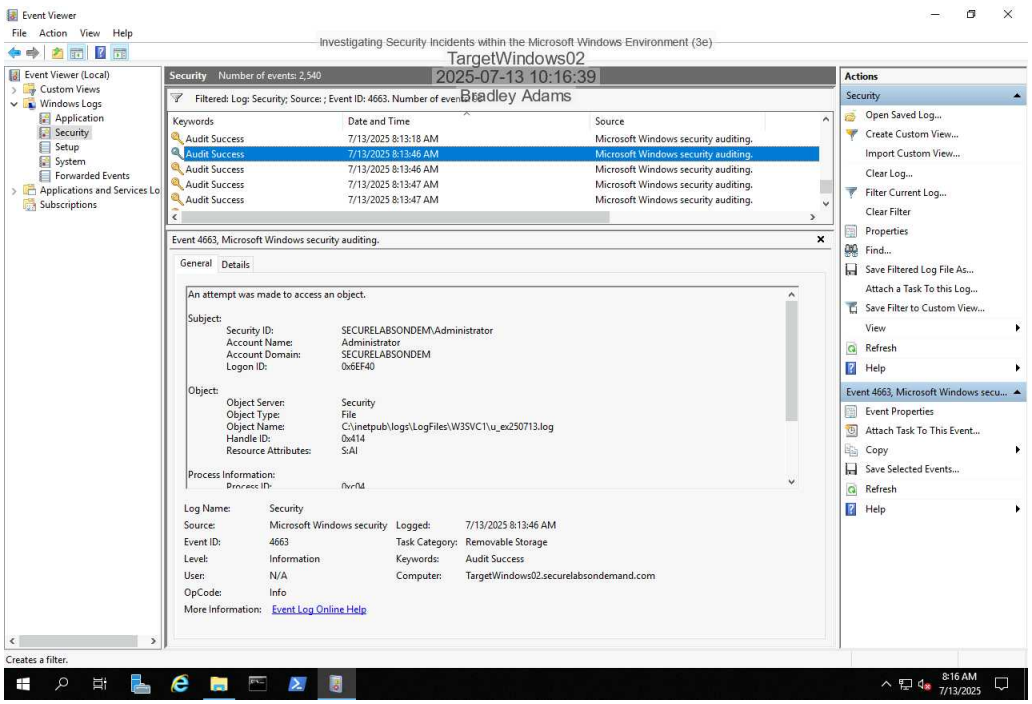
All of these suspicious requests return a 404 Not Found status. This status means the files were not present at the requested locations. This activity shows active reconnaissance to determine vulnerabilities. The response should include blocking the IP address, auditing the server for any misconfigurations, reviewing any web-executable permissions, and deploying additional monitoring and updating firewall rules to detect similar activity in real-time.

Part 3: Enable Auditing for IIS Log File Access

8. **Make a screen capture** showing the **updated Audit policy**.



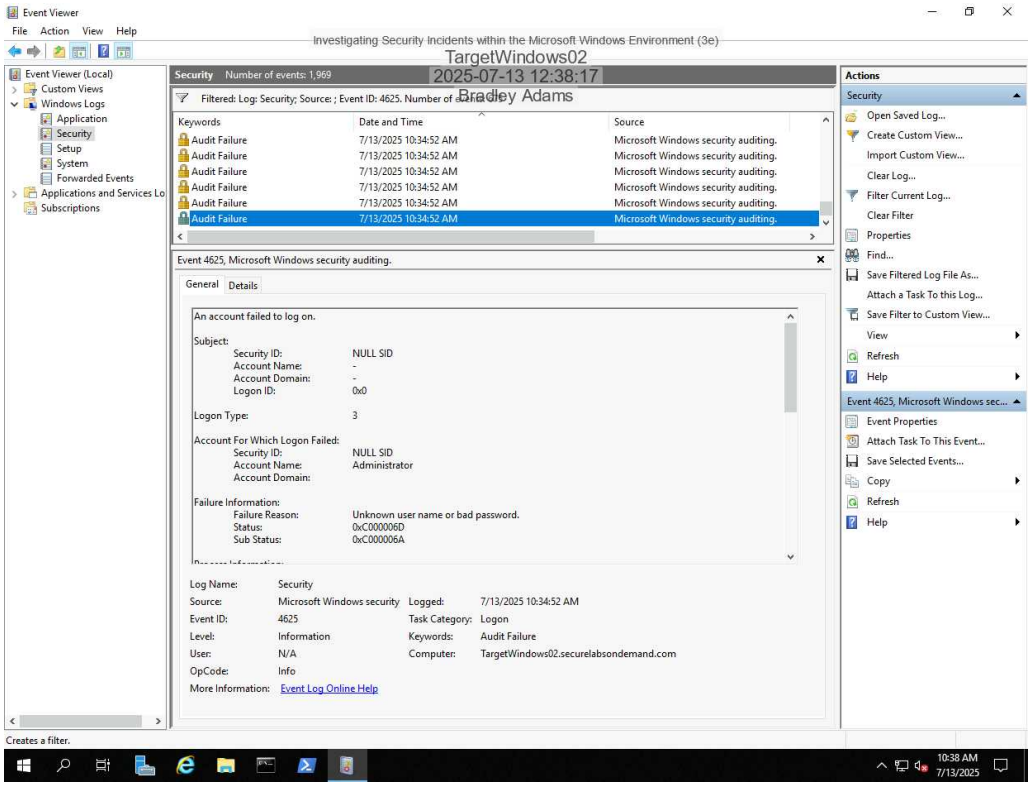
36. **Make a screen capture** showing the **event details for the file you modified**.



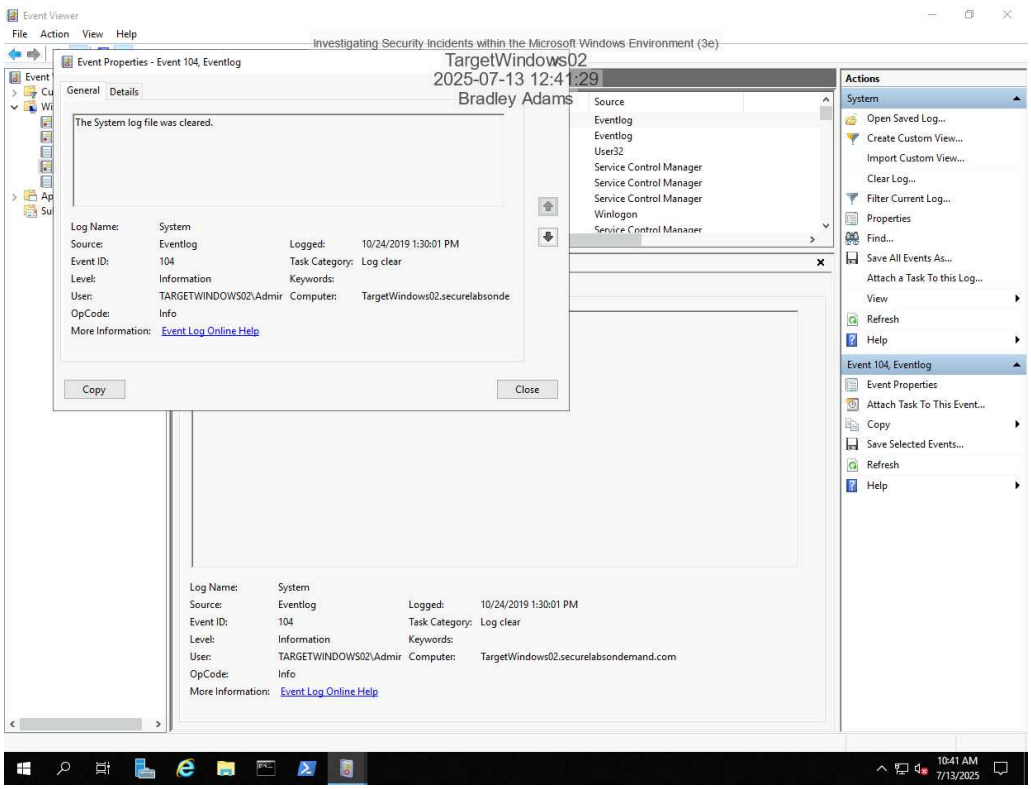
Section 2: Applied Learning

Part 1: Use the Event Viewer to Detect Failed Log-in Attempts

5. **Make a screen capture** showing the **Event Properties for the first Audit Failure with *today's date***.

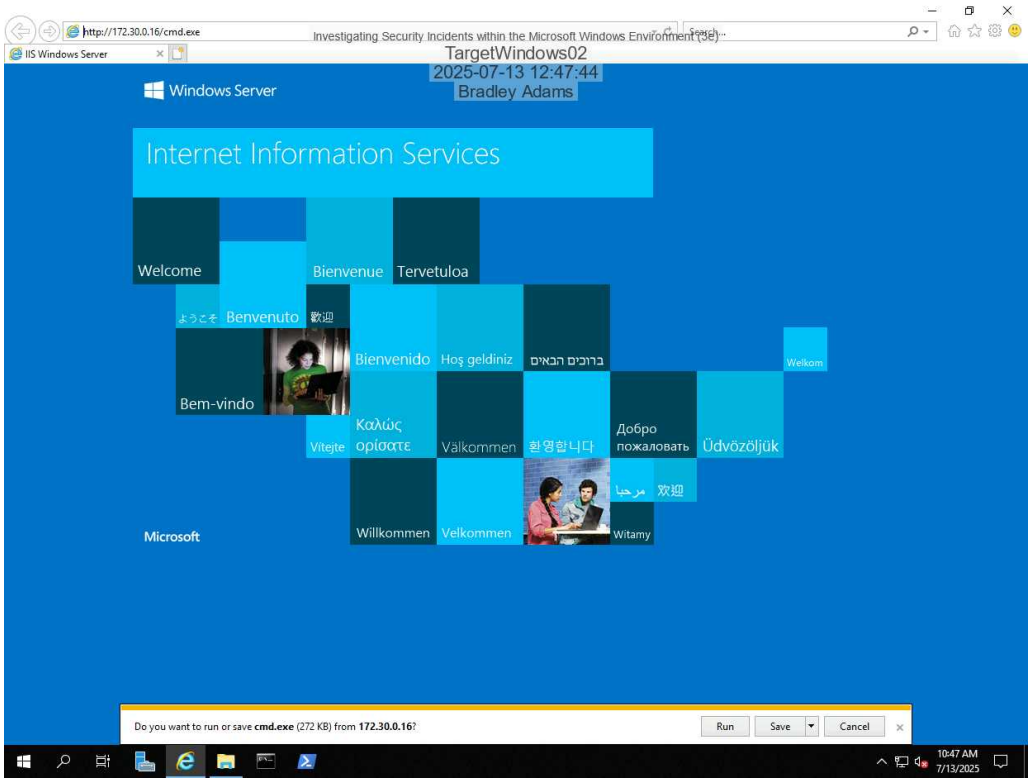


9. **Make a screen capture** showing the **System Event Properties dialog box on TargetWindows02**.

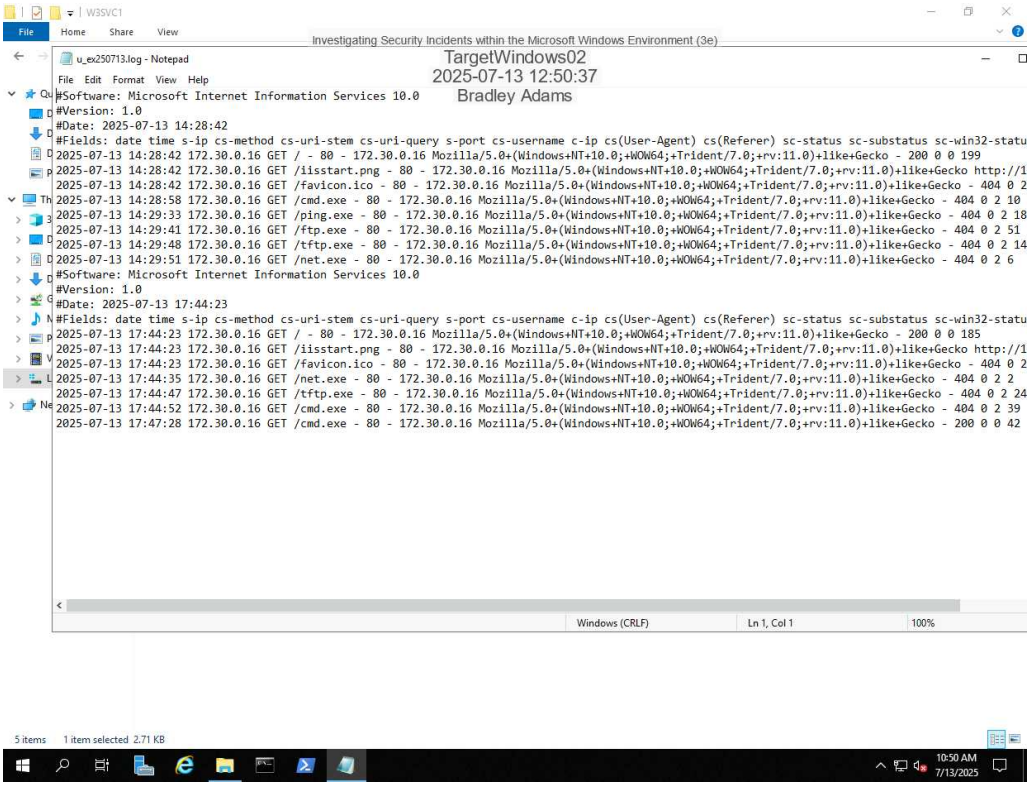


Part 2: Identify Errors in IIS Logs

5. **Make a screen capture** showing the **new results of the cmd.exe command**.



7. **Make a screen capture** showing the **relevant log entries**.



8. **Describe** the **differences between the two log entries**.

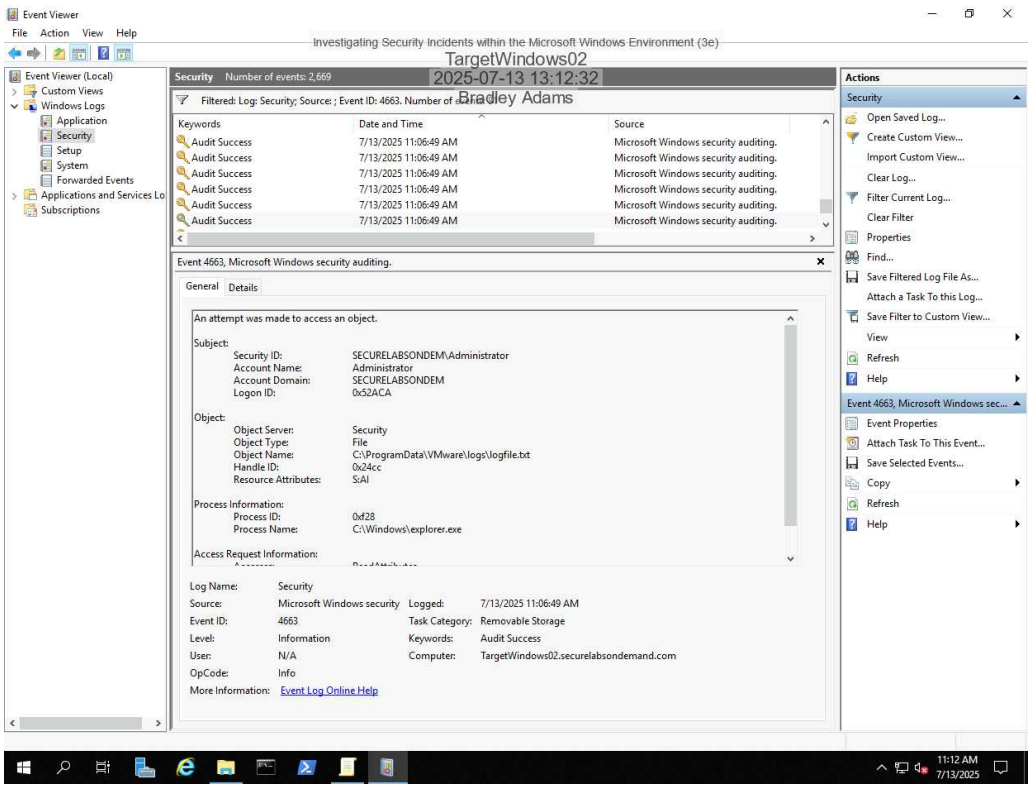
In a real-world scenario, the log shows two separate attack attempts from the same IP address, 172.30.0.16, but at different times on the same date.

The first attack occurs at approximately 14:28 and shows a reconnaissance followed by attempted access to executables. All of these requests return 404 Not Found, meaning the files were not there.

The second attack starts around 17:44, repeating the same pattern followed again by attempts to access executables. In the final request at 17:47:28, the attacker successfully gets a 200 OK response when requesting cmd.exe. This means that the cmd executable file was found and served. This indicates a possible breach or server misconfiguration presented between those times.

Part 3: Enable Auditing for VMware Log File Access

9. **Make a screen capture** showing the **event details for the logfile.txt file**.



Section 3: Challenge and Analysis

Part 1: Analysis and Discussion

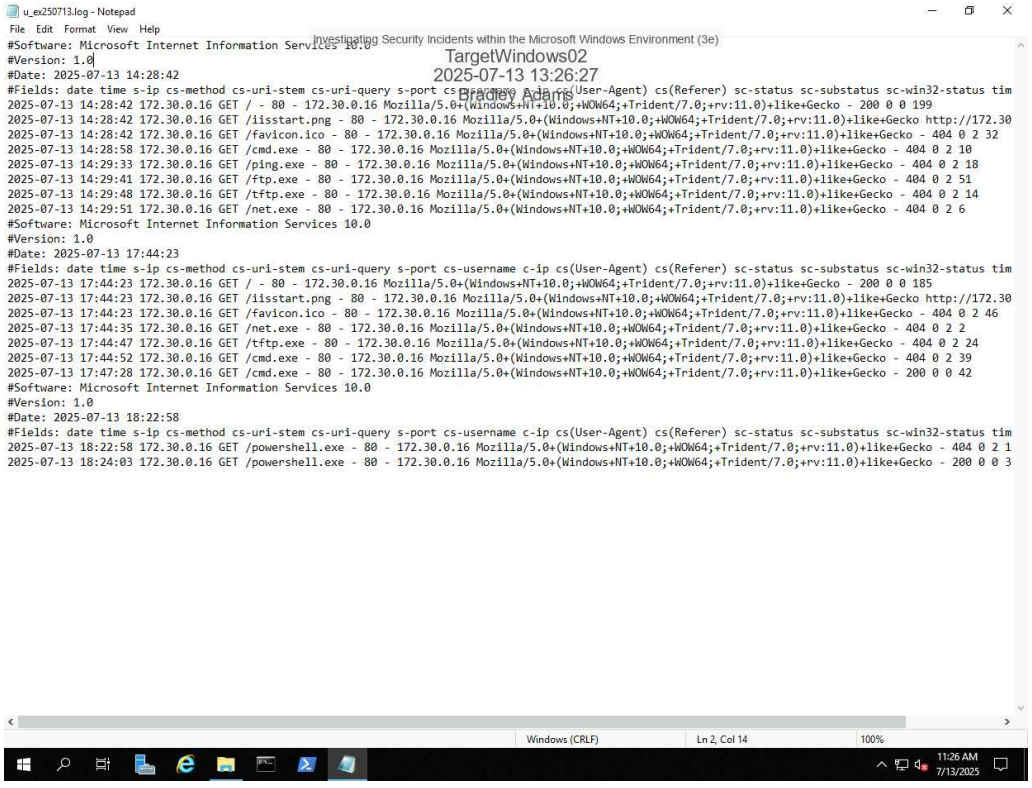
What options are available to prevent brute force authentication attacks in a Windows-based domain? In your opinion, which of these options - or combination of options - would be most effective?

Administrators can use account lockout policies and strong password requirements, and they can also rename or disable default accounts like Administrator. Monitoring failed login attempts, using firewalls to restrict access, and enforcing VPN or smart card logon helps mitigate this risk. Administrators can apply controls in Group Policy and monitor them with an SIEM tool for detection and alerting.

The most effective defense is combining account lockout policies with multi-factor authentication. Lockouts slow brute force attempts, and MFA blocks unauthorized access even if passwords are compromised.

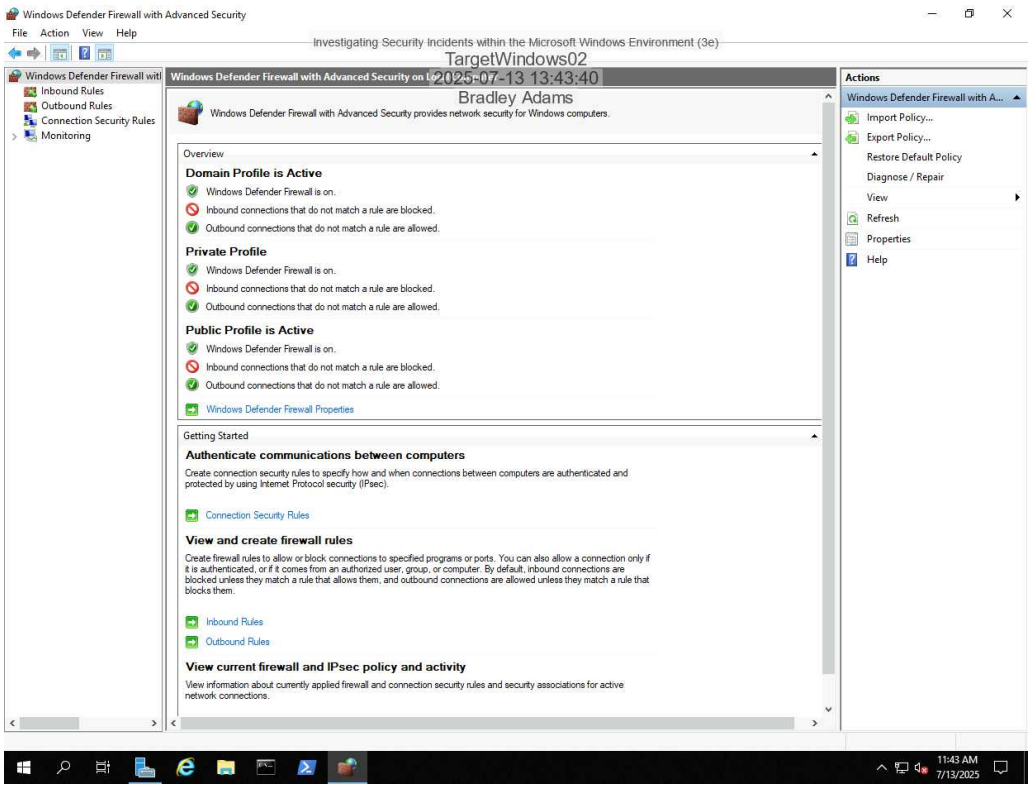
Part 2: Tools and Commands

Make a screen capture showing the **IIS log that contains these events**.



Part 3: Challenge Exercise

Make a screen capture showing the **activated Windows Defender firewall**.



Make a screen capture showing the **blocked IIS home page**.