SeventhEleventh

By Ben Wright, Jacob Senn, Ethan Ze’evi, Jason Yeung

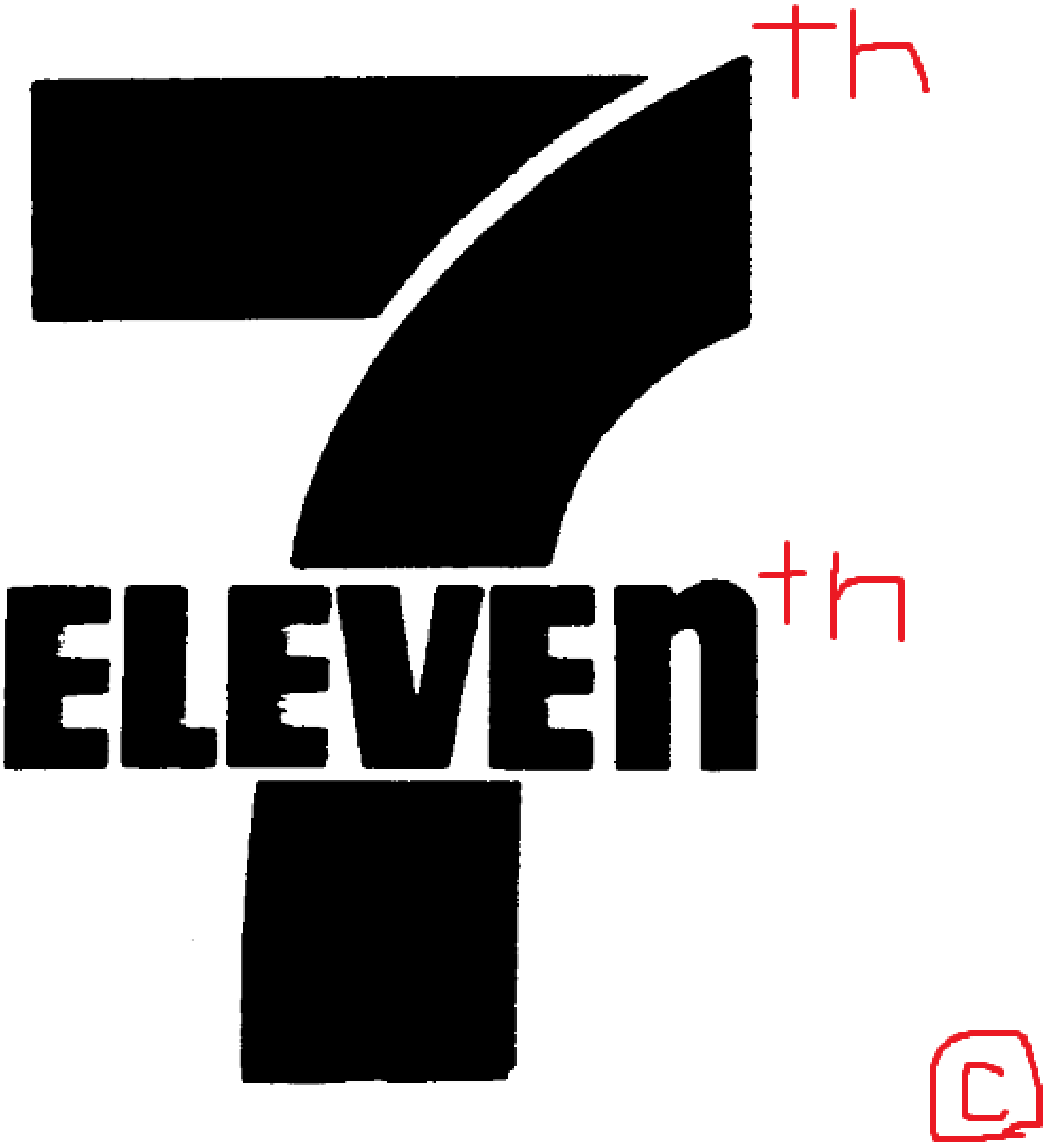


Table of Contents

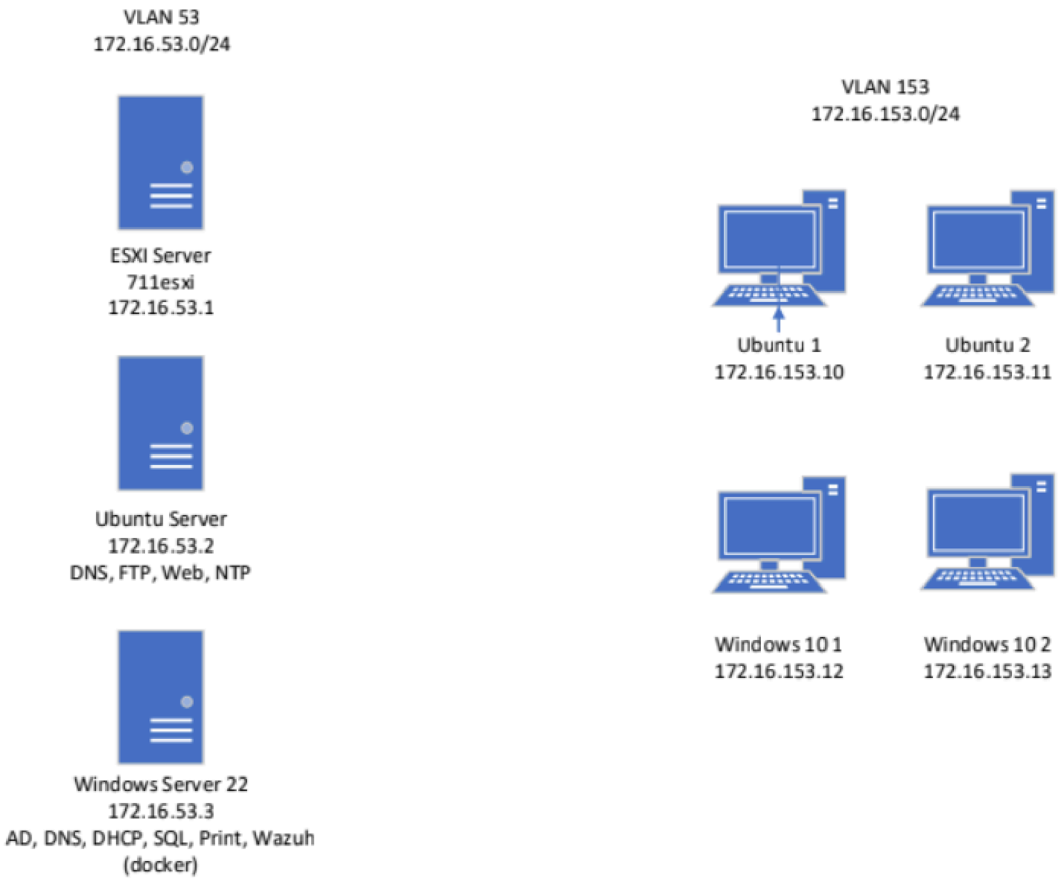
Mission Statement

Provide a secure and reliable infrastructure for our customers while maintaining a quality user experience. We pledge to serve the hottest dogs and the biggest gulps. 😼

Group Members

- Ben Wright - 3rd year Cybersecurity student expected to graduate in 2025
- Ethan Zeevi - Cybersecurity student graduating in 2025 😎
- Jacob Senn - 3rd year Cybersecurity student with expected graduation in 2025
- Jason Yeung - Cybersecurity student expected graduation in 2025

Topology



Systems

- Windows Server - Windows Server 2022 21H2 OS Build 20348.2113

  - AD Domain Controller hosting DNS, DHCP, SQL server, print server, and docker for Wazuh
- Ubuntu Server - Ubuntu 22.04.3 LTS
  - Hosting secondary DNS, web server, NTP server, and FTP server
- Windows 10 Client 1 - Windows 10 22H2 OS Build 19045.3693
- Windows 10 Client 2 - Windows 10 22H2 OS Build 19045.3693
- Ubuntu Client 1 - Ubuntu 22.04.3 LTS
- Ubuntu Client 2 - Ubuntu 22.04.3 LTS

Applications/Services

- AD - Windows Server 2022
- Primary DNS - 10.0.20348.2110
- Secondary DNS - BIND 9.18.18-0
- DHCP - 10.0
- FTP - vsftpd 3.0.5
- NTP - Chrony 4.2
- SSH - OpenSSH_8.9p1
- RDP - 10.0.20348
- SQL - 16.0.1000.6 Enterprise Evaluation Edition
- Web Server - Apache 2.4.52
- Wazuh - 4.6.0-1
- Print - 10.0.20348.1

Reasoning for the versions we chose

We chose the most recent versions at the time of building our infrastructure for our software and operating systems with the exception of not using Windows 11. We chose Ubuntu for our linux clients and server due to the abundance of documentation and familiarity with the OS.

Users

1.	Username: slurpee	Password: 128Ozofgulp!!
2.	Username: biggestgulp	Password: freeslurpee1234!
3.	Username: gulp1	Password: bluerasp9876!*
4.	Username: gulp2	Password: bajablast4657@
5.	Username: gulp3	Password: bloodorange3780#
6.	Username: gulp4	Password: powerberry2840$
7.	Username: slurp1	Password: blackcherry1224%
8.	Username: slurp2	Password: lemonlime5780^
9.	Username: slurp3	Password: strawberry6842&
10.	Username: slurp4	Password: orange8771*4!1

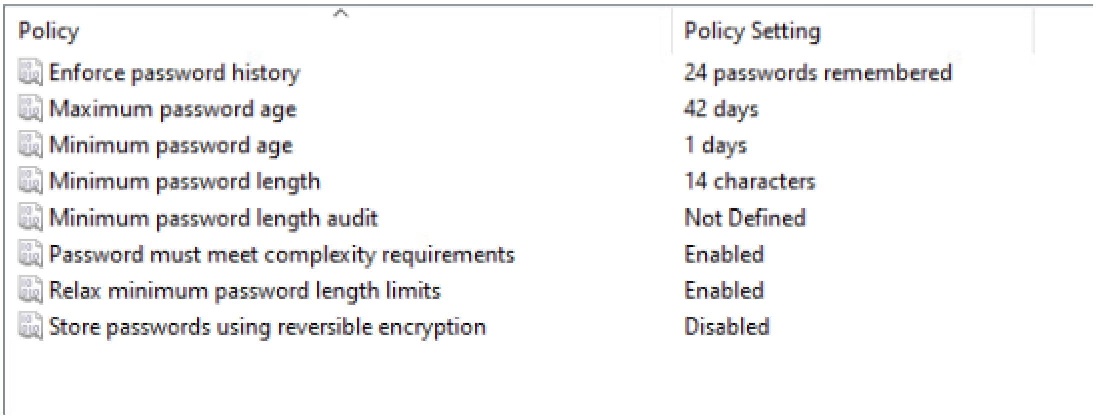
Subnets & VLANs

We allocated our VLANs to separate our client and server systems. The first VLAN is reserved for servers and the second VLAN is for the clients. Servers were assigned to subnet 172.16.53.0/24 while clients were assigned to 172.16.153.0/24.

Security Controls

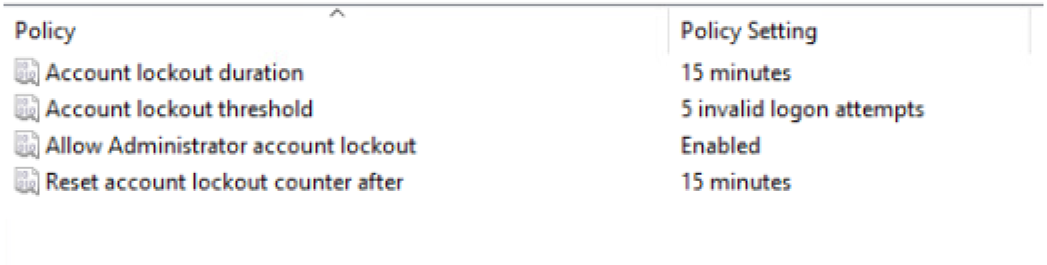
CIS Windows 10 Enterprise 2022 Controls:

- 1.1 Account Policy



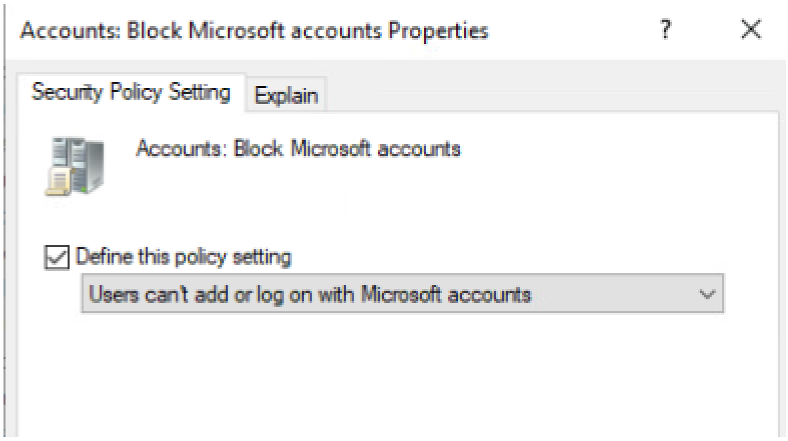
Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	14 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Enabled
Store passwords using reversible encryption	Disabled

- 1.2 Account Lockout Policy



Policy	Policy Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	15 minutes

- 2.3.1.1 Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'



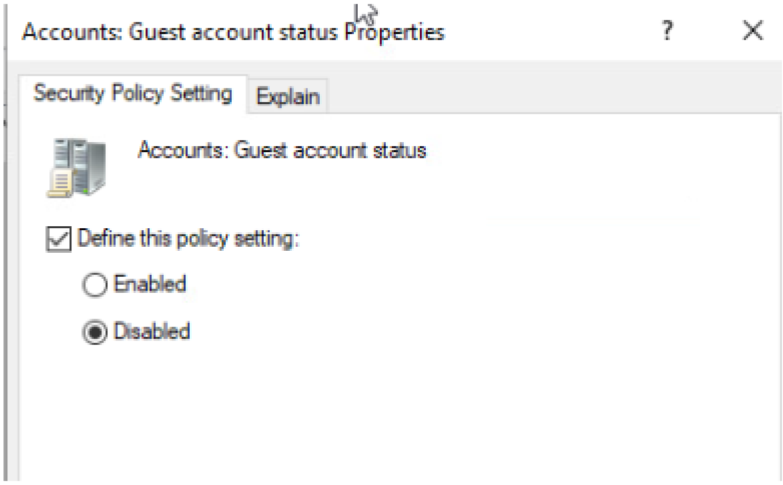
Accounts: Block Microsoft accounts Properties

Accounts: Block Microsoft accounts

☑ Define this policy setting

Users can't add or log on with Microsoft accounts

- 2.3.1.2 Ensure 'Accounts: Guest account status' is set to 'Disabled'



Accounts: Guest account status Properties

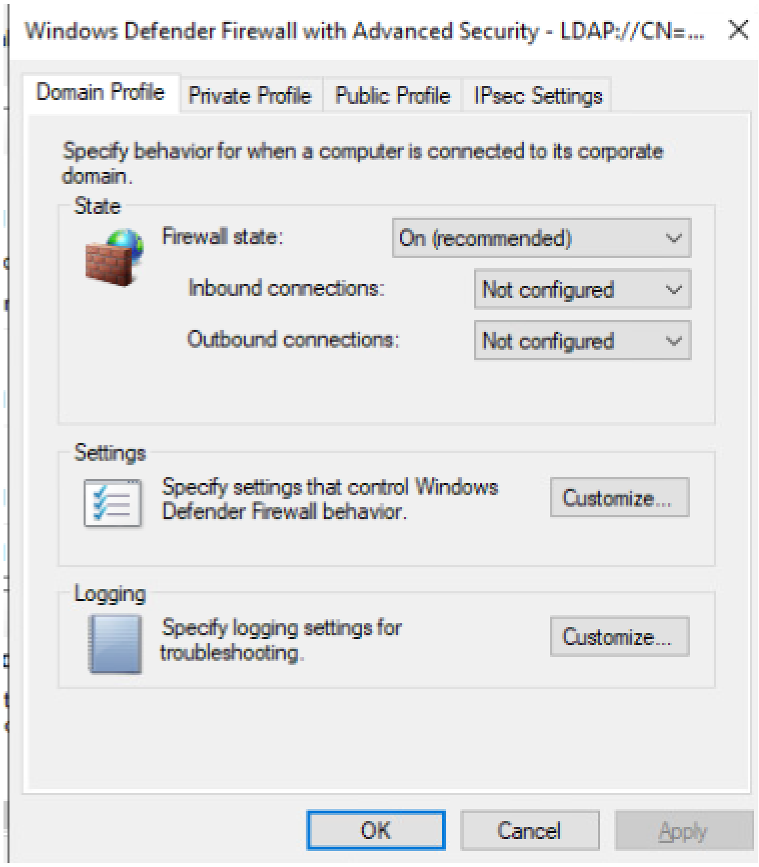
Accounts: Guest account status

☑ Define this policy setting:

○ Enabled

● Disabled

- 9.1.1 Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'



Windows Defender Firewall with Advanced Security - LDAP://CN=...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Not configured

Outbound connections: Not configured

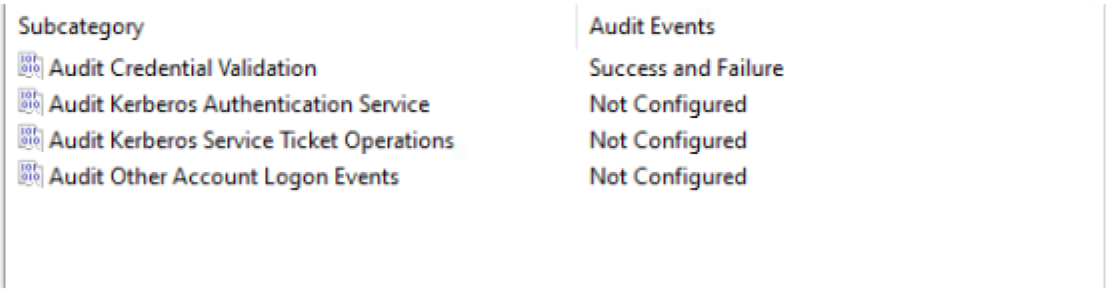
Settings

Specify settings that control Windows Defender Firewall behavior.

Logging

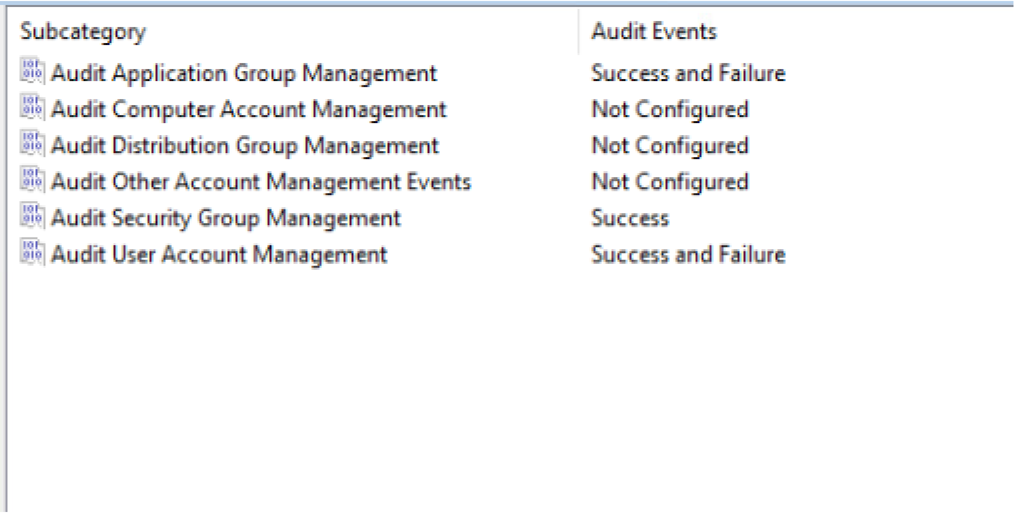
Specify logging settings for troubleshooting.

- 17.1 Account Login



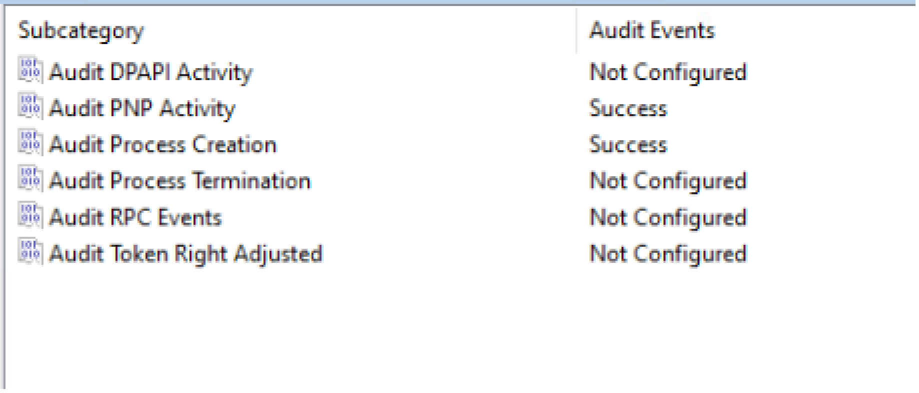
Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Not Configured
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Not Configured

- 17.2 Account Management



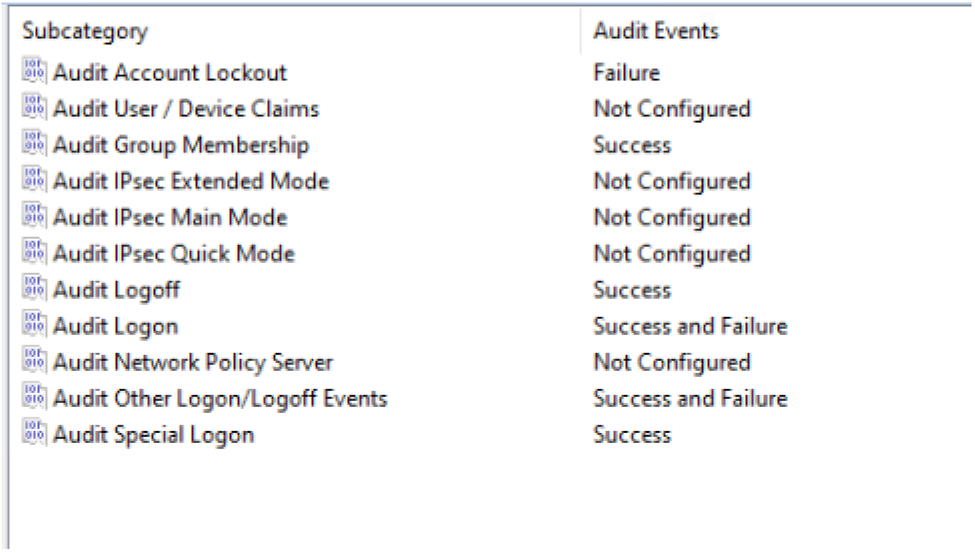
Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Not Configured
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Success
Audit User Account Management	Success and Failure

- 17.3 Detailed Tracking



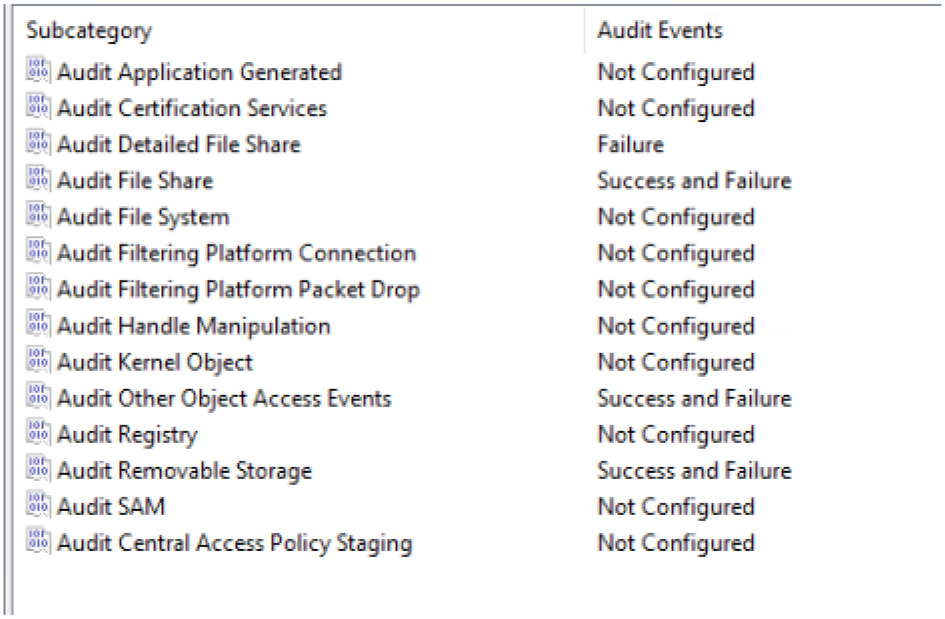
Subcategory	Audit Events
Audit DPAPI Activity	Not Configured
Audit PNP Activity	Success
Audit Process Creation	Success
Audit Process Termination	Not Configured
Audit RPC Events	Not Configured
Audit Token Right Adjusted	Not Configured

- 17.5 Logon/Logoff



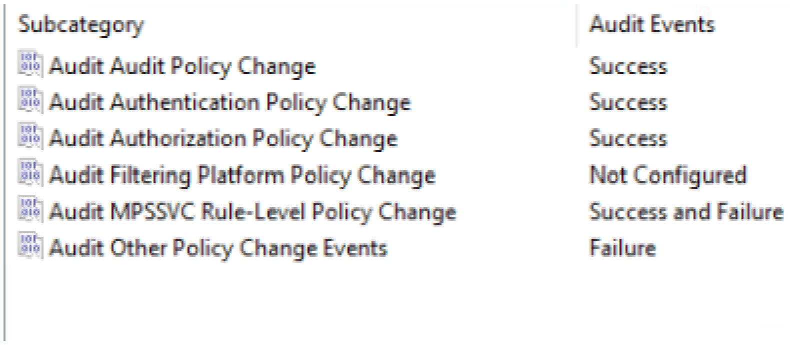
Subcategory	Audit Events
Audit Account Lockout	Failure
Audit User / Device Claims	Not Configured
Audit Group Membership	Success
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success

- 17.6 Object Access



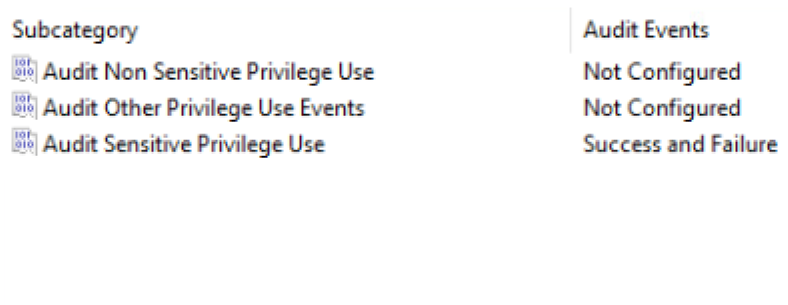
Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Failure
Audit File Share	Success and Failure
Audit File System	Not Configured
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Success and Failure
Audit Registry	Not Configured
Audit Removable Storage	Success and Failure
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

- 17.7 Policy Change



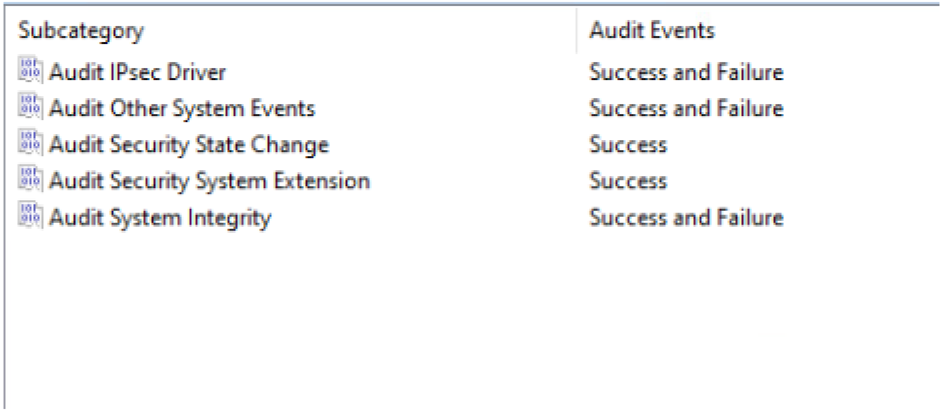
Subcategory	Audit Events
Audit Audit Policy Change	Success
Audit Authentication Policy Change	Success
Audit Authorization Policy Change	Success
Audit Filtering Platform Policy Change	Not Configured
Audit MPSSVC Rule-Level Policy Change	Success and Failure
Audit Other Policy Change Events	Failure

- 17.8 Privilege Use



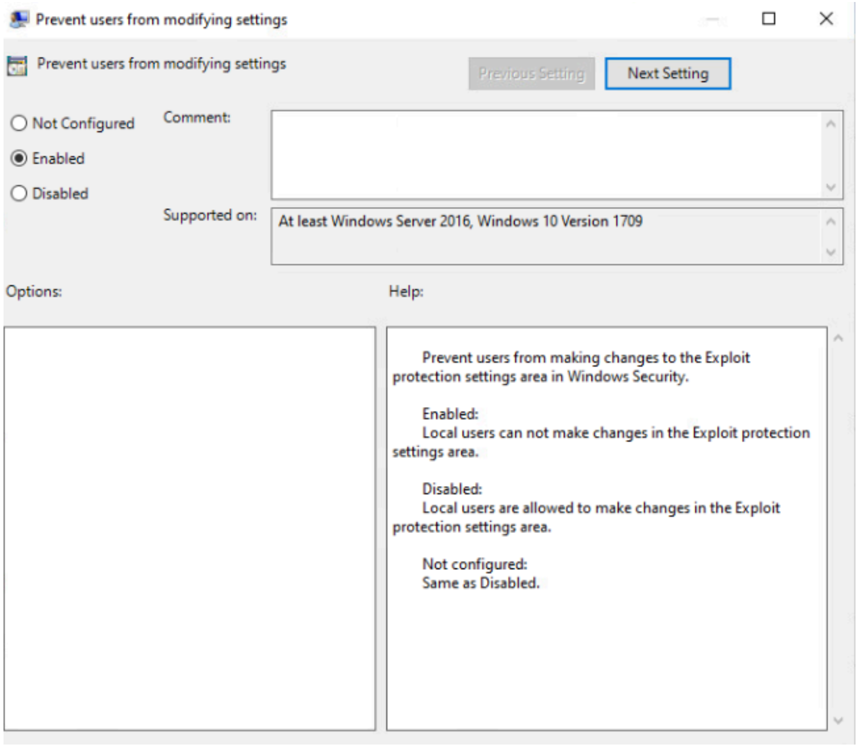
Subcategory	Audit Events
Audit Non Sensitive Privilege Use	Not Configured
Audit Other Privilege Use Events	Not Configured
Audit Sensitive Privilege Use	Success and Failure

- 17.9 System



Subcategory	Audit Events
Audit IPsec Driver	Success and Failure
Audit Other System Events	Success and Failure
Audit Security State Change	Success
Audit Security System Extension	Success
Audit System Integrity	Success and Failure

- 18.10.92.2.1 Ensure 'Prevent users from modifying settings' is set to 'Enabled'



Prevent users from modifying settings

Prevent users from modifying settings

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016, Windows 10 Version 1709

Options:

Help:

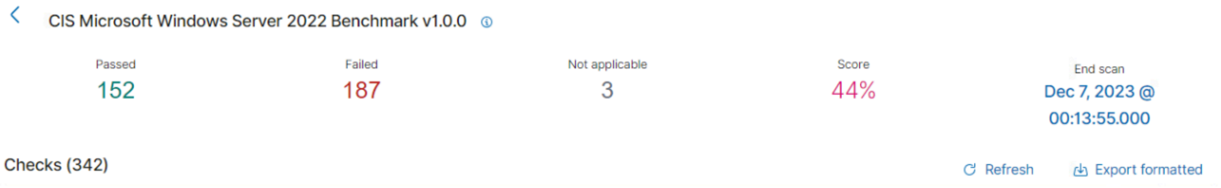
Prevent users from making changes to the Exploit protection settings area in Windows Security.

Enabled:
Local users can not make changes in the Exploit protection settings area.

Disabled:
Local users are allowed to make changes in the Exploit protection settings area.

Not configured:
Same as Disabled.

CIS Benchmark Score For Windows Server:



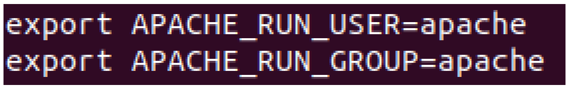
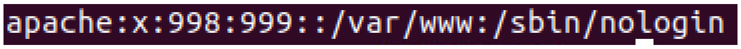
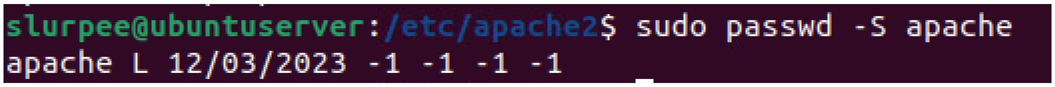
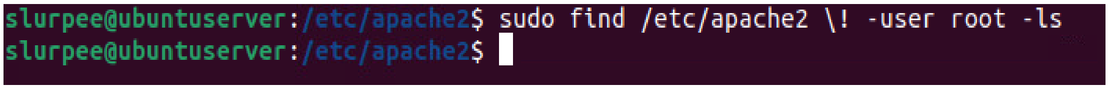
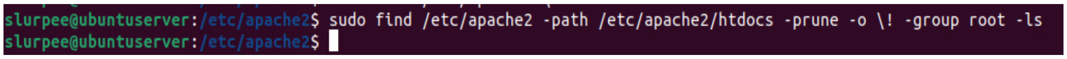
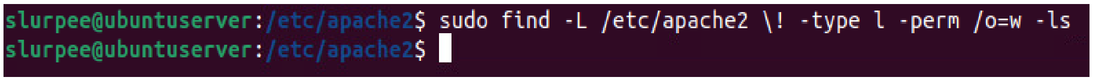
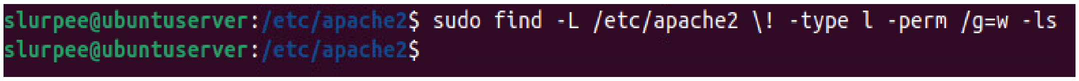
CIS Microsoft Windows Server 2022 Benchmark v1.0.0

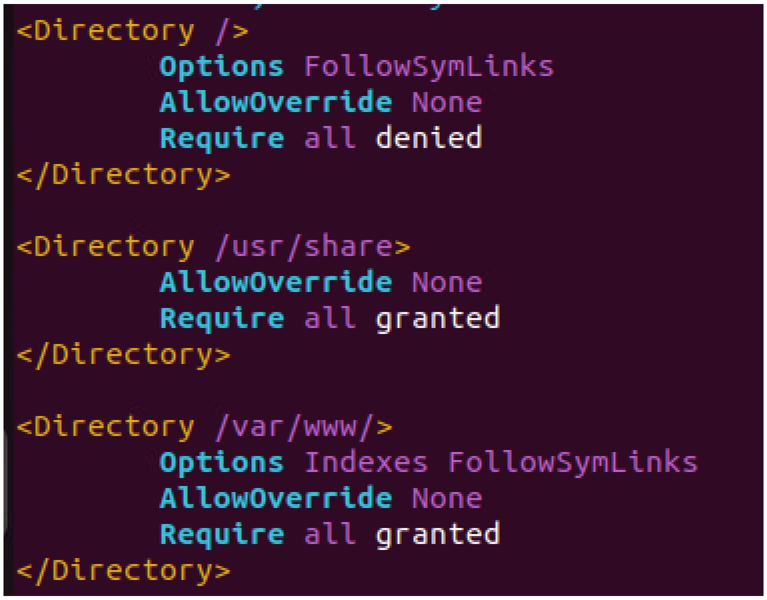
Passed	Failed	Not applicable	Score	End scan
152	187	3	44%	Dec 7, 2023 @ 00:13:55.000

Checks (342)

CIS Apache HTTP Server 2.4 Benchmark V2.1.0:

*Screenshots with no command output are showing that there are no files/directories that break the rule.

- 3.1 Ensure the Apache Web Server Runs As a Non-Root User
    - 
      ```
      export APACHE_RUN_USER=apache
      export APACHE_RUN_GROUP=apache
      ```
- 3.2 Ensure the Apache User Account Has an Invalid Shell
    - 
      ```
      apache:x:998:999::/var/www:/sbin/nologin
      ```
- 3.3 Ensure the Apache User Account Is Locked
    - 
      ```
      slurpee@ubuntuserver:/etc/apache2$ sudo passwd -S apache
      apache L 12/03/2023 -1 -1 -1 -1
      ```
- 3.4 Ensure Apache Directories and Files Are Owned By Root
    - 
      ```
      slurpee@ubuntuserver:/etc/apache2$ sudo find /etc/apache2 \! -user root -ls
      slurpee@ubuntuserver:/etc/apache2$
      ```
- 3.5 Ensure the Group Is Set Correctly on Apache Directories and Files
    - 
      ```
      slurpee@ubuntuserver:/etc/apache2$ sudo find /etc/apache2 -path /etc/apache2/htdocs -prune -o \! -group root -ls
      slurpee@ubuntuserver:/etc/apache2$
      ```
- 3.6 Ensure Other Write Access on Apache Directories and Files Is Restricted
    - 
      ```
      slurpee@ubuntuserver:/etc/apache2$ sudo find -L /etc/apache2 \! -type l -perm /o=w -ls
      slurpee@ubuntuserver:/etc/apache2$
      ```
- 3.11 Ensure Group Write Access for the Apache Directories and Files Is Properly Restricted
    - 
      ```
      slurpee@ubuntuserver:/etc/apache2$ sudo find -L /etc/apache2 \! -type l -perm /g=w -ls
      slurpee@ubuntuserver:/etc/apache2$
      ```
- 4.1 Ensure Access to OS Root Directory Is Denied By Default

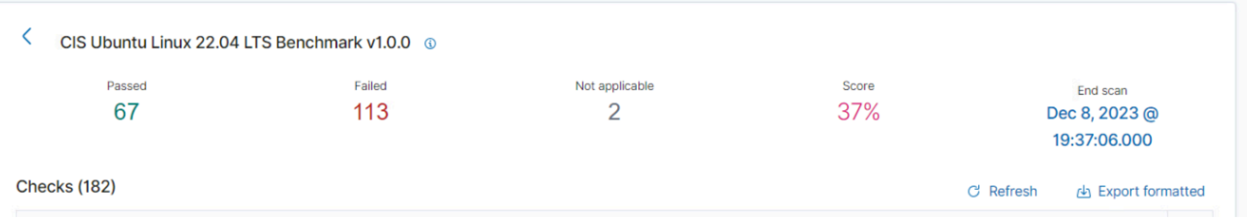
○ 

```
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

CIS Benchmark Score For Ubuntu Server:



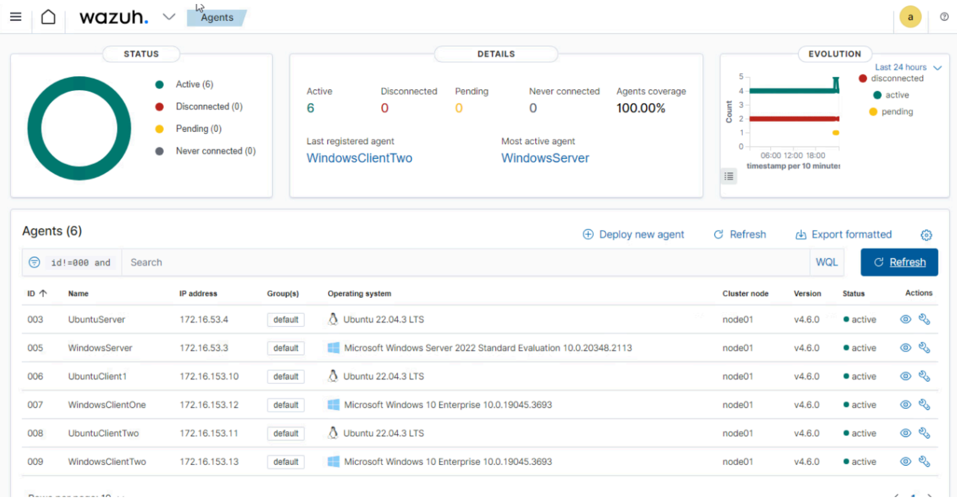
CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0

Passed	Failed	Not applicable	Score	End scan
67	113	2	37%	Dec 8, 2023 @ 19:37:06.000

Checks (182)

Wazuh:

We deployed Wazuh 4.6.0 in a docker container on the Windows Server. Every client and server had Wazuh agent 4.6.0 installed and were connected to the Wazuh docker container.



● Active (6)
● Disconnected (0)
● Pending (0)
● Never connected (0)

Active	Disconnected	Pending	Never connected	Agents coverage
6	0	0	0	100.00%

Last registered agent: WindowsClientTwo

Most active agent: WindowsServer

Agents (6)

id!=000 and Search

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
003	UbuntuServer	172.16.53.4	default	Ubuntu 22.04.3 LTS	node01	v4.6.0	● active	
005	WindowsServer	172.16.53.3	default	Microsoft Windows Server 2022 Standard Evaluation 10.0.20348.2113	node01	v4.6.0	● active	
006	UbuntuClient1	172.16.153.10	default	Ubuntu 22.04.3 LTS	node01	v4.6.0	● active	
007	WindowsClientOne	172.16.153.12	default	Microsoft Windows 10 Enterprise 10.0.19045.3693	node01	v4.6.0	● active	
008	UbuntuClientTwo	172.16.153.11	default	Ubuntu 22.04.3 LTS	node01	v4.6.0	● active	
009	WindowsClientTwo	172.16.153.13	default	Microsoft Windows 10 Enterprise 10.0.19045.3693	node01	v4.6.0	● active	

MITRE ATT&CK Techniques

- T1003.008: OS Credential Dumping: /etc/passwd and /etc/shadow
  - No user is assigned to the shadow group which would grant access to the /etc/shadow file which the attacker could then try to brute force the password hashes.
- T1136: Create Account
  - In our AD we have no GPOs created that give users the ability to create new accounts in our infrastructure.
- T1222: File and Directory Permissions Modification
  - We have logging set up in the Windows Server and in Wazuh to detect critical file changes, and most critical configuration files on the Ubuntu Server are not accessible by unprivileged users.
- T1484: Domain Policy Modification
  - Only one user has the privilege to edit GPO and/or domain policy settings, we have extensive auditing enabled on the Windows Server to alert if this Domain Admin account is compromised.
- T1505.003: Server Software Component: Web Shell
  - The HTTPD local user on the Ubuntu server has as few permissions as possible, and the web directory is configured to not be meaningfully accessible to unprivileged users, mitigating an attack like this.
- T1565.001: Data Manipulation: Stored Data Manipulation
  - Wazuh can detect when the integrity of the system is changed.

CTI Report

We chose the Mandiant, “APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION”, CTI report. The wide variety of malware and tools used in this report would be incredibly difficult to defend against completely, but our security controls and logging configuration can detect and protect against some of the attack vectors used in the report. The APT41 attack starts with a spear phishing attack with compiled HTML files including malware, stealing credentials, or using a compromised web shell. “To maintain presence, APT41 relies on backdoors, a Sticky Keys vulnerability, scheduled tasks, bootkits, rootkits, registry modifications, and creating or modifying startup files.” The Windows credential editor is used to dump password hashes, and those are brute forced to log into other privileged users on the domain. Active RDP sessions are enumerated to find system information, as well as port scans and TCP/UDP connection scans. APT41 uses “stolen credentials, adding accounts to User and Admin groups, and password brute-forcing Utilities” to achieve lateral movement throughout the network. “APT41 has also been observed modifying firewall rules to enable file and printer sharing to allow for inbound Server Message Block (SMB) traffic.”

Our security controls would not be able to defend against most of the attacks used in APT41, but our detection configurations would be able to detect the use of password brute forcing, registry key modifications, and adding accounts to user and admin groups. The use of a web shell to initially gain access to our network may be defended against by the Ubuntu Apache server’s least privilege configuration, but there are many other ways of gaining access, as stated previously.

CTI Report: https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf