sdd

0 penalties assessed, for a loss of 0 points:

28 out of 40 scored security issues fixed, for a gain of 72 points:

Forensics Question 1 correct - 4 pts
Forensics Question 2 correct - 4 pts
Forensics Question 3 correct - 4 pts
Removed unauthorized user administrat0r - 3 pts
Removed unauthorized user giant - 3 pts
Created user account tulipsnake - 5 pts
User masked is not an administrator - 3 pts
User thumper is not an Domain Admin - 3 pts
Changed insecure password for user jess - 2 pts
A secure minimum password length is required - 2 pts
Everyone may not enable computer and user accounts to be trusted for delegation - 2 pts
Domain Admins may not act as part of the operating system - 2 pts
LDAP server signing requirements [Require signing] - 2 pts
Do not allow anonymous enumeration of SAM accounts and shares [enabled] - 2 pts
Firewall protection has been enabled - 3 pts
Hardened UNC Paths configured for SYSVOL and NETLOGON - 2 pts
File sharing disabled for NTDS dump NTDS$ - 3 pts
Notepad++ has been updated - 2 pts
7-Zip has been updated - 2 pts
Removed rustscan - 2 pts
Removed qBittorrent - 2 pts
Removed Cain and Abel - 2 pts
Removed StickyKeys backdoor - 3 pts
Google Chrome HTTPS-Only mode enabled - 1 pts
Require secure RPC communication - 2 pts
WinRM service no longer allows plug-ins to store RunAs credentials - 2 pts
WinRM service no longer allows basic authentication - 2 pts
Anonymous LDAP bind is disabled - 3 pts

Removed reverse HTTP meterpreter - 3 pts

signing dnssec on 2016

Report Generated At: 2024/05/20 00:04:48 UTC

Approximate Image Running Time: 00:44:57

Approximate Team Running Time: 02:13:50

48 out of 100 points received

Click here to view the public scoreboard

Connection Status: Scoring Data Uploaded Successfully: No Errors Detected

Internet Connectivity Check: OK
CCS Server Connection Status: OK
CCS Server Score Upload Status: OK

0 penalties assessed, for a loss of 0 points:

20 out of 40 scored security issues fixed, for a gain of 48 points:

Forensics Question 1 correct - 4 pts
Removed unauthorized user yippee - 2 pts
Removed unauthorized user worm - 2 pts
Removed unauthorized user xAdministrator - 3 pts
Removed unauthorized user cybersecurityIT - 2 pts
A secure maximum password age exists - 2 pts
A secure account lockout observation window exists - 2 pts
Audit Audit Policy Change [Success] - 2 pts
Audit File Share [Success] - 2 pts
Deny access to this computer from the network includes Guest - 2 pts
Authenticated Users may not act as part of the operating system - 2 pts
Microsoft network client: Digitally sign communications (always) [enabled] - 2 pts
Allow UIAccess applications to prompt for elevation without using the secure desktop [disabled] - 2 pts
Windows Defender Real-time protection has been enabled - 3 pts
Windows Defender does not exclude .exe file extensions - 3 pts
Windows automatically checks for updates - 2 pts
FileZilla Client has been updated - 2 pts
Removed Radmin Server - 3 pts
Removed Reveal Keylogger - 3 pts
IIS application pool does not run as LocalSystem identity - 3 pts

- there was another user in the groups

20 out of 40 scored security issues fixed, for a gain of 48 points:

Forensics Question 1 correct - 4 pts
Forensics Question 2 correct - 4 pts
Removed unauthorized user giant - 3 pts
User thumper is not an Domain Admin - 3 pts
A secure minimum password length is required - 2 pts
Audit User Account Management [Success] - 2 pts
Everyone may not enable computer and user accounts to be trusted for delegation - 2 pts
Domain Admins may not act as part of the operating system - 2 pts
LDAP server signing requirements [Require signing] - 2 pts
Do not allow anonymous enumeration of SAM accounts and shares [enabled] - 2 pts
Firewall protection has been enabled - 3 pts
Hardened UNC Paths configured for SYSVOL and NETLOGON - 2 pts
Remote Registry service has been stopped and disabled - 2 pts
Removed rustscan - 2 pts
Removed qBittorrent - 2 pts
Removed Cain and Abel - 2 pts
Require secure RPC communication - 2 pts
WinRM service no longer allows plug-ins to store RunAs credentials - 2 pts
WinRM service no longer allows basic authentication - 2 pts
Anonymous LDAP bind is disabled - 3 pts

29 out of 40 scored security issues fixed, for a gain of 74 points:

Forensics Question 1 correct - 4 pts
Forensics Question 2 correct - 4 pts
Forensics Question 3 correct - 4 pts
Removed unauthorized user yippee - 2 pts
Removed unauthorized user worm - 2 pts
Removed unauthorized user xAdministrator - 3 pts
Removed unauthorized user cybersecurityIT - 2 pts
A secure maximum password age exists - 2 pts
A secure account lockout observation window exists - 2 pts
Audit Audit Policy Change [Success] - 2 pts
Audit File Share [Success] - 2 pts
Deny access to this computer from the network includes Guest - 2 pts
Authenticated Users may not act as part of the operating system - 2 pts
Microsoft network client: Digitally sign communications (always) [enabled] - 2 pts
Allow automatic administrative logon [disabled] - 2 pts
Allow UIAccess applications to prompt for elevation without using the secure desktop [disabled] - 2 pts
Windows Defender Real-time protection has been enabled - 3 pts
Windows Defender does not exclude .exe file extensions - 3 pts
Windows Defender Firewall service is running - 3 pts
Windows automatically checks for updates - 2 pts
FileZilla Client has been updated - 2 pts
Removed malicious administrative SSH key - 3 pts
Removed EvilWordle - 2 pts
Removed Radmin Server - 3 pts
Removed Reveal Keylogger - 3 pts
Insecure php functions are disabled - 3 pts
IIS application pool does not run as LocalSystem identity - 3 pts
OpenSSH Server strict mode is enabled - 2 pts
OpenSSH shell has been configured to powershell or cmd - 3 pts

65 out of 100 points received

Click here to view the public scoreboard

Connection Status: Scoring Data Uploaded Successfully: No Errors Detected

Internet Connectivity Check: OK
CCS Server Connection Status: OK
CCS Server Score Upload Status: OK

0 penalties assessed, for a loss of 0 points:

27 out of 40 scored security issues fixed, for a gain of 65 points:

Forensics Question 2 correct - 4 pts
Removed unauthorized user administrat0r - 3 pts
Removed unauthorized user giant - 3 pts
Created user account tulipsnake - 5 pts
Changed insecure password for user jess - 2 pts
A secure minimum password length is required - 2 pts
A secure kerberos maximum lifetime for service ticket is set - 2 pts
Audit User Account Management [Success] - 2 pts
Everyone may not enable computer and user accounts to be trusted for delegation - 2 pts
Domain Admins may not act as part of the operating system - 2 pts
LDAP server signing requirements [Require signing] - 2 pts
Do not allow anonymous enumeration of SAM accounts and shares [enabled] - 2 pts
Firewall protection has been enabled - 3 pts
File sharing disabled for NTDS dump NTDS$ - 3 pts
Remote Registry service has been stopped and disabled - 2 pts
Notepad++ has been updated - 2 pts
7-Zip has been updated - 2 pts
Removed NTDS dump - 3 pts
Removed rustscan - 2 pts
Removed qBittorrent - 2 pts
Removed New Club Penguin - 1 pts
Removed Cain and Abel - 2 pts
Removed reverse HTTP meterpreter - 3 pts
Removed StickyKeys backdoor - 3 pts
Google Chrome HTTPS-Only mode enabled - 1 pts
Require secure RPC communication - 2 pts
Anonymous LDAP bind is disabled - 3 pts

22 out of 40 scored security issues fixed, for a gain of 50 points:

Removed unauthorized user yippee - 2 pts
Removed unauthorized user worm - 2 pts
Removed unauthorized user xAdministrator - 3 pts
Removed unauthorized user cybersecurityIT - 2 pts
A secure maximum password age exists - 2 pts
A secure account lockout observation window exists - 2 pts
Audit Audit Policy Change [Success] - 2 pts
Audit File Share [Success] - 2 pts
Deny access to this computer from the network includes Guest - 2 pts
Authenticated Users may not act as part of the operating system - 2 pts
Microsoft network client: Digitally sign communications (always) [enabled] - 2 pts
Allow automatic administrative logon [disabled] - 2 pts
Allow UIAccess applications to prompt for elevation without using the secure desktop [disabled] - 2 pts
Windows Defender does not exclude .exe file extensions - 3 pts
Windows Defender Firewall service is running - 3 pts
Google Chrome has been updated - 2 pts
FileZilla Client has been updated - 2 pts
Removed EvilWordle - 2 pts
Removed WinDirStat - 2 pts
Removed Radmin Server - 3 pts
Removed Reveal Keylogger - 3 pts
OpenSSH shell has been configured to powershell or cmd - 3 pts

```
34  What is the decrypted password of the user COMPANY\lucas?
35
36  HINT: NTDS may have been compromised and shared in another area on the system.
37
38  ( EXAMPLE: password123! )
39
40  ANSWER: scared
41
```

```
38
39  NOTE: Please use the exact format in the example below to receive credit.
40
41  ( EXAMPLE: HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature )
42
43  ANSWER: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe\Debugger
44
```

```
2
3   ANSWER: giant
4   ANSWER: 192.168.2.11
5
```

34 out of 40 scored security issues fixed, for a gain of 86 points:

Forensics Question 1 correct - 4 pts
Forensics Question 2 correct - 4 pts
Forensics Question 3 correct - 4 pts
Removed unauthorized user administrat0r - 3 pts
Removed unauthorized user giant - 3 pts
Created user account tulipsnake - 5 pts
User masked is not an administrator - 3 pts
User thumper is not an Domain Admin - 3 pts
Changed insecure password for user jess - 2 pts
A secure minimum password length is required - 2 pts
A secure kerberos maximum lifetime for service ticket is set - 2 pts
Audit User Account Management [Success] - 2 pts
Everyone may not enable computer and user accounts to be trusted for delegation - 2 pts
Domain Admins may not act as part of the operating system - 2 pts
LDAP server signing requirements [Require signing] - 2 pts
Do not allow anonymous enumeration of SAM accounts and shares [enabled] - 2 pts
Hardened UNC Paths configured for SYSVOL and NETLOGON - 2 pts
File sharing disabled for NTDS dump NTDS$ - 3 pts
Remote Registry service has been stopped and disabled - 2 pts
OpenSSH SSH Server service has been stopped and disabled - 2 pts
Notepad++ has been updated - 2 pts
7-Zip has been updated - 2 pts
Removed NTDS dump - 3 pts
Removed qBittorrent - 2 pts
Removed Cain and Abel - 2 pts
Removed reverse HTTP meterpreter - 3 pts
Removed StickyKeys backdoor - 3 pts
Google Chrome HTTPS-Only mode enabled - 1 pts
Require secure RPC communication - 2 pts
WinRM service no longer allows plug-ins to store RunAs credentials - 2 pts
WinRM service no longer allows basic authentication - 2 pts
Zone signed with DNSSEC - 2 pts
Anonymous LDAP bind is disabled - 3 pts
Everyone no longer has Replicating Directory Changes permissions on COMPANY.LOCAL - 3 pts

27 out of 40 scored security issues fixed, for a gain of 67 points:

Forensics Question 1 correct - 4 pts
Forensics Question 2 correct - 4 pts
Forensics Question 3 correct - 4 pts
Removed unauthorized user yippee - 2 pts
Removed unauthorized user worm - 2 pts
Removed unauthorized user xAdministrator - 3 pts
Removed unauthorized user cybersecurityIT - 2 pts
Domain user manticoil is not an administrator - 2 pts
A secure maximum password age exists - 2 pts
A secure account lockout observation window exists - 2 pts
Audit Audit Policy Change [Success] - 2 pts
Audit File Share [Success] - 2 pts
Deny access to this computer from the network includes Guest - 2 pts
Authenticated Users may not act as part of the operating system - 2 pts
Microsoft network client: Digitally sign communications (always) [enabled] - 2 pts
Allow automatic administrative logon [disabled] - 2 pts
Allow UIAccess applications to prompt for elevation without using the secure desktop [disabled] - 2 pts
Windows Defender Real-time protection has been enabled - 3 pts
Windows Defender does not exclude .exe file extensions - 3 pts
Windows Defender Firewall service is running - 3 pts
Windows automatically checks for updates - 2 pts
Google Chrome has been updated - 2 pts
FileZilla Client has been updated - 2 pts
Removed malicious administrative SSH key - 3 pts
Removed WinDirStat - 2 pts
Removed Radmin Server - 3 pts
Removed Reveal Keylogger - 3 pts