Ubuntu 18 (37/37)

1. Forensics Question 1 correct - 6 pts
2. Forensics Question 2 correct - 6 pts
3. Forensics Question 3 correct - 6 pts
4. Removed hidden user akatosh - 3 pts
5. Removed unauthorized user alduin - 2 pts
6. User belethor is not an administrator - 2 pts
7. Disabled password login for user bin - 3 pts
8. Disabled shell login for user irc - 3 pts
9. Previous passwords are remembered - 3 pts
10. A default minimum password age is set - 2 pts
11. An account lockout policy is configured - 3 pts
12. Null passwords do not authenticate - 3 pts
13. X Server does not allow TCP connections - 3 pts
14. IPv4 TCP SYN cookies have been enabled - 2 pts
15. Ignore broadcast ICMP echo requests enabled - 2 pts
16. Insecure sudo configuration fixed - 3 pts
17. Uncomplicated Firewall (UFW) protection has been enabled - 2 pts
18. Insecure permissions on shadow file fixed - 3 pts
19. IRC daemon has been disabled or removed - 2 pts
20. AppArmor service has been started - 3 pts
21. Install updates from important security updates - 1 pts
22. Linux kernel has been updated - 2 pts
23. APT has been updated- 1 pts
24. Firefox has been updated - 2 pts
25. Samba has been updated - 2 pts
26. Prohibited MP3 files are removed - 3 pts
27. Removed SUID bit from find - 4 pts
28. Prohibited software dsniff removed - 2 pts
29. Prohibited software linuxdcpp removed - 2 pts
30. Prohibited software rfdump removed - 2 pts
31. Prohibited software heartbleeder removed - 2 pts
32. Removed perl owl-shell backdoor - 4 pts
33. Firefox checks the current validity of certificates - 2 pts
34. Samba SMB1 protocol is disabled - 3 pts
35. Unauthorized Samba share is disabled - 3 pts
36. Insecure permissions on Samba share fixed - 2 pts
37. Samba encryption is required - 3 pts

Debian 9 (37/37)

1. Forensics Question 1 correct - 5 pts
2. Forensics Question 2 correct - 5 pts
3. Forensics Question 3 correct - 5 pts
4. Forensics Question 4 correct - 5 pts
5. Removed unauthorized user bahamut - 2 pts
6. Removed hidden user sephiroth - 3 pts
7. User jessie is not an administrator - 2 pts
8. Disable shell login for user games - 2 pts
9. User rtuesti has a maximum password age - 2 pts
10. Password for zfair is hashed with secure algorithm - 3 pts
11. A minimum password length is required - 2 pts
12. Extra dictionary based password strength checks enabled - 3 pts
13. A secure password hashing algorithm is used - 2 pts
14. A default maximum password age is set - 2 pts
15. IPv4 TIME-WAIT assassination protection enabled - 3 pts
16. Logging of martian packets enabled - 2 pts
17. Restrict unprivileged access to kernel syslog enabled - 3 pts
18. Uncomplicated Firewall (UFW) protection has been enabled - 2 pts
19. Insecure permissions on PostgreSQL configuration files fixed - 3 pts
20. GRUB configuration is not world readable - 2 pts
21. Apache2 service has been disabled or removed - 2 pts
22. Samba service has been disabled or removed - 2 pts
23. DNS service has been disabled or removed - 2 pts
24. Install updates from important security updates - 1 pts
25. PostgreSQL has been updated - 3 pts
26. Firefox has been updated - 2 pts
27. Prohibited MP3 files removed - 3 pts
28. Prohibited software cupp3 removed - 2 pts
29. Prohibited software cmospwd removed - 2 pts
30. Prohibited software fcrackzip removed - 2 pts
31. Removed netcat backdoor - 3 pts
32. Removed python backdoor - 3 pts
33. PostgreSQL rejects all non-local connection requests without SSL - 3 pts
34. PostgreSQL requires authentication for all connections - 4 pts
35. PostgreSQL has ssl enabled - 4 pts
36. PostgreSQL configured to log connections - 2 pts
37. PostgreSQL does not map any user to the postgres account - 2 pts

Windows 10 (34/40)

1. Forensics Question 1 correct - 6 pts
2. Forensics Question 2 correct - 6 pts
3. Forensics Question 3 correct - 6 pts
4. Removed unauthorized user vex - 4 pts
5. Removed unauthorized user brynjolf - 2 pts
6. Changed insecure password for delphine - 2 pts
7. User borri password expires - 2 pts
8. User einarth password expires - 2 pts
9. Passwords are not stored using reversible encryption - 2 pts
10. A secure maximum password age exists - 2 pts
11. Audit User Account Management [Success] - 2 pts
12. Audit System Integrity [Failure] - 2 pts
13. User irileth may not manage auditing and security log - 3 pts
14. Early Launch Antimalware does not initialize known non-critical bad drivers - 2 pts
15. Firewall protection has been enabled - 2 pts
16. Validate heap integrity setting enabled - 2 pts
17. AutoPlay has been disabled [all users] - 2 pts
18. Everyone may not write to the Skynet IIS directory - 2pts
19. Remote Registry service has been stopped and disabled - 2 pts
20. Xbox Live Game Save service has been stopped and disabled - 2 pts
21. Majority of Windows updates are installed - 2 pts
    a. Couldn't restart for updates
22. Firefox has been updated - 1 pts
23. Removed phpinfo file - 3 pts
24. Removed Etherium cryptominer Geth -1 pts
25. Removed MySQL-G0ld - 2 pts
26. Removed SDR tools - 2 pts
27. Removed PHP backdoor - 3 pts
28. Removed WindowsRAT - 3 pts
29. PHP expose header configuration set to disabled - 2 pts
30. PHP display errors has been disabled - 3 pts
31. IIS web server logging enabled for Skynet website - 2 pts
32. IIS HTTP error responses for remote requests not set to Detailed - 3 pts
33. IIS server information is not included in response header - 2 pts
34. IIS web server requires SSL connections - 3 pts

Windows Server 2019 (37/41)

1. Forensics Question 1 correct - 5 pts
2. Forensics Question 2 correct - 5 pts
    a. OS Forensics
3. Forensics Question 3 correct - 5 pts
4. Forensics Question 4 correct - 5 pts
5. Removed unauthorized user tolfdir - 1 pts
6. User wulfgar is not an Enterprise Admin - 1 pts
7. Farengar is not disabled - 1 pts
8. Changed insecure password for balgruuf - 1 pts
9. User ralof password expires - 1 pts
10. Domain Users removed from DnsAdmins group - 2 pts
11. A secure lockout threshold exists - 2 pts
12. Audit Credential Validation [Success] - 1 pts
13. Audit Kerberos Authentication [Success] - 1 pts
14. Everyone may not enable computer and user accounts to be trusted for delegation - 2 pts
15. LDAP server signing requirements [Require signing] - 3 pts
16. Recovery console: Allow automatic administrative logon [disabled] - 2 pts
17. Configure encryption types allowed for Kerberos [AES Only] - 3 pts
18. Switch to the secure desktop when prompting for elevation [enabled] - 2 pts
19. Autoplay has been disabled [all users] - 2 pts
20. Everyone is no longer allowed full share permissions to SYSVOL - 3 pts
21. NTDS dump share is disabled - 2 pts
22. Domain Users are no longer allowed access to NTDS - 3 pts
23. Windows automatically checks for updates - 2 pts
24. Firefox has been updated - 2 pts
25. Removed NTDS dump - 3 pts
26. Removed prohibited music files - 2 pts
27. Removed Teamspeak - 2 pts
28. Removed mimikatz script file - 2 pts
29. Reverse TCP DLL Removed from DNS Server - 3 pts
    - sc.exe stop dns (Stop DNS service)
    - Remove-Item C:\Windows\System32\DNS\ipv6_dnsapi.dll -Force
    - Delete ServerLevelPluginDll registry entry in "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters"
    - sc.exe start dns (Start DNS service)
30. Removed NTDS dump script file - 3 pts
31. Removed Backdoor - 3 pts
32. Audit DNS events - 3 pts

    a. Set-DnsServerDiagnostics -EventLogLevel 3
33. DNS Service restarts after failure - 3 pts
    - sc.exe failure DNS reset= 10 actions= restart/10000/restart/10000/restart/10000
34. Dynamic updates to the DNS server are disabled - 3 pts
35. SIGRed workaround implemented - 3 pts
36. SMB 1.0 removed or disabled - 3 pts
37. Firefox blocks dangerous downloads - 2 pts