Windows

Forensics Questions:

1. Forensics Question 1 is correct
2. Forensics Question 2 is correct
3. Forensics Question 3 is correct
4. Forensics Question 4 is correct
5. Forensics Question 5 is correct

User Auditing:

6. Created group ExGroup
7. Added users to group ExGroup
8. Created user account ExNewUser
9. Guest account is not enabled
10. Admin Account is disabled
11. Removed terminated employee's user account "ExTerminatedUser"
12. Removed unauthorized user BadUser
13. User ExUser is not a Domain Admin
14. User ExUser is not an Enterprise Admin
15. User NotAuthAdmin is not an administrator
16. User ExNewUser is an administrator
17. User ExUser has a password
18. Changed insecure password for ExUser1
19. User ExUser2 password Expires
20. User Account ExUser3 is enabled
21. User ExUser4 is not locked out
22. User ExUser5 can change password
23. Domain Users removed from DnsAdmins group
24. Operations group removed from DnsAdmins
25. Remote Desktop Users group includes all authorized users

Account Policies

26. A sufficient password history is being kept
27. A secure maximum password age exists
28. A secure minimum password age exists
29. A secure minimum password length is required
30. Valid length set for minimum password length audit policy
31. Passwords must meet complexity requirements
32. A secure account lockout duration exists
33. A secure account lockout threshold exists
34. A secure account lockout observation window exists

Security Policy:

35. Audit *Security Policy* [Success]
36. Audit *Security Policy* [Failure]
37. Everyone may not create a token object
38. User *ExUser6* can no longer manage auditing and security log
39. User *ExUser6* may not take ownership of files or other objects
40. Everyone may not access this computer from the network
41. Users may not change the system time
42. Users may not load and unload drivers
43. Everyone can no longer access credential manager as a trusted caller
44. Users may not access Credential Manager as a trusted caller
45. User *ExUser7* may not create global objects
46. Everyone may not Enable delegation privilege
47. Authenticated Users may not remotely shutdown the system
48. Everyone may not create a token object
49. Deny access to this computer from the network includes Guest
50. Administrators are allowed to log on through Remote Desktop Services
51. Accounts: Limit local account use of blank passwords to console logon only [enabled]
52. Devices: Prevent users from installing printer drivers [enabled]
53. Devices: Restrict CD-ROM access to locally logged-on user only [enabled]
54. Domain controller: LDAP server signing requirements [require signing]
55. Domain member: Digitally encrypt or sign secure channel data (always) [enabled]
56. Domain member: Require strong (Windows 2000 or later) session key [enabled]
57. Interactive Logon: Do not require CTRL+ALT+DEL [disabled]
58. Interactive logon: Do not display last user name [enabled]
59. Microsoft Network Client: Digitally sign communications (always) [enabled]
60. Microsoft Network Client: Send unencrypted password to connect to third-party SMB servers [disabled]
61. Microsoft Network Server: Digitally sign communications (always) [enabled]
62. Network access: Let everyone permissions apply to anonymous users [disabled]
63. Network access: Do not allow anonymous enumeration of SAM accounts and shares [enabled]
64. Network access: Do not allow anonymous enumeration Of SAM accounts [enabled]
65. Network access: Restrict anonymous access to Named Pipes and Shares [enabled]
66. Network access: Shares that can be accessed anonymously [None]
67. Network security: Configure encryption types allowed for Kerberos [AES Only]
68. Network security: Do not store LAN Manager hash value on next password change [enabled]
69. Network security: LAN Manager authentication level [Send NTLMv2 response only. Refuse LM & NTLM]

70. Network security: Allow LocalSystem NULL session fallback [disabled]
71. Recovery Console: Allow automatic administrative logon [disabled]
72. Shutdown: Allow shutdown without having to log on [disabled]
73. Shutdown: Clear virtual memory pagefile [enabled]
74. User Account Control: Admin Approval Mode for the Built-in Administrator account [enabled]
75. User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop [disabled]
76. User Account Control: Only elevate UIAccess applications that are installed in secure locations [enabled]
77. User Account Control: Switch to the secure desktop when prompting for elevation [enabled]
78. User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode [prompt for credentials on secure desktop]

Defensive Countermeasures:

79. Firewall protection has been enabled
80. Antivirus protection has been enabled
81. BitLocker drive encryption service is running
82. Control flow guard setting enabled
83. Windows Defender exclusions removed
84. Program exception chain integrity enabled
85. Early Launch Antimalware does not initialize known non-critical bad drivers

Uncategorized operating system settings:

86. Remote Desktop Sharing is turned off
87. Remote Assistance connections have been disabled
88. Desktop gadgets have been completely disabled [Outdated- Windows 7]
89. C sharing is disabled
90. Hidden share *exsharename* is disabled
91. DEP enabled for all programs and services
92. Enumerate administrator accounts on elevation [disabled]
93. Screen saver is password protected
94. Screen saver is password protected [all users]
95. AutoRun commands have been disabled [all users]
96. Autoplay has been disabled [all users]
97. Randomize memory allocations setting enabled
98. Data-only memory pages have code execution prevention enabled
99. Everyone is no longer allowed to write to C:\Share
100. Validate heap integrity setting enabled
101. Everyone may not write to the IIS directory
102. Controlled folder access for ransomware protection enabled for share

103. Everyone is no longer allowed full share permissions to SYSVOL
104. Users may not read from the MUTINY postoffice directory
105. Domain Users are no longer allowed access to NTDS
106. Ip Source Routing is completely disabled

Service Auditing:

107. Bluetooth Support Service has been stopped or disabled
108. DNS Server service has been stopped and disabled
109. FTP service has been stopped and disabled
110. Microsoft FTP service has stopped and disabled
111. Microsoft ISNS service has stopped and disabled
112. MultiPoint Service has been stopped and disabled
113. LPD service has been stopped and disabled
114. Net. TCP Port Sharing service has been stopped and disabled
115. RIP Listener service has been stopped and disabled
116. RPC Locator service has been stopped and disabled
117. Remote Access Connection Manager service has been stopped and disabled
118. Remote Registry service has been stopped and disabled
119. Simple Mail Transfer Protocol (SMTP) service has been stopped and disabled
120. SNMP service has been stopped and disabled
121. SNMP Trap service has been stopped and disabled
122. SSDP Discovery service has been stopped and disabled
123. Simple TCP/IP service has been stopped and disabled
124. Telephony service has been stopped and disabled
125. Telnet service has been stopped and disabled
126. UPnP Device Host service has been stopped and disabled
127. WebClient service has been stopped and disabled
128. World Wide Web Publishing Service has been stopped and disabled
129. Xbox Live Auth Manager has been stopped and disabled
130. Xbox Live Game Save service has been stopped and disabled
131. Windows Update service is enabled
132. Event Log service is enabled
133. Adobe Acrobat Update service is enabled
134. Windows Firewall service is enabled

Operating System Updates:

135. Windows automatically checks for updates
136. Give me updates for other Microsoft products when I update Windows
137. The majority of Windows updates are installed

Application Updates:

138. Acrobat Reader DC has been updated
139. FileZilla has been updated

140. FileZilla Client has been updated
141. Firefox has been updated
142. Foxit Reader has been updated
143. Geany has been updated
144. Gimp has been updated
145. IrfanView has been updated
146. Java JRE 8 has been updated
147. Krita has been updated
148. LibreOffice has been updated
149. MailEnable has been enabled
150. MobaXterm has been updated
151. Notepad++ has been updated
152. OpenCPN has been updated
153. PeaZip has been updated
154. PHP has been updated
155. Powershell has been updated
156. PuTTY has been updated
157. Thunderbird has been updated
158. TortoiseHG has been updated
159. Visual Studio Code has been updated
160. VLC has been updated
161. Firefox automatically updates

Prohibited Files:

162. Removed prohibited MP3 files
163. Removed prohibited MP4 files
164. Removed prohibited OGG files
165. Removed prohibited music files
166. Removed NTDS dump
167. Removed shodan queries archive
168. Removed Brutus password cracker archive
169. Removed Cain and Abel software archive
170. Removed Hashcat password cracker archive
171. Removed Nikto scanning software archive
172. Removed PowerShell Empire software archive
173. Removed minikatz archive
174. Removed Rubeus archive
175. Removed plain text file with passwords
176. Removed alternate data stream file containing user passwords
177. Removed PHP Backdoor
178. Removed phpinfo file

179. Removed file containing confidential customer information
180. Removed phishing email templates
181. Removed comic book pdf

Prohibited Software:

182. Microsoft Baseline Security Analyzer 2 has been installed -
183. Removed Abyss Web Server
184. Removed Adaware WebCompanion
185. Removed Advanced Port Scanner
186. Removed Angry Ip scanner
187. Removed AnyDesk
188. Removed Arcade Lines
189. Removed Avernum
190. Removed Beware IRC server
191. Removed BitComet
192. Removed BitTornado
193. Removed BoomBox Radio Player
194. Removed ButtonBeats Virtual Piano Black
195. Removed BZFlag
196. Removed Chicken Invaders
197. Removed CleanMyPC
198. Removed Deluge
199. Removed DOSBox
200. Removed Driver Booster
201. Removed Driver Support
202. Removed Epic Games Launcher
203. Removed Etherium cryptominer Geth
204. Removed Fake an Error program
205. Removed Firefox addon Video DownloadHelper
206. Removed Garden Planner
207. Removed HTTP Explorer
208. Removed Hashcat
209. Removed Hash Suite
210. Removed Home Web Server
211. Removed Itunes
212. Removed John the Ripper
213. Removed K-Lite Codec Pack
214. Removed KNCTR
215. Removed Kodi
216. Removed Lazersoft
217. Removed MyCleanPC PC Optimizer

218. Removed MySQL-G0ld
219. Removed Ncrack
220. Removed Nmap
221. Removed Open TFTP Server
222. Removed Ophcrack
223. Removed osquery
224. Removed Plex Media Server
225. Removed Progress Telerik Fiddler Web Debugger
226. Removed Rainbowcrack
227. Removed Radmin server
228. Removed Reimage Repair
229. Removed SDR tools
230. Removed SuperScan
231. Removed TeamViewer
232. Removed Tetris
233. Removed TightVNC Server
234. Removed Tiny Web Server
235. Removed Tonido Server
236. Removed TV 3L PC
237. Removed uTorrent
238. Removed Vega
239. Removed VirtualDJ8
240. Removed Vistumbler
241. Removed WebDiscover browser
242. Removed Wireshark
243. Removed Zed attack proxy

Malware:

244. Scheduled task “Bad_Task” Removed
245. Removed netcat backdoor
246. Removed tini backdoor
247. Remove ntbindshell backdoor
248. Removed TX backdoor
249. Removed NetBus Pro
250. Removed Sticky Keys backdoor
251. Removed Custom backdoor
252. Removed Actual Keylogger
253. Removed Keylogger
254. Removed Spyrix Keylogger
255. Removed Reveal Keylogger

256. Removed WindowsRAT
257. Removed RAT
258. Removed WinUserProfileManager
259. Removed mimikatz script file
260. Removed NTDS dump script file
261. Reverse TCP DLL Removed from DNS Server
262. Removed simple ASPX web shell
263. Removed LT ASPX web shell
264. Removed dnknflka backdoor

Application Security Settings

265. Internet Explorer has been installed
266. Internet Explorer SmartScreen Filter
267. Windows SmartScreen configured to warn or block
268. Internet Explorer Enhanced Security Configuration is enabled
269. Internet Explorer Phishing filter is enabled
270. Internet Explorer 8+ Smart Screen Filter [enabled]
271. Internet Properties: Enable Enhanced Protected Mode [Enabled]
272. Internet Zone: Initialize and script ActiveX controls not marked as safe for scripting [disabled]
273. Internet Zone: Enable Protected Mode [Enabled]
274. Firefox pop-up blocker enabled
275. Firefox blocks dangerous downloads
276. Firefox warns when sites try to install add-ons
277. Firefox displays warning on known malware sites
278. Firefox display warning on known malware sites [all users]
279. Firefox HTTPS-Only mode enabled for all windows
280. Firefox blocks reported web forgeries
281. Google Chrome safe browsing enabled
282. Google Chrome HTTPS-Only mode enabled
283. PHP log errors have been enabled
284. PHP system function is disabled
285. PHP expose header configuration set to disabled
286. PHP display errors has been disabled
287. Require RPC communication
288. RDP network level authentication enabled
289. RDP connection encryption level has been set to high
290. RDP TLS Communication enabled
291. Do not allow drive redirection
292. Do not allow supported Plug and Play device redirection

293. SMB 1.x removed or disabled
294. IIS default website directory browsing disabled
295. IIS HTTP error responses for remote requests not set to Detailed
296. IIS server information is not included in response header
297. IIS server requires SSL connections
298. IIS application pool does not run as LocalSystem identity
299. IIS logging enabled
300. Audit DNS events
301. DNS Service restarts after failure
302. DNS zone transfers to any server is disabled
303. Dynamic updates to the DNS server are disabled
304. SIGRed workaround implemented
305. FTP anonymous write disabled
306. MailEnable uses encrypted passwords
307. MailEnable configured with default SSL certificate
308. Unauthorized MailEnable account disabled or removed

Linux

Forensics Questions:

1. Forensics Question 1 is correct
2. Forensics Question 2 is correct
3. Forensics Question 3 is correct
4. Forensics Question 4 is correct
5. Forensics Question 5 is correct

User Auditing:

6. Guest account is disabled
7. Removed unauthorized user [user]
8. Removed hidden user [user]
9. Removed ftp user
10. User [user] is not an administrator
11. User [user] is an administrator
12. Changed insecure password for [user]
13. Created user group [group]
14. Created user account [user]
15. Users added to group [group]
16. User [user] cannot login without a password
17. [User] password expires
18. Root password is no longer blank / Changed insecure Root password

19. User [user] has a maximum password age
20. User [user] has a minimum password age
21. Password for [user] is hashed with a secure algorithm
22. Disabled password login for user [system user]
23. Disabled shell login for user [system user]

Account Policies

24. A default maximum password age is set
25. A default minimum password age is set
26. Previous passwords are remembered
27. A minimum password length is required
28. Extra dictionary based password strength checks enabled
29. Extra non-dictionary based password strength checks enabled
30. Extra GECOS password strength checks enabled
31. A secure password hashing algorithm is used
32. Null passwords do not authenticate
33. Null passwords do not authenticate on insecure consols
34. An account lockout policy is configured
35. Greeter does not enumerate user accounts

Security Policy:

36. X Server does not allow TCP connections (xserver-allow-tcp = false)
37. Address space layout randomization enabled (kernel.randomize_va_space=2)
38. IPv4 TCP SYN cookies have been enabled (net.ipv4.tcp_syncookies=1)
39. IPv4 TCP SYN,ACK retries reduced (net.ipv4.tcp_synack_retries = 2)
40. IPv4 TIME-WAIT assassination protection enabled (net.ipv4.tcp_rfc1337=1)
41. IPv4 forwarding has been disabled (net.ipv4.ip_forward=0)
42. IPv4 sending ICMP redirects disabled (net.ipv4.conf.all.send_redirects=0 net.ipv4.conf.default.send_redirects=0)
43. IPv4 accept ICMP redirects disabled (net.ipv4.conf.all.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0)
44. IPv4 accept source routing disabled (net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0)
45. IPv4 source route verification enabled (net.ipv4.conf.default.rp_filter = 0 net.ipv4.conf.all.rp_filter = 1)
46. Ignore bogus ICMP errors enabled (net.ipv4.icmp_ignore_bogus_error_responses=1)
47. Ignore broadcast ICMP echo requests enabled (net.ipv4.icmp_echo_ignore_broadcasts=1)
48. Kernel pointers hidden from unprivileged users (kptr_restrict=0)
49. Magic SysRq key disabled (kernel.sysrq = 0)
50. Only root may create new namespaces (kernel.unprivileged_userns_clone=0)
51. Restrict unprivileged access to kernel syslog enabled (kernel.dmesg_restrict=1)

52. Logging of martian packets enabled (net.ipv4.conf.all.log_martians=1 net.ipv4.conf.default.log_martians=1)
53. Sudo requires authentication
54. Group [group] does not have sudo privileges

Defensive Countermeasures:

55. Uncomplicated Firewall (UFW) protection has been enabled
56. UFW does not accept incoming ICMP echo-requests

Uncategorized operating system settings:

57. GRUB configuration is not world readable
58. GRUB uses encrypted password protection
59. Insecure permissions on shadow file fixed
60. Resolver checks for IP spoofing
61. Stricter defaults have been enabled for shared memory
62. TMP has been mounted securely
63. Process information hidden from other users
64. Xserver TCP Connections disabled
65. Insecure permissions on OpenVPN server configuration file fixed
66. Root login through GDM is not allowed
67. Grub does not default to disabling noexec
68. TTY Shell is not launched on root login

Service Auditing:

69. Apache2 service has been disabled or removed
70. AppArmor service is enabled
71. Bind9 service is stopped and removed
72. DNS service is disabled or removed
73. FTP service has been disabled or removed
74. Icecast2 service has been disabled or removed
75. IRC daemon has been stopped and disabled
76. Journald service is enabled and running
77. Jupyter Notebook service has been disabled or removed
78. MariaDB service has been disabled or removed
79. Minetest service has been disabled or removed
80. MySQL has been disabled or removed
81. Nginx service has been disabled or removed
82. NFS services is stopped and removed
83. OpenArena service has been disabled or removed
84. POP3 service has been disabled or removed
85. POPS service has been disabled or removed
86. Postgresql has been disabled or removed
87. QTorrent Service has been stopped and disabled

88. Rsync service has been disabled or removed
89. Rsyslog service has been enabled and enabled
90. Samba service has been disabled or removed
91. SMTP service has been disabled or removed
92. SNMP service has been disabled or removed
93. Squid proxy service has been disabled or removed
94. VNC service has been disabled or removed
95. WorldForge service has been disabled or removed

Operating System Updates:

96. The system automatically checks for updates daily
97. Install updates from important security updates
98. Important Security Downloads have been conducted
99. Linux kernel has been updated
100. Bash has been updated
101. BusyBox has been updated
102. OpenSSL shared libraries have been updated
103. Glibc has been updated
104. APT has been updated
105. Debian has valid lists

Application Updates:

106. 7zip has been updated
107. Apache2 has been updated
108. Bluefish has been updated
109. DNS (bind9) has been updated
110. FileZilla has been updated
111. Firefox has been updated
112. GIMP has been updatedZ
113. Iceweasel has been updated to firefox-esr
114. LibreOffice has been updated
115. Nginx has been updated
116. OpenSSH has been updated
117. PHP has been updated
118. PHP5 has been updated
119. PostgreSQL has been updated
120. Pro FTP daemon has been updated
121. Pure FTP has been updated
122. Samba has been updated
123. Thunderbird has been updated
124. Tilda has been updated
125. Vsftpd has been updated

126. WordPress has been updated

Prohibited Files:

127. Prohibited MP3 files are removed
128. Prohibited OGG music files removed
129. Removed plaintext file containing passwords
130. Removed file containing password hash
131. Removed PHP backdoor
132. Removed phpinfo() php file
133. Removed UFONet archive
134. Removed Secure Shell Bruteforcer archive

Prohibited Software:

135. Stellarium has been installed
136. Prohibited software aMule removed
137. Prohibited software Angry IP Scanner removed
138. Prohibited software Arp-scan removed
139. Prohibited software Cmospwd removed
140. Prohibited software Cupp3 removed
141. Prohibited software Deluge removed
142. Prohibited software doona removed
143. Prohibited software Doomsday removed
144. Prohibited software Dsniff removed
145. Prohibited software Endless Sky removed
146. Prohibited software Ettercap removed
147. Prohibited software Fcrackzip removed
148. Prohibited software Freeciv removed
149. Prohibited software goldeneye removed
150. Prohibited software Heartbleeder removed
151. Prohibited software Hunt removed
152. Prohibited software Hydra removed
153. Prohibited software John the ripper removed
154. Prohibited software Kismet removed
155. Prohibited software Knocker removed
156. Prohibited software linuxdcpp removed
157. Prohibited software Minetest removed
158. Prohibited software NBTScan removed
159. Prohibited software nmapsi4 removed
160. Prohibited software Nmap and Zenmap removed
161. Prohibited software OpenRa removed
162. Prohibited software Ophcrack removed
163. Prohibited software P0f removed

164. Prohibited software packit removed
165. Prohibited software Pixel Dungeon removed
166. Prohibited software pompem removed
167. Prohibited software proxychains removed
168. Prohibited software Pnscan removed
169. Prohibited software pyrdp archive removed
170. Prohibited software Reaver removed
171. Prohibited software Rfdump removed
172. Prohibited software Remmina removed
173. Prohibited software TCPSpray removed
174. Prohibited software themole removed
175. Prohibited software Wireshark removed
176. Prohibited software Xprobe removed
177. Prohibited software Yersinia removed
178. Prohibited software Zangband removed

Malware:

179. Removed python backdoor
180. Removed perl backdoor
181. Removed perl bindshell backdoor
182. Removed perl owl-shell backdoor
183. Removed SSH MOTD reverse shell
184. Removed netcat backdoor
185. SUID backdoor removed
186. Removed SUID bit from find (fixed insecure permissions on find)
187. Removed zod backdoor
188. Removed kbind backdoor
189. Removed appleqtcsrvr backdoor

Application Security Settings

190. SSH root login has been disabled
191. SSH protocol 1 has been disabled
192. SSH only listens on port 222(situational)
193. SSH allows only public key authentication
194. SSH does not permit empty passwords
195. SSH user environment processing is disabled
196. Anonymous Samba access is disabled
197. Unauthorized Samba share is disabled
198. Samba blank passwords are disabled

199. Insecure permissions on Samba share fixed
200. Samba SMB1 protocol is disabled
201. Samba encryption is required
202. NTLM authentication is disabled
203. FTP local users must log in as anonymous
204. FTP anonymous write commands are disabled
205. FTP anonymous user is not root
206. FTP anonymous access is disabled
207. FTP Server identity is off
208. Insecure permissions on FTP root directory fixed
209. FTP plain-text authentication disabled (SSL?????)
210. FTP service is not running as root
211. Anonymous and local FTP user login correctly configured
212. FTP anonymous root directory is set correctly
213. Root user explicitly denied from FTP login
214. FTP PASV and PORT security checks enabled
215. MySQL remote access is disabled
216. MySQL SSL Certificates are valid and enabled
217. SQL is not ran as root
218. PostgreSQL rejects all non-local connection requests without SSL
219. PostgreSQL requires authentication for all connections
220. PostgreSQL configured to log connections
221. PostgreSQL has ssl enabled
222. PostgreSQL does not map any user to the postgres account
223. Removed phpinfo() php file
224. PHP expose is Off
225. PHP system function is disabled
226. PHP URL-aware fopen wrappers are disabled
227. PHP secure sessions are enabled
228. PHP does not display errors
229. PHP strict session mode enabled
230. Apache server signature is disabled
231. Apache trace requests disabled
232. Apache etags disabled
233. Apache server tokens set to least
234. OpenVPN server is not configured to run as root
235. OpenVPN server has logging enabled
236. Firefox pop-up blocker enabled
237. Firefox displays warning on known malware sites
238. Firefox warns when sites try to install add-ons

239. Firefox block dangerous and deceptive content
240. Firefox checks the current validity of certificates
241. Firefox HTTP-Only mode enabled for all windows
242. Inline scripts not allowed by nginx content security policy
243. Nginx set to block XSS attacks for legacy browsers
244. Nginx server tokens disabled