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 NotAuthAdmin is not an administrator
14. User ExNewUser is an administrator
15. User ExUser has a password
16. Changed insecure password for ExUser1
17. User ExUser2 password Expires
18. User Account ExUser3 is enabled
19. User ExUser4 is not locked out
20. User ExUser5 can change password

Account Policies

21. A sufficient password history is being kept
22. A secure maximum password age exists
23. A secure minimum password age exists
24. A secure minimum password length is required
25. Passwords must meet complexity requirements
26. A secure account lockout duration exists
27. A secure account lockout threshold exists
28. A secure account lockout observation window exists

Security Policy:

29. Audit *Security Policy* [Success]
30. Audit *Security Policy* [Failure]
31. Everyone may not create a token object
32. User *ExUser6* can no longer manage auditing and security log
33. User ExUser6 may not take ownership of files or other objects

34. Everyone may not access this computer from the network
35. Users may not change the system time
36. Users may not load and unload drivers
37. Everyone can no longer access credential manager as a trusted caller
38. Users may not access Credential Manager as a trusted caller
39. User *ExUser7* may not create global objects
40. Everyone may not Enable delegation privilege
41. Authenticated Users may not remotely shutdown the system
42. Everyone may not create a token object
43. Deny access to this computer from the network includes Guest
44. Accounts: Limit local account use of blank passwords to console logon only [enabled]
45. Devices: Prevent users from installing printer drivers [enabled]
46. Domain controller: LDAP server signing requirements [require signing]
47. Domain member: Digitally encrypt or sign secure channel data (always) [enabled]
48. Domain member: Require strong (Windows 2000 or later) session key [enabled]
49. Interactive Logon: Do not require CTRL+ALT+DEL [disabled]
50. Interactive logon: Do not display last user name [enabled]
51. Microsoft Network Client: Digitally sign communications (always) [enabled]
52. Microsoft Network Client: Send unencrypted password to connect to third-party SMB servers [disabled]
53. Microsoft Network Server: Digitally sign communications (always) [enabled]
54. Network access: Let everyone permissions apply to anonymous users [disabled]
55. Network access: Do not allow anonymous enumeration of SAM accounts and shares [enabled]
56. Network access: Do not allow anonymous enumeration Of SAM accounts [enabled]
57. Network access: Restrict anonymous access to Named Pipes and Shares [enabled]
58. Network access: Shares that can be accessed anonymously [None]
59. Network security: Do not store LAN Manager hash value on next password change [enabled]
60. Network security: LAN Manager authentication level [Send NTLMv2 response only. Refuse LM & NTLM]
61. Network security: Allow LocalSystem NULL session fallback [disabled]
62. Recovery Console: Allow automatic administrative logon [disabled]
63. Shutdown: Allow shutdown without having to log on [disabled]
64. Shutdown: Clear virtual memory pagefile [enabled]
65. User Account Control: Admin Approval Mode for the Built-in Administrator account [enabled]
66. User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop [disabled]

67. User Account Control: Only elevate UIAccess applications that are installed in secure locations [enabled]
68. User Account Control: Switch to the secure desktop when prompting for elevation [enabled]

Defensive Countermeasures:

69. Firewall protection has been enabled
70. Antivirus protection has been enabled
71. BitLocker drive encryption service is running

Uncategorized operating system settings:

72. Remote Desktop Sharing is turned off
73. Remote Assistance connections have been disabled
74. Desktop gadgets have been completely disabled [Outdated- Windows 7]
75. C sharing is disabled
76. Hidden share *exsharename* is disabled
77. DEP enabled for all programs and services
78. Enumerate administrator accounts on elevation [disabled]
79. Screen saver is password protected
80. Screen saver is password protected [all users]
81. AutoRun commands have been disabled [all users]
82. Autoplay has been disabled [all users]
83. Randomize memory allocations setting enabled
84. Data-only memory pages have code execution prevention enabled
85. Everyone is no longer allowed to write to C:\Share

Service Auditing:

86. DNS Server service has been stopped and disabled
87. FTP service has been stopped and disabled
88. Microsoft FTP service has stopped and disabled
89. LPD service has been stopped and disabled
90. Net. TCP Port Sharing service has been stopped and disabled
91. RIP Listener service has been stopped and disabled
92. RPC Locator service has been stopped and disabled
93. Remote Access Connection Manager service has been stopped and disabled
94. Remote Registry service has been stopped and disabled
95. Simple Mail Transfer Protocol (SMTP) service has been stopped and disabled
96. SNMP service has been stopped and disabled
97. SNMP Trap service has been stopped and disabled
98. SSDP Discovery service has been stopped and disabled
99. Simple TCP/IP service has been stopped and disabled
100. Telephony service has been stopped and disabled
101. Telnet service has been stopped and disabled

102. UPnP Device Host service has been stopped and disabled
103. WebClient service has been stopped and disabled
104. World Wide Web Publishing Service has been stopped and disabled
105. Xbox Live Auth Manager has been stopped and disabled
106. Xbox Live Game Save service has been stopped and disabled
107. Windows Update service is enabled
108. Event Log service is enabled
109. Adobe Acrobat Update service is enabled
110. Windows Firewall service is enabled

Operating System Updates:

111. Windows automatically checks for updates
112. Give me updates for other Microsoft products when I update Windows
113. The majority of Windows updates are installed

Application Updates:

114. Acrobat Reader DC has been updated
115. FileZilla has been updated
116. FileZilla Client has been updated
117. Firefox has been updated
118. Geany has been updated
119. Gimp has been updated
120. IrfanView has been updated
121. Java JRE 8 has been updated
122. Krita has been updated
123. LibreOffice has been updated
124. MobaXterm has been updated
125. Notepad++ has been updated
126. PeaZip has been updated
127. PHP has been updated
128. Powershell has been updated
129. PuTTY has been updated
130. Thunderbird has been updated
131. TortoiseHG has been updated
132. Visual Studio Code has been updated
133. VLC has been updated
134. Firefox automatically updates

Prohibited Files:

135. Removed prohibited MP3 files
136. Removed prohibited MP4 files
137. Removed prohibited OGG files
138. Removed shodan queries archive

139. Removed Brutus password cracker archive
140. Removed Cain and Abel software archive
141. Removed Hashcat password cracker archive
142. Removed Nikto scanning software archive
143. Removed plain text file with passwords
144. Removed PHP Backdoor
145. Removed file containing confidential customer information

Prohibited Software:

146. Removed Abyss Web Server
147. Removed Adaware WebCompanion
148. Removed Advanced Port Scanner
149. Removed Angry Ip scanner
150. Removed AnyDesk
151. Removed Arcade Lines
152. Removed Avernum
153. Removed Beware IRC server
154. Removed BitComet
155. Removed BitTornado
156. Removed BoomBox Radio Player
157. Removed Chicken Invaders
158. Removed CleanMyPC
159. Removed Driver Support
160. Removed Epic Games Launcher
161. Removed Firefox addon Video DownloadHelper
162. Removed HTTP Explorer
163. Removed Hashcat
164. Removed Home Web Server
165. Removed Itunes
166. Removed John the Ripper
167. Removed K-Lite Codec Pack
168. Removed KNCTR
169. Removed Kodi
170. Removed MyCleanPC PC Optimizer
171. Removed Nmap
172. Removed Open TFTP Server
173. Removed Ophcrack
174. Removed Plex Media Server
175. Removed Progress Telerik Fiddler Web Debugger
176. Removed Radmin server
177. Removed Reimage Repair

178. Removed SuperScan
179. Removed TeamViewer
180. Removed Tetris
181. Removed TightVNC Server
182. Removed Tiny Web Server
183. Removed Tonido Server
184. Removed uTorrent
185. Removed Vistumbler
186. Removed WebDiscover browser
187. Removed Wireshark
188. Removed Zed attack proxy

Malware:

189. Scheduled task “Bad_Task” Removed
190. Removed netcat backdoor
191. Removed tini backdoor
192. Remove ntbindshell backdoor
193. Removed TX backdoor
194. Removed NetBus Pro
195. Removed Sticky Keys backdoor
196. Removed Custom backdoor
197. Removed Actual Keylogger
198. Removed Keylogger
199. Removed Spyrix Keylogger
200. Removed Reveal Keylogger
201. Removed WinUserProfileManager

Application Security Settings

202. Internet Explorer has been installed
203. Internet Explorer SmartScreen Filter
204. Windows SmartScreen configured to warn or block
205. Internet Explorer Enhanced Security Configuration is enabled
206. Internet Explorer Phishing filter is enabled
207. Internet Explorer 8+ Smart Screen Filter [enabled]
208. Internet Properties: Enable Enhanced Protected Mode [Enabled]
209. Internet Zone: Initialize and script ActiveX controls not marked as safe for scripting [disabled]
210. Firefox pop-up blocker enabled
211. Firefox blocks dangerous downloads
212. Firefox warns when sites try to install add-ons
213. Firefox displays warning on known malware sites
214. Firefox display warning on known malware sites [all users]

215. Firefox HTTPS-Only mode enabled for all windows
216. PHP log errors have been enabled
217. PHP system function is disabled
218. Require RPC communication
219. RDP network level authentication enabled
220. RDP connection encryption level has been set to high
221. RDP TLS Communication enabled
222. RDP PNP Redirect Disabled
223. Do not allow drive redirection
224. Do not allow supported Plug and Play device redirection
225. SMB 1.x removed or disabled
226. IIS default website directory browsing disabled
227. IIS detailed error messages disabled
228. DNS zone transfers to any server is disabled
229. Dynamic updated to the DNS server are disabled

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. Changed insecure password for [user]
12. Created user group [group]
13. Created user account [user]
14. Users added to group [group]
15. User [user] cannot login without a password
16. [User] password expires
17. Root password is no longer blank / Changed insecure Root password
18. User [user] has a maximum password age
19. User [user] has a minimum password age
20. Password for [user] is hashed with a secure algorithm

21. Disabled password login for user [system user]

Account Policies

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

Security Policy:

34. Address space layout randomization enabled
35. IPv4 TCP SYN cookies have been enabled
36. IPv4 TCP SYN,ACK retries reduced
37. IPv4 TIME-WAIT assassination protection enabled
38. IPv4 forwarding has been disabled
39. IPv4 sending ICMP redirects disabled
40. IPv4 accept ICMP redirects disabled
41. IPv4 accept source routing disabled
42. IPv4 source route verification enabled
43. Ignore bogus ICMP errors enabled
44. Ignore broadcast ICMP echo requests enabled
45. Kernel pointers hidden from unprivileged users
46. Magic SysRq key disabled
47. Only root may create new namespaces
48. Restrict unprivileged access to kernel syslog enabled
49. Logging of martian packets enabled
50. Sudo requires authentication
51. Group [group] does not have sudo privileges

Defensive Countermeasures:

52. Uncomplicated Firewall (UFW) protection has been enabled

Uncategorized operating system settings:

53. GRUB configuration is not world readable
54. GRUB uses encrypted password protection
55. Insecure permissions on shadow file fixed
56. Resolver checks for IP spoofing

57. Stricter defaults have been enabled for shared memory
58. Stricter defaults have been enabled for temporary storage
59. Process information hidden from other users
60. Xserver TCP Connections disabled

Service Auditing:

61. Apache2 service has been disabled or removed
62. Bind9 service is stopped and removed
63. DNS service is disabled or removed
64. FTP service has been disabled or removed
65. IRC daemon has been stopped and disabled
66. Minetest service has been disabled or removed
67. Nginx service has been disabled or removed
68. Nfs services is stopped and removed
69. OpenArena service has been disabled or removed
70. POP3 service has been disabled or removed
71. Postgresql has been disabled or removed
72. Rsync service has been disabled or removed
73. Samba service has been disabled or removed
74. SMTP service has been disabled or removed
75. SNMP service has been disabled or removed
76. Squid proxy service has been disabled or removed
77. WorldForge service has been disabled or removed

Operating System Updates:

78. The system automatically checks for updates daily
79. Install updates from important security updates
80. Linux kernel has been updated
81. Bash has been updated
82. BusyBox has been updated
83. OpenSSL shared libraries have been updated
84. Glibc has been updated
85. Debian has valid lists

Application Updates:

86. 7zip has been updated
87. Apache2 has been updated
88. Bluefish has been updated
89. DNS (bind9) has been updated
90. FileZilla has been updated
91. Firefox has been updated
92. Iceweasel has been updated to firefox-esr
93. LibreOffice has been updated

94. Nginx has been updated
95. OpenSSH has been updated
96. PHP has been updated
97. PHP5 has been updated
98. Pro FTP daemon has been updated
99. Pure FTP has been updated
100. Samba has been updated
101. Thunderbird has been updated
102. WordPress has been updated

Prohibited Files:

103. Prohibited MP3 files are removed
104. Removed plaintext file containing passwords
105. Removed file containing password hash
106. Removed PHP backdoor
107. Removed phpinfo() php file

Prohibited Software:

108. Stellarium has been installed
109. Removed prohibited software Angry IP Scanner
110. Removed prohibited software Arp-scan
111. Removed prohibited software Deluge
112. Removed prohibited software Dsniff
113. Removed prohibited software Endless Sky
114. Removed prohibited software Ettercap
115. Removed prohibited software Freeciv
116. Removed prohibited software Hunt
117. Removed prohibited software Hydra
118. Removed prohibited software John the ripper
119. Removed prohibited software Kismet
120. Removed prohibited software Knocker
121. Removed prohibited software Minetest
122. Removed prohibited software NBTScan
123. Removed prohibited software Nmap and Zenmap
124. Removed prohibited software OpenRa
125. Removed prohibited software Ophcrack
126. Removed prohibited software P0f
127. Removed prohibited software TCPSpray
128. Removed prohibited software Wireshark
129. Removed prohibited software Xprobe
130. Removed prohibited software Yersinia

Malware:

131. Removed python backdoor
132. Removed perl backdoor
133. Removed perl bindshell backdoor
134. Removed netcat backdoor
135. SUID backdoor removed

Application Security Settings

136. SSH root login has been disabled
137. SSH protocol 1 has been disabled
138. SSH only listens on port 222(situational)
139. SSH allows only public key authentication
140. SSH does not permit empty passwords
141. SSH user environment processing is disabled
142. Anonymous Samba access is disabled
143. Unauthorized Samba share is disabled
144. Samba blank passwords are disabled
145. Samba SMB1 protocol is disabled
146. SMB share is not world writeable
147. Encrypt smb traffic is enabled
148. ntlm authentication is disabled
149. FTP local users must log in as anonymous
150. FTP anonymous write commands are disabled
151. FTP PASV security checks enabled
152. FTP anonymous user is not root
153. FTP anonymous access is disabled
154. FTP Server identity is off
155. Insecure permissions on FTP root directory fixed
156. FTP plain-text authentication disabled
157. FTP service is not running as root
158. MySQL remote access is disabled
159. SQL is not ran as root
160. Removed phpinfo() php file
161. PHP expose is Off
162. PHP system function is disabled
163. PHP URL-aware fopen wrappers are disabled
164. PHP secure sessions are enabled
165. PHP does not display errors
166. Apache server signature is disabled
167. Apache trace requests disabled
168. Apache etags disabled
169. Apache server tokens set to least

170. Firefox pop-up blocker enabled
171. Firefox displays warning on known malware sites
172. Firefox warns when sites try to install add-ons
173. Firefox block dangerous and deceptive content
174. Inline scripts not allowed by nginx content security policy
175. Nginx set to block XSS attacks for legacy browsers
176. Nginx server tokens disabled