WINDOWS OFFICIAL CHECKLIST

\*top secret information\*

Team Number: 15-1881

Team Name: Charlie's Angels

Team Unique ID: 335G-N8DC-PRV2

2022-2023 year

*Checklist*

1. **UP RAM**
2. **Check and snip scenario**
3. **Forensics Questions**
4. **Baseline**
5. **User Configuration**
6. **Services**
7. **Firefox**
8. **Uninstall suspicious programs**
9. **Delete Non-Work Files**
10. **System and Security**
11. **Computer Management**
12. **IIS**
13. **Windows Features**
14. **Malwarebytes**
15. **Benchmarks**
16. **Internet Explorer**
17. **IIS Benchmark**

**Baseline**

**netstat -anob > name.txt**

***User Configuration***

**-type in search lusrmgr.msc**

**-Double click on Local users and groups**

**-Go to users folder**

**-Give a password to all users**

**-Disable guest and any unauthorized users**

**-Make sure the admins are in the admins group and the users are in the users group**

**-Create backup admin**

***Services***

**-Type services into search**

**-List of bad services to disable**

* FTP (Port 21)
* Telnet (Port 3389 or 23)
* Desktop group
* LPD
* Webclinet
* FIP
* Remote Registry (Port 445)
* RDP (Port 3389)
* IIS
* SSDP Discovery -Simple Service Discovery Protocol (1900) advertises networks that have plug and play
* Telephony
* Plug and play (if you insert a flash drive, it runs it automatically)
* Geolocation
* Fax
* IP Helper
* Net TCP Port Sharing
* Netlogon (authenticates users in domain)
* Phone Service
* Remote Desktop service (scenario based)- RDP is Port 3389
* Secondary logon- enables admin to login into a non admin account
* SNMP Trap- grabs IP’s and allows remote devices to send messages to admin
* TCP/ IP NetBios Helper port 137 – enables users to share files and print and access/ logon the network
* Print Spooler
* Smart Card- force you to have a key to login
* Simple TCP/ IP Services (Echo- (Port 7), Daytime (Port 13), QOTD (Port 17), Character Generator (Port 19), and Discard (Port 9))
* World Wide Web Publishing Service- used for IIS
* Remote access connection manager
* Infrared Monitor Service (not built into windows)

Infrared **-List of good services to enable**

* DNS (Port 53, URL Name to Number, loopback (127.0.0.1, hosts file (path is Windows\System 32\ Drivers\ etc)
* DHCP (Port 67 (server) and 68 (client), gives out Ips, ipconfig /all to show IP address, static or dynamic)
* BITS (updates won’t work if this is off)
* WIN UPDATE
* WMI
* Windows Event Log (stores the data from windows event collector)
* CCS Client (Helps scoring on Image)
* Windows Defender Advanced Threat Protection
* Windows Defender Antivirus Network
* Windows Defender Firewall (reject, inspect)
* Windows Event Collector (acts as an agent, gathers data)
* Windows Search
* Windows Firewall
* Windows Installer
* Windows Time (NTP Port 123)
* Windows Modules Installer
* Diagnostic Policy Service
* Diagnostic Execution Service
* Diagnostic Service Host
* IPSec Policy agent(port 500, builds tunnels and encrypts traffic,

***Firefox Settings***

**-Download or update firefox**

**-Top right corner> three dots> options**

**- Automatic updates**

**-Check block pop up windows**

**-Check warn websites try to install add ons**

**-Check prevent accessibility**

**-Check block dangerous content**

***S3@shell***

**Uninstall Suspicious Programs**

**-Type control panel in search> Programs> Uninstall a Program**

**-Uninstall any suspicious programs- some include the following (unless told to keep in scenario)**

**-Wire Shark**

**-CCleaner**

**-Look through file explorer for any files that the scenario says not to have or hacking tools and delete them**

***Delete Non-work-related Files***

**-Search file explorer> local disks> users**

**-Go to view and check show hidden**

**-Go through all user’s folders**

**-To quick search these file types:**

**-\*.jpg**

**-\*.gif**

**-\*.mp3**

**-\*.mp4**

**-\*.mov**

**-\*.png**

**-\*.avi**

**-\*.wav**

**-\*.rip**

**-\*.bat**

**-\*.ps**

**-\*.aspx**

**-\*cda**

**-\*.exe**

**-\*.htm**

**-\*.mpeg**

**-\*.pdf**

**-\*.jpeg**

**-\*.bmp**

**-\*.eps**

**-\*.ps1**

**-\*.rtf**

**-\*.txt**

**-\*.vbs**

**-\*.gz**

**-\*.tar**

**-\*.rar**

**-\*.sys**

**-\*.msi**

**-\*.html**

**-\*.c**

***Secpol.msc***

**-Type in search secpol.msc**

**-Change password policies to settings shown below:**

**-Passwords remembered: 5**

**-Max password age: 90**

**-Min password age: 30**

**-Min password length: 14**

**-Password must meet complexity requirements: enable**

**-Store password using reversible condition: disable**

**-Change account lockout settings shown below:**

**-Account lockout duration: 30 minutes**

**-Account lockout threshold: 5 invalid logout attempts**

**-Secpol is broken?**

**Audit logon**

**-Use this link:** [**https://winaero.com/reset-local-security-policy-settings-all-at-once-in-windows-10/**](https://winaero.com/reset-local-security-policy-settings-all-at-once-in-windows-10/)

**System and Security**

**-Type in search control panel> system and security**

**-Security and Maintenance**

**-Change user account control settings to always notify**

**-Read any of the notifications that pop up here**

**-Windows Firewall**

**-Turn firewall on (use recommended settings)**

**-System Settings> remote settings> remote tabs**

**-Disable remote assistance**

**Computer Management**

**-Type in search computer management**

**-Turn on these services if the internet is not working**

**-DNS**

**-DHCP**

**-The only shares that should be in the shared folder**

**($ means hidden):**

**-C$**

**-IPC$**

**-ADMIN$**

**-Task Scheduler**

**-Look at task library for any tasks that start bad programs or could be bad**

**-Check hidden tasks**

**Windows Features**

**-Type in search windows features**

**-Depends on scenario but things to turn off:**

**-Internet Information Services**

**-Print and Document Services**

**-Turn off this definitely:**

**-SMB 1.0**

**-Telnet client**

**-TFTP client**

**IIS**

**127.0.0.1 in browser**

**Benchmarks**

**-Link to benchmarks:**

<https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf>

<file:///C:/Users/arsachs2024/Downloads/CIS_Microsoft_Windows_10_Stand-alone_Benchmark_v1.0.1.pdf>

<file:///C:/Users/arsachs2024/Downloads/CIS_Microsoft_Windows_10_Enterprise_Release_21H1_Benchmark_v1.11.0_1%20(3).pdf>

<https://www.hardenwindows10forsecurity.com/Configuration%20Pack%20for%20Windows%2010%20Pro%20Domain%20Joined.html>

**Internet Properties**

**-type in Internet Properties**

**-Security**

**-check protected mode**

**-Internet medium high/protected mode**

**Local internet> medium low**

**Trusted sites>medium**

**Restricted sites> high/protected mode**

**Check trusted and restricted sites**

**-Privacy**

**-Check turn on pop up blocker**

**-Check in private**

**-Check location**

**-Advanced**

**-check block**

**-Advanced**

**-Multimedia**

**-Uncheck all except the first two boxes**

**-Security**

**-Anything that says allow uncheck**

**-Anything that says block check**

**-Anything that says check check**

**-Turn on protected mode**

**-Integrated windows authentication**

**-check smart screen filter**

**-check most updated ssl and tsl options**

**-check the last three warn options**

**REGISTRY:**

**RUN KEY**

**Other points**

**Enable of booting known bad drivers- disable**

[**file:///C:/Users/arsachs2024/Downloads/CIS\_Microsoft\_W indows\_10\_Enterprise\_Benchmark\_v2.0.0.pdf**](file:///C:/Users/arsachs2024/Downloads/CIS_Microsoft_Windows_10_Enterprise_Benchmark_v2.0.0.pdf)

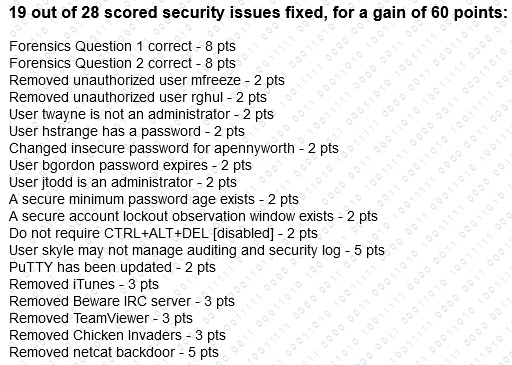
**NOTES FROM OTHERS:**

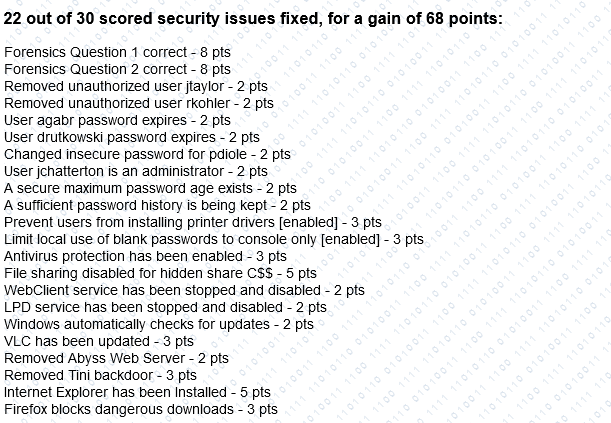
[**https://docs.google.com/document/d/1H8xP2mBr7Ioo8C-afGjBjCnUaKJ3z-4YHw6s\_v2vS\_E/edit**](https://docs.google.com/document/d/1H8xP2mBr7Ioo8C-afGjBjCnUaKJ3z-4YHw6s_v2vS_E/edit)

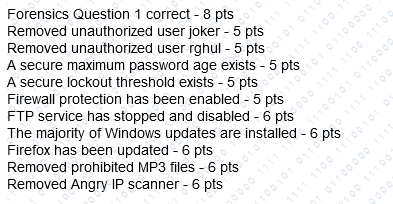
[**https://docs.google.com/document/d/1Qhwc76qSXC\_6OEHzhWtrpekgQjEWQcKyfZPW5b\_GfA8/edit**](https://docs.google.com/document/d/1Qhwc76qSXC_6OEHzhWtrpekgQjEWQcKyfZPW5b_GfA8/edit)

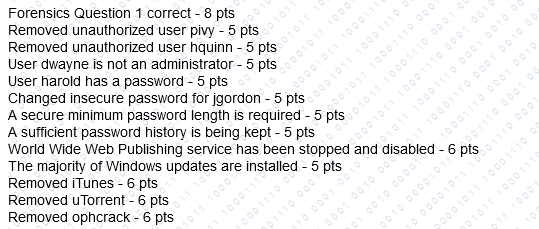
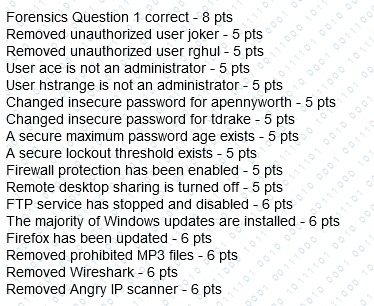
[**https://docs.google.com/document/d/1oEUz9Wl-5P24F01PZXC7z82833X5QMcd/edit**](https://docs.google.com/document/d/1oEUz9Wl-5P24F01PZXC7z82833X5QMcd/edit)

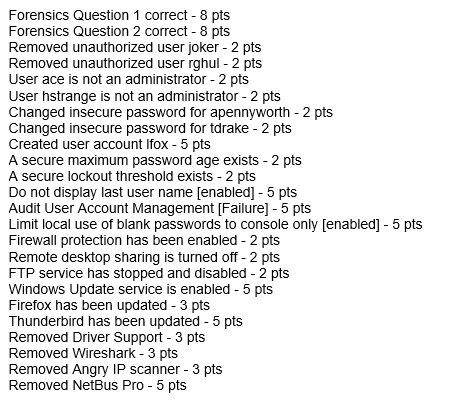
Scores to Reference



****

****

** **

** **

**-Event Log service is running**

