**Team TJXV** CyberPatriot Checklist

All data organized and compiled by the TJXV Team

**Brian Ho, Raymond Fu, Adam Alami, Justin Kim**

# 

# 

# Key Resources

<https://github.com/ponkio/CyberPatriot>  **(ALL systems, checklist + script)**

[Securing Windows (Youtube)](https://www.youtube.com/watch?v=tZI_dfxEM8E) **(WINDOWS, hardening walkthrough)**

[Securing Ubuntu (Youtube)](https://www.youtube.com/watch?v=JVxkTqLoyGY) **(UBUNTU, hardening walkthrough)**

[**https://activities.tjhsst.edu/cyberpatriot/lectures.html**](https://activities.tjhsst.edu/cyberpatriot/lectures.html) **(TJ Site, navigate to 2022 lectures or resources)**

# Windows

1. Read me
2. Start updates
3. Forensics
4. Users
5. Control panel/settings
6. Services/windows features
7. LGFG (?)
8. Remove media files (use everything voidtools)
9. Uninstall software/malware
10. Service configuration
    1. (smb), disable v1 even if its critical service
    2. Remote desktop
       1. Control panel

## Checklists

* CIS benchmarks

## Past Vulnerabilites

### **Round 2 2021 Vulnerabilities** (Notes)

* 3 forensics (21 pts)
* Guest account (remove)
* Remove unauthorized users
* Removing unauthorized administrators
* 2 pt values - Passwords(setting secure pass to all users)
* Configure all passwords to expire
* Configuring account policies (min age, max days, length, complexity req, acc lockout, etc.)
* Audit policy
* Sys harden pdf, download import security policy
* Remote desktop sharing
* Installing updates, need to restart twice
* Uninstall unnecessary programs
* Update GNU cache
* Prohibited mp3 files (\*.mp3 search)
* Remove backdoor from forensics (NARC.exe)
* No points from firefox + 7-zip updates
* Block dangerous downloads on firefox
* Black Viper - Complete checklist of what services on a normal windows PC
* Windows SmartScreen configure to block dangerous apps
* DIsable autoplay
* App + Browser controls -> Exploit Protection - turn on Validate keep integrity
* Windows defender does not exclude file extensions

### Round 2 Vulnerabilities (Found online)

* Disable Guest Account (if possible, only score through GPO)
* User Deleted sasuke
* User Deleted ryugi
* User has insecure password (taiga)
* Created new user (jeff)
* Turn on UAC
  + 6 TOTAL FOR USERS
* Updates for other microsoft products ENABLED
* Autoplay COMPLETELY Disabled (GPEDIT)
* Limit local use of blank passwords to local console ENABLED
* Do not require CTRLALTDEL: DISABLED
* Clear virtual memory pagefile: ENABLED
* Smartscreen enabled
* Disable remote
* RDP network level authentication enabled (GPEDIT)
* Check apps and files ON (Smartscreen)
  + 9 TOTAL FOR "LSP"
* Routing and Remote Access Disabled
* Net. Tcp port sharing Disabled
* DHCP turned ON (turn it off so they don’t get internet) hehexd
* Firewall service on
* Firewall turned on
  + 5 TOTAL FOR SERVICES
* Program removed (CCLEANER)
* Program removed (CHROMIUM)
* Program removed (OPHCRACK (in program files > Windows PC))
* REMOVED BABYLON
* Removed converter search bar
* Removed slimcleaner
* Removed DriverUpdate
  + 7 TOTAL FOR PROGRAMS/VIRUSES
* Update Mozilla Firefox
* Update Notepad++
  + 2 TOTAL FOR UPDATES
* Removed hidden text file in Program Files called CREDITCARD.TXT
* ANSWERS TO FORENSICS:
* 1. hoho
* 2. MYNAMEISJEFF (decoded using onetimepad)
* 3. There was no correct answer for this one; checksums were different for each computer,
  + the important thing was that they used the certutil -hashfile command
* 4. 10.0.0.0, 172.16.0.0, 192.168.0.0
* Made by Brandon Shin and Silas Shen

### Round 1 2022 Vulnerabilities

* Forensics 1
* Forensics 2
* Unauthorized user
* Unauthorized user
* Unauthorized admin
* Create password
* Create user esinclair (readme)
* Create group dragonfire (readme)
* Add users to dragonfire (readme)
* Set secure maximum password age and lockout threshold
* Group policy (limit local use of blank passwords to console only)
* Do not allow anonymous enumeration of SAM accounts (sis benchmarks)
* Firewall protection has been enabled
* Remote assistance connections have been disabled
* FTP service has been stopped or disabled (Start -> turn windows features on or off -> deselect ftp in control panel)
* Update machine
* Update tiled
* Remove wireshark
* Remove netstumbler
* Remove PCCleaner

# Windows Server

## Checklists

## Past Vulnerabilities

### Round 2 2021 Vulnerabilities (Notes)

* Unauthorized users
* Unauthorized admins
* Set pass for a user, change insecure pass
* Make sure all passwords expire
* Local security policy
* Enable firewall
* Install windows updates, around 2 restarts
* 3 programs to be removed
* Plain textfile with passwords (REmove)
* Update 7-zip
* Configure firefox
* Advanced auditing
* Printer drivers (prevent users from installing)
* Disabling a service (LPD) - following black viper
* Disable remote connections to printer (print spooler archive)

### Round 1 2022 Vulnerabilities

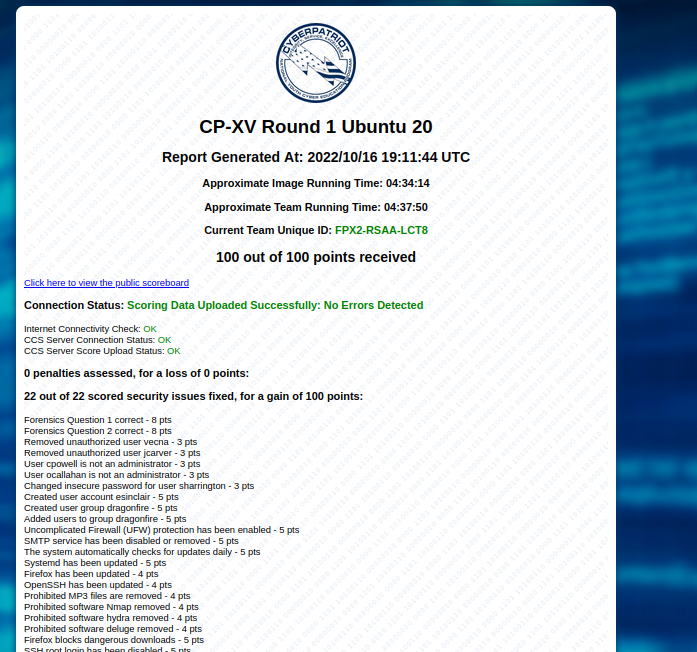
* Forensics Question 1
* Forensics Question 2
* Removed unauthorized user jsullivan
* Removed unauthorized user grigori
* User mbrenner is not an administrator
* User sowens is not an administrator
* Changed insecure password for sharrington
* A secure minimum password length is required
* A sufficient password history is being kept
* Do not require CTRL+ALT+DEL [disabled]
* Do not display last user name [enabled]
* Remote desktop sharing is turned off
* File sharing disabled for C drive
* SNMP Trap service has been stopped and disabled
* Inkscape has been updated
* Gimp has been updated
* Remove prohibited MP3 files
* Removed L0phtCrack
* Removed JDownloader
* Removed Hola VPN
* Removed Web Companion
* Firefox pop-up blocker enabled

# Ubuntu

## Checklists

## Past Vulnerabilities

### Ubuntu Rd 1 2022 Vulnerabilities



Critical Service: Open SSH

Add user sinclair and add user group dragonfire

Image completed by Brian Ho

### Ubuntu Rd 2 2021 Vulnerabilities (Notes)

* Configuring Users
* Cat /etc/passwd |grep
* 4 digit UID = user
* Sudo cat/etc/group/oc/ grep “sudo” /etc/group
* 2 admins to be demoted
* Insecure password
* Add sha512 in common-password pam.unix.so
* Login.defs max pass (99, 10, 7)
* /etc/sudoers.tmp remove & Users ALL = ALL
* Sudo ufw enable
* Opensmtpd sudo opensmtpd stop
* Sudo netstat -tupan
* Sudo -kill -a (processID)
* Sudo px aux | grep (processID)
* Check for automatic updates
* Modify sources.list file /etc/apt
* Sudo gedit sources.lst
* Sources.list from blank ubuntu machine, copy and paste
* Apt get update + upgrade
* Dpkg –getselections
* /var/log/apt (can see which packages cyberpatriot installed)
* Golden eye, pixel dungeon, the mole, 2 more
* Snap list
* Google programs you dont know (OpenVPN security hardening)
* Firefox - Enable pop up blocker

# Cisco

## Resources

### Packet Tracer Rd 1 and 2 Lecture 2022 (TJ)

STP - link management protocol that provides path redundancy while preventing undesirable loops in the network

* Enabling STP
  + Switch (config): spanning-tree vlan 10
    - Enables STP on specific VLAN
  + Setting priority and root
    - Switch (config): spanning-tree vlan 10 root primary
      * Sets switch as root - automatically calculates priority to do so
    - Switch(config)# spanning-tree vlan 20 root secondary
      * Sets switch as secondary root switch with a priority of 28672
    - Switch(config)# exit
    - Switch#: sh spanning-tree
      * View configurations
    - Switch(config)#spanning-tree vlan 20 priority 4096
      * Manually assign a priority - default is 32768, so any lower will set to root
  + Additional Configurations
    - Switch (config): spanning-tree mode pvst
      * To configure the STP protocol to run on the switch, enter the following:
        + pvst
        + rapid-pvst
        + stp — Classic STP provides a single path between any two endpoints, eliminating and preventing networking loops.
        + rstp — RSTP detects network topologies to provide faster convergence of the spanning tree. This option is enabled by default.
        + mst — MSTP is based on RSTP. It detects Layer 2 loops, and attempts to mitigate them by preventing the involved port from transmitting traffic.
    - Switch (config): spanning-tree vlan 10 hello-time 4
      * Sets the hello-time - default is 2 seconds
    - Switch (config): spanning-tree vlan 10 max-age 25
      * Sets max-age - default is 20 seconds
    - Switch (config): spanning-tree vlan 10 forward-time 20
      * Sets forward time - default is 15 seconds
  + Check configurations
    - Switch#: sh spanning-tree

**OSPF**

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria.

**Router 1 Configuration Commands**

R1>en

R1#config t

R1(config)#router ospf 10

* Assign process ID (config)
* Often times 1

R1(config-router)#router-id 1.1.1.1

* Assign router ID

R1(config-router)#network 172.16.1.0 0.0.0.255 area 0

* Assign network address / network statements for EACH interface (config-router)
* network <**NETWORK**-address> <WILDCARD-BITS> area <#>
  + Area # usually 0 if not specified
  + <https://www.cloudaccess.net/cloud-control-panel-ccp/157-dns-management/322-subnet-masks-reference-table.html>
  + <http://jodies.de/ipcalc?host=172.31.0.0&mask1=23&mask2=>
* If wildcard mask:
  + network <**NETWORK**-address> <WILDCARD-mask> area <#>

R1(config-router)#network 192.168.10.4 0.0.0.3 area 0

R1(config-router)#network 172.16.3.0 0.0.0.3 area 0

R1(config-router)#passive-int g0/0

* LAN interface set to passive
* Interface: on topology, see interface connecting **router** to **switch**

**Router 2 Configuration Commands**

R2>en R2

R2#conf t

R2(config)#router ospf 10

R2(config-router)#router-id 2.2.2.2

R2(config-router)#network 172.16.2.0 0.0.0.255 area 0

R2(config-router)#network 172.16.3.0 0.0.0.3 area 0

00:13:00: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

R2(config-router)#network 192.168.10.8 0.0.0.3 area 0

R2(config-router)#passive-int g0/0

**Router 3 Configuration Commands**

R3>en

R3#conf t

R3(config)#router ospf 10

R3(config-router)#router-id 3.3.3.3

R3(config-router)#network 192.168.10.4 0.0.0.3 area 0

R3(config-router)#network 192.168.1.0 0.0.0.3 area 0

R3(config-router)#network 192.168.10.8 0.0.0.3 area 0

R3(config-router)#passive-int g0/0

R3(config)#int g0/0

R3(config-if)#ip ospf hello-interval 5

* Set Hello and dead Interval for interface
* Default hello: 10

R3(config-if)#ip ospf dead-interval 20

* Set Hello and dead Interval for interface
* Default dead: 40

R2(config-if)#ip ospf cost 30

* Set cost

**LACP**

Switch(config-if)#int port-channel 1

* **Specifies the port-channel interface to configure**, and enters the interface configuration mode. The range is from 1 to 4096. The. Cisco NX-OS software **automatically creates the channel group if it does not already exist**.

Switch(config-if)#int range fa0/1-2

Switch(config-if-range)#switchport trunk encapsulation dot1

* the switch that the interface should use IEEE 802.1Q encapsulation on the frames when the interface is configured as a trunk

Switch(config-if-range)#channel-group 1 mode active

* **Configures the port in a channel group and sets the mode**
* Associates port channel with channel group
* **You must set all LACP-enabled port-channel interfaces to active or passive. The default mode is on.**

Switch(config-if-range)#int port-channel 2

Switch(config-if)#int range fa0/3-4

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#channel-group 2 mode on

* **DOES NOT set as LACP - Careful w this**

Switch(config-if)#int port-channel 3

Switch(config-if)#int range fa0/5-6

Switch(config-if-range)#no switchport

* **Sets as layer 3 switch**

Switch(config-if-range)#channel-group 3 mode active

Switch# exit

Switch# show etherchannel summary

* Verifies everything is good
* **Notice the ‘-’ where we put ‘on’ instead of active**

### Cisco Round 1 Quiz 2022

### Cisco Round 1 Packet Tracer 2022