VAPatriot ScubaSquad

Version 2

Ryan Kim, Darin Mao, Darius Kianersi, Alex Suh

Goals of Version 2:

- Make it more concise
- Organize it intuitively
- Make finding things easier
- List items in order of importance

When making contributions:

- Turn off smart quotes in Google Docs
- Try to follow the same format
- Critical services are in alphabetical order
- Don't edit the table of contents, click refresh instead

Organization of this document:

- Checklists: broad sequence of tasks, OS-agnostic
- Command Line: helpful things to run
- OS Configuration: OS-specific hardening instructions
- Shortcut Links: links to helpful pages
- Applications, Services, Systems: hardening instructions for services and applications

Table of Contents

Checklists

The first thing you should do for any system is to read the README and Forensics Questions. These procedures are the same for all systems. The goal is to understand how to complete all of these tasks without needing reference.

In the online rounds the goal is to be as fast as possible. More difficult items that would allow attackers to compromise the system can be done later. At finals your goal is to close possible entry points as fast as possible to avoid having services taken down by red team.

Online Rounds

1. Run updates in the background
   Getting these started soon lets you do them faster since the other teams in the building will get updates going if you don't

2. Complete forensics questions
   Do not spend too much time

3. User auditing
   set secure passwords, remove unauthorized users, remove unauthorized group members, lock built-in admin/guest accounts

4. Firewall
   Turn it on, block as much as possible (incoming, outgoing is optional) without blocking critical service ports

5. Illegal files and software
   Find illegal files, set file permissions for important files and folders

6. System hardening
   Refer to hardening instructions for each operating system

7. Remove backdoors and unnecessary services
   Check listening ports, check for bad executables and files in important directories, check scheduled tasks

8. Application security
   Configure required software

9. Service hardening
   Refer to hardening instructions for individual services

10. Miscellaneous hardening

National Finals

1. Firewall
   Turn it on, block as much as possible without blocking critical service ports

2. User auditing
   set secure passwords, remove unauthorized users, remove unauthorized group members, lock built-in admin/guest accounts

3. **Backup data for services**
   Red team may delete some of this, and your services will be scored as down

4. Remove backdoors and unnecessary services
   Check listening ports, check for bad executables and files in important directories, check scheduled tasks

5. System hardening
   Refer to hardening instructions for each operating system

6. Service hardening
   Refer to hardening instructions for individual services

7. Run updates in the background

8. Complete forensics questions
   Do not spend too much time

9. Illegal files and software
   Find illegal files, set file permissions for important files and folders

10. Application security
    Configure required software

11. Miscellaneous hardening

Command Line and Code Reference

All Systems

Logging IP to a file (PHP)

```
<?php file_put_contents("<FILENAME>", $_SERVER["REMOTE_ADDR"]."\n", FILE_APPEND);
?>
```

Linux

Running a script for TCP connections on a port
Can use four environment variables $SOCAT_(PEER|SOCK)(ADDR|PORT)
If these are not needed you may omit pktinfo

```
socat tcp-l:<PORT>,pktinfo,fork,reuseaddr exec:"./script.sh"
```

Blocking a host IP with UFW
Combine this with the command above and replace host with $SOCAT_PEERADDR to auto-firewall connections to a port

```
ufw insert 1 deny from <HOST> to any
```

File perms - you need this everywhere

```
chmod -R <directory> o-w
```

User management

```
for i in $(grep -E ":[0-9]{4}:" /etc/passwd | cut -d : -f1);
do pw=$(cat /dev/urandom | tr -dc 'A-Za-z0-9!@#$%&^*_+<>?=' | head -c 14);
echo -e "$pw\n$pw" | sudo passwd $i && echo -e "\033[0;31m$i: $pw\033[0m";
sudo usermod -s /bin/bash $i;
sudo chage -m 2 -M 30 -I 30 -W 7 $i;
done;
pw=""
```

Print command line of listening processes

```
sudo netstat -tulpn | grep -oE "[0-9]+/" | sort -u | xargs -n1 -I~
sh -c "cat '/proc/~cmdline'; echo"
```

Windows

Loop through users and set password on active directory
MAKE SURE TO SET YOUR OWN PASSWORD IMMEDIATELY AFTER OR YOU WILL GET LOCKED OUT

```
Get-aduser -f * | %{$p="$(get-random)!2Qw"; set-adaccountpassword $_ -reset
-newpassword (convertto-securestring -asplaintext $p -force);echo $_.name$p }
Set-adaccountpassword -identity <your username> -reset
```

for local users do this instead

```
get-localuser | % {$p="$(get-random)!2Qw";set-localuser $_ -password
(convertto-securestring -asplaintext $p -force);echo $_.name$p}
```

Loop through users and ensure their passwords expire (first AD, second local)

```
Get-aduser -f * | set-aduser -passwordneverexpires 0
get-localuser | set-localuser -passwordneverexpires 0
```

Firewall blocking hosts connecting to a TCP port (PowerShell)

```
ncat -knvlp <PORT> 2>&1 | sls -pattern "m ([\d\.]+):" | %
{$ip=$_.matches.groups[1].value;new-netfirewallrule -displayname "Block $ip" -direction in
-action b -remoteaddress $ip;"Blocked $ip";}
```

Operating System Configuration Instructions

This section is included for reference. Ideally, most of this should be done from memory. For the sake of speed, these are listed in order of the National Finals checklist.

Windows

Enable and Configure Firewall

You can use gpedit.msc > Computer Configuration > Windows Settings > Security Settings > Windows Defender Firewall (GUI) or netsh advfirewall (CLI). Please note that for firewall, the GUI may be more efficient for some configurations.

1. Reset the firewall settings to default

```
netsh advfirewall reset
```

2. Enable the firewall for all profiles (Windows Defender Firewall Properties)

```
netsh advfirewall set allprofiles state on
```

3. Block inbound and outbound connections for all profiles (Windows Defender Firewall Properties)

```
netsh advfirewall set allprofiles firewallpolicy blockinboundalways,blockoutbound
```

4. Enable logging, set the log file path and max size as listed below for all profiles (Windows Defender Firewall Properties > Logging)

```
netsh advfirewall set allprofiles logging allowedconnections enable
netsh advfirewall set allprofiles logging droppedconnections enable
netsh advfirewall set allprofiles logging maxfilesize 16384
netsh advfirewall set allprofiles logging filename
%SYSTEMROOT%\System32\LogFiles\Firewall\domainfw.log
```

5. Additional settings (Windows Defender Firewall Properties > Settings)
   Disable remote management, disable unicast response, enable both local firewall rules, disable inbound user notification for all profiles

```
netsh advfirewall set allprofiles settings remotemanagement disable
netsh advfirewall set allprofiles settings unicastresponsetomulticast disable
netsh advfirewall set allprofiles settings localfirewallrules enable
netsh advfirewall set allprofiles settings localconsecrules enable
netsh advfirewall set allprofiles settings inboundusernotification enable
```

6. Disable all rules through GUI, do not use CLI for this

Make sure to allow the necessary ports. Allow 53 (DNS), 80 (HTTP), and 443 (HTTPS). Allow incoming ports for critical services.

User auditing

You can use lusrmgr.msc (GUI) or net user, net localgroup, wmic useraccount (CLI). For AD users, use Active Directory Users and Computers or PowerShell

1. Disable unauthorized users

```
net user [user] /active:no
```

2. Remove unauthorized administrators (check other groups as well)

```
net localgroup administrators [user] /delete
```

3. Set user passwords, set them to expire, and make them change the password
   THIS IS DANGEROUS BECAUSE IT LEAVES PASSWORDS IN HISTORY

```
for /f %G in ('dir /b C:\Users') do (
        net user "%G" CyberPatriot!1
        wmic useraccount where name="%G" set passwordexpires=true
        net user "%G" /logonpasswordchg:yes
)
```

Find and Remove Backdoors

It is a good idea to first enable Windows Defender and run MalwareBytes. Use cports as well. Look for "Listening" processes that do not have a Product Name of Microsoft Windows or a Process Path of System. You may optionally kill every listening process, **although this may break some things**. yeah don't do this one

```
for /f "tokens=5" %G in ('netstat -aon ^| findstr "LISTENING"') do taskkill /f /pid %G
```

Common hiding tactics

- Named similarly to real Windows components (winhelp.exe and winhlp32.exe)
- Named identically but placed in different directories (config\csrss.exe and csrss.exe)
- Hidden in an ADS (usually attached to a real file)
  To find them and delete them, run streams -sd <directory>

National Finals: Once you have removed as many as you can find, **actively monitor connections** with ProcMon or TCPView. If you see one that isn't an SLA check, **stop what you are doing and kill it**, then figure out how it happened.

Remove Unnecessary Services

If you are on Server, use the ServerManager to Remove Roles and Features. If you are on Windows, use optionalfeatures. Disable anything not in use (don’t remove powershell).

System Hardening

These are likely to be scored. Make sure to do ALL of these. Do not get lazy and leave it for later.

Remote Desktop

Turn off Remote Desktop and Remote Assistance through control panel or group policy. Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections > Allow users to connect

Services

Configure services with services.msc. The black viper checklist is good, also make sure good services (Windows Event Log and Windows Update have been scored) are enabled and running.

Services that you can stop:

- Remote anything (If you are running Active Directory, you need remote registry)
- Secondary Logon (seclogon)

You can get some idea of what services are problematic with the sysinternals accesschk tool. Make sure that you don't find any globally writable services. If the commands show anything, stop those services.

```
accesschk -uwcqv "Everyone" *
accesschk -uwcqv "Authenticated Users" *
```

File Permissions

Find globally writeable files and folders by using accesschk

```
accesschk - ws "[Everyone|Users|Authenticated Users]" <Directory>
```

Authenticated Users is a different group than just Users.

File Shares

List file shares with net share and delete them with net share [name] /delete. Make sure they are not required by the README.

Group Policy Items

Open the group policy and check for configured items under Administrative Templates > All Settings. By default these are all undefined, so the defined ones are either set by programs or henry_case.

You can do the following to apply SCT gpos:

Visit bit.ly/vascuba-winsct1 for the SCT gpos. Make sure to also download LGPO while you are at this. Then go into the folder that you just unzipped. Run this command to have the policies take effect:

```
Location\Of\lgpo.exe /g GPOs
```

Security Policy

Configure security policy through group policy according to a reference. For online rounds, use a template! For national finals, do this on the Domain Controller and apply it to an OU containing all the connected computers. I have had issues with firewall blocking forced propagations, so either allow "Dynamic RPC Ports" on the members or just reboot all the systems.

You may find that the security policy is unavailable! This is likely because it has been configured explicitly through a GPO. You can resolve this by resetting the group policy by removing the C:\Windows\System32\GroupPolicy directory. Note that this will remove every configured group policy item, so take notes on what you/henry_case have configured.

Windows Settings tuning

Search for Exploit Protection in the windows search bar and turn all of these to on by default.
Then go to App & Browser control and enable Reputation based protection.
Then go to Device Security -> Core isolation details and enable Memory integrity

Also search for developer settings and make sure that the **use developer features** section is set to Microsoft Store apps. Also check the **powershell** section and ensure that scripts require signing.

Audit Policy

Security policy should theoretically set audit policy. However, you may find that these settings are bad and reset themselves randomly. This is due to Windows being broken and henry_case

putting an audit.csv file in the GroupPolicy folder that Windows for some reason does not overwrite. Refer to the link below for more information.
https://blogs.msdn.microsoft.com/spatdsg/2011/06/06/audit-policy-not-registering-audits/

The solution is to delete this file and set audit policy afterwards.

```
del C:\Windows\System32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv
auditpol /set /category:* /success:enable /failure:enable
```

Antivirus

Enable Windows Defender through Group Policy. Since Defender is bad, install some antivirus software like MalwareBytes or AVG. Do some scans, as these will often find hidden files and executables.

BCDEdit Settings

```
bcdedit /set {current} nointegritychecks off
bcdedit /set {current} nx AlwaysOn
```

The computer needs to be restarted for these settings to take effect

Service Hardening

Look at the guides for every critical service and make them secure!

Configure and Perform Windows Update

Through Group Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Update, configure

- Configure Automatic Updates: enabled and set to 3 or 4
- Any additional settings you think are useful

Complete Forensics Questions

If you don't know how to do these, skip them and come back later. Don't spend too much time.

Find and Remove Illegal Files and Software

Illegal files will usually only be found in the C:\Users directory or a shared directory. Shared directories are in the README and can be found with net share. **Be aware that not all files are in C:\Users.** You should become familiar with the contents of most directories in C:\Windows, as there are often files hidden here too in later rounds

The C:\Users directory is easy enough - simply delete everything and make new folders.
do not do this during national finals

```
cd C:\Users
for /f %G in ('dir /b ^| findstr /v "%USERNAME%"') do (
        takeown /f "%G" /r
        icacls "%G" /grant %USERNAME%:F /t /q
        rd /s /q "%G"
        mkdir "%G"
)
```

This will exclude your own directory so look through that separately.

Search for files by file extension

```
Get-ChildItem -Path <FOLDER> -Filter *.ext -Recurse -ErrorAction SilentlyContinue -Force
```

During online rounds you may want to copy the entire Users directory out of the VM and look through it on the host with software like WinDirStat.

Software is easier. Use appwiz.cpl to remove any software not mentioned in the README. CyberPatriot also likes to hide executables in random directories. Check ProgramData, Program Files, AppData, and anywhere else you can think of. Some things won't uninstall properly; you may have to download and use RevoUninstaller.

Clear Possibly Poisoned Caches

Run the following commands to clear your dns and arp cache

```
Ipconfig /flushdns
Netsh interface ip delete arpcache
```

Securely Configure Required Applications

Look at the guides for every required application and make them secure!

CyberPatriot USB Structure

This is a great way to figure out what is bad and what is good
E:\ (usually)

- **Software**
    - 7zip.exe
    - Acro Reader.exe
    - Malwarebytes installer.exe
    - Notepad++ installer.exe

    - Putty installer.exe
    - Pycharm community.exe
    - Thunderbird installer.exe
    - Vlc installer.exe
    - Filezilla.exe
    - Filezilla Server.exe
    - Firefox.exe
- **Unwanted Software**
    - **Adware**
        - SmartPCFixer installer.exe
    - **Backdoors**
        - Tini.exe
        - Nc.exe
    - Abyss Web Server.exe (abwsx1.exe)
    - Advanced Port Scanner.exe
    - Angry IP Scanner (ipscan-win64.exe)
    - Bittorrent client.exe
    - Chicken Invaders installer.exe
    - iTunes Setup.exe
    - Netbus pro installer (nbpro.exe)
    - Nmap.exe
    - OpenTFTPServer.exe
    - PC Drivers Support.exe (DriverSupport.exe)
    - Revealer Keylogger.exe (rkfree_setup.exe)
    - Tini.exe
    - Utorrent client installer.exe
    - Wireshark installer.exe
    - RetroArch.exe
- **Base Image Builder**
    - Jre-8 installer.exe
    - Old version of firefox installer.exe
    - CCleaner.exe
    - LGPO.exe
- **CCS/<version number>/CCS_Client_Windows**
    - CCleaner.exe
    - CCSClientDebug.exe
    - CCSClient.exe
    - Psexec.exe
    - Sdelete.exe
    - Sox.exe
    - Stop.exe
- **Image Name**
    - Forensics Questions.txt

- **Scripts**
    - psexec.exe
- **Graphics**
- Setup64.exe
- SanDiskSecureAccess.exe
- VmwareToolsUpgrader.exe

Sysinternals Overview

- AccessChk
    - Good for figuring out what files are globally writable and also for figuring out globally writable services
- AccessEnum
    - Good for scanning directories to find world writable files/folders
- AutoRuns
    - View potentially problematic processes that are running in places like the task scheduler
- Procmon
- Streams
    - Monitor Alternate Data Streams that may have contain vulns
    - Syntax: Streams <directory> -s
- TCPView
    - Find listening connections that could indicate a backdoor

Miscellaneous Hardening

These are unlikely to be scored. Do them if you have time AFTER completing everything else.

- Check Task Manager details for suspicious running processes
- Check Task Manager startup items and Task Scheduler for scheduled tasks
- Set UAC to the max
- Check file permissions on important files
- Check files by date to see what cyberpatriot may have modified
- Use the registry scanner for forensics information https://nirsoft.net/utils/regscanner.html, search for registry keys matching "Registry contains any value" in a specific time range
- Read the event viewer
- Clear hosts file
- Sysinternals autoruns

Tips and Tricks

Some tips to get you going when you're stuck.

- If you don't have access to a file or folder, use takeown /f [file] followed by icacls [file] /grant [username]:f
- Sometimes running cmd as Administrator just isn't enough… get Sysinternals psexec and run psexec -i -s cmd.exe to get a shell under NT Authority\System

Linux

Check and clear aliases

```
alias
unalias -a
```

Enable and Configure Firewall

ufw

1. Reset the firewall, and reenable

   ```
   ufw --force reset
   ufw enable
   ```

2. Disable all incoming connections and enable all outgoing

   ```
   ufw default deny incoming
   ufw default allow outgoing
   ```

3. Accept incoming connections for required services. See services for further detail.

   ```
   ufw allow [port num.] # defaults to incoming
   ufw allow out [port num.]
   ```

4. List all rules

   ```
   ufw status
   ```

Optionally, configure the firewall using iptables. Skip this step if you already set up ufw.

iptables

1. Disable the ufw

   ```
   sudo ufw disable
   ```

2. Flush all chains of existing rules, and delete all non-default chains

   ```
   sudo iptables -F
   sudo iptables -X
   ```

3. Accept already established connections

   ```
   sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
   ```

4. Accept icmp requests

   ```
   sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
   ```

5.

6. Accept traffic from loopback interface

```
sudo iptables -A INPUT -i lo -j ACCEPT
```

7. Accept incoming connections for required services. See services for further detail. Ex:

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT // Accepts incoming connections for port 22 (ssh)
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT // Accepts incoming connections for port 80 (http)
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT // Accepts incoming connections for port 443 (https)
```

8. Set the default policy for each chain

```
sudo iptables -P INPUT DROP // drop all incoming connections
sudo iptables -P OUTPUT ACCEPT // accept all outgoing connections
```

9. List all iptable rules

```
sudo iptables -L -n --line-numbers
```

10. Save iptable rules

```
sudo apt-get install iptables-persistent
sudo netfilter-persistent save
```

User Auditing

PAM

Before changing user passwords, it is important to first configure PAM. This is so that if any passwords are not hashed in SHA-512, they will be automatically after configuring pam.

Install cracklib for PAM

```
sudo apt-get install libpam-cracklib
```

Remove any instances of nullok in /etc/pam.d

Consult the guide to configure all PAM files.

Passwords/Shells/Expiry

Enter the following command in one line to change every user's password and configure their shells/password expiry. **Make sure to take careful note of every user's password that is printed to the tty.**

Online rounds:

```
for i in $(grep -E ":[0-9]{4}:" /etc/passwd | cut -d : -f1); do echo -e "CyberPatriot@2\nCyberPatriot@2" | sudo passwd $i; sudo usermod -s /bin/bash $i; sudo chage -m 2 -M 30 -I 30 -W 7 $i; done; pw=""
```

National rounds:

```
for i in $(grep -E ":[0-9]{4}:" /etc/passwd | cut -d : -f1); do pw=$(cat /dev/urandom | tr -dc 'A-Za-z0-9!@#$%&^*_+<>?=' | head -c 14); echo -e "$pw\n$pw" | sudo passwd $i && echo -e "\033[0;31m$i: $pw\033[0m"; sudo usermod -s /bin/bash $i; sudo chage -m 2 -M 30 -I 30 -W 7 $i; done; pw=""
```

Make sure to change the passwords for any service admin accounts (ex. Mysql root, mediawiki admin)

Clear your console history to prevent red team spying.

```
history -c
```

Lock Root

Lock the root account.

```
passwd -l root
```

Unauthorized users/admins

Use the README for the following commands.

a. List users

```
cat /etc/passwd | grep -E ":[0-9]{4}:" | cut -d : -f 1
```

b. Add or remove users

```
userdel -r [user]
useradd -m [username]
```

c. List administrators

```
cat /etc/group | grep sudo
```

d. Add or remove users as administrators

```
adduser [user] adm
adduser [user] sudo

deluser [user] adm
deluser [user] sudo
```

Hidden Users

Remove users that aren't root with a UID of 0. Remove or change the shell of users without a 4 digit UID with a shell that isn't /bin/false, /sbin/nologin, or /bin/sync (hidden users).

```
grep ":0:" /etc/passwd

grep -E ":([0-9]{1,3}|[0-9]{5,}):" /etc/passwd | grep -E -v
"(\/bin\/false|\/sbin\/nologin|\/bin\/sync)"
```

Hidden users may also be found in /etc/lightdm/users.conf. Ignore the defaults "nobody nobody4 noaccess''

Find and Remove Backdoors

1. Print out all listening and established ports and append to a file for possible use in forensic questions.
   ```
   netstat -tupan | tee -a ~/Desktop/ports.txt
   ```
2. Determine the port of a suspicious process from the second column of the output and block the port from the UFW. Ex: 127.0.0.1:53 Port is 53
   ```
   ufw deny out [port]
   ```
3. Also use ps aux to find what is running the process as well as where it may be from
   ```
   ps aux | tee -a ~/Desktop/processes.txt
   ps aux | grep [process name/pid]
   ```
4. Kill the process using its process id found in the 2nd column of ps aux or last of netstat
   ```
   kill -9 [pid]
   ```
5. Remove the source of the program by finding its directory
   ```
   which [program name]
   ```
6. If there is an accompanying package, remove it as well

You can ignore avahi, dhclient, cupsd, and dnsmasq, but everything else should be checked and treated with caution. Make sure NOT to kill your critical services when you are doing this.

Scheduled Tasks

If a backdoor is restoring itself periodically

1. If it restores after you reboot, consider checking /etc/systemd/system/, /etc/init.d/, /etc/rc.local, /home/*/.bashrc, all of which affect startup services
2. Otherwise, consider checking crontabs (/var/spool/cron/crontabs/, /etc/crontab, /etc/cron.*), aliases, or binary files (see tips)

LAMP Backdoors

Make sure to check your website folder (if it applies) at /var/www/html, as well as any other folders for services running on your LAMP stack. If there's something that just runs a php command, it's probably a backdoor. Also make sure your .htaccess file does not expose your website's directory.

Use the following keywords to find common PHP backdoors. Remove (or at least inspect) the file that they are found in (often .php files).

```
grep -E -irl
“(r99|c55|passthru|shell_exec|system|base64_decode|fopen|fclose|eval|phpinfo)”
/var/www/
```

Service Hardening

Look at the guides for every critical service and make them secure!

For **all** services, ensure that their necessary files all have secure permissions.

You can try doing this

```
chmod -R a-xw <folder>
```

System Hardening

Sudoers

Configure the sudoers file with the following command. Consult the guide for the default sudoers configuration.

```
sudo visudo
```

Inspect or delete everything that isn't CCS related in the sudoers.d directory

```
rm -rf /etc/sudoers.d/*
```

gdm3

```
[security]
AllowRoot=false
```

Lightdm

Disable the guest user from /etc/lightdm/lightdm.conf and restart Lightdm in order to apply changes. Also inspect files in /etc/lightdm/lightdm.conf.d/

```
[SeatDefaults]
allow-guest=false
```

Restart lightdm to apply changes

```
service lightdm restart
```

Sysctl

Consult the guide for sysctl to secure.
After configuring, run the following command to apply changes.

```
sysctl -p
```

Grub

Create an encrypted password and set superuser as root. **Be aware that the next time you reboot, you will be prompted to login as "root" with the specified password.**

```
grub-mkpasswd-pbkdf2
```

Using the encrypted password that is generated, append the following *text* to the /etc/grub.d/00_header file.

```
cat <<EOF
set superusers="root"
password_pbkdf2 root <encrypted-password>
EOF
```

Update the grub to save your changes.

```
update-grub
```

AppArmor

```
apt-get install apparmor apparmor-profiles apparmor-utils
service apparmor start
aa-enforce /etc/apparmor.d/*
```

Remove Unnecessary Services

Run the following command to check what services are running.

```
service --status-all
```

Default output on Ubuntu 16.04:

```
[ + ]  acpid
[ - ]  alsa-utils
[ - ]  anacron
[ + ]  apparmor
[ + ]  apport
[ + ]  avahi-daemon
[ - ]  bootmisc.sh
[ - ]  brltty
[ - ]  checkfs.sh
[ - ]  checkroot-bootclean.sh
[ - ]  checkroot.sh
[ + ]  console-setup
[ + ]  cron
[ + ]  dbus
[ - ]  dns-clean
[ + ]  grub-common
[ - ]  hostname.sh
[ - ]  hwclock.sh
[ + ]  irqbalance
[ - ]  kerneloops
[ - ]  killprocs
[ + ]  kmod
[ + ]  lightdm
[ - ]  mountall-bootclean.sh
[ - ]  mountall.sh
[ - ]  mountdevsubfs.sh
[ - ]  mountkernfs.sh
[ - ]  mountnfs-bootclean.sh
[ - ]  mountnfs.sh
[ + ]  network-manager
[ + ]  networking
[ + ]  ondemand
[ - ]  plymouth
[ - ]  plymouth-log
[ - ]  pppd-dns
[ - ]  procps
[ + ]  rc.local
[ + ]  resolvconf
[ - ]  rsync
```

```
[+] rsyslog
[-] saned
[-] sendsigs
[+] speech-dispatcher
[-] thermald
[+] udev
[+] ufw
[-] umountfs
[-] umountnfs.sh
[-] umountroot
[+] unattended-upgrades
[+] urandom
[-] uuidd
[+] whoopsie
[-] x11-common
```

Stop suspicious services with

```
service [name] stop
```

Find and Remove Illegal Files and Software

Illegal Software

You may find recently installed software from /var/log/apt/*, however be prepared for CyberPatriot to have cleared this directory in later rounds.

```
gunzip /var/log/apt/*
grep "Commandline" /var/log/apt/*
```

Therefore, you should look at the files you listed that were modified in the last 60 days from /usr/share/doc. You will get an approximate list of things to uninstall.
Once you come across a package, use apt search *PACKAGE_NAME* to determine whether it is safe or not.

Use the following command to also find suspicious software.

```
dpkg --get-selections | grep -Ei
"(john|x11|crack|hydra|weplab|pyrit|cain|netc|ploit|Wireshark|Nessus|Nikto|Kismet|nmap|ftp|php|lightweight|inet|bind9|nginx|traf|scan|teln|passwo|remmina|minetest|openciv|fakeroot|ettercap|tcpspray|dsniff|nbtscan|named|vnc|snmp|irc|dns|dovecot)"
```

Media Files

```
for ext in mp4 mp3 ogg m4b flv mov exe bash; do sudo find / -iname "*.$ext" 2>/dev/null;
done
for extpic in jpg jpeg png txt; do sudo find /home -iname "*.$extpic"; done
```

Further Reconnaissance

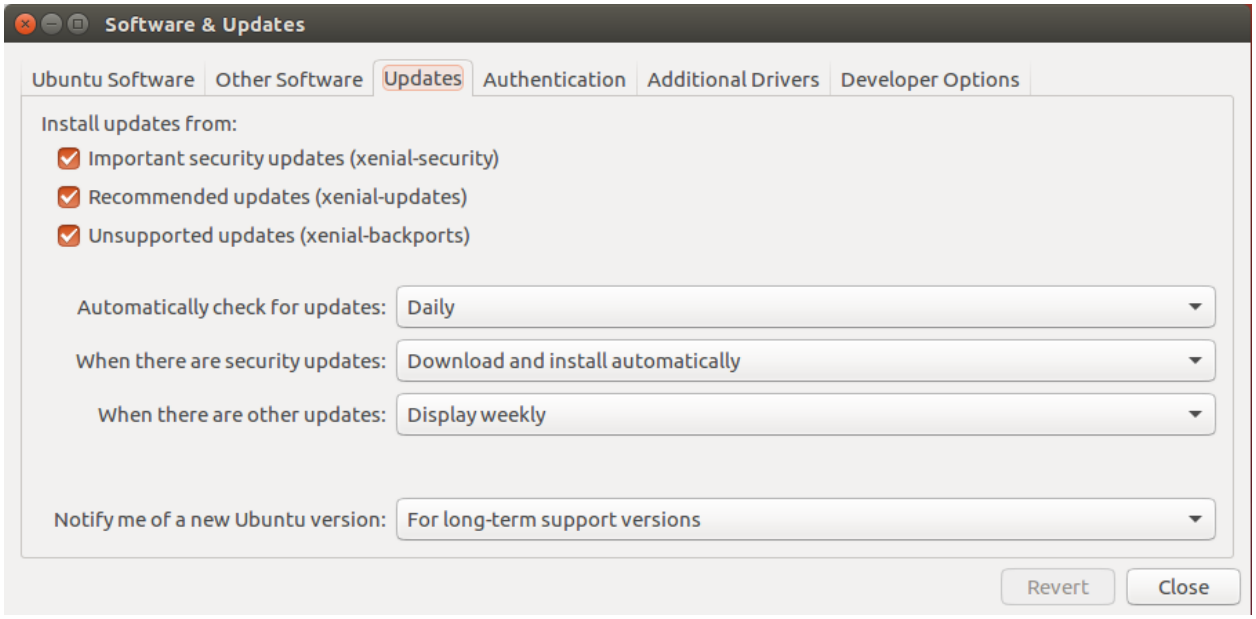
Use the package "ranger" to navigate quickly through the file system. Upon running, type 'z' then 'h' to enable hidden files.

```
sudo apt-get install ranger
ranger
```

Configure and Perform Updates

First import the correct sources.list config found in the guide.

Next, you can then either set up auto updates with config or the gui. In this case, it is faster to fix this with the gui, so you should go to **Settings -> Software & Updates -> Updates** and then set the options as follows.



If you wanted to do it via config files instead, you would need to edit 10periodic, 20auto-upgrades, and 50unattended-upgrades in /etc/apt/apt.conf.d/ to do this.

After that, run the following to update and upgrade:

```
apt-get update
apt-get upgrade -y
```

Clean up residual packages

```
apt-get autoremove
apt-get autoclean
```

Complete Forensics Questions

If you don't know how to do these, skip them and come back later. Don't spend too much time.

Securely Configure Required Applications

Configure Firefox
Look at the guides for every critical service and make them secure!
Also download and update any software specified in the README.

Miscellaneous Hardening

Mount the /tmp directory correctly

This way people can't abuse the /tmp directory

```
sudo mount -t tmpfs -o noexec,nosuid,rw tmpfs /tmp
```

SUID and SGID Binaries

Search for SUID and SGID binaries. Check any that aren't on the default list.

```
find /usr/bin /bin /sbin -perm -4000 -o -perm -2000
```

Default output:

```
/usr/bin/chsh
/usr/bin/crontab
/usr/bin/newgrp
/usr/bin/expiry
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/bsd-write
/usr/bin/wall
/usr/bin/ssh-agent
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/chage
/usr/bin/mlocate
/usr/bin/gpasswd
/bin/ping6
/bin/su
/bin/umount
/bin/mount
/bin/fusermount
/bin/ping
/sbin/unix_chkpwd
```

```
/sbin/pam_extrausers_chkpwd
```

Inspect SUID or SGID binaries that are not on the default list and delete. Remove the flag from their permissions with the following command.

```
chmod -R  ug-s [file dir]
```

File Permissions

Configure file permissions with the following commands. **Bold** denotes commonly modified permissions.

For **all** services, ensure that their necessary files all have secure permissions.

```
chown -R  root:root /boot/grub/grub.cfg
chmod -R  400 /boot/grub/grub.cfg
chmod -R 740 /etc/grub.d
chown -R root:root /etc/grub.d
chown -R  root:root /etc/issue
chmod -R  644 /etc/issue
chown -R  root:root /etc/issue.net
chmod -R  644 /etc/issue.net
chown -R  root:root /etc/hosts.allow
chmod -R  644 /etc/hosts.allow
chown -R  root:root /etc/hosts.deny
chmod -R  644 /etc/hosts.deny
chmod -R  640 /var/log/*
chown -R  root:root /etc/crontab
chmod -R  600 /etc/crontab
chown -R  root:root /etc/cron.hourly
chmod -R  700 /etc/cron.hourly
chown -R  root:root /etc/cron.daily
chmod -R  700 /etc/cron.daily
chown -R  root:root /etc/cron.weekly
chmod -R  700 /etc/cron.weekly
chown -R  root:root /etc/cron.monthly
chmod -R  700 /etc/cron.monthly
chown -R  root:root /etc/cron.d
chmod -R  700 /etc/cron.d
chown -R  root:root /etc/ssh/sshd_config
chmod -R  600 /etc/ssh/sshd_config
chown -R  root:root /etc/passwd
chmod -R  644 /etc/passwd
chown -R  root:shadow /etc/shadow
chmod -R  640 /etc/shadow
chown -R root:root /etc/sudoers
chmod -R 440 /etc/sudoers
chown -R  root:root /etc/group
chmod -R  644 /etc/group
chown -R  root:shadow /etc/gshadow
chmod -R  640 /etc/gshadow
chown -R  root:root /etc/passwd-
chmod -R  644 /etc/passwd-
chown -R  root:shadow /etc/shadow-
chmod -R  640 /etc/shadow-
chown -R  root:root /etc/group-
chmod -R  644 /etc/group-
chown -R  root:shadow /etc/gshadow-
chmod -R  640 /etc/gshadow-
chmod -R o-w <directory>
```

Disable IP Spoofing

/etc/host.conf
Add the following lines

```
order bind,hosts
nospoof on
```

Delete the following lines

```
multi on
```

Resolv.conf

Change the file to use the following line.

```
nameserver 8.8.8.8
```

Tips and Tricks

1. If a command is giving you strange output (getting output/errors that correspond to a different command), which the command to find its binary, and cat the contents of the binary to determine that it isn't running anything else.
   You can also use file to determine file type. Executables should be reported as "ELF LSB shared object"
   a. Execute the following command to search for a shebang line (#!/bin/bash) throughout /bin and /sbin

      ```
      sudo grep -R "\#\!/" -- /bin /sbin
      ```

2. If a file is immutable (even though you are root), list its attributes with lsattr and remove the immutable attributes using

   ```
   chattr -uia [file]
   ```

3. If you are unable to use apt commands (/var/lib/dpkg is occupied by another process), run the following commands

   ```
   ps aux | grep -E "apt|dpkg"
   kill -9 [pid]
   ```

4. If Wi-Fi goes down, run the following command

   ```
   sudo dhclient eth0
   ```

5. If points are lost after rebooting, there are three probable reasons: Firefox configuration resetting (if configured from prefs.js), a backdoor/service that runs on startup, or sysctl configuration resetting (remediate this by running sysctl -p)
6. If your user is locked out and passwd -u and usermod -U don't work, run the following command

```
pam_tally2 --user=[username] --reset
```

Useful Shortcut Links

- **Windows related links**
    - bit.ly/vascuba-winsct1 - link to download Microsoft SCT
    - bit.ly/vascuba-wintutorials - link to the tenforums tutorials
- **Linux related links**
    - bit.ly/vascuba-ubush - JShielder script for ubuntu config
    - bit.ly/vascuba-cyberciti - custom search on cyberciti
    - bit.ly/vascuba-sysctl - link to sysctl configuration
    - bit.ly/vascuba-sysctl2 - cyberciti sysctl page
    - bit.ly/vascuba-lampdocs - link for documentation on lamp stack apps
    - do.co/vascuba-digo - digital ocean tutorials
    - do.co/vascuba-https - digital ocean https tutorial

Applications, Services, and Systems Configuration

This section includes instructions and references on how to configure things.

Port Number Reference

Remember to allow the correct port in the firewall.

ftp	21
ssh/sftp	22
Smtp (mail sending)	25
dns	53
http	80
POP3 (mail receiving)	110
IMAP (mail receiving)	143
https	443
smb/samba	445
rdp	135, 3389
mysql	3306[0]

Configuration Flipping

This is a dangerous technique (as it can totally destroy things like sysctl), but it works fairly well on certain applications such as Firefox. Basically how to cheeze the comp

List of values used to represent booleans:

- true/false
- off/on
- yes/no
- 1/0 (be careful not to change integer 0s and 1s unnecessarily)
- enabled/disabled

Places to try config flipping:

- Firefox
- Openssh (as long as you don't restart it's fine. Basically means this is a last resort option)

Linux command

```
sed -ie 's/<true val>/r3pl@ce/; s/<false val>/<true val>/; s/r3pl@ce/<false val>' <file path>
```

Windows command (powershell)

```
(gc <file path>) -replace '<true val>', 'r3pl@ce' -replace '<false val>', '<true val>', -replace 'r3pl@ce', '<false val>' | sc <file path>
```

All Systems - Services that allow anonymous access

Make sure that all files have read-only permissions. Also ensure that services are configured to only allow read permissions.

All Systems - Mozilla Firefox

You can go to about:preferences to configure things.

- General: Always check if FF is default, show blank page on start, default home page, auto updates, use a background service to install, automatically update search
- Privacy and Security: Do not remember logins, do not use a master password, never remember history, uncheck all address bar, always use tracking protection, always send do not track, block pop-ups, warn when websites try to install, check all deceptive content, check query OCSP
- Go to about:addons and delete everything bad

During an online round, it is best to import a user.js file. There are excellent ones here: https://github.com/pyllyukko/user.js/. Copy the file into the appropriate directory and open/close Firefox.

All Systems - MySQL

Make sure MySQL is bound to localhost or 127.0.0.1 and not running as root/administrator. **DO NOT** bind to localhost if the server is needed by an external service.

Ensure that no files have the string MYSQL_PWD in it by running grep -R MYSQL_PWD /home or findstr /s /c:"MYSQL_PWD" C:\Users*. Also do this in /root.

Login to the MySQL terminal.

- Run mysql_secure_installation on the normal terminal
- Look up all the users and the host they come from by running SELECT host, user FROM mysql.user;
- Look at this website for changing passwords: https://www.cyberciti.biz/faq/mysql-change-user-password/

- Run this to change user password expiry info: ALTER USER '[user]@localhost' password expire interval 30 day;
- Ensure that memcached is not installed by running uninstall plugin daemon_memcached;
- Check section 5 of the MySQL CIS benchmark
- Ensure that no users have wildcard hostnames by running SELECT user, host FROM mysql.user WHERE host = '%'; and changing every user's host to localhost
  DO NOT change it to localhost for national finals
- Ensure that no anonymous accounts exist by running SELECT user,host FROM mysql.user WHERE user = ''; and deleting any accounts that appear from the query
- Make sure no users have a "super" status by running REVOKE SUPER ON *.* FROM '<user>';
- Check additional database permissions for allusers
- Configure "local-infile=0" in the main config file under [mysqld]
- Check permissions with SHOW GRANTS FOR <user>@<host> and assign limited permissions with REVOKE ALL FROM <user>@<host> and GRANT <permissions> ON <object> TO <user>@<host>

All Systems - OpenSSH

For Linux: Allow ssh from the firewall

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

Alternatively with ufw:

```
sudo ufw allow 22
```

On linux, most of the configuration for OpenSSH is done through /etc/ssh/sshd_config. These are the most important settings. On windows these settings should be set through %ProgramData%\ssh\sshd_config. It also appears as though a default config exists in %windir%\System32\OpenSSH\sshd_config_default
TODO: add pubkeyauthentication information for nats

```
PermitRootLogin no
PermitEmptyPasswords no
Protocol 2
LogLevel INFO
#X11Forwarding No #not supported by Windows
MaxAuthTries 3
PermitUserEnvironment no
ClientAliveInterval 300
ClientAliveCountMax 1
LoginGraceTime 50
PasswordAuthentication yes #no if you need to use pubkeyauth
```

```
PermitBlacklistedKeys no
UseDNS yes
```

SSH keys allow users to login without a password. Unless the README says otherwise, remove all of these. These will be located in ~/.ssh/authorized_keys.

Make sure to restart ssh once you are done for changes to take effect.

```
service ssh restart
```

All Systems - PHP

LINUX - This file is located at /etc/php/7.0/fpm/conf.d/99-security.conf for version 7 and /etc/php.d/security.ini for other versions

```
#more critical things
expose_php=Off
display_errors=Off
file_uploads=Off
allow_url_fopen=Off
allow_url_include=Off
safe_mode=On #removed in php 5.4
sql.safe_mode=On
disable_functions=exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source
session.use_strict_mode=On
register_globals=Off #removed in php 5.4
session.cookie_lifetime=0
session.cookie_secure=On
session.hash_function="sha256"

#less critical things
mail.add_x_header = Off
cgi.force_redirect=On
post_max_size=1K
max_execution_time=30
```

Restart the apache service for changes to take effect

All Systems - WordPress

- Update WordPress through the Dashboard
- Change account credentials, particularly the default admin user/pass
- Restrict the MySQL user to only SELECT, INSERT, UPDATE, DELETE

- Backup core files and database to somewhere safe

Plugins to install, if allowed by proxy

- Sucuri, enable all the protection
- Really Simple SSL plugin, enable SSL
- Login LockDown, set login retries and lockout like you would a regular system
- Inactive Logout, set inactivity timeout

Block files with an .htaccess file in the same directory

- xmlrpc.php
- wp-config.php

```
<Files [filename]>
deny from all
</Files>
```

wp-config.php options

```
define('DISALLOW_FILE_EDIT', true);
define('DISALLOW_FILE_MODS', true);
```

Generate a new secret key at https://api.wordpress.org/secret-key/1.1/salt/ and replace the old ones in wp-config.php

Disable PHP in vulnerable directories, such as /wp-content/uploads/ by creating a .htaccess file in that directory

```
<Files *.php>
deny from all
</Files>
```

Linux - Apache

Allow http and https from the firewall

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

Alternatively with UFW

```
sudo ufw allow 80
sudo ufw allow 443
```

Run the following commands

```
Sudo a2dismod cgi -f
sudo a2dismod dav* -f
```

```
sudo a2dismod status* -f
sudo a2dismod autoindex* -f
sudo a2dismod proxy* -f
sudo a2dismod userdir* -f
sudo a2dismod info* -f
sudo a2enmod ssl
sudo a2ensite default-ssl
```

- Delete any shares that are not needed, but are listed in /etc/apache2/apache2.conf (Like the root directory element)
- Change bad config to good config in apache2.conf (make config match these options if possible)

```
<Directory />
. . .
Order deny,allow
Deny from all
. . .
</Directory>

AllowOverride None
Options None
```

^If these do not exist, create them

Make sure the \.ht area has Require all denied

```
<FilesMatch "^\.ht">
Order allow,deny
Deny from all
</FilesMatch>
```

Remove default content
Clear the /usr/lib/cgi-bin folder
Change bad config to good config in /etc/apache2/conf-enabled. If the security configuration is not enabled, run a2enconf security and then reload apache before trying this. Also make sure nothing in the conf-enabled folder is making the service less secure.

- TraceEnable Off
- ServerTokens Minimal
- ServerSignature Off
- FileETag Off

Install mod security by running sudo apt-get install libapache2-modsecurity
Make sure to check the sites-enabled folder for bad conf too

Generate SSL certificates

```
openssl req -x509 -newkey rsa:1024 -keyout /etc/ssl/private/apache2.key -out
/etc/ssl/certs/apache2.crt  -nodes -days 365
```

Enable SSL from sites-available/default-ssl.conf

```
SSLEngine on
SSLCertificateFile /etc/ssl/certs/apache2.crt
SSLCertificateKeyFile /etc/ssl/private/apache2.key
```

Restart the Apache service

```
sudo service apache2 restart
```

Example of a secure configuration is on JShielder:
https://github.com/Jsitech/JShielder/blob/master/UbuntuServer_18.04LTS/templates/apache

Linux - Bind9

Make sure that the service is NOT running as root.
Modify things in /etc/bind/named.conf.options

```
options {
  dnssec-enable yes;
  dnssec-validation yes;
  random-device "/dev/random";
};
```

Find the location of dns zones (the file should contain several "zone" keywords)
For each zone, you should check the following configuration options

```
#remove global options in these options such as 0.0.0.0
zone <zone-name> {
  allow-transfer {localhost};
  allow-query {localhost};
  allow-recursion {localhost};
  allow-update {none};
};
```

Linux - PAM

Delete any instances of nullok among any of the files

```
grep -r "nullok" /etc/pam.d
```

/etc/pam.d/common-password

```
password        requisite                       pam_cracklib.so retry=3 minlen=8 difok=3
ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 reject_username gecoscheck
enforce_for_root
password        [success=1 default=ignore]      pam_unix.so obscure shadow sha512
use_authtok remember=5 minlen=8 rounds=5000
password        requisite                       pam_deny.so
password        requisite                       pam_permit.so
password        optional        pam_gnome_keyring.so
```

/etc/pam.d/common-auth

```
auth    [success=1 default=ignore]      pam_unix.so
auth    requisite                       pam_deny.so
auth    required                        pam_permit.so
auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800
```

/etc/login.defs

The following are the only lines you may need to change

```
CHFN_AUTH yes
CHSH_AUTH yes
CREATE_HOME yes
DEFAULT_HOME no #default
ENCRYPT_METHOD SHA512
PASS_MAX_DAYS       30
PASS_MIN_DAYS       10
PASS_WARN_AGE       7
SHA_CRYPT_MIN_ROUNDS 50000
UMASK                       055
```

Linux - PostgreSQL

/etc/postgresql/9.x/main/pg_hba.conf

```
local   all         postgres                    peer
local   all         all                         peer
hostssl   all         all         127.0.0.1/32      md5
hostssl   all         all         ::1/128           md5
```

- Be careful modifying this if the README specifies certain interfaces/addresses to allow.
- Replace all instances of "trust" or "password" in last column with "md5"

Generate SSL certificates

```
openssl req -x509 -newkey rsa:1024 -keyout /etc/ssl/private/postgres.key -out
/etc/ssl/certs/postgres.crt  -nodes -days 365
```

Change all instances of "host" to "hostssl" in /etc/postgresl/9.5/main/pg_hba.conf

/etc/postgresql/9.5/main/postgresql.conf

```
listen_addresses = 'localhost'
work_mem = 4MB
maintenance_work_mem = 64MB
temp_buffers = 1MB
max_prepared_transactions = 0
temp_file_limit = -1
ssl = true
ssl_cert_file = '/etc/ssl/certs/postgres.crt'
ssl_key_file = '/etc/ssl/certs/postgres.key'
password_encryption = on
row_security = on
log_connections = on
```

Ensure that /etc/postgresql/9.5/main/pg_ident.conf is **empty** (unless an identity/user mapping is specified in the README).

- If configured insecurely, this file may permit unauthorized users (SYSTEM-USERNAME) to connect to the db as a superuser or privileged user (PG-USERNAME).

Restart PostgreSQL

```
service postgresql restart
```

Linux - ProFTPD

Allow ftp from the firewall

```
sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 20 -j ACCEPT
sudo iptables -A PREROUTING -t raw -p tcp --dport 21 -j CT --helper ftp
```

Alternatively from UFW

```
sudo ufw allow 21
sudo ufw allow 22
```

Most of the configuration for ProFTPD is done through /etc/proftpd/proftpd.conf and other files in that directory. Do not replace the entire file, or at least make a copy or take notes. **This is the first round we've had ProFTPD and we're all in the dark. We have no idea what is correct and what is incorrect.**
Check out anything that is configured and not left default.
proftpd.conf handles global server config.

```
AllowFilter "^[a-zA-Z0-9 ,]*$"
AllowForeignAddress off
AllowLogSymlinks off
AllowOverwrite off
AuthOrder mod_auth_pam.c* mod_auth_unix.c
AuthPAM on
AuthUsingAlias off
CommandBufferSize 512
CreateHome off
DefaultRoot ~
DebugLevel 0
#DefaultAddress delete any instances of this
DeferWelcome on
DenyFilter ""
DirFakeGroup on
DirFakeUser on
IdentLookups off
MaxClients 1
MaxInstances 10
MaxLoginAttempts 3
MaxRetrieveFileSize 5 Mb
MaxStoreFileSize 5 Mb
RequireValidShell on
ServerName "something, probably the one already there"
ServerType standalone
ShowSymlinks off
UseIPv6 off
User [someone who isn't root]
Group [group of the user]
<Limit LOGIN>
    AllowUser [username]
    ...
    AllowGroup [group]
    DenyAll
</Limit>
```

Unless the README says not to, remove any <Anonymous> sections from all configuration files.

Now, for each folder that is supposed to exist (or the entire server), configure access control as per the README instructions.

```
<Directory [path]>
    <Limit [command]> # use as many as necessary
        AllowUser [user]
        [etc, check the documentation on what you can put in here]
    </Limit>
</Directory>
```

To configure TLS, there should exist a file /etc/proftpd/tls.conf, but if it does not exist you can create it.

Generate an SSL Certificate:

```
openssl req -x509 -newkey rsa:1024 -keyout /etc/ssl/private/proftpd.key -out
/etc/ssl/certs/proftpd.crt  -nodes -days 365
```

```
<IfModule mod_tls.c>
    TLSEngine on
    TLSLog /var/log/proftpd/tls.log
    TLSProtocol TLSv1.2
    TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
    TLSRSACertificateKeyFile  /etc/ssl/private/proftpd.key
    TLSRequired on
</IfModule>
```

Make sure to uncomment or add Include /etc/proftpd/tls.conf to the main configuration.

Restart the proftpd service

```
sudo service proftpd restart
```

Linux - samba

I will write this section after I finish the round tomorrow. For now, it's storing links to guides that I think will be useful. - Lauren

https://linuxize.com/post/how-to-install-and-configure-samba-on-ubuntu-18-04/
https://www.digitalocean.com/community/tutorials/how-to-set-up-a-samba-share-for-a-small-organization-on-ubuntu-16-04
https://ubuntu.com/server/docs/samba-securing

Linux - SELinux

Search for any instances of selinux=0 or enforcing=0 in a linux line in the grub config.

```
grep "^\s*linux" /boot/grub/grub.cfg
```

If found, delete the instances from all CMDLINE_LINUX parameters in /etc/default/grub.

```
update-grub
```

Enable SELinux at boot time. Edit the /etc/selinux/configfile to set the SELINUX parameter:

```
SELINUX=enforcing
```

Linux - sources.list

Defaults:
/etc/apt/sources.list
Ubuntu 14.04

```
deb http://us.archive.ubuntu.com/ubuntu/ trusty main restricted
deb http://us.archive.ubuntu.com/ubuntu/ trusty-updates main restricted

deb http://us.archive.ubuntu.com/ubuntu/ trusty universe
deb http://us.archive.ubuntu.com/ubuntu/ trusty-updates universe

deb http://us.archive.ubuntu.com/ubuntu/ trusty multiverse
deb http://us.archive.ubuntu.com/ubuntu/ trusty-updates multiverse

deb http://us.archive.ubuntu.com/ubuntu/ trusty-backports main restricted universe
multiverse
deb http://security.ubuntu.com/ubuntu trusty-security main restricted
deb http://security.ubuntu.com/ubuntu trusty-security universe
deb http://security.ubuntu.com/ubuntu trusty-security multiverse
deb http://extras.ubuntu.com/ubuntu trusty main
```

Ubuntu 16.04

```
deb http://us.archive.ubuntu.com/ubuntu/ xenial main restricted
deb http://us.archive.ubuntu.com/ubuntu/ xenial-updates main restricted

deb http://us.archive.ubuntu.com/ubuntu/ xenial universe
deb http://us.archive.ubuntu.com/ubuntu/ xenial-updates universe

deb http://us.archive.ubuntu.com/ubuntu/ xenial multiverse
deb http://us.archive.ubuntu.com/ubuntu/ xenial-updates multiverse

deb http://us.archive.ubuntu.com/ubuntu/ xenial-backports main restricted universe
multiverse
deb http://security.ubuntu.com/ubuntu xenial-security main restricted
```

```
deb http://security.ubuntu.com/ubuntu xenial-security universe
deb http://security.ubuntu.com/ubuntu xenial-security multiverse
```

Ubuntu 18.04

```
deb http://us.archive.ubuntu.com/ubuntu/ bionic main restricted

deb http://us.archive.ubuntu.com/ubuntu/ bionic-updates main restricted

deb http://us.archive.ubuntu.com/ubuntu/ bionic universe
deb http://us.archive.ubuntu.com/ubuntu/ bionic-updates universe

deb http://us.archive.ubuntu.com/ubuntu/ bionic multiverse
deb http://us.archive.ubuntu.com/ubuntu/ bionic-updates multiverse

deb http://security.ubuntu.com/ubuntu bionic-security main restricted
deb http://security.ubuntu.com/ubuntu bionic-security universe
deb http://security.ubuntu.com/ubuntu bionic-security multiverse
```

Ubuntu 20.04

```
deb http://archive.ubuntu.com/ubuntu/ focal main restricted universe multiverse
deb-src http://archive.ubuntu.com/ubuntu/ focal main restricted universe multiverse

deb http://archive.ubuntu.com/ubuntu/ focal-updates main restricted universe multiverse
deb-src http://archive.ubuntu.com/ubuntu/ focal-updates main restricted universe
multiverse

deb http://archive.ubuntu.com/ubuntu/ focal-security main restricted universe multiverse
deb-src http://archive.ubuntu.com/ubuntu/ focal-security main restricted universe
multiverse

deb http://archive.ubuntu.com/ubuntu/ focal-backports main restricted universe multiverse
deb-src http://archive.ubuntu.com/ubuntu/ focal-backports main restricted universe
multiverse

deb http://archive.canonical.com/ubuntu focal partner
deb-src http://archive.canonical.com/ubuntu focal partner
```

Debian 8

```
deb http://ftp.us.debian.org/debian/ jessie main
deb http://security.debian.org/ jessie/updates main contrib
deb http://ftp.us.debian.org/debian/ jessie-updates main contrib
```

Debian 9

```
deb http://deb.debian.org/debian stretch main
deb-src http://deb.debian.org/debian stretch main

deb http://deb.debian.org/debian stretch-updates main
deb-src http://deb.debian.org/debian stretch-updates main

deb http://security.debian.org/debian-security/ stretch/updates main
deb-src http://security.debian.org/debian-security/ stretch/updates main
```

Linux - sudoers

Output from running visudo

```
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
root    ALL=(ALL:ALL) ALL
%admin ALL=(ALL) ALL
%sudo    ALL=(ALL:ALL) ALL
```

Linux - sysctl

/etc/sysctl.conf

```
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.icmp_echo_ignore_all = 1
net.ipv4.tcp_max_tw_buckets = 1440000
net.ipv4.tcp_timestamps = 0
net.ipv4.tcp_sack = 0
net.ipv4.tcp_window_scaling = 0
net.ipv4.tcp_keepalive_time = 1800
net.ipv4.tcp_fin_timeout = 15
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 1024
```

```
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5
net.ipv4.tcp_max_orphans = 256
net.ipv4.tcp_rfc1337 = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.ip_forward = 0
kernel.core_uses_pid = 1
kernel.dmesg_restrict=1
kernel.pid_max = 65536
kernel.sysrq = 0
kernel.exec-shield = 1
kernel.randomize_va_space = 2
kernel.unprivileged_userns_clone = 0
fs.suid.dumpable = 0
fs.file_max = 65535
```

Linux - VSFTPD

Allow ftp from the firewall

```
sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 20 -j ACCEPT
sudo iptables -A PREROUTING -t raw -p tcp --dport 21 -j CT --helper ftp
```

Alternatively from UFW

```
sudo ufw allow 21
sudo ufw allow 22
```

Most of the configuration for VSFTPD is done through /etc/vsftpd.conf. These are the most important settings.

```
anonymous_enable=NO
hide_ids=YES
no_anon_password=YES
pasv_promiscuous=NO
write_enable=NO
local_enable=YES
chroot_local_user=YES
anon_max_rate=30000
local_max_rate=30000
idle_session_timeout=60
max_per_ip=10
xferlog_enable=YES
xferlog_std_format=NO
xferlog_file=/var/log/vsftpd.log
```

```
log_ftp_protocol=YES
debug_ssl=YES
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
```

Generate an SSL Certificate with this command.

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout
/etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
```

Restart the vsftpd service.

Linux - nginx

Generate SSL certificates

```
openssl req -x509 -newkey rsa:1024 -keyout /etc/ssl/private/nginx.key -out
/etc/ssl/certs/nginx.crt  -nodes -days 365
```

Configure /etc/nginx/conf.d/ssl.conf

```
server {
listen 443 ssl;
server_name <domain>;
ssl on;
ssl_protocols TLSv1.2;
ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384
EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4
EECDH EDH+aRSA HIGH !RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS";
ssl_prefer_server_ciphers on;
ssl_certificate /etc/ssl/cert/nginx.cert;
ssl_certificate_key /etc/ssl/private/nginx.key;
}
```

Configure /etc/nginx/conf.d/nginx.conf

```
if ($request_method !~ ^(GET|HEAD|POST)$ )
{
return 405;
}
if ($http_user_agent ~* LWP::Simple|BBBike|wget) {
return 403;
}

##buffer policy
```

```
client_body_buffer_size 1K;
client_header_buffer_size 1k;
client_max_body_size 1k;
large_client_header_buffers 2 1k;
##end buffer policy

add_header X-Frame-Options "SAMEORIGIN";
add_header X-XSS-Protection "1; mode=block";
add_header Content-Security-Policy "default-src 'self';";
add_header Strict-Transport-Security max-age=15768000;

server_tokens off;
```

Configure additional stuff using https://www.digitalocean.com/community/tools/nginx

Restart nginx

```
service nginx restart
```

Linux - Magento

Do Apache2/PHP configuration.

In /var/www/magento

```
chown -R web-server-name .
find . -type f -exec chmod 400 {} +
find . -type d -exec chmod 500 {} +
find var/ -type f -exec chmod 600 {} +
find media/ -type f -exec chmod 600 {} +
find var/ -type d -exec chmod 700 {} +
find media/ -type d -exec chmod 700 {} +
chmod 700 includes
chmod 600 includes/config.php
```

Windows - Active Directory

- Relevant Active Directory .msc files https://www.technig.com/msc-shortcut-commands-windows-server/
- Secure your SYSVOL folder permissions - make sure only authenticated users have read perms. The SYSVOL directory is at C:\Windows\SYSVOL
- Using AD Users and Computers, put computers and the DC in the necessary OUs
- Using Group Policy Management, create and link GPOs to OUs
- Right click the OU and click Group Policy Update

    - If the firewall is configured (and it should be), you must allow Local port: Dynamic RPC in inbound rules
    - You may configure this through GPOs on DC **I have found that this does not usually work, do it manually on each system**
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
    - Set NT4Crypto to 0

Windows - Apache

We haven't written this yet so follow Linux Apache as best as you can

Windows - DNS Server

Most configuration is done through DNS Manager

- DNSSEC sign the zone, use the wizard, check both boxes on the Trust Anchors page
- Turn on debug logging and configure as needed
- Zone transfer off
- Secure updates or no updates at all

Apply a GPO for "Windows Settings > Name Resolution Policy" to apply the correct suffix (should be the domain name) and check Enable DNSSEC.
Use the DNS Best Practices Analyzer in the Server Manager

Windows - FileZilla FTP Server

https://www.alibabacloud.com/help/faq-detail/49564.htm may be helpful. Configure through Edit > Settings > FileZilla Server Options

- Change admin password under "Admin Interface Settings" to a complex one
- Change custom welcome message to hide server version information - General settings > Welcome message (remove %v variable)
- If required, enable FTP for only one address under General settings > IP Bindings & change the default value (*) to a specified address for the server
- Configure access control - under general settings > IP Filters if needed to whitelist or blacklist any ip addresses
    - Alternatively, go to Edit > Users/Groups to edit user-level and user-group-level IP address filters under "IP Filters"
- Mitigate bounce attacks by checking (default) "**Require matching peer address of control and data connection"** in General settings > Security settings
- Enable automatic bans under Autoban
- Ensure complex user passwords
- Configure least privilege under "Users" - add an account and group first to perform the authorization operation!
- Utilize TLS encryption authentication under "FTP over TLS settings" - use a certificate or generate a new one and select "Enable FTP over TLS support (FTPS)"

- Under users, enable force TLS encrypted access for user logon
- Under "Logging", select "Enable logging to file" and try "Use a different logfile each day (example: fzs-2003-02-10.log)". Under "Miscellaneous", check the "Don't show passwords in message log" option.

Windows - IIS FTP

All of your settings will be in %windir%\System32\inetsrv\config\applicationHost.config

```
<location path="<site name>">
 <system.ftpServer>
  <authentication>
   <denyByFailure enabled="true />
  </authentication>
 </system.ftpServer>
</location>
```

Windows - IIS Server

If the web.config file does not already exist on your iis server, make it. Otherwise, replace it with this. You may also want to replace these configuration options in %windir%\System32\inetsrv\config\applicationHost.config
Setting names are case sensitive, but their values are not.
Make sure your web.config file looks like this:

```
<configuration>
 <system.webServer>
  <handlers accessPolicy="Read, Script">**
  <isapiCgiRestriction notListedIsapisAllowed="false" notListedCgisAllowed="false"/>**
   #don't modify stuff in here except for maybe trace
  </handlers>
  <directoryBrowse enabled="false" />
  <httpErrors errorMode="DetailedLocalOnly" />
  <security>
   <requestFiltering removeServerHeader="true" allowHighBitCharacters="false">
    <requestLimits maxUrl="4096" maxQueryString="2048" />
    <verbs>
     <add verb="TRACE" allowed="false" />
    </verbs>
    <fileExtensions allowUnlisted="false"> #I would hesitate to use this
     <add fileExtension=".html" allowed="true" />
    </fileExtensions>
   </requestFiltering>
  </security>
 </system.webServer>
```

```
 <system.web>
  <deployment retail="true" />
  <compilation debug="false" />
  <customErrors mode="on" />
  <trace enabled="false" />
  <sessionState cookieless="UseCookies" />
  <httpCookies httpOnlyCookies="true" />
  <machineKey validation="HMACSHA256" />*
  <trust level="medium" />*
 </system.web>
</configuration>
```

* This configuration option will be in %windir%\Microsoft.NET\Framework64\<version number>\Config\web.config instead
**only modify this in %windir%\System32\inetsrv\config\applicationHost.config

Windows - Internet Explorer

There isn't much to do here. These are almost never scored, but do them anyway.

- Turn on smartscreen
- Turn on protected mode
- Turn on do not track me, never allow websites to request location
- Turn on pop-up blocker
- Disable toolbars and extensions
- Delete browsing history on exit
- Max security on all zones

Advanced tab:

- Nothing accelerated graphics
- Nothing accessibility
- BROWSING Disable script debugging, do not tell if IE is not default, always underline links
- HTTP settings all checked
- Security do not allow any active content, do not allow software to run or install, check all three "Check for", empty temporary internet files, enable all do not track, no ssl3, no tls1, yes tls1.1, yes tls1.2, all warn options, enhanced protected mode

Also disable all add-ons, if there are any.

Windows - RDP Server

RDP secure configuration is done from Group Policy. Configure through Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host. We don't have a well-defined configuration for everything, but use your best judgement.

- Connections
    - Automatic reconnection: disable
    - Allow users to connect remotely: enable
    - Deny logoff of an administrator: enable
    - Configure keep-alive: disable
    - Limit number of connections: 1
    - Restrict Remote Desktop Services users: enabled
- Redirection
    - Block everything
- Security
    - Set client connection encryption: enable, high
    - Always prompt for password: enable
    - Require secure RPC: enable
    - Require use of specific security layer: enable
    - Do not allow local administrators: enable
    - Require user authentication: enable
- Session Time Limits
    - Set time limit: 1 minute
    - End session when time limits are reached: enable

Windows - Security Policy

These are always scored. Use SCT or another list, there are plenty available here.

Windows - SMB

First disable SMB 1.0 through features. Then, run these in Administrator PowerShell.

```
set-smbserverconfiguration -AnnounceServer $False -Force
set-smbserverconfiguration -AuditSmb1Access $True -Force
set-smbserverconfiguration -AutoShareServer $False -Force
set-smbserverconfiguration -AutoShareWorkstation $False -Force
set-smbserverconfiguration -EnableAuthenticateUserSharing $False -Force
set-smbserverconfiguration -EnableOpLocks $True -Force
set-smbserverconfiguration -EnableSMB1Protocol $False -Force
set-smbserverconfiguration -EnableSecuritySignature $True -Force
set-smbserverconfiguration -EnableStrictNameChecking $True -Force
set-smbserverconfiguration -EncryptData $True -Force
set-smbserverconfiguration -MaxMpxCount 0 -Force
set-smbserverconfiguration -MaxWorkItems 0 -Force
set-smbserverconfiguration -NullSessionPipes
set-smbserverconfiguration -RejectUnencryptedAccess $True -Force
set-smbserverconfiguration -RequireSecuritySignature $True -Force
set-smbserverconfiguration -SmbServerNameHardeningLevel 3 -Force
```

For each required share, run these.

```
set-smbshare -Name [share] -EncryptData $True -Force
set-smbshare -Name [share] -FolderEnumerationMode AccessBased -Force
```