AFA CYBERCAMP

STUDENT WORKBOOK

ADVANCED CAMP 2023

Table of Contents

Table of Contents **2**

Welcome! (Pre- and Post-Camp Surveys) **4**

Supplemental Resources **5**

Preventing Cyberbullying 5

Activities **6**

Activity 1: Windows Graphical Utilities 6
Activity 2: Windows Command Line 8
Activity 3: Windows Sysinternal Suite 10
Activity 4: Linux Init Systems 12
Activity 5: Linux Advanced Command Line 13
Activity 6: Linux Processes and Scheduled Tasks 14
Activity 7: Linux Security Policies and PAM 15
Activity 8: Linux Networking 16
Activity 9: Base64 Decoding and Steganography 17

Windows Command Cheat Sheet **18**

Linux Command Cheat Sheet **20**

Glossary of Terms **25**

CyberPatriot Code of Conduct **33**

This page is intentionally blank.

Welcome! (Pre- and Post-Camp Surveys)

Dear CyberCamp Participant,

Welcome to your AFA CyberCamp! We hope you have a fun and exciting week learning about cybersecurity.

At the start of the camp, you'll be asked to complete a pre-camp survey so that we can determine your current cybersecurity skill level. Use the Pre-Camp Survey QR code (or URL) to open and complete the survey. It should take no more than 2-3 minutes. Surveys can be complete on a smartphone or computer.

Pre-Camp Survey

To be completed on the first day of camp.

https://forms.gle/PuTSdLsxXxz2KRGe6

So that we can see how your cyber skills have improved throughout the camp, you'll be asked to complete a similar survey at the end of the week (QR code below). **DO NOT complete this survey until your instructor directs you to do so once the camp is complete.**

Post-Camp Survey

To be completed on the last day of camp, after the competition.

https://forms.gle/x8Y8m6EQwPfq9Xcd9

Your feedback will be used to improve the camp experience for the next group of students like you!

Sincerely,

The CyberPatriot Staff

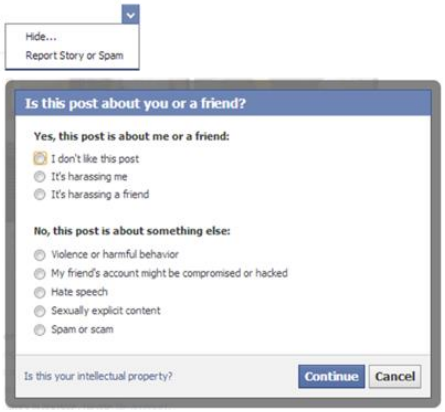
Supplemental Resources

Preventing Cyberbullying

Cyberbullying Prevention Tips:

Unfortunately, cyberbullying has become far too common, especially among teens and young adults. If you are ever a victim of cyberbullying, keep in mind the following tips:

- Do not respond to the cyberbullying message/post.
- Block the cyberbullying offender.
- Report the cyberbullying or other abuse to the site.
  - Social media sites give users the ability to flag content they see as offensive.



If you experience cyberbullying at school, inform your teacher or a school administrator immediately, just like you would with any other type of bullying.

If you experience cyberbullying at home, tell a responsible adult (parent, guardian, teacher, etc.) immediately, regardless of the severity. Law enforcement officials may need to get involved if the cyberbullying involves threats of violence, harassment, explicit messages or photos, photos or videos of someone in a place where he/she would expect privacy, stalking and/or hate crimes.

Additional tips:

- Remain calm and safe. Resist the temptation to respond to the bully or audience if the cyberbullying is in a public forum.
- Keep screenshots or records of the bullying to provide as evidence. This is especially important if the authorities need to get involved.

Activities

Activity 1: Windows Graphical Utilities

This lab will review Windows Graphical Utilities

Instructions: *Use the Local Security Policy to help answer the following questions and complete any assigned tasks. You should be signed into the cyberpatriot user account (password: Cyb3rD3mo!)*

Do NOT enable Windows Defender (or make any other changes you are not instructed to) in the Local Group Policy Editor. If you do, you may be unable to complete the rest of this module.

1. What is the run command to start the Local Security Policy?

   Answer: _____

2. The default value for Load and unload device drivers is Administrators. Which non-admin user has been granted rights to Load and unload device drivers?

   Answer: _____

3. Restore Load and unload device drivers to the default security setting.

4. What is the default value for the User Rights Assignment Increase scheduling priority?

   Answer: _____

5. Restore Increase scheduling priority to the default value.
   a) Click Add User or Group
   b) Type the answer to #4 above
   c) Click Object Types
   d) Check Groups
   e) Click OK
   f) Click OK
   g) Click OK

6. What is the default value for the Security Option Network access: Do not allow anonymous enumeration of SAM accounts?

   Answer: _____

(Continued on next page)

7. Make sure the Security Option Network access: Do not allow anonymous enumeration of SAM accounts is set to the default value.

   Answer: _____

8. What is the run command to start the Local Group Policy Editor?

   Answer: _____

9. In class, you disabled Allow users to connect remotely by using Remote Desktop Services. In addition to this setting, three other settings are disabled somewhere under Computer Configuration → Administrative Templates. List these three settings below. (For example, you could look under System or Windows Components and sort any column by clicking the column header)

   Answer: _____

   Answer: _____

   Answer: _____

10. In class, you enabled Turn off Autoplay. In addition to this setting, three other settings are enabled somewhere under Computer Configuration → Administrative Templates. List these three settings below:

    Answer: _____

    Answer: _____

    Answer: _____

***Instructions**: Use the Shared Folders to help answer the following questions and complete any assigned tasks.*

11. What is the run command to start Shared Folders?

    Answer: _____

12. There are four hidden shares on your system; which three are default administrative shares?

    Answer: _____

13. There are four hidden shares on your system; which one is NOT a default administrative share?

    Answer: _____

14. Stop sharing any hidden shares that are NOT default administrative shares.

Activity 2: Windows Command Line

This lab will review performing tasks using the Windows Command Line.

***Instructions**: Use the Windows Command Line and the **net** service commands to help answer the following questions and complete any assigned tasks. Make sure you start the command line using Run as administrator (Search, type cmd, right-click on Command Prompt, Run as administrator).*

1. What is the current lockout threshold, duration, and observation window according to net accounts?

   Answer: _____

2. Use net accounts to set a secure minimum password length. What did you type on the command line to set this new password length policy?

   Answer: _____

3. The users vtaylor and rpatel are unauthorized. Please remove them immediately and record the command(s) you used to remove them.

   Answer: _____

4. Your company just hired a new employee, Katherine Johnson. Create a new user for her named **kjohnson** and don't forget to put in a password.

5. The user ssingh has an insecure password; change it to something secure.

6. According to net user, when did the user ekanye last log on?

   Answer: _____

7. The users rsmith and kwong are not authorized administrators; remove them from the Administrators group.

8. Add kjohnson to the Administrators group.

9. Which users are members of the group Backup Operators? (HINT: Put Backup Operators in quotes because of the space between the words)

   Answer: _____

10. What is the comment for the group Replicator?

    Answer: _____

(Continued on next page)

11. What is the full path of the directory shared with a share name of ftproot?

    Answer: _____

12. Which two users or groups have Full Access to the ftproot share according to the share permissions? (NOTE: This is NOT the same as the NTFS permissions).

    Answer: _____

13. Delete the ftproot share (do not delete the directory).

Instructions*: Use the Windows Command Line and the icacls command to help answer the following questions and complete any assigned tasks. Make sure you start the command line using Run as administrator.*

14. There are six unique users or groups that are listed as having Full Access to the directory C:\inetpub\ftproot in the folders ACLs. List the six users below:

    Answer: _____

    Answer: _____

    Answer: _____

    Answer: _____

    Answer: _____

    Answer: _____

15. Remove Everyone from the ACLs of the folder C:\inetpub\ftproot.

Instructions*: Use the Windows Command Line and the netstat command to help answer the following questions and complete any assigned tasks. Make sure you start the command line using Run as administrator.*

16. The svchost.exe is responsible for running many different services. The service name of the service running on port 21 is ftpsvc. What is the service name of the service running on port 135?

    Answer: _____

17. What are the ports and protocol of the service with the service name Dnscache? *Note: you may see more than one entry.*

    Answer: _____

Activity 3: Windows Sysinternal Suite

This lab will review Windows 10 Sysinternal Suite.

Instructions: Use **Process Explorer** (and the integrated **VirusTotal.com**) to help answer the following questions and complete any assigned tasks. Make sure you start **Process Explorer** using **Run as administrator**.

1. What is the parent process of dwm.exe? **Answer:** _____
2. What is the PID (Process ID) of System? **Answer:** _____
3. The csrss.exe process has a number of parameters passed to it on the command line, what parameter is MaxRequestThreads set to?

   Answer: _____
4. The process started with the command line "C:\Windows\system32\svchost.exe -k RPCSS -p" is responsible for managing two different services. What is the Display Name for those services?

   Answer: _____

   Answer: _____
5. What are the last four characters of the SHA256 hash of nc.exe?

   Answer: _____

***Instructions**: Use TcpView to help answer the following questions and complete any assigned tasks.*

6. What is the PID (Process ID) of the process listening on UDP port 137? **Answer:** _____
7. List all of the TCP or UDP ports that are open below 1024? Click on Local Port to search by port number.

   Answer: _____
8. Leave TcpView running and open Firefox. Navigate to google.com and watch TcpView to see what happens.

(Continued on next page)

***Instructions**: Use Autoruns (and the integrated VirusTotal.com) to help answer the following questions and complete any assigned tasks. Make sure you start Autoruns using Run as administrator.*

9. The Adobe Acrobat Update task is automatically run by Task Scheduler. What is the name of this executable?

   Answer: _____

10. Is the Adobe Acrobat Update task signature verified?

    Answer: _____

11. What is the name of the signer/publisher for the Adobe Acrobat Update task?

    Answer: _____

12. What is the name of the signer/publisher for the 7-zip shell extensions?

    Answer: _____

13. What is the image path of the 7-zip shell extensions?

    Answer: _____

14. What is the Registry Key related to the backdoorz service? (full path please)

    Answer: _____

When you're finished, use TcpView to close Connection and End Process, and use Autoruns to delete the backdoorz service from your computer.

Activity 4: Linux Init Systems

This lab will review Linux Init Systems

Instructions*: Use Linux terminal to answer the following questions and perform the following tasks. Sign into your Ubuntu 18 demo image using the cyberpatriot user account (password: CyberPatriot!)*

1. Use update-rc.d to disable the Apache service.
2. Use the Apache System-V init script to stop the Apache service.
3. According to the SysV rc directories, what services are stopped (or not started) when entering runlevel 3?

   Answer: _____
4. According to the SysV rc directories, which runlevels automatically start unattended-upgrades?

   Answer: _____
5. Use systemctl to start and enable the cups-browsed service.
6. Systemctl has many commands. You already learned start, stop, enable, and disable. According to the Systemctl man page, what is the command that “Asks all units listed on the command line to reload their configuration?”

   Answer: _____
7. The command hostnamectl is also part of systemd. What does hostnamectl say your “Kernel” is?

   Answer: _____
8. The command localectl is also part of systemd. What does localectl say your “System Locale” is*?*

   Answer: _____

Activity 5: Linux Advanced Command Line

This lab will review advanced Linux command lines.

***Instructions**: Use the Linux terminal in your Ubuntu 18 demo image to answer the following questions and perform the following tasks.*

1. According to diff, what line is in Documents/menu2.txt, but not in Documents/menu1.txt?

   Answer: _____

2. There are three unauthorized mp3 files on this computer. Use locate to find these files and list them below.

   Answer: _____

   Answer: _____

   Answer: _____

3. The command find is located in which directory? (HINT: Use the command which to help you.)

   Answer: _____

4. Using grep and wc, how many users have their home directory set to /bin/bash?

   Answer: _____

5. According to the wc man page, what does the -m option do?

   Answer: _____

Bonus Questions:

1. When using less, what keyboard command goes to the last line of the file? (HINT: You can use less --help to help you answer this question.)

   Answer: _____

2. There is an empty, regular file on your computer called “catchmeifyoucan” (without quotes). Using find to help you, what directory is this file in?

   Answer: _____

Activity 6: Linux Processes and Scheduled Tasks

This lab will review completing processes and scheduled tasks using the Linux command line.

***Instructions**: Use Linux terminal to answer the following questions and perform the following tasks.*

1. According to the man page for crontab, which command line option removes the user's existing crontab?

   Answer: _____

2. Look at the crontab for the user root. What is the full command that is being executed, including any command line options?

   Answer: _____

3. How often is the command from question #1 being executed?

   Answer: _____

4. This is a backdoor. Delete it from the crontab.

5. There are a number of nc processes running on your computer. Kill all the nc processes now and verify with ps -ef.

6. How many smbd processes are currently running on your computer?

   Answer: _____

7. The policy kit daemon **polkitd** was started with what command line option?

   Answer: _____

8. The /proc/self/ directory always points to the currently running process. If you do an "ls -la /proc/self/exe" where does the symlink point to?

   Answer: _____

Activity 7: Linux Security Policies and PAM

This lab will review Linux security policies and PAM.

***Instructions**: Use Linux terminal to answer the following questions and perform the following tasks.*

1. What is the current value of the kernel parameter /proc/sys/kernel/randomize_va_space?

   Answer: _____

2. Which sysctl configuration file contains the randomize_va_space setting?

   Answer: _____

3. A more secure value for this parameter is 2. Change it to 2 and reload the kernel parameters from the sysctl configuration files.

4. What is the value of /proc/sys/kernel/osrelease?

   Answer: _____

5. According to the pam_unix manual page, what file is used to store the password history for every user?

   Answer: _____

6. Look at the PAM configuration file for su. Which module is not enabled, but would allow you to require users to be members of the root group (or any other group)?

   Answer: _____

7. By default, pam_tally2 does not lock out the root account as a safeguard against denial of service attacks, and to prevent you from locking yourself out completely. According to the pam_tally2 manual, what option will allow the root account to become locked out?

   Answer: _____

8. Modify the minimum password length to be 12.

9. Modify the account lockout threshold to be 8.

Activity 8: Linux Networking

This lab will review Linux networking and firewalls.

Instructions: Use Linux terminal to answer the following questions and perform the following tasks.

1. What is the address and netmask of your loopback network device “lo?”

   Answer: _____

2. Which two TCP ports is smbd listening on?

   Answer: _____

3. Which UDP port is dhclient listening on?

   Answer: _____

4. What is the local IP address that systemd-resolve is listening on?

   Answer: _____

5. According to the ufw man page, how would you enable firewall logging?

   Answer: _____

6. Allow all incoming connections to samba through the firewall.

7. What TCP ports were allowed through the firewall for samba?

   Answer: _____

8. What UDP ports were allowed through the firewall for samba?

   Answer: _____

Activity 9: Base64 Decoding and Steganography

This activity discusses decoding and steganography with Steghide:

Base64 is an encoding algorithm often used in the sending of non-text data, including image and sound binary files. Binary data is long and difficult to transfer, so Base64 is used to encode data into shorter, more efficient strings. Steganography is an additional step used with encoding to hide information in images or audio files.

Decode the following Base64 encoded message:

Q3liZXJXYXJyaW9ycw==

This is the passphrase to use with Steghide to decode the message hidden in the image on the Desktop of the cyberpatriot user as cyberpatriot.bmp. Open the Ubuntu 18 Demo Image in VMWare Workstation Player. You will be logged in as the cyberpatriot account automatically. The password for this account is *CyberPatriot!*

1. First, decode the above base64 phrase by going to the following website or any trusted Base64 conversion tool: https://www.base64decode.org/
2. Paste the text into the “Base64 field” and select the “Decode” option.
3. The field below will show the decoded message in regular text format. This will be the passphrase (password) to use with Steghide.
4. Open a terminal and type cd Desktop.
5. Type “ls” and you will see sunset.jpg listed. At the cyberpatriot@ubuntu:~/Desktop$ prompt, type “steghide extract -sf sunset.jpg -xf answer.txt” on the command line.
6. Type the passphrase twice to extract the answer.

Answer: _____

Windows Command Cheat Sheet

Command	Action	Execution
cd	Displays the name of the current directory or changes the current folder	cd [filepath] cd.. (goes one directory up)
dir	Displays a list of a folder's files and subfolders	dir dir [myfolder]
help	Provides details about commands	help (lists all commands) help [command]
net accounts	Displays or configure information about the current configuration of the operating system	net /? (shows the available net commands) net help [command] (displays syntax of a net command) net accounts (displays current settings) net accounts /minpwlen:length (set minimum password length) net accounts /maxpwage: [# of days] (maximum password age) net accounts /minpwage:days (set the minimum password age) net accounts /uniqepw:number (enforce a password history) net accounts /lockoutthreshold:number (set the account lockout threshold) net accounts /lockoutwindow:minutes (set the account lockout window) net accounts /lockoutduration:minutes (set the account lockout duration)
net user	Displays, creates or modifies user accounts	net user (lists user accounts) net user username (shows user account and password settings) net username password (set user password)
net localgroup	Displays or modifies local groups	net localgroup (displays local groups on the system) net localgroup groupname (display members of a local group)
net share	List or modify resources being shared on the computer	net share (list resources being shared)

Command	Action	Execution
net share	List or modify resources being shared on the computer	net share sharename (display information about a specific resource) net share sharename=drive:path (add a new share) net share sharename /grant:user,perm (ass or remove permissions from a share)
icacls	Reset permissions for a file	icacls name /reset (reset a file with default inherited permissions) icacls name /grant user:perm (grant permissions to a user or group) icacls name /deny user:perm (deny permissions to a user or group) icacls name /remove user (remove all permissions for a user) icacls name /setowner user (change owner)
netstat	Displays connections, listening ports, routes, and statistics	Netstat /? (shows the available netstat commands) -a (displays all connections and listening ports) -n (displays numerical addresses and port numbers) -o (displays owning process IDs) -b (displays the executable that created the connection or listening port) -r (displays the routing table)
telnet	See what is running on a port	telnet localhost [port #] (connect to a port)
whoami	Displays the current username	

Linux Command Cheat Sheet

Command	Action	Execution
pwd	Presents working directory	pwd (prints out your current working directory)
ls	Lists Segments	ls [FILE] (lists files) ls -l [FILE] (shows a file's owner, group, permissions and other information) ls -a [FILE] (shows all files, including hidden files) ls -la [FILE] (shows all files using the long listing format)
cd	Change directory	cd [DIR] (changes to a specific directory) cd.. (changes to the parent directory)
man	Displays the manual for a command	man [SECTION] (displays the manual for the specific command)
cp	Can copy a file or directory to a new location	cp [SOURCE] [DESTINATION]
mv	Can move or rename a file or directory	mv [SOURCE] [DESTINATION]
touch	Opens and closes a file. Can be used to create a file	touch [FILE]
rm	Remove one or more files or directories	rm [FILE]
cat	Concatenate files and prints to standard output	cat [FILE]
file	Determines the type of a file	file [FILE]
echo	Displays a line of text in the command line	echo [STRING]
>	The standard output of any command can be redirected to a file with a greater than symbol	[COMMAND] > [FILE] (this will create a new file or overwrite an existing file)
<	Redirects standard input to read from a file	[COMMAND] < [FILE]
>>	Redirects standard output to print to a file	[COMMAND] >> [FILE]

Command	Action	Execution
|	The pipe redirects standard output to go to another command as standard input	[COMMAND] | [COMMAND]
gedit	Open the files in a common graphical editor	gedit [FILE]
whoami	Prints your current username	whoami
users	Prints the usernames of users currently logged in to the current host	users
who	Prints information about users who are currently logged in	who
w	Displays information about the users currently on the machine, and their processes	w
groups	Shows the groups a user is in	Groups [USERNAME]
getent	Displays information from the password, group, or shadow file	getent [DATABASE] [KEY]
su	Allows you to become a different user	su [USERNAME]
sudo	Allows you to run commands as another user	sudo [COMMAND] (runs command as root) sudo [-u USERNAME] [COMMAND] (runs command as a specific user) sudo su (switch to root)
useradd userdel adduser deluser	Utility for adding or deleting users	useradd [LOGIN] userdel [LOGIN] adduser [USER] adduser [OPTIONS] [USER] (create a new user) deluser [USER] deluser [OPTIONS] [USER] (delete a user)
groupadd groupdel addgroup delgroup	Creates a new group or deletes an existing group	groupadd [GROUP] groupdel [GROUP] addgroup [OPTIONS] [GROUP] (create a new group) delgroup [OPTIONS] [GROUP] (delete a group)
gpasswd	Add or delete a user from a group	gpasswd -a [USER] [GROUP] (add a user to a group) gpasswd -d [USER] [GROUP] (delete a user from a group)

Command	Action	Execution
passwd	Change a user's password	passwd [LOGIN]
chown	Change ownership	chown [OWNER] [FILE]
chgrp	Change group	chgrp [GROUP] [FILE]
chmod	Change mode	chmod [MODE] [FILE]
apt update apt upgrade apt dist-upgrade apt install apt remove apt purge	Manages packages	apt update (Get the latest list of available packages) apt upgrade (Install the newest version of all packages currently installed) apt dist-upgrade (A more robust way to handle package dependencies and resolve conflict) apt install (Install a new package) apt remove (removes a package) apt purge (removes a package and removes old configuration files)
mkdir rmdir	Make and remove a directory	mkdir [DIRECTORY] (make a directory) rmdir [DIRECTORY] (removes a directory)
update-rc.d	Start a service or stop a service at boot	update-rc.d [SERVICE] enable (automatically start service at boot) update-rc.d [SERVICE] disable (don't automatically start service at boot)
/etc/init.d/	Start, stop, or get information about a service	/etc/init.d/[SERVICE] start (start the service manually) /etc/init.d/[SERVICE] stop (stop the service manually) /etc/init.d/[SERVICE] status (get the status of the service)
service	Runs a System-V init script passing its command as an argument	service [SCRIPT] [COMMAND]
systemctl	Command for managing services	systemctl enable [SERVICE] (configure service to start at boot) systemctl disable [SERVICE] (do not start the service at boot) systemctl start [SERVICE] (manually start the service now) systemctl stop [SERVICE] (manually stop the service now) systemctl status [STATUS] (displays the current status of the service)
more	Displays the contents of a file on the screen	more [FILE]

Command	Action	Execution
less	Opens a file for reading in the terminal	less [FILE]
diff	Compares two different files and displays the difference between the two files	diff [FILE1] [FILE2]
find	Searches a directory	find [DIRECTORY] [EXPRESSION]
locate	Finds files that match a pattern	locate [PATTERN]
updatedb	Updates the local database	updatedb
grep	Search files contents	grep [PATTERN] [FILE] (search the contents of file for a pattern) grep -R [PATTERN] [FILE] (if [file] is inside a directory, searches recursively for a pattern)
head	Outputting file parts	head [OPTION] [FILE] (prints the first 10 lines)
tail	Outputting file parts	tail [OPTION] [FILE] (prints the last 10 lines)
wc	Counting lines	wc -l [FILE] (counts the number of lines in a file)
ps	Listing current processes	ps [OPTIONS]
kill killall	Defaults to SIGTERM	kill –[SIGNAL] [PID] killall [name]
Ctrl+C	Kills a program in the foreground	Ctrl+C
top	Prints system summary information and list of running services	top
ifconfig	Network interface configuration	ifconfig -a (shows status of all network interfaces) ifconfig [INTERFACE] (shows status of a specific interface) ifconfig [INTERFACE] up (activates the interface) ifconfig [INTERFACE] [ADDRESS] netmask [MASK] (configures network interface)
route	Displays current network routes	route -n (does not resolve name) route add default gw [GATEWAY] (adds a default route through gateway) route add -net [TARGET] [NETMASK] mask gw [GATEWAY] (adds a route to the target network through gateway IP)

Command	Action	Execution
route	Displays current network routes	route add -net [TARGET] [NETMASK] mask dev [INTERFACE] (add a route to the target network through interface)
netstat	Viewing network connections	netstat –[OPTIONS]
IP address show	Shows interface information	IP address show
IP route show	Shows route information	IP route show
ss	Dump socket statistics	ss -A inet -anp (lists all open IP ports, including IPv4 and IPv6)
ufw	Command line firewall	ufw enable (turns on the firewall) ufw disable (turns off the firewall) ufw status verbose (shows the firewall status) ufw allow [PROGRAM] (allows a program through the firewall

Glossary of Terms

Account Lockout Duration	the number of minutes an account remains locked before automatically becoming unlocked.
Account Lockout Policy	limits how frequently someone can unsuccessfully attempt to login to an account.
Account Lockout Threshold	the number of failed log-on attempts that causes a user account to be locked out.
Advanced Package Tool (APT)	application used to manage packages on Linux distributions.
Audit Policy Settings	determine whether the OS audits process-related events such as process creation, process termination, handle duplication, and indirect object access.
Auth.log	tracks authentication events on Linux distributions
Authentication	the process of verifying the identity of a person or device. (username and password)
Backup	a copy of one or more files created as an alternate in the event the original data becomes unusable.
Bash	the default shell.
Basic Input Output System (BIOS)	the core software that performs the routine processes that connect the CPU with input, output, and storage devices.
Binary	a numeric system that only uses two digits, 0 and 1.
Biometrics	biological characteristics, such as fingerprints and retina patterns, which are unique to individuals.
Bit	the smallest unit of digital data. Can be a 1 or a 0, on or off.
Boot Process	process of loading the startup instructions from the computer's ROM, followed by loading the operating system from the current boot disk.
Boot Up Manager (BUM)	lists all currently running services and allows a user to start, stop, and disable them on a system.
Brute Force Attack	an attack that tests every possible combination of letters, numbers, and characters until the password is found.
Byte	eight bits.
Cache	stores recently used information so it can be quickly retrieved.
Central Processing Unit (CPU)	the component of a computer that processes instructions. In Task Manager, monitors current and past resource use.
Checksum	an alphanumeric code derived from the data in a file.
Clickbait	refers to a photo or headline which is tailored to grab your attention and prompt you to click through to learn more.

Client	device that asks for content.
Command Line Interface (CLI)	a text-based user interface (UI) used to view and manage computer files. Referred to as Terminal in Linux and Command Prompt in Windows.
Configuration File (Config File)	a local file used to control the operation of a program. It must be static.
Control Panel	the Windows OS main menu for most configuration settings (essentially the Windows cybersecurity toolbox).
Critical Infrastructure	the body of systems, networks, and assets that are so essential that their continued operation is required to ensure the security of a nation, economy, and public health and safety.
Crontab	primary cron configuration file that tells cron what to run is located at /etc/crontab.
Cups	printing service for Linux.
Cyber Ethics	the code of acting responsibly when using computers and mobile devices.
Cyber Hygiene	basic personal practices that keep computers and data safe.
Cybersecurity	refers to all the tools we use and actions we take to keep computers, networks, and information safe and available for those who need it, and unavailable for those who should not have it.
Data Breach	a confirmed incident where sensitive data has been accessed in an unauthorized fashion.
Decapsulate	the process of removing the layers around a packet to retrieve information.
Default Gateway	the node in a computer network that acts as a gate between two networks.
Demodulate	process of extracting the original information signal from a carrier wave.
Denying Traffic	in UFW, denying the traffic without informing the connection that it has been blocked.
Dependency	a component, file or package that is required for a program to work correctly.
Desktop Environment (DE)	a graphical user interface (GUI) that enables a user to access and manage the important and frequently used features of an operating system.
Dictionary Cracking	an attack used to crack passwords by testing words and combination of words found in the dictionary or a slightly shorter list of words known to be commonly used in a password.
Discretionary Access Control (DAC)	restricting access to objects based on the user's identity or groups to which they belong.
Distribution	used to denote a specific variant of Linux operating systems, also referred to as flavors.
Domain Name System (DNS)	used for mapping alphabetic names to to numeric IP addresses.
Dpkg.log	tracks software events on Linux distributions

Dynamic Host Control Protocol (DHCP)	auto assigns IP addresses to clients.
Dynamic Library	separate files outside of the executable file that share objects. Also referred to as shared libraries. In Linux, commonly end with the ".so" suffix.
Dynamically Linked Libraries (DLL)	a file that contains a library of functions and information accessed by Windows program.
Encapsulate	packets wrapped in layers.
Encryption	the process of altering data to an unrecognizable form (so that it is unreadable by anyone who does not have a decryption key). Often used to protect sensitive data. Requires decryption key to decode.
Ethernet	computers connected on a network over a wired connection.
Event Viewer (Linux)	a security tool that allows you to view records of changes and other events that have happened on a computer.
Event Viewer (Windows)	a default administrative tool found in Windows that allows a user to view events, errors, and information about the operating system.
File Transfer Protocol (FTP)	a communication protocol used for transferring files from a server to a client.
Firewall	designed to prevent unauthorized access to a system. Can be implemented via hardware or software. A barrier that sits in between a secure device or network and a less secure or open network or device, such as the internet.
GNU Findutils	set of programs to help make it easy to find files on a system.
GNU Network Object Model Environment (GNOME)	a GUI and set of computer desktop applications for Linux distributions.
Graphical Uncomplicated Firewall (GUFW)	the GUI interface of the Uncomplicated Firewall (UFW).
Graphical User Interface (GUI)	a user interface that includes graphical elements.
Group ID (GID)	how groups are identified in Linux and are typically reserved for system use. A GID of 0 refers to the root group and GID of 100 represents the users group. Also, a name that associates a system user with other users sharing something in common.
Group Policies	settings used by an administrator to apply security policies across all computers on a network or for specific groups.
Handle	a Windows utility that lets a user find out what processes have a file open, or what files a process has open.
Hardware	the physical components of the computer system.
Header	piece of data that is attached to the front of some data that we want to send over the Internet.
Home Directory	the current working directory when a user logs in.

Hop	the trip a data packet takes from one router or intermediate point to another point in the network.
Host	term used for any kind of computer on a network.
Hypertext Transfer Protocol (HTTP)	language that clients and servers use to communicate with each other and transfer data over the web. Operates on the Application Layer.
Hypertext Transfer Protocol Secure (HTTPS)	where encrypted HTTP connections take place; designed for secure data transmission with encryption.
Init	In Linux OS, the first process executed by the kernel.
Integrated Control Access Control Lists (icacls)	the command line utility that can be used to modify NTFS file system permissions in older versions of Window Operating Systems.
Internet	a global wide area network that connects computer networks (a network of networks).
Internet of Things (IoT)	an umbrella term that is dedicated to any device connected to the internet.
Internet Protocol (IP)	unique address for a device on a network.
Internet Protocol version 4 (IPv4)	the most common system of logical addressing in a four 8-bit octet or 32-bit format, which looks like 123.123.123.123. Each three-digit octet can be assigned a number from 0 to 255.
Internet Protocol version 6 (IPv6)	logical addressing with 128 bits.
Internet Service Provider (ISP)	provides access to the Internet.
Kernel	the most fundamental layer of an operating system. Manages system resources for memory, processes, and input and output devices.
Library	a collection of pre-compiled pieces of code.
LightDM	a display manager in Ubuntu that displays what the login screen looks like.
Linux	an open-source family of operating systems, similar to Unix, Windows and OS X. Linux can come in many different flavors, including Ubuntu, Mint, Fedora, and Red Hat, just to name a few.
Local Area Network (LAN)	network of connected devices that exist within a specific location.
Local Security Policy	set of information about the security of a local computer.
Log	a file that contains a list of events.
MAC Address	the physical address.
Malware (malicious software)	term for any software that is intentionally designed to cause harm or do illegal and unethical activities.
Maximum Password Age	dictates how long a user can use the same password.
Memory	can refer to any medium of data storage, typically refers to RAM.
Minimum Password Age	the number of days a password must be used before it can be changed by a user.

Minimum password length	the least number of characters that can make up a password for a user account.
Modem	converts (modulates and demodulates) between analog (cable or DSL) signals and digital signals.
Modulate	the process of converting data into radio waves.
Netstat	a command line TCP/IP networking utility.
Network	a group of computers that can talk to one another.
Network Address Translation (NAT)	allows your internal Private IP address to connect to to local servers and host via the Internet.
Network Interface (NIC)	component that provides networking capabilities for a computer.
Nslookup	used to check the IP address in the Domain Name System for a website's friendly name.
Octet	sequence of eight bits.
Open Source	software that anyone may use, modify, or distribute.
Operating System (OS)	the software that manages or executes the hardware system and its physical resources, including memory, storage and the central processing unit or CPU. The OS connects all the software on your computer to the resources. Examples include Apple macOS, Microsoft Windows and Linux.
Owner	the user who owns a file.
Package Manager	controls and inventories packages in Linux.
Packages	in Linux, a package is a collection of many files bundled into a single file, which makes them easier to handle.
Packet	information packaged to allow routers to read source and destination addresses.
Packet	a small amount of data sent over a network.
Packet Tracer	a visual simulation tool designed by Cisco Systems that allows users to create network topologies.
Parent Process Identifier (PPID)	the PID of the process that created it.
Passphrase	a password composed of a sentence or a combination of words, can include letters, numbers, and symbols.
Password	the most common type of authentication.
Password cracking	the process of using various techniques to discover passwords OR in Linux, the process of recovering passwords from data.
Password Management Systems	a software application that stores and manages a user's credentials for various online accounts.
Password Policy	policies governing unsuccessful attempts to log into an account.

Personal Identifiable Information (PII)	any information that is potentially identifying to a specific person (social security numbers, credit card numbers, home addresses, etc.).
Phishing	refers to spoofing or fraud attempts perpetrated by random attackers against a wide number of users. (e.g., Fraudulent emails and websites).
Ping	is used to verify connectivity to a given IP address is reachable.
Pluggable Authentication Modules (PAM)	used for authentication by almost all Linux distributions.
Pre-Shared Key	a shared secret, like a password, shared between two parties.
Private IP Address	IP address only visible on the local network.
Privilege Access Manager (PAM)	allows for control over the elevated or privileged access by setting access and permissions for users, accounts, processes, and systems throughout an IT environment.
Process Identifier (PID)	unique number assigned to running processes and can be reused after a process dies.
Procmon	a Windows utility that monitors system calls made by processes.
Protocol	a standard set of rules that allow electronic devices to communicate.
PsExec	a Windows utility that allows the user to run programs as other users, including systems.
Public IP Address	IP address that is displayed on a website and is visible to the whole internet.
Random Access Memory (RAM)	a hardware component that determines how much memory the operating system can use.
Rejecting Traffic	in UFW, denying traffic and informing the outside connection that it's data packet has been blocked.
Restore	to return to a former condition.
Root	the top-level directory of a file system, which is represented as a single forward slash (/). Also a superuser with a UID of zero.
Router	Default gateway for internet traffic.
Secure Shell (SSH)	a network protocol that encrypts communication between two computers.
Server	hosts that provide content.
Service Set Identifier (SSID)	wireless network name.
Services.msc	processes that run invisibly in the background on a computer, such as Windows Defender and Windows Firewall. These programs are not generally visible from the desktop, and if they are enabled, they will load up and run automatically when the computer is turned on.
Shadow File	stores encrypted passwords.
Shell	a command line interface that processes commands from users so that the OS can understand and perform an action or function.

Smishing	phishing attempts sent by SMS (text messaging).
Snap-In	refers to an object that can be attached to another object to function as a whole.
Sniffing	a process of monitoring and capturing data packets passing through a network.
Social Engineering	manipulation of people into giving up their personal information.
Socket Layer (SSL)	a secure protocol for transmitting information between a client (browser) and the server (web server). SSL drives the secure part of https://
Software	term that refers to computer programs, applications, and scripts.
Spear phishing	the act of sending malicious emails to specific and well-researched targets while purporting to be a trusted sender.
Standard Error (stderr)	an output stream used by programs to print error messages.
Standard Input	characters you type into the terminal, input data.
Standard Output (stdout)	an output stream to which a program writes the text.
Static IP address	IP address that is manually assigned by a computer.
Static Library	a collection of objects that are compiled to produce an object file and a stand-alone executable. In Linux, commonly end with the ".a" suffix.
STIME	the starting time of a process.
Subnet Mask	tells us which bits in an IP address are used to identify the Network, and which bits are used to identify a Host.
Swap Space	virtual memory.
Switch	has several Ethernet ports, which allow connections to a wired Local Area Network (LAN).
Syntax	the set of rules that define what the various combinations of symbols mean.
Syslog	tracks operating system events on Linux distributions.
Systemd	software suite that provides an array of system components for Linux distributions.
Task Manager	a default feature in Windows that provides details about programs and processes running on the computer.
TCP Syncookies	technique that can help prevent SYN flood attacks.
Telnet	a network protocol used to establish a remote connection.
Terminal	Linux's version of the Command Line Interface, a text-based user interface (UI).
Terminal Pager	allows a user to view text files on the console.
Time (in terms of running processes)	the total amount of CPU time used by the process.
TTY	name of the console or terminal that a process is running under.

Two-Factor Authentication	an electronic authentication method in which a device user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to identify oneself. Factors include something you are (such as a biometric, fingerprint, or voice), something you have (such as an ATM card, phone or fob), and something you know (such as a personal identification number, password or a pattern).
Ubuntu Password File	contains user information and usually no longer contains password files.
Uncomplicated Firewall (UFW)	in Ubuntu, the built-in firewall.
Update Manager	in Linux, an easy way to install updates.
Upstart	an alternative init system initially developed for Ubuntu but can be used on other Linux distributions.
User ID (UID)	a number assigned by Linux to each user on the system and are stored in the /etc/passwd file.
User Interface (UI)	used to control a software application or hardware device.
User List	contains a comma-separated list of users that belong to a group. If a user has this group set as his or her “primary group”, then this user belongs to this group and may or may not be listed in in the “User List” field.
Username	the name associated with the user account and is primarily used to log in by humans and is a form of identification.
Virtual Machine (VM)	an environment, such as a program or operating system, that does not physically exist but is created within another environment. It does not have hardware, a power supply, or other resources that would allow it to run on its own.
Vishing	refers to attempts by thieves to get confidential information over the phone.
Web Browser	software application used for retrieving, presenting, and navigating information resources on the World Wide Web.
Wi-Fi Protected Access (WPA)	security protocol designed to secure wireless networks, referred to as the transitional standard. This protocol is no longer used.
Windows Defender	built-in feature that protects against known spyware, viruses, and malware.
Windows Registry	a database of settings.
Wired Equivalent Privacy (WEP)	security protocol for Wi-Fi networks that is no longer secure.
Wireless Access Point (WAP)	broadcasts a wireless network.
WPA2 PSK	security protocol with a Pre-Shared Key designed to secure wireless networks. Referred to as the de facto standard.
Xorg.0.log	tracks desktop events on Linux distributions

This page is intentionally blank.

CyberPatriot Code of Conduct

AFA CYBERCAMP
PARTICIPANT CODE OF CONDUCT

Updated 5/19/2023

As a participant in an AFA CyberCamp, I agree to the following terms:

1. I will consider the ethical and legal implications of my online actions during my time in the AFA CyberCamp, and will demonstrate honesty, fairness, and integrity throughout the camp activities and competition.

2. I will not conduct, nor will I condone, any actions that attack, hack, penetrate, or interfere with another team's or individual's computer system, nor will I use the cyber defense skills I learn in the AFA CyberCamp to develop hacking or other offensive skills.

3. I will not disclose any of the training material or any other confidential information that I will receive to anyone other than my peers enrolled in this specific AFA CyberCamp.

4. I will protect all the confidential information that I receive and will not make any efforts to recreate, sell, or design a product that contains the confidential information.

5. I will not keep or download any instances of the images used during the AFA CyberCamp after the conclusion of the event.

6. I will not visit inappropriate websites while participating in the AFA CyberCamp.

7. I will be respectful and courteous to fellow campers, staff, and guests at all times. I will not participate in or condone cyberbullying, which includes such behaviors as teasing, threatening, intimidating, humiliating, sexual harassment, racial harassment, and stalking.

8. I understand that failure of myself or any of my teammates to participate actively in all AFA CyberCamp activities will render our team ineligible for any team recognition, regardless of our recorded score.

_____
Print Name

_____
Signature

_____
Date

This page is intentionally blank.

CyberPatriot is the Air & Space Forces Association's National Youth Cyber Education Program.

For additional information visit www.uscyberpatriot.org.