Why Cybersecurity?

Professional Opportunities

Cyberseek

JOB OPENINGS IN THE U.S.
313,735

JOB OPENINGS IN VIRGINIA
33,530

JOB GROWTH RATE
28%

MEDIAN SALARY
$95,510

Cyberseek and US Department of Labor, Bureau of Labor Statistics

Pathways to Success

HIGH SCHOOL

Cybersecurity is an exciting career choice! Any job in the field will require some sort of credential or degree.

BACHELOR'S DEGREE

ENTRY-LEVEL POSITIONS	AVERAGE SALARY
Cybersecurity Specialist/Technician	$81,000
Cybercrime Analyst	$88,000
Incident Analyst/Responder	$70,000
IT Auditor	$85,000

ASSOCIATE'S DEGREE

ENTRY-LEVEL POSITIONS	AVERAGE SALARY
Network Support Specialist	$48,000
Computer Forensics Analyst	$59,000
Cybersecurity Specialist	$60,000

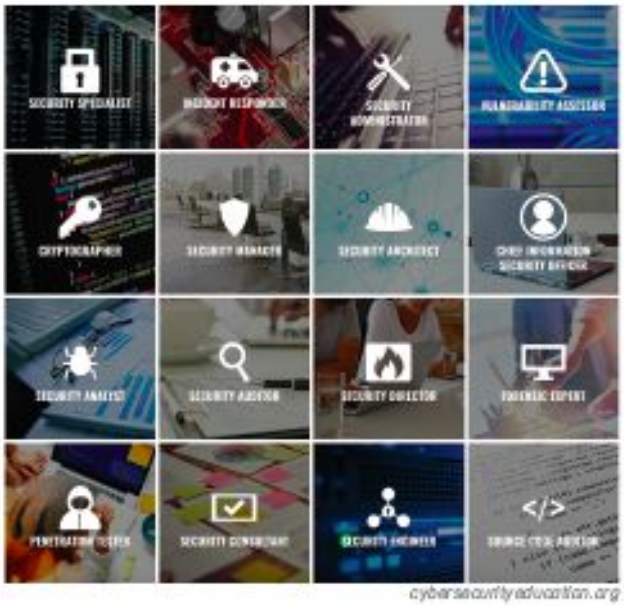
CYBERSECURITY CERTIFICATION

ENTRY-LEVEL POSITIONS	AVERAGE SALARY
IT Support Specialist	$40,000
Associate Cybersecurity Analyst	$37,900

US Department of Labor, Bureau of Labor Statistics

Types of Careers

Cybersecurity professionals are needed in every industry and organization to protect information systems and data from becoming compromised.



cybersecurityeducation.org

Connect with us
@vacyberrange
virginiacyberrange.org

VIRGINIA CYBER RANGE

Get Started In Linux Here!

Beginner Linux Command Line

`cd`	Change directory
`cd -`	Change to previous directory
`cd ~`	Change to $HOME directory
`cd ../`	Change to parent directory
`pwd`	Print working directory
`ls`	List files
`ls -la`	List long listing, all files
`ls -ltr`	List long listing, by age, in reverse
`man ls`	Read the user manual for a command.
`mkdir`	Make a directory
`mkdir -p 1/2`	Make dir 1 along with subdir 2
`rmdir dir1`	Remove empty directory dir1
`rm file`	Remove file
`rm file*`	Remove all files starting w/"file"
`rm -r oldir`	Recursively remove oldir & contents
`touch fileX`	Create empty file fileX, or update its time
`cat f1 f2`	Concatenate and print files f1 & f2
`nano file1`	Nano editor, create or edit file1 (easy, simple)
`vim file1`	vim editor, create or edit file1 (difficult, powerful)
`leafpad f1`	Leafpad graphical file editor (in XCFE, easiest)
`ristretto f.jpg`	Default graphic viewer in XFCE
`wget www`	Web/file downloader (www= a full URL)
`curl -L www.ex.com/script1.sh | bash -C`	Download & run a www hosted script locally
`grep XX [file]`	Filter & print any lines in file with XX in it
`grep "^Nmap"`	Filter & print any lines ^(beginning with) "NMap "
`somecommand | mail -s "Subject" me@example.com`	Send output from somecommand to email to email me@example.com
`date`	Print the time/date
`date +%Y-%m-%d`	Prints formatted YYYY-mm-dd date
`$(date +%Y-%m-%d)`	Run embedded command and return text
`cat /etc/passwd | cut -f1 -d":" | mail -s"Usernames on $HOST" me@example.com`	Print out all usernames on system, cut the 1st column, and email it to me.
`sudo su -`	Super User Do, run the "su -" command to become root (if allowed)
`ps auxw | less`	List all processes, their PID #s, stats and process names (with less pager)
`pstree | less`	List all processes in a relational tree format (with less pager)

Learning Linux Cyber Security!

See your Cybersecurity teacher about getting an account on VirginiaCyberRange.org

OR

1) Download Kali "Weekly amd64":
www.kali.org

2) Burn→CD or dd write→USB stick:
Win: use Win32 Disk Imager
Lin:
`sudo dd if=kali.iso of=/dev/sdX`
(where X = the dev file of your thumb drive)

3) Reboot PC, hitting F12 to boot from USB

4) Learn more about Kali Linux Commands!

Congrats! You're now learning Kali Linux!

Networking & Network Security Commands

`ifconfig eth0`	Show IP and VLSM(255) subnet mask
`ip addr show eth0`	Show IP and CIDR(/24) subnet mask
	Number of IPs on your LAN = 2^(32 - CIDR#) e.g. 2^(32-24)= 256 IPs
`hostname -f`	Show the machine's (f)ull hostname
`hostname -i`	Show (I)P address of the hostname
`ping -c 3 8.8.8.8`	Ping google's nameserver (8.8.8.8) three times
`netstat -antp`	*Show (a)ll local to remote (T)CP IP/port connections & (p)rocess name
`iptables -L -n`	*(L)list pf firewall settings (n)umerically
`route -n`	Show IP routing tables (n)umerically
`nmap -sP [IP/N]`	**Ping scan the [P/subnet address space of hosts
`nmap -sP -nS -oG..`	**Ping scan (provide IP or network) and output in greppable format
`nmap -oG - ..|`	**Same, but pipe scan stdOut [-] to other command(s) (like grep)
`nmap -O -n - [IP/N]`	**Nmap OS fingerprint scan w/no DNS
`nmap -O --osscan-limit [IP/N]`	**Limit OS port scan to promising targets
	More namp usage: https://www.stationx.net/nmap-cheat-sheet/

`nc -lnk [IP#] [port#]` Have netcat listen locally on [your IP#] and [port#] * root needed for ports under 1024

`echo "can you hear me?" | nc [remoteIP] [remote port]`
Send a message to a remote process/listener on remote IP on remote port#

`nikto -h www.example.com` **Scan webserver for known vulnerabilities

VIRGINIA CYBER RANGE

* - Command must be run as root, or via `sudo command` .

** - **WARNING!** Do not run this without the target-host or network owner's permission.