Recon and Scanning Intro

whoami

- Whoami
  - Matt Fiely
  - Titan on slack

- What do I do?
  - Student
  - Intern in the security realm

Disclaimer

- Hacking without written consent is **illegal**
  - **DO NOT** practice on systems you don’t own!!!!

- I am not a lawyer
  - I can’t help you if you use this knowledge for evil

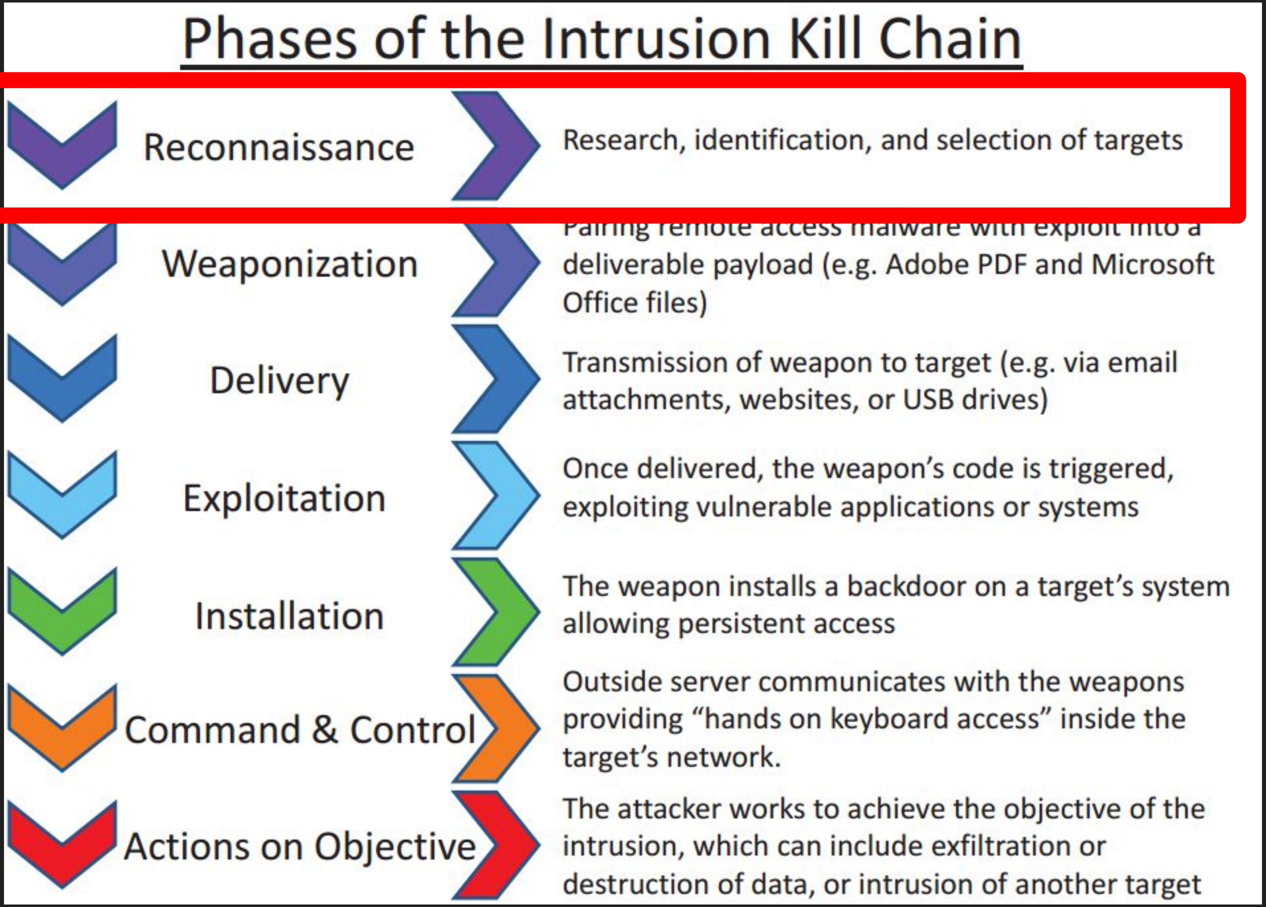
- **What I’m going over today is for educational purposes only!**

Prerequisites

- Kali
  - Can use Windows, I will be using Kali
- Metasploitable

What is recon?

- Aka reconnaissance
- First step in ***CYBER KILL CHAIN***
- Scoping out a target
    - Looking for possible vulnerabilities to exploit



Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

By U.S. Senate Committee on Commerce, Science, and Transportation - http://www.public.navy.mil/spawar/Press/Documents/Publications/03.26.15_USSenate.pdf, Public Domain, https://commons.wikimedia.org/w/index.php?curid=49822676

Types of recon

Passive

- Gain information about a target without interacting

Active

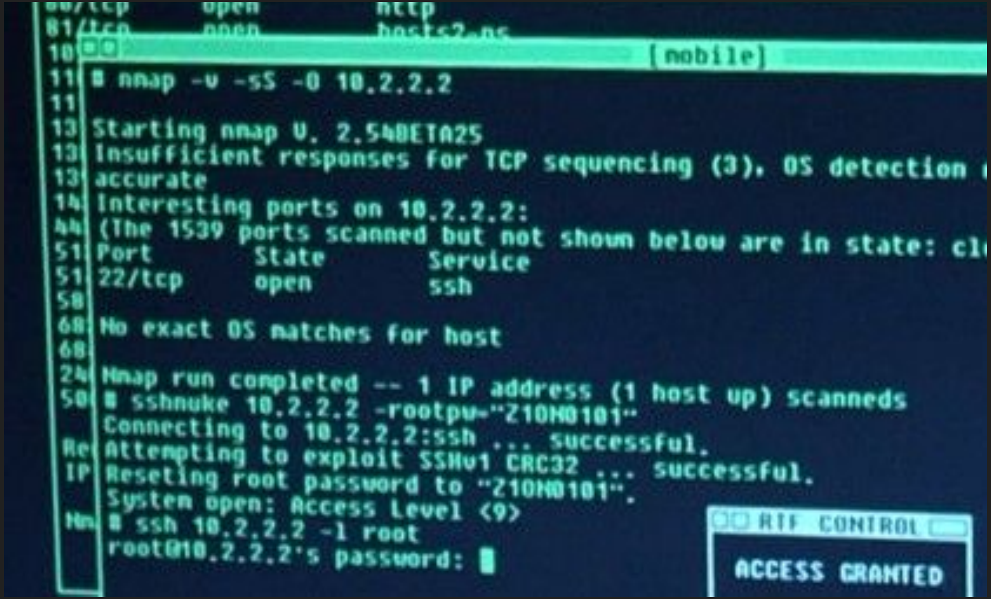
- Directly interacting with a target

Active

- Directly interacting with target
- Nmap
- Nessus
- Nikto

- Many more

nmap



```
# nmap -v -sS -O 10.2.2.2

Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: cl
Port       State       Service
22/tcp     open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

nmap

- Primary focus is port scanning
  - Designed to check hosts for open (listening) ports
- Other features
  - Host Discovery
  - Software Version Detection
  - Operating System detection
  - Script interaction with targets
    - Nmap scripting Engine (NSE)

nmap address probing

- Probing before scanning
  - Is there a host?
- If target is on the same subnet
  - ARP request
  - WHO HAS THIS IP????
- If the target is on a different subnet
  - ICMP Echo Request aka PING
  - TCP SYN to port 443
  - TCP ACK to port 80
  - ICMP Timestamp Request

# nmap timing options		nmap -t

- 0: paranoid
  - One packet every 5 minute
- 1: sneaky
- 2: polite
- 3: normal (default)
  - Multiple packets as soon as possible
- 4: aggressive
- 5: insane
  - Nmap will not spend more than 15 minutes on a target, will not wait longer than 0.3 seconds for a response

Ex: nmap -t3 X.X.X.X

nmap output options nmap -o

- Normal
- Greppable
- XML
- 1337 Format
- grepable output

```
Ex: nmap -oN nmap-output.txt
```

nmap commonly used flags

- No flags
    - Just checks if ports are open
    - Only scans top 1000 most popular ports
    - Ex: nmap X.X.X.X
- -sP
    - Ping scan target(s)
        - Good for mapping the network
    - Ex: nmap -sP X.X.X.X

nmap commonly used flags

- -p
    - Specify which port(s) you want to scan
    - Ex: nmap -p 80 X.X.X.X
- -v
    - Verbose
    - Gives more detail about what the scan is doing
    - Ex: nmap -v X.X.X.X
- -O
    - Determine the operating system of the target
    - Ex: nmap -O X.X.X.X
- -sV
    - Determine version of software running on an open port
    - Ex: nmap -sV X.X.X.X

nmap commonly used flags

- -A
  - Combination of operating system scan, version scan, script scanning, traceroute
  - This is very helpful if you have a small scope and know your targets

Examples

- Nmap scan multiple IP addresses
  - Example:
    - nmap 192.168.1.1-50
    - nmap 192.168.1.1/24
    - nmap -iL IPs.txt
- Nmap scan specific ports
  - Example:
    - nmap -p 1-1000 127.0.0.1
    - nmap -p- 127.0.0.1
- List of available nmap scripts
  - /usr/share/nmap/scripts

Now your turn

- Launch Kali, Metasploitable on Host-Only

- Try to find the IP of your metasploitable box
- See if you can determine which ports are open
- What is the operating system?
- Can you see what services are running?

Walkthrough

- In kali open a terminal - ifconfig
  - Note the IP Address
- Get a scope of targets
  - nmap -sP X.X.X.X-X
    - This is pinging everything on your network
- nmap -A X.X.X.X -oN nmap-output.txt
  - This way our output will be saved in a file

Nikto

- Web server vulnerability scanning tool
- Looks for more than 3500 potentially dangerous files
- Looks for server version-specific problems
- Can sometimes find XSS
- Is really good for well known issues

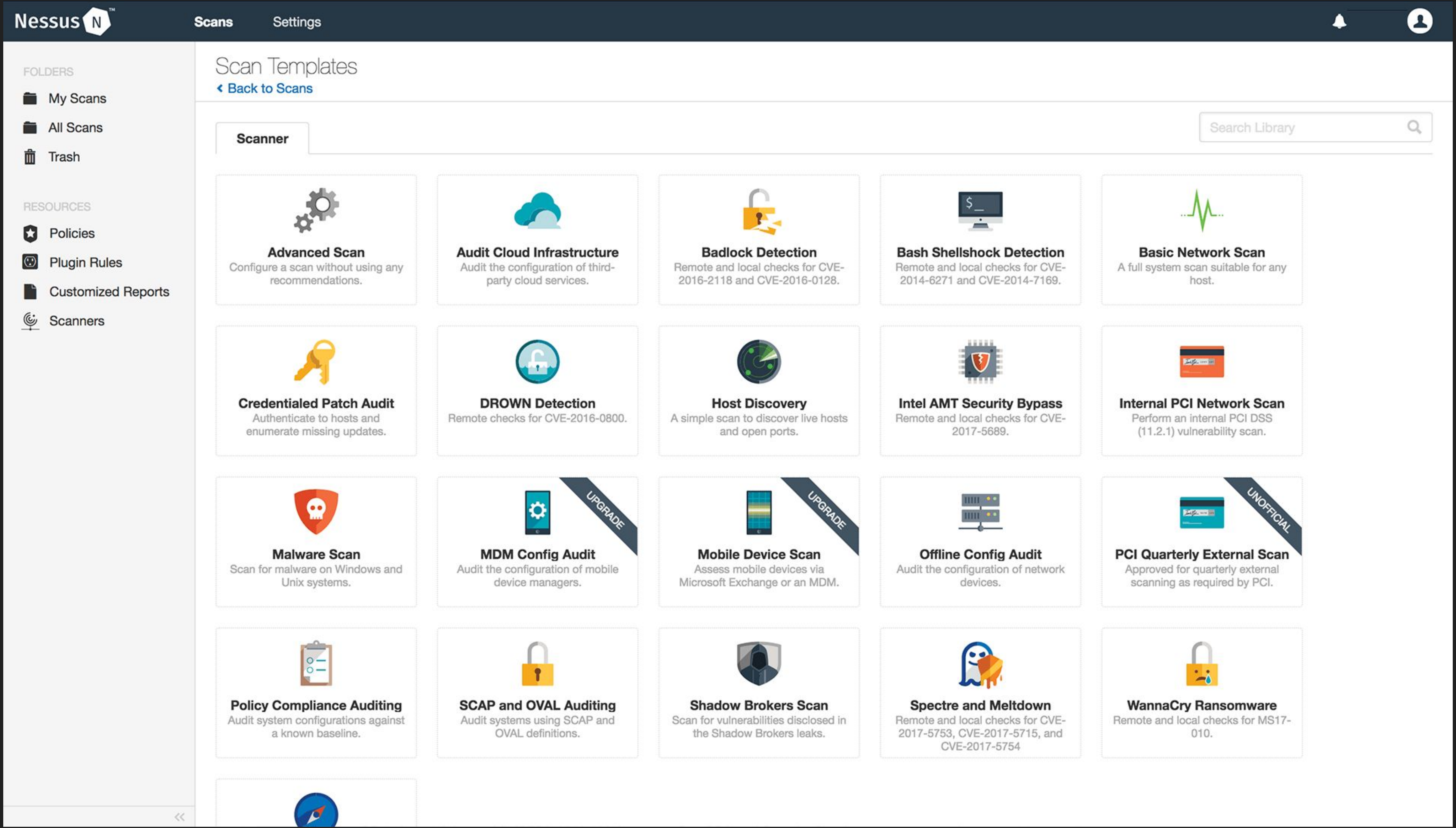
Nikto Hands on

- Given what we saw in our nmap report
  - There is a webserver running

- Let’s try
  - Nikto -h X.X.X.X:80
  - Nikto -h HTTP://X.X.X.X/mutillidae -port 80 -output nikto.txt

Nessus

- Vulnerability scanning
- Over 1200 vulnerability checks on a target
- Updated regularly with vulnerability and related information
- Patching (and exploitation) Suggestions
- GUI Based



FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

Scan Templates

‹ Back to Scans

Scanner

Search Library

Advanced Scan
Configure a scan without using any recommendations.

Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

DROWN Detection
Remote checks for CVE-2016-0800.

Host Discovery
A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan
Scan for malware on Windows and Unix systems.

UPGRADE
MDM Config Audit
Audit the configuration of mobile device managers.

UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit
Audit the configuration of network devices.

UNOFFICIAL
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing
Audit system configurations against a known baseline.

SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.

Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Questions?