Kaitlin Hoffmann

Office Hours:

SH 243 Monday 1:15 - 3:15 PM. Tuesday 2:45 - 4:45 PM.

Email: hoffmank4@newpaltz.edu

NMAP

NETWORK SECURITY

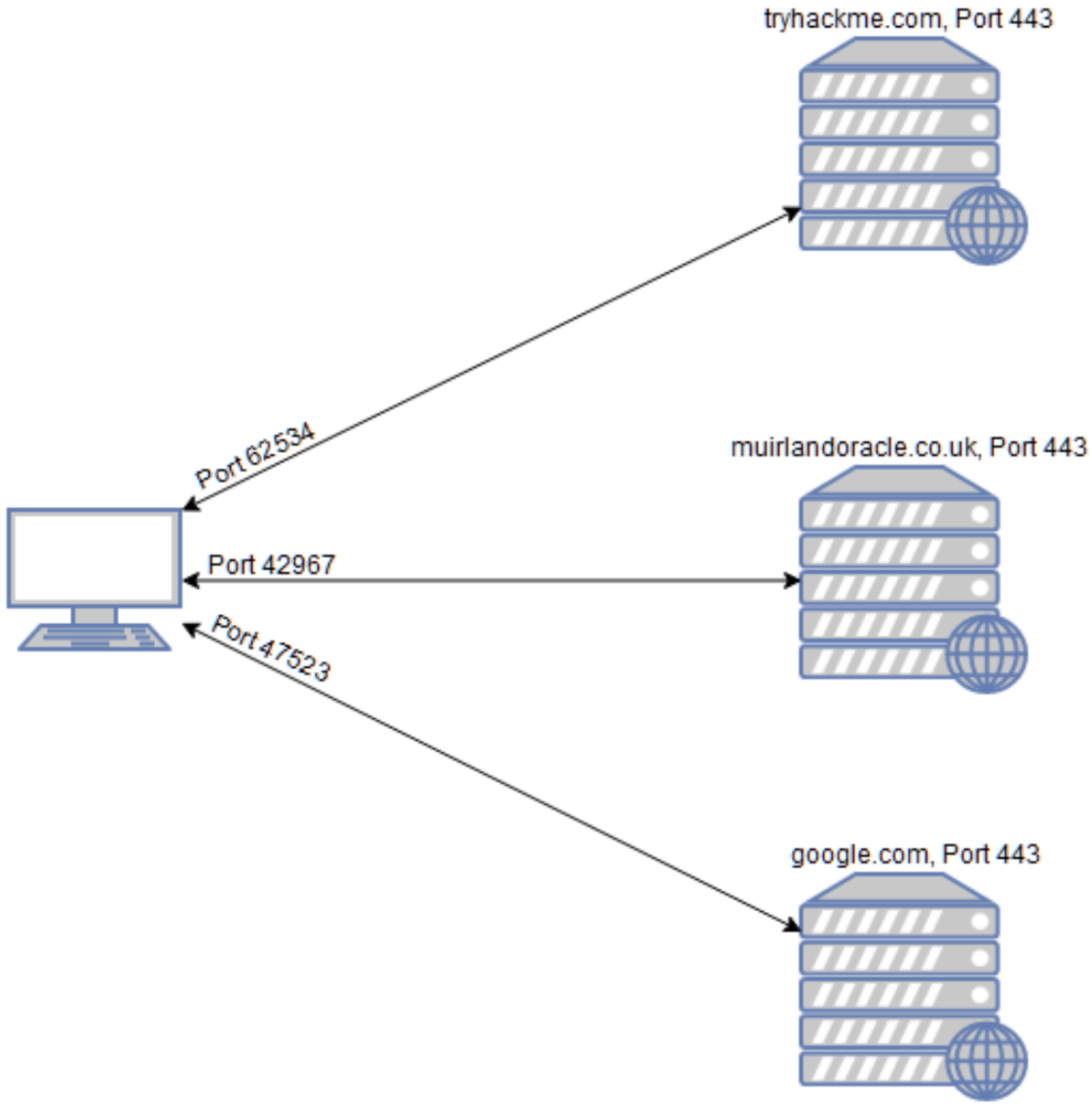
OBJECTIVES

- Introduction
- Port Scanning
- OS and Service Scanning
- TCP and UDP Scanning
- Nmap Scripting Engine

KNOWLEDGE IS POWER – PORT SCANNING

- When given an IP address to perform a security audit on, we need to get info on the landscape of what we are attacking (which services are running on your target).
- First stage of establishing this "map" of the landscape is **port scanning**.
- When a computer runs a network service, it opens a networking construct called a "port" to receive the connection. Ports are necessary for making multiple network requests or having multiple services available. Example…

- When you connect to numerous websites at the same time, your computer opens up a different, high-numbered port (at random), which it uses for all its communications with the remote server.
- Every computer has a total of 65535 available ports; however, many of these are registered as standard ports (443 for HTTPS, 25 for SMTP, etc.)



NMAP

- **Nmap** will connect to each port of the target in turn.
- Nmap is a network scanner. It's used to discover hosts and services on a computer network by sending packets and analyzing the responses. https://nmap.org/
- Depending on how the port responds, it can be determined as being open, closed, or filtered (usually by a firewall). Next, we can find which services are running on each port by also using Nmap.

NMAP — IMPORTANT!!!!!!!!!!

- Scanning IP addresses can be **ILLEGAL**!!!!! DO NOT use this on any site without permission!!
- You can use it on hydra.newpaltz.edu (I promise not to turn you into the authorities 😁). However, do not try to execute any attacks on it. Instead, you can create a VM that you attack and test Nmap and other active recon tools on.

KNOWLEDGE IS POWER – PORT SCANNING

- Simplest Nmap port scan command: `nmap -p 80 X.X.X.X`

```
kaitlinhoffmann ~ $ nmap -p 80 hydra.newpaltz.edu
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 13:14 EST
Nmap scan report for hydra.newpaltz.edu (50.74.239.202)
Host is up (0.025s latency).
rDNS record for 50.74.239.202: rrcs-50-74-239-202.nyc.biz.rr.com

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
kaitlinhoffmann ~ $
```

https://nmap.org/download.html

PORT SCANNING — TOP PORTS

- Using `--top-ports` parameter along with a specific number lets you scan the top X most common ports for that host:

```
kaitlinhoffmann ~ $ nmap --top-ports 20 50.74.239.202
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 13:20 EST
Nmap scan report for rrcs-50-74-239-202.nyc.biz.rr.com (50.74.239.202)
Host is up (0.022s latency).

PORT     STATE    SERVICE
21/tcp   closed   ftp
22/tcp   open     ssh
23/tcp   closed   telnet
25/tcp   filtered smtp
53/tcp   closed   domain
80/tcp   open     http
110/tcp  closed   pop3
111/tcp  closed   rpcbind
135/tcp  filtered msrpc
```

PORT SCANNING — FILES

- Scan hosts and IP addresses reading from a text file.
- Create your text file with your IP addresses and/or domains:

```
192.168.1.106
cloudflare.com
microsoft.com
securitytrails.com
```

- Command to scan hosts from file: `nmap -iL` *`fileName.txt`*
- Example...

PORT SCANNING — FILES

```
kaitlinhoffmann Module 13 $ cat addresses.txt
192.168.1.1
hydra.newpaltz.edu
127.0.0.1
```

```
kaitlinhoffmann Module 13 $ nmap -iL addresses.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 19:54 ES
Nmap scan report for Docsis-Gateway (192.168.1.1)
Host is up (0.0047s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    filtered ssh
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
```

PORT SCANNING — SAVE OUTPUT

- Save your Nmap scan results to a file. Command:
- `nmap -oN fileName.txt ipAddress`
- Example:

```
kaitlinhoffmann Module 13 $ nmap -oN results.txt hydra.newpaltz.edu
kaitlinhoffmann Module 13 $ cat results.txt
# Nmap 7.93 scan initiated Wed Dec  6 19:58:20 2023 as: nmap -oN results.t
Nmap scan report for hydra.newpaltz.edu (50.74.239.202)
Host is up (0.022s latency).
rDNS record for 50.74.239.202: rrcs-50-74-239-202.nyc.biz.rr.com
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  filtered smtp
80/tcp  open     http
135/tcp filtered msrpc
```

OS AND SERVICE SCANNING

- Nmap can also be used to find the operating system used on a service as well as software details.
- The –A parameter enables you to perform OS and service detection
- A **timing template** is a set of parameters in Nmap that affect how quickly and aggressiveness of a scan. –T4 is used for a faster and more aggressive. https://www.educative.io/answers/what-are-nmap-timing-templates
- Command: `nmap –A –T4 ipAddress` https://www.educative.io/answers/what-are-nmap-timing-templates
- Example…

OS AND SERVICE SCANNING

```
kaitlinhoffmann Module 13 $ nmap -A -T4 hydra.newpaltz.edu
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 20:01 EST
NSOCK ERROR [0.0790s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for hydra.newpaltz.edu (50.74.239.202)
Host is up (0.026s latency).
rDNS record for 50.74.239.202: rrcs-50-74-239-202.nyc.biz.rr.com
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE    SERVICE      VERSION
22/tcp  open     ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0
| ssh-hostkey:
|   256 5d07ea2e11b719162237d5357fdc08b6 (ECDSA)
|_  256 3bde3a5641bc6ec697e05d41f397b41e (ED25519)
25/tcp  filtered smtp
80/tcp  open     http         Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Did not follow redirect to https://hydra.newpaltz.edu/
|_http-server-header: Apache/2.4.52 (Ubuntu)
```

SERVICES AND DAEMONS VERSIONS

- Detect service/daemon versions:
- `nmap -sV` *`ipAddress`*

```
kaitlinhoffmann Module 13 $ nmap -sV hydra.newpaltz.edu
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 20:08 EST
NSOCK ERROR [0.0760s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for hydra.newpaltz.edu (50.74.239.202)
Host is up (0.022s latency).
rDNS record for 50.74.239.202: rrcs-50-74-239-202.nyc.biz.rr.com
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE    SERVICE      VERSION
22/tcp  open     ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
25/tcp  filtered smtp
80/tcp  open     http         Apache httpd 2.4.52 ((Ubuntu))
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     ssl/http     Apache httpd 2.4.52
445/tcp filtered microsoft-ds
Service Info: Host: hydra.newpaltz.edu; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit
```

SERVICES AND DAEMONS VERSIONS

- Example on localhost:

```
kaitlinhoffmann Module 13 $ nmap -sV localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 20:10 EST
NSOCK ERROR [0.0770s] ssl_init_helper(): OpenSSL legacy provider failed to loa
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000046s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 8.0.28
5900/tcp open  vnc     Apple remote desktop vnc
Service Info: OS: Mac OS X; CPE: cpe:/o:apple:mac_os_x

Service detection performed. Please report any incorrect results at https://nm
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

TCP AND UDP PROTOCOLS

- Scan both TCP or UDP protocols:
- Standard **TCP** scanning output: `nmap -sT` *`ipAddress`*

```
kaitlinhoffmann Module 13 $ nmap -sT hydra.newpaltz.edu
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 20:18 EST
Nmap scan report for hydra.newpaltz.edu (50.74.239.202)
Host is up (0.022s latency).
rDNS record for 50.74.239.202: rrcs-50-74-239-202.nyc.biz.rr.com
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  filtered smtp
80/tcp  open     http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds
```

TCP AND UDP PROTOCOLS

- Scan both TCP or UDP protocols:
- Standard **UDP** scanning output: `nmap -sU` *`ipAddress`*

```
[kaitlinhoffmann Module 13 $ nmap -sU hydra.newpaltz.edu
You requested a scan type which requires root privileges.
QUITTING!
```

- Looks like we can’t do this from my own computer. Let’s try this while logged in on hydra!

NMAP SCRIPTING ENGINE (NSE)

- **Nmap Scripting Engine (NSE)** is a scripting engine that allows users to use a pre-defined set of scripts, or write their own using **Lua programming language**.
- Using Nmap scripts is crucial in order to automate system and vulnerability scans. For example, if you want to run a full vulnerability test against your target, you can use these parameters: `nmap -Pn --script vuln` *`ipAddress`*
- Example...

NMAP SCRIPTING ENGINE (NSE)

```
kaitlinhoffmann Module 13 $ nmap -Pn --script vuln hydra.newpaltz.edu
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 20:27 EST
NSOCK ERROR [0.0800s] ssl_init_helper(): OpenSSL legacy provider failed to lo

Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for hydra.newpaltz.edu (50.74.239.202)
Host is up (0.022s latency).
rDNS record for 50.74.239.202: rrcs-50-74-239-202.nyc.biz.rr.com
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  filtered smtp
80/tcp  open     http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-passwd: ERROR: Script execution failed (use -d to debug)
```

NMAP SCRIPTING ENGINE (NSE)

- Example site with a vulnerability:

```
80/tcp open http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

NMAP SCRIPTING ENGINE (NSE)

- There are a plethora of scripts that already exist that are very useful. The following is used to detect any **malware**:
- `nmap -sV --script=http-malware-host` *`ipAddress`*
- Example…

NMAP SCRIPTING ENGINE (NSE)

```
kaitlinhoffmann Module 13 $ nmap -sV --script=http-malware-host hydra.newpaltz.edu
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 20:36 EST
NSOCK ERROR [0.0720s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for hydra.newpaltz.edu (50.74.239.202)
Host is up (0.021s latency).
rDNS record for 50.74.239.202: rrcs-50-74-239-202.nyc.biz.rr.com
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE    SERVICE      VERSION
22/tcp  open     ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
25/tcp  filtered smtp
80/tcp  open     http         Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-malware-host: Host appears to be clean
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     ssl/http     Apache httpd 2.4.52
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-malware-host: Host appears to be clean
445/tcp filtered microsoft-ds
Service Info: Host: hydra.newpaltz.edu; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 54.08 seconds
```

NMAP – ASSIGNMENT 4

- We only scraped the surface with Nmap! Nmap has so many other capabilities.
- Complete the following TryHackMe lab: https://tryhackme.com/room/nmap01
- Explore your VM using command line tools. See PDF under Assignment folder.