Network Reconnaissance using NMAP

Christopher Rodman

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0596

Agenda

Introduction to NMAP

- Target specification
- Output
- Scan Types

Defense evasion

Scan performance

Introduction to NSE Scripts

Hands-on lab (Network mapping with NMAP and xprobe)

Recon using NMAP

Introduction

Overview

- Simple network mapper used for port scanning, network discovery and vulnerability enumeration
- Basic syntax (nmap <target> -args)

```
root@demokali:~# nmap 192.168.31.14 -sS -Pn -p 80,443
```

- Help is your friend

```
root@demokali:~# nmap --help
```

- Complimentary tools include:
  - Xprobe
  - recon-ng
  - Sparta
  - Zenmap
  - Nessus

Target specification

- Single IP address or hostname

```
root@demokali:~# nmap 192.168.31.16
```

- IP address range*

```
root@demokali:~# nmap 192.168.31.14-16
```

- CIDR notation*

```
root@demokali:~# nmap 192.168.31.14/27
```

- Input file (-iL)

```
root@demokali:~# nmap -iL scanlist.txt
```

- Port Definition (-p)
  - -p- scans all 65535

```
root@demokali:~# nmap -p 21-25,80,443 192.168.31.14-16
```

* exclude addresses using --exclude

Output results

- Output interpretation
- Setting verbosity (-v)
- Setting debugging (-d)
- Output to file
  - Text (-oN)
  - XML (-oX)
  - Grep (-oG)
  - All three formats (-oA)

Port State	Description
Open	Responds to an incoming connection.
Closed	Responds to probes, but does not appear to be running a service. Commonly found on systems with no firewall in place.
Filtered	Typically protected by a firewall. Scanning tool is unable to determine if the port is open or closed.
Unfiltered	Port can be accessed, but tool is unable to determine if the port is opened or closed.
Open|Filtered	Port is believed to be open, but tool cannot definitely determine the port's state.
Closed|Filtered	Port is believed to be closed or filtered, but tool cannot definitely determine the port's state.

Basic scan methods

- TCP SYN scan (-sS) – default scan method
- TCP Connect() (-sT) – method used if sS is not possible
- ACK (-sA)
- Window (-sW)
- Maimon (-sM)
- Ping sweep (-sn)
- Discovery scan (-Pn)
- Service scan (-sV)
- Operating System discovery (-O)
- UDP scanning (-sU)

Recon example

- Ping sweep
- Discovery scan
- Service scan
- Operating System

```
root@demokali:~# nmap 192.168.31.1/27 -sn
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 16:54 EDT
Nmap scan report for 192.168.31.14
Host is up (0.00019s latency).
MAC Address: 00:0C:29:73:A5:35 (VMware)
Nmap scan report for 192.168.31.15
root@demokali:~# nmap -Pn 192.168.31.14-16
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 17:09 EDT
Nmap scan report for 192.168.31.14
root@demokali:~# nmap -Pn -sV -O 192.168.31.14
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 10:16 EDT
Nmap scan report for 192.168.31.14
Host is up (0.00041s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
8080/tcp open  http          Microsoft IIS httpd 10.0
MAC Address: 00:0C:29:73:A5:35 (VMware)
Warning: OSScan results may be unreliable because we could not f
pen and 1 closed port
Device type: general purpose
```

Recon using NMAP

Defense Evasion

Scan alteration

- Set timing (-T1 – 5)*
  - 1 = paranoid, 5 = insane
  - Default is 3
- Set packet header bits (--scan-flags)
- Set packet fragmentation (-f and specify MTU -mtu)
- Set target randomness (--randomize-hosts)
- Spoof MAC (--spoof-mac)
- Add decoy noise (-D)*
- TCP Idle scan (-sI)*

*timing templates primarily adjust values for RTT, retries and other timeout values

Evasion example

```
root@demokali:~# nmap -Pn -T2 -O -D RND,ME --randomize-hosts 192.168.31.14-16
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 14:18 EDT
Stats: 0:37:59 elapsed; 0 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.62% done; ETC: 14:58 (0:02:09 remaining)
Stats: 0:38:00 elapsed; 0 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.67% done; ETC: 14:58 (0:02:08 remaining)
Stats: 0:38:02 elapsed; 0 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.70% done; ETC: 14:58 (0:02:07 remaining)
Stats: 0:38:02 elapsed; 0 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.72% done; ETC: 14:58 (0:02:07 remaining)
Stats: 0:38:03 elapsed; 0 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.77% done; ETC: 14:58 (0:02:05 remaining)
```

- Disable ping scan
- Set timing
- Set random decoy
- Set randomness

* --data-string can be used to fill packets with garbage data or to include useful information

Recon using NMAP

Scan Performance

Scan alteration

- Skip port scanning (-sn) if you only need to know if hosts are online
- Limit number of ports being scanned (default is top 1000)
  - Utilize Fast scan (-F) or --top-ports
- Skip advanced scans (-sC, -sV, -O, -A)
- Turn off DNS resolution if not needed (-n)
- Separate TCP and UDP scans
- Adjust timeouts and retries as desired*
  - Parallelism (--min/max-parallelism)
  - Retries (--min/max-retries)
  - Host time (--host-timeout)

Performance example

```
root@demokali:~# nmap 192.168.31.1/27
Nmap done: 32 IP addresses (3 hosts up) scanned in 22.16 seconds
```

- Set timing

```
root@demokali:~# nmap -T5 192.168.31.1/27
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-06 08:47 EDT
Nmap done: 32 IP addresses (3 hosts up) scanned in 18.48 seconds
```

- Remove unnecessary DNS resolution
- Remove port scan

```
root@demokali:~# nmap -sn -n -T5 192.168.31.1/27
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-06 08:48 EDT
Nmap scan report for 192.168.31.14
Host is up (0.00035s latency).
MAC Address: 00:0C:29:73:A5:35 (VMware)
Nmap scan report for 192.168.31.15
Host is up (0.00039s latency).
MAC Address: 00:0C:29:93:42:B9 (VMware)
Nmap scan report for 192.168.31.16
Host is up (0.00039s latency).
MAC Address: 00:0C:29:00:16:E2 (VMware)
Nmap done: 32 IP addresses (3 hosts up) scanned in 0.54 seconds
```

Recon using NMAP

NSE (NMAP Scripting Engine)

NSE Scripts

- Script files located in */usr/share/nmap/scripts* with *.nse* file extension
- Syntax (-sC or --script)
- Script help (--script-help)
- Scripts are categorized

```
root@demokali:~# locate *.nse | wc -l
591
```

```
root@demokali:~# nmap --script-help broadcast-wpad*
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05

broadcast-wpad-discover
Categories: broadcast safe
https://nmap.org/nsedoc/scripts/broadcast-wpad-discov
  Retrieves a list of proxy servers on a LAN using th
```

- Types
  - Prerule
  - Host
  - Service
  - Postrule

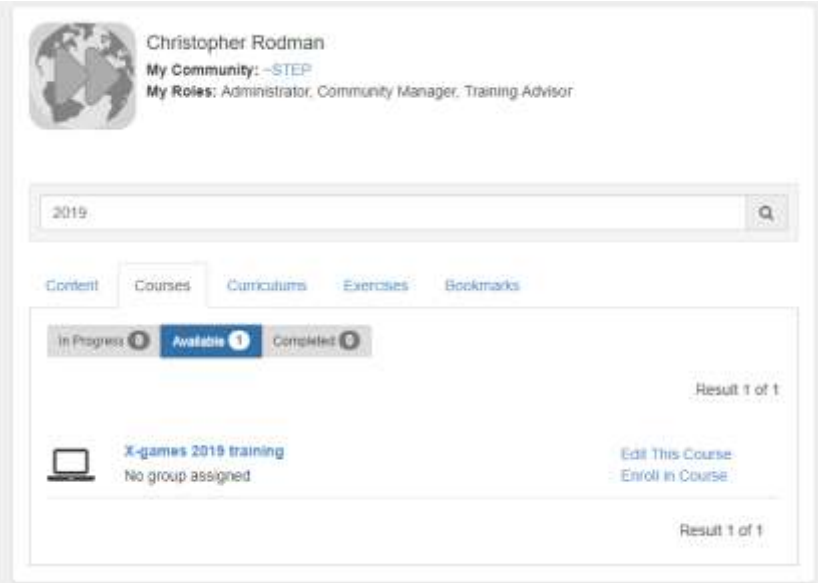
```
root@demokali:~# nmap -n -Pn --script http-chrono 192.168.31.14
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-06 10:55 EDT
Nmap scan report for 192.168.31.14
Host is up (0.00032s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
|_http-chrono: Request times for /; avg: 2.13ms; min: 1.47ms; max
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

Hands-on Lab

Network scanning with NMAP and xprobe

Hands-on lab

- https://stepfwd.cert.org
  - Login credentials provided on entry
- Search for “X-Games 2019”
- Select “X-games 2019 training”
  - Under Courses/Available



- Select Launch