cyber Threat Emulation (CTE)

Module 2, Lesson 2:

Active Scanning and Enumeration

# Course Objectives

After completing this course, students will be able to:

* Summarize the CTE squad's responsibilities, objectives, and deliverables from each CPT stage
* Analyze threat information
* Develop a Threat Emulation Plan (TEP)
* Generate mitigative and preemptive recommendations for local defenders
* Develop mission reporting
* Conduct participative operations
* Conduct reconnaissance
* Analyze network logs for offensive and defensive measures 

# Course Objectives (Continued)

Students will also be able to:

* Analyze network traffic and tunneling protocols for offensive and defensive measures
* Plan non-participative operations using commonly used tools, techniques and procedures (TTPs)

# Module 2: Threat Emulation (Objectives)

* Conduct reconnaissance
* Generate mission reports from non-participative operations  Plan a non-participative operation using social engineering
* Plan a non-participative operation using Metasploit
* Analyze network logs for offensive and defensive measures
* Analyze network traffic and tunneling protocols for offensive and defensive measures
* Plan a non-participative operation using Python
* Develop fuzzing scripts
* Develop buffer overflow exploits

# Module 2 — Lesson 2: Active Scanning and Enumeration (Objectives)

* Conduct active reconnaissance
* Develop mission reports from results of exploitation

Methods of Scanning

# Passive discovery techniques

* Monitor communications
* Transparent

' Take more time

Active discovery techniques

. Fast

* Provide a lot of information
* Can trigger alerts

## Methods of Scanning

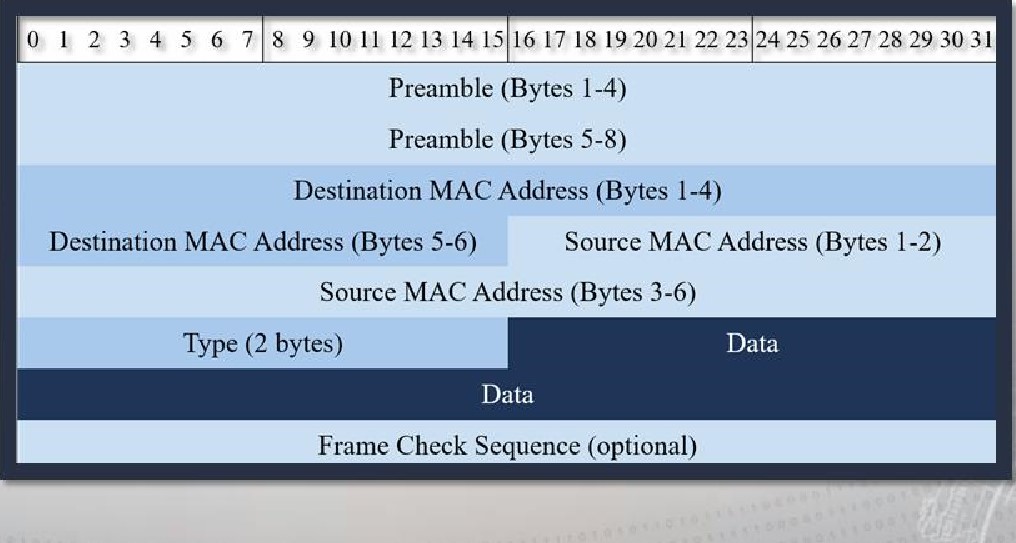
Port Scanning

* Determining ports that are open
* Reveals presence of devices
* Reconnaissance tool for attackers

# Vulnerability Scanning

* Combines port scanning
* Reveals hosts and servers for known vulnerabilities
* Provides report

## Major Protocols Review

• Ethernet

## Major Protocols Review

. IPv4

|  |  |  |  |
| --- | --- | --- | --- |
| 0 1 2 3 4 5 6 7 | 8 9 10 11 12 13 1415 | 16 17 18 192021 2223 | 242526272829 30 31 |
|  | | | |
|  | | | |

## Major Protocols Review

### • ICMP



ICMP Echo Request

|  |  |
| --- | --- |
| oxoo | ICMP Echo Reply |
| ox03 | ICMP Destination Unreachable |
| ORO B | ICMP TTL Exceeded |

## Major Protocols Review

• TCP

|  |  |  |  |
| --- | --- | --- | --- |
| 6 7 | 8 9 10 11 12 13 1415 | 16 17 18 19 2021 22 23 | 2425 262728293031 |
|  | | | |
| Data (optional) | | | |
|  | | | |

## Major Protocols Review

### • UDP

|  |  |  |
| --- | --- | --- |
| 67 | S 10 11 12 13 14 15 | 16 17 18 19 20 21222324 25 262728 29 30 31 |
|  | | |
| Data | | |
|  | | |

## Active Scanning Techniques

* Discovering Hosts (Network Mapping)
* MAC and IP addresses
* Host names
* Operating systems (OSS)
* Services running
* Broadcast pings and ping sweeps
* ARP scans
* ICMPv6 neighbor discovery

## Active Scanning Techniques

* Scanning ports
* What will happen when connecting to a TCP port?
* What about UDP?
* OS detection
* Service and version detection
* Timing and optimization
* Firewall and IDS evasion
* Packet manipulation

## Scapy

* What is Scapy?
* Why use Scapy? • Important concepts
* Crafting packets
* Sending and receiving packets

What is Scapy?

* Program for manipulating packets
* Capable of sniffing and transmitting packets
* Can handle many tasks:
* Scanning
* Traceroute
* Host discovery
* Probing
* And more

## Scapy

* Very useful tool
* Cross platform
* Scripting in Python  Replay packets

## Crafting Packets with Scapy

* Create a packet • Show the contents of the packet



* Combine the layers



### Sending Packets with Scapy

• Sending packets is easy!

|  |  |
| --- | --- |
| >>> send (packet )  Sent 1 packets. | |
|  |  |



•

Or

you

could

use

### Sending and Receiving Packets

Functions:

• Send and Receive

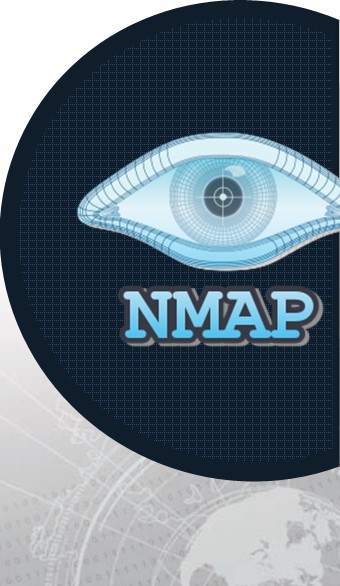
#### • sr()

* Send and Receive one packet
* srl()

|  |
| --- |
| srl IP / ICMP / n Hello World ' Begin emission:  . Finished sending 1 packets.  Received 2 packets, got 1 answers, remaining 0 packets  <IP version=4 ihl=5 tos=0x0 len=39 id=102 flags= frag=o ttl  =128 proto=icmp chksum=oxeef3  .229.29 <ICMP type=echo-reply code=0 chksum=0xa e31 id=0x0 seq=0x0 1<Raw load='Hello World' 1<Padding load |

#### Nmap

Features include

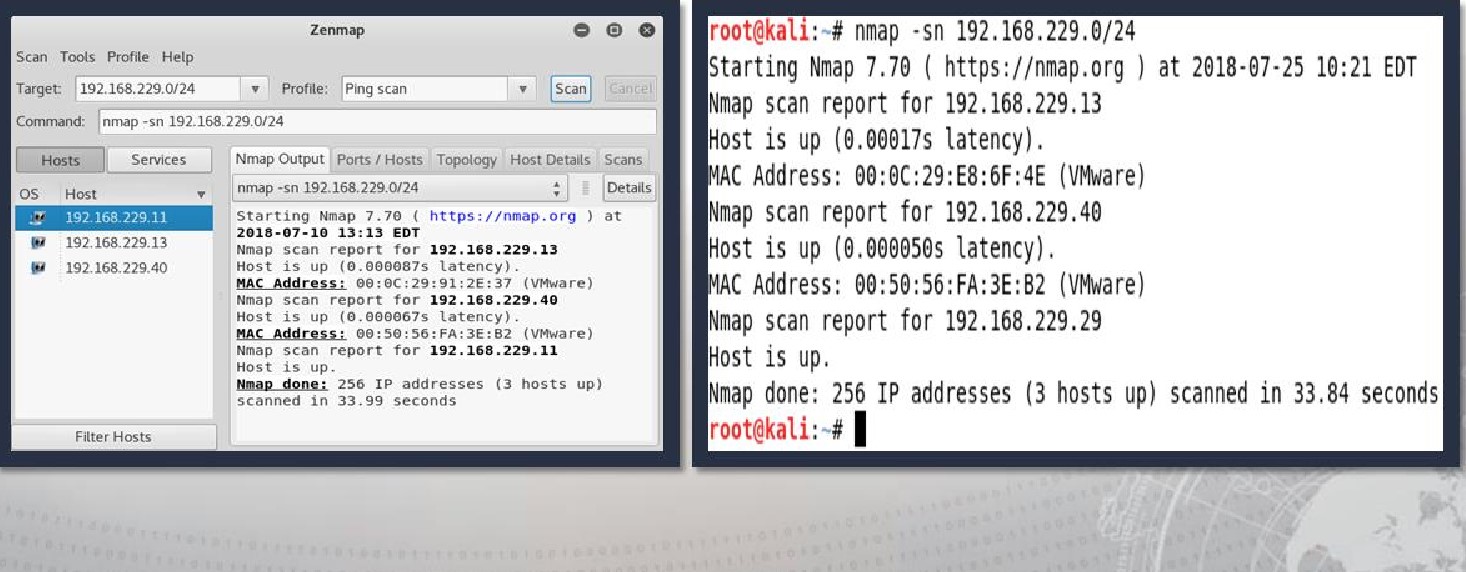
* Host and port scanning
* OS detection
* Detecting versions
* Scriptable

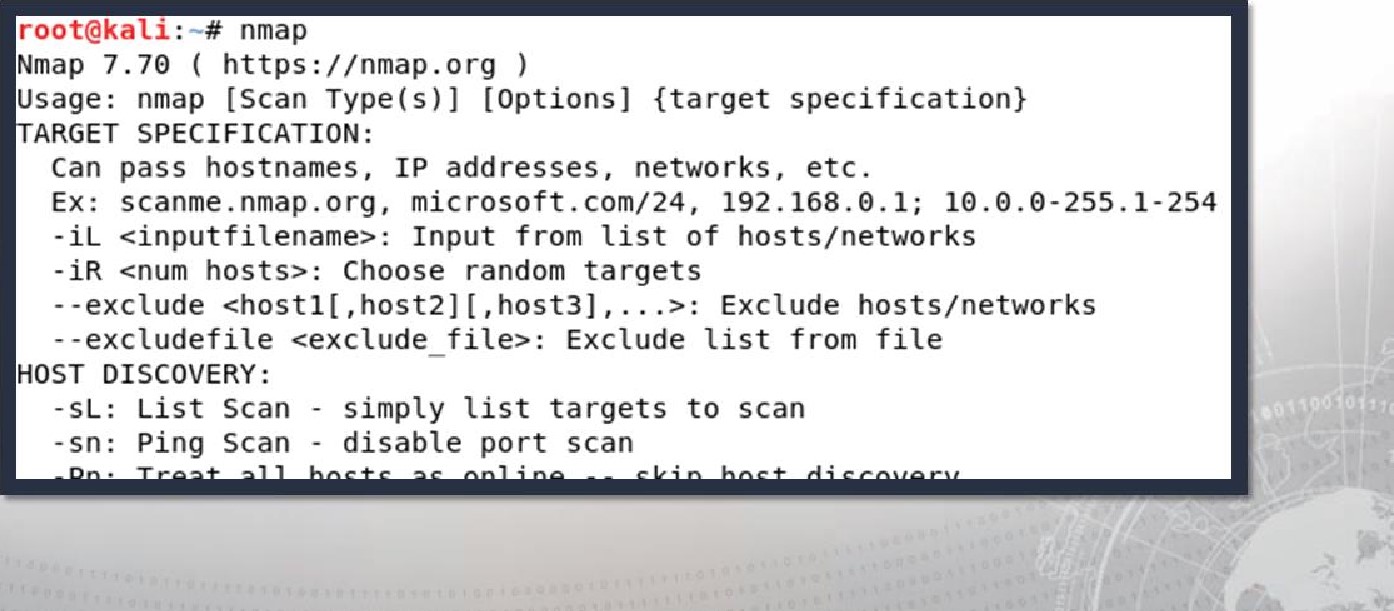
Uses include

* Mapping networks
* Identifying open ports
* Security Auditing

### Nmap

|  |  |
| --- | --- |
| Zenmap  Scan Tools Profile Help  Target 192.168.229024 Profile: Ping scan   |  | | --- | | nrnap sn |   Command:  D Nmap Output Ports Hosts Topology Host Details Scans  192-168229-0/24  OS H ost 'Deceits  starting Nmap 7.70 ( https:/.•nmap.org ) at 2016-07-10 13:13 Ébt  "map scan report for  192-168229.40 Host is up Latency).  Nmap scan report for 192.163.229.40  Host is up 5öö067s Latencyn tvmware) "map scan report for 192.168.229.11 Host is up.  256 IP addresses (3 hosts up) scanned in 33, 99 seconds  Filter Hosts |
|  |

Graphical User Interface (Zenmap): Command Line:



Nmap

Options

Mapping the Environment— Discovering Hosts

Discovery options

• List scan (-sL) No port scan (-sn)

No ping (-Pn)

#### • TCP SYN ping (-PS) TCP ACK ping (-PA)

* UDP ping (-PU)
* SCTP INIT ping (-PY)
* ICMP ping Types (-PE, \_pp, \_PM)
* IP protocol ping (-PO)
* ARP ping (-PR)

#### Mapping the Environment - Outputting Results

|  |
| --- |
| OUTPUT :  -oN/-oX/-oS/-oG Output scan in normal, ML, sl<rlpt klddi3, and Grepable formats respectively, to the given filename.  -OA <basename»: Output in the three major formats at once  -v: Increase verbosity level (use -vv or more for greater effect)  -d: Increase debugging level (use -dd or more for greater effect)  --reason: Display the reason a port is in a particular state  --open: Only show open (or possibly open) ports  --packet-trace: Show all packets sent and received  --iflist: Print host interfaces and routes (for debugging)  --append-output: Append to rather than clobber specified output files  --resume <filename»: Resume an aborted scan  --stylesheet <path/lJRL>: XSL stylesheet to transform XML output to HTML  --webxml: Reference stylesheet from Nmap.Org for more portable XML  --no-stylesheet: Prevent associating of XSL stylesheet w/ XML output |

Mapping the Environment— Port Scanning

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  | | --- | | Option | |  | | |  | | --- | | Scan Type | |  | |

Ping scan only

TCP SYN

TCP connect

TCP ACK sN/-TCP NULL, FIN, and Xmas

TCP window

TCP

UDP

-sl Idle

-b FTP bounce

-SO IP protocol

#### OS Fingerprinting and Version Detection

OS DETECTION:

-O: Enable OS detection

--osscan-limit: Limit OS detection to promising targets --osscan-guess: Guess OS more aggressively

SERVICE/VERSION DETECTION:

-sV: Probe open ports to determine service/ version info

--version-intensity set from o (light) to 9 (try all probes)

- -version-light: Limit to most likely probes (intensity 2)

--version-all: Try every single probe (intensity 9)

--version-trace: Show detailed version scan activity (for debugging)

#### Nmap Scripting Engine (NSE)

Automates networking tasks

* Network discovery
* More sophisticated version detection
* Vulnerability detection
* Backdoor detection
* Vulnerability exploitation

#### Nmap Scripting Engine (NSE)

|  |  |  |
| --- | --- | --- |
| Types of Scripts: | Categories: |  |
| • Prerule | • Auth | • Fuzzer |
| • Host | • Broadcast | • Intrusive |
| • Service | • Brute | • Malware |
| • Postrule | • Default | • Safe |
|  | • Discovery | • Version |
|  | * DOS * Exploit * External | • Vuln |

### Using Nmap Scripting Engine (NSE)

* Selecting scripts
* locate \*.nse
* find / -name "\*.nse"
* Performing Script Scans

SCRIPT SCAN:

-sc: equivalent to --script=default scripts>: <Lua scripts> is a comma separated list of directories, script-files or script-categories

[n2=v2,.. . provide arguments to scripts

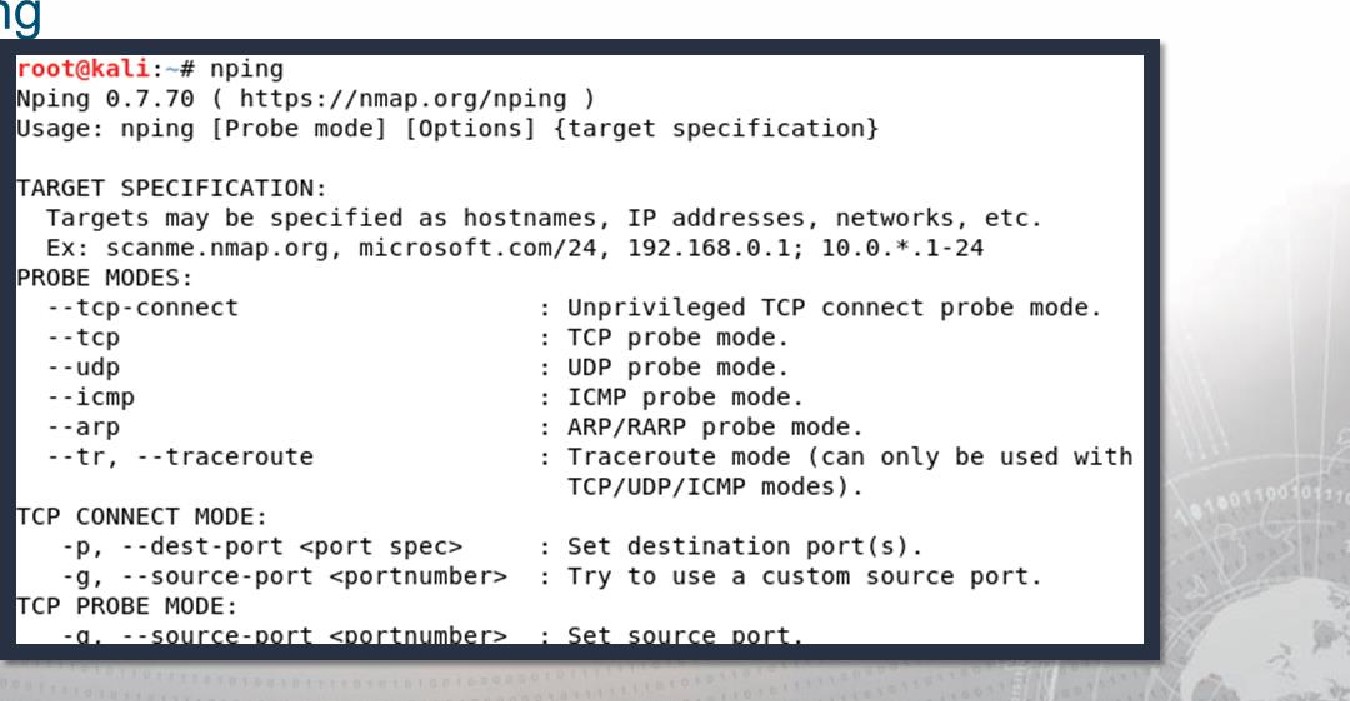
--script-args-file=fitename: provide NSE script args in a file --script-trace: Show all data sent and received --script-updatedb: Update the script database.

scripts>: Show help about scripts.

<Lua scripts> is a comma-separated list of script-files or script-categories .

### Ncat

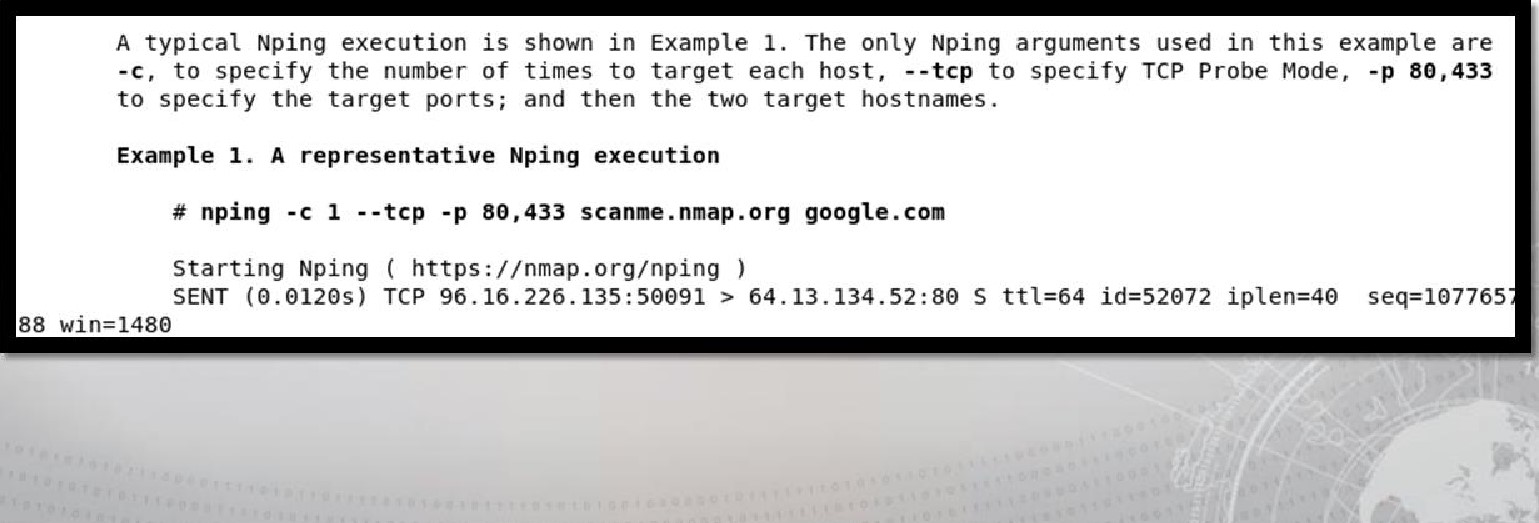
|  |
| --- |
| ncat -h  Ncat 7.70 ( https://nmap.org/ncat )  Usage: ncat [options) [hostname] [port]  Options taking a time assume seconds. Append i ms ' for milliseconds, 's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms) .  -4 Use IPv4 only  -6 Use IPv6 only  U, - -unixsock Use Unix domain sockets only C, --crtf Use CRLF for EOL sequence c, --sh-exec <command> Executes the given command via /bin/sh e, - -exec <command> Executes the given command  - -lua-exec Executes the given Lua script  -g hopl[,hop2, . . ] Loose source routing hop points (8 max) |



Npin

#### Nping

• Use man nping to find syntax examples



#### Nping

|  |  |
| --- | --- |
| roo w a nplng -c cp -p  starting Nping €.7.79 ( https://nmap.org/nping ) at 2018-€7-25 13:50 EDT  SENT (0.081B) TCP 192.168.229.29:1837 > 192. 168.229.13:8€ S tt1=64 id=4814 ip1en=40 seq=145641095 win=1480  SENT (1.08275) TCP 192.168.229.29:1837 > 192. 168.229.80:8€ S tt1=64 id=4814 ip1en=40 seq=145641095 win-1480  RCVD (1.08345) TCP 192.168.229.80:80 > 192.168.229.29: 1837 tt1=128 id=891 ip1en=44 seq=3928731479 win-8192 <mss 1460>  SENT (2.08405) TCP 192.168.229.29.•1837 > 192. 168.229. 13:433 s tt1=64 id=4814 ip1en=40 seq=145641095 win=1480  SENT (3.08575) TCP 192.168.229.29:1837 > 192. 168.229.80:433 S tt1=64 id=4814 ip1en=40 seq=145641095 win-1480 RCVD (3.08605) TCP 192.168.229.80:433 > 192.168.229.29:1837 RA tt1=128 id=892 ip1en=40 seq:o win-o  Statistics for host 192.168.229.13:  I Probes sent: 2 | Rcvd: O I Lost: 2 (100.00%) I \_ Max rtt: N/A I Min rtt: N/A I Avg rtt: N/A Statistics for host 192.168.229.80:  I Probes Sent: 2 | Rcvd: 2 | Lost: o (0.00%)  I \_ Max rtt: 0.567ms I Min rtt: Or177ms I Avg rtt: O. 372ms Raw packets sent: 4 (160B) I Rcvd: 2 (92B) I Lost: 2 (50.00%)  N in done: 2 IP addresses in ed in 3.12 seconds | |
|  |  |

##### Ndiff

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2018 as:  2018 as: | nmap nmap | -SS -ox scanl.xml 19  -SS -ox scan2.xml 19 |  |

#### Evasion Techniques

* Customizing TCP scan flag (--scan-flags)
* Fragmentation (-f / --mtu)
* Adding decoy IP addresses (-D)
* Idle Scan (-sl)
* Changing the Source port (-g)
* Spoofing IP (-S) and MAC address (--spoof-mac)
* Randomize target scan order (--randomize-hosts)
* Add random data to packets (--data-length)
* Manipulating the time-to-live field (--ttl)
* Send packets with bogus TCP or UDP checksums (--badsums)
* Firewalk (--script firewalk)

#### Evasion Techniques

root@ka nmap 192.168.229.80 -p 80 -sc Starting Nmap 7.70

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nmap scan report fo  Host is up (8.00831 | ip.addr—192.168,229.80 |  | | | •l Expression„. |
|  | No, Time Source | Destination | | | Protocol Lengt |
| PORT STATE SERVIC | 41 5.072546990 192.168 , 229,29 | 192 168 . 229 . 80 | | | TCP |
| 80/tcp open http | 42 5, 072936370 192,168 , 229.29 | 192 168 229 80 | | |  |
| I http-methods: | 43 5.072990485 192 .168.229 29 | 192 .168 . 229 . | | | HTTp 23 |
| Potentially ris  I http-title: IIS]  MAC | 44 5.073036035 192 .168.229.29 connection: | 192 .168 .229 80 | | | TCP |
|  |  |  |
| Nmap done: 1 TP add | User-Agent: Mozilla/5.() (compatible; Host :  Content-Length: | Nmap | Scripting | Eng 1 ne; | https://nrnap.org/. |
|  | €960 6f 73 65 55 73 65 72 | 41 67 | 65 6e | lose , | - Agent |
|  | 20 69 61 35 | 30 | 20 2B 63 | MOZi11 a/5.ø (C | |
|  | (Joao 70 61 74 69 62 65 3b |  | 61 70 2€ | ompat ibI e; Nmap | |
|  | €690 53 63 72 69 70 74 69 67 20 45 | 67 | 69 65 | Scriptin g Engine | |
|  | 3b 20 6B 74 74 70 73 2f 6e | Ed 61 | 70 2e 6f | • https: // nmap. o | |
|  | 72 67 62 Of 6b 73 65 | 2e 68 | 74 6d 6c | r g/book/ nse . html | |
|  | 29 48 6f 73 74 3a 20 31 39 | 32 2e | 31 36 38 | ) • . Host: 192 .168 | |
|  | 2e 32 32 39 2e 38 30 43 | 6e 74 | 65 6e 74 | . 229.86. Content | |

#### Evasion Techniques

nmap 192. 168.229.80 -p 80 -sc -script-args http . useragent

"Some other Bro Starting Nmap 7. Nmap scan report Host is up (0.00

PORT STATE SE 80/tcp open htt http-methods: Potentially http-title: Il MAC Address: 00:

Nmap done: 1 IP

|  |  |  |  |
| --- | --- | --- | --- |
| ip.addr—-=192.168.229.80 |  |  | Expression... |
| No. Time | Source | Destination | Protocol Le |
| 82 35.315968064 | 192.168.229 .29 | 192.168.229.8@ | HTTP 1 |
| 83 35 316027774 | 192 168 229 29 | 192 168 229 80 |  |
| 84 | 192 . 168 . 229 .29 | 192 . . 229 .80 | HTTP 1 |
| 85 35 . 316141196 | 192 . . 229 .29 | 192 . . 229 .80 | TCP |

Request Version: HTTP/I.I Connection: close\r\n Host:

user -Agent Some other

36 32 32 38 30 55 73 65 72 20 68. 229.8 User41 67 65 74 20 6d 65 74 68 65 gent: S ome othe 72 20 42 77 73 65 72 41 75 74 68 r Browse utho

72 69 61 74 69 54 4d 20 54 r ization NTLM T

52 4d 54 54 55 41 41 42 41 41 41 41 42 IRMTVNTU AABAAAAB

34 49 49 41 41 41 41 41 41 41 41 41 41 41 41 4110AAAA AAAAAAAA

### OpenVAS

* Open source vulnerability scanner
* It's free!
* Over 50,000 network vulnerability tests
* Identifies vulnerabilities - Does not fix them
* Allows customized:
* Targets
* Scans

#### Depth of scans, and scan regions

 Reports

### OpenVAS — Accessing the Web Interface



#### OpenVAS - Configuring a Scan

a

Task Wizard

Advanced Task Wizard Tas k Wizard

Modify Task Wizard Quick start: Immediately scan an IP address

Tasks (O IP address or hostname:

192168.22913

The default address is either your computer or your network gateway. As a short-cut I will do the following for you:

. Create a new Target

1. Create a new Task
2. Start this scan task right away
3. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

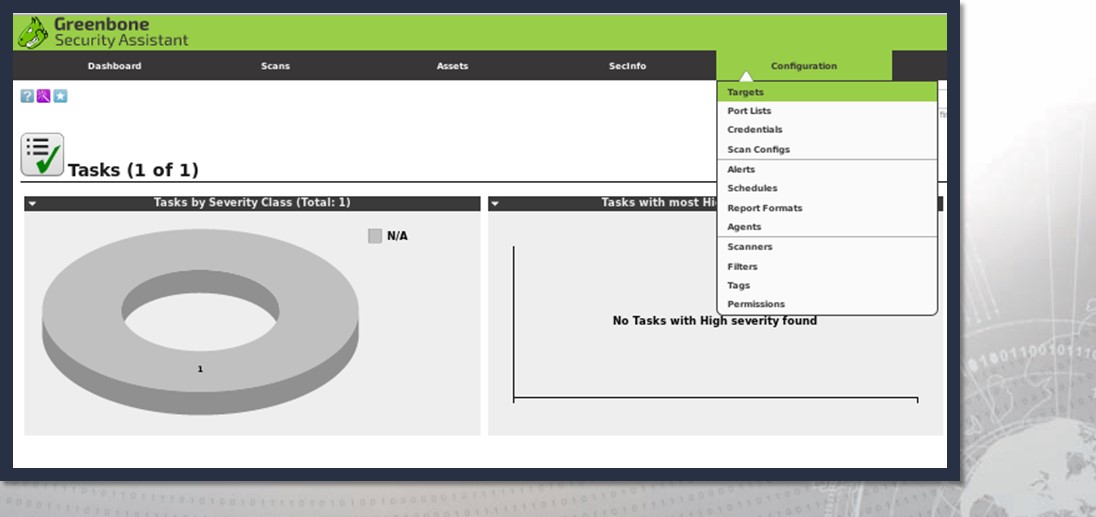
In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

ay clicking the New Task icon you can create a new Task yourself.

Start Sc an

I



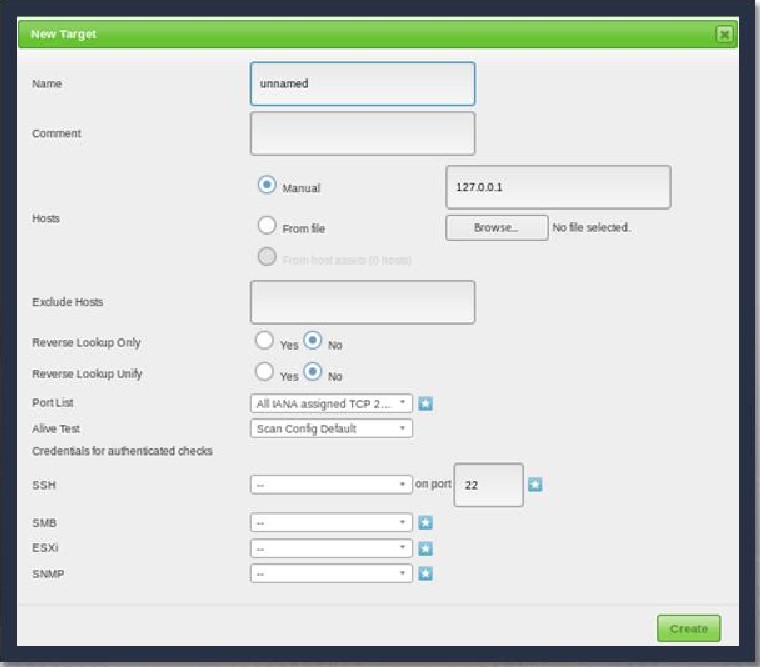
OpenVAS

—

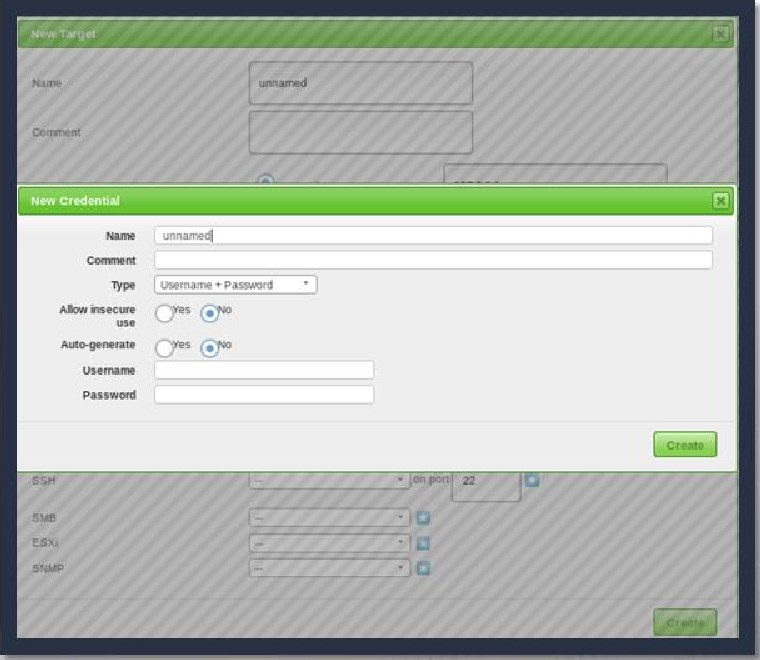
Adding

Targets

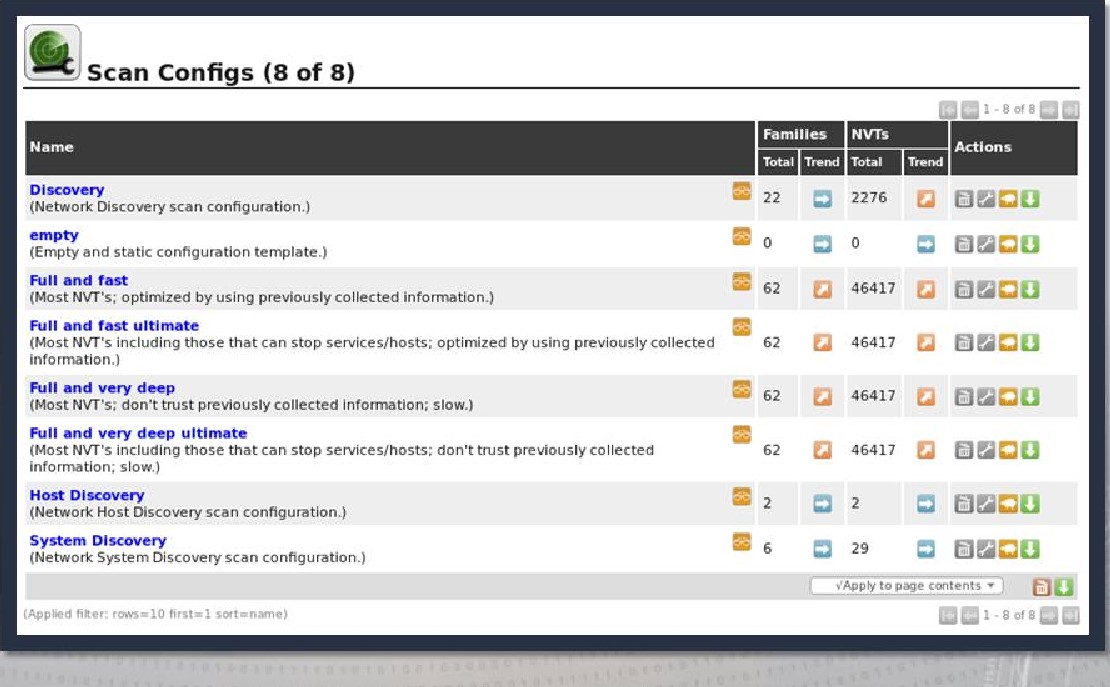
#### OpenVAS — Adding Targets



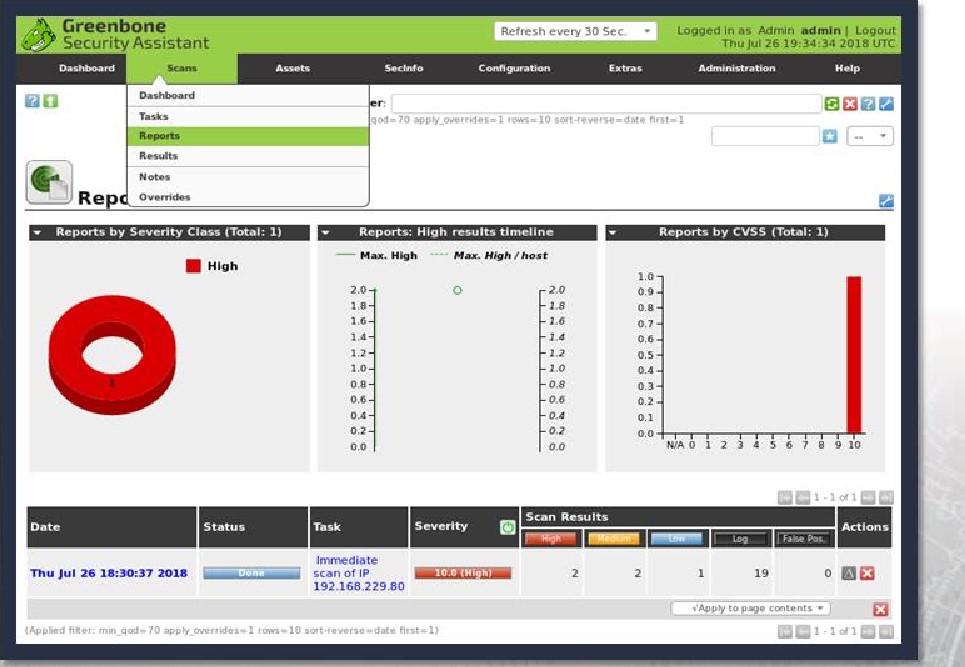
#### OpenVAS — Adding Credentials



OpenVAS — Changing the Network Vulnerability Tests (NVTs)



### OpenVAS — Reviewing Scan Results

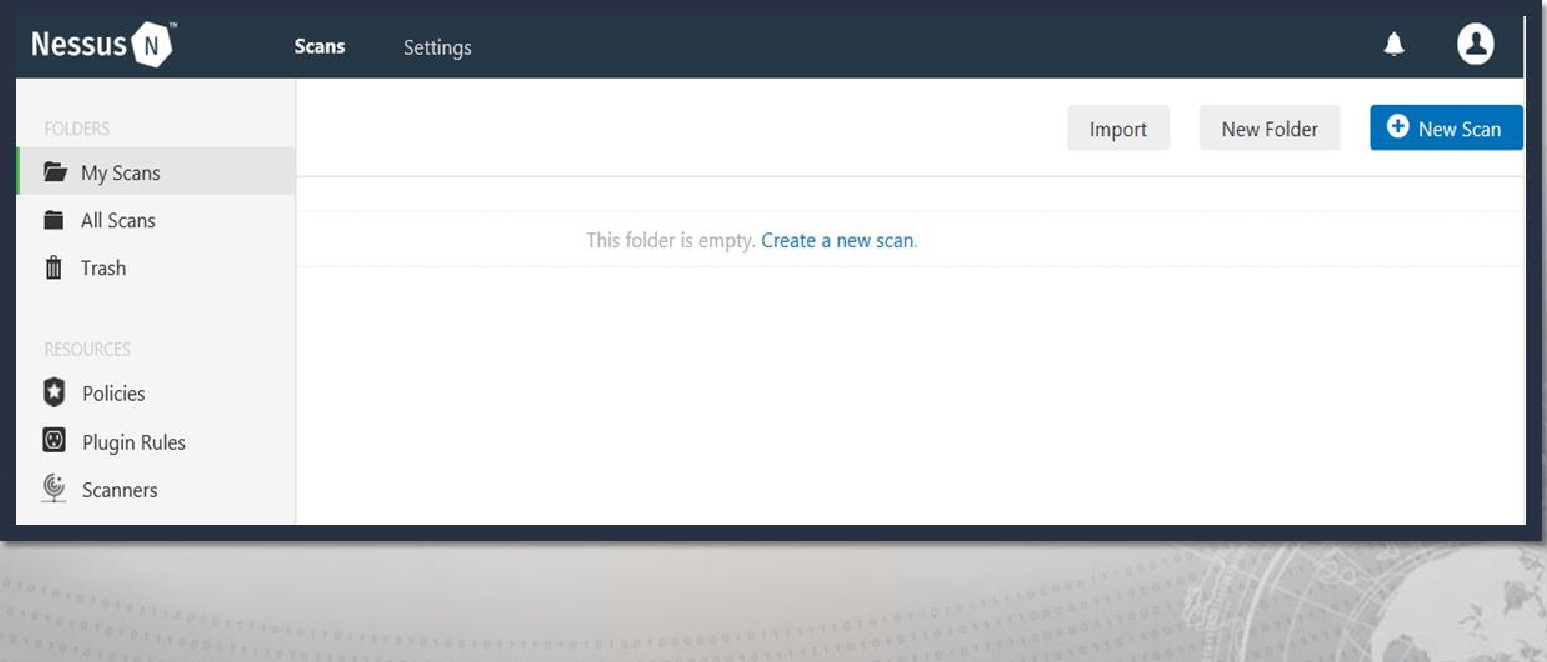


I

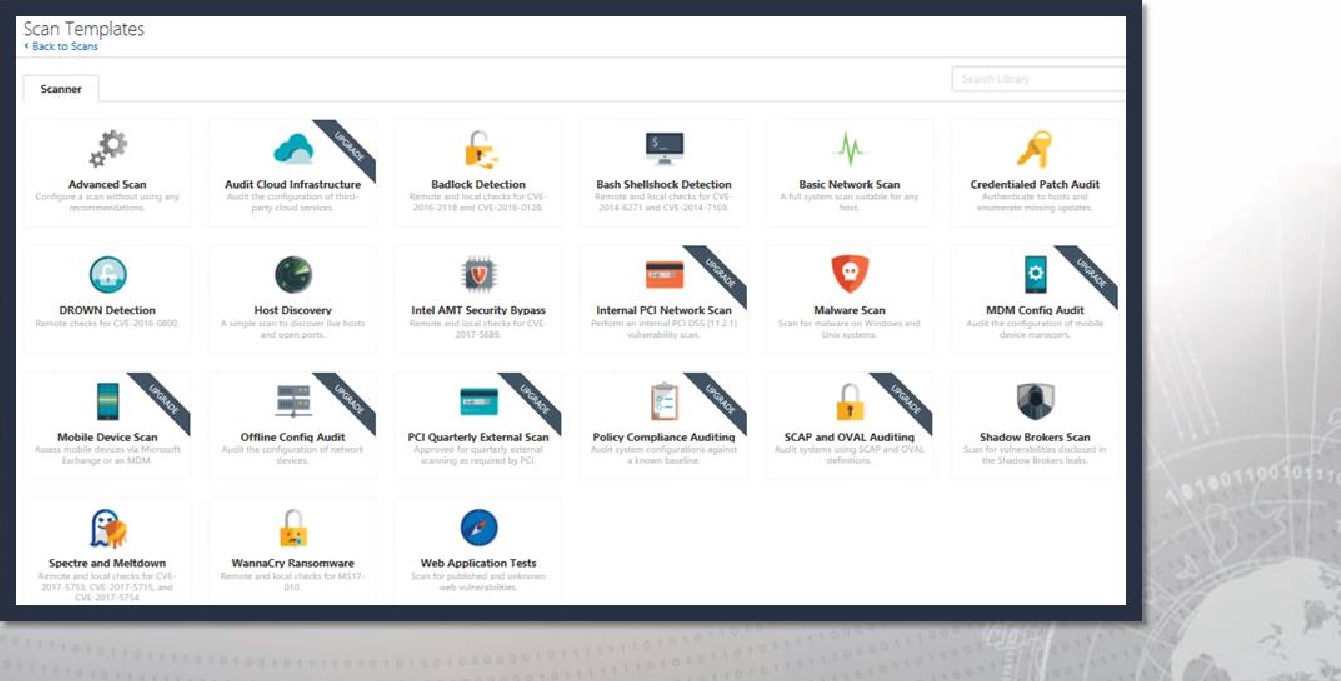
### OpenVAS — Reviewing Scan Results

|  |
| --- |
| Dashboa rd Secl nfo Configuration Extras Administration Help  I |
|  |

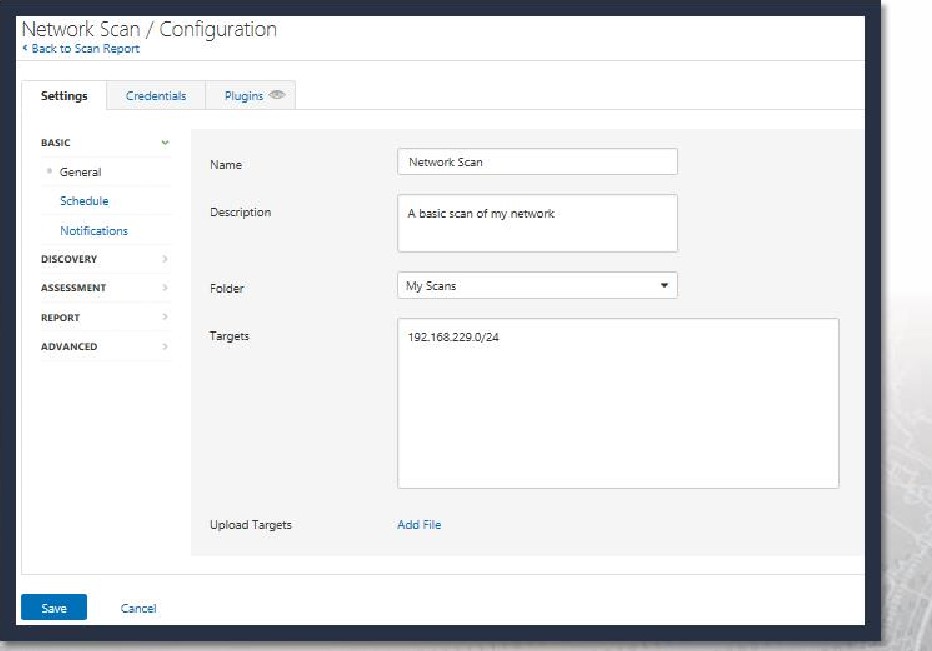
Nessus — Accessing



#### Nessus — Configuring a Scan



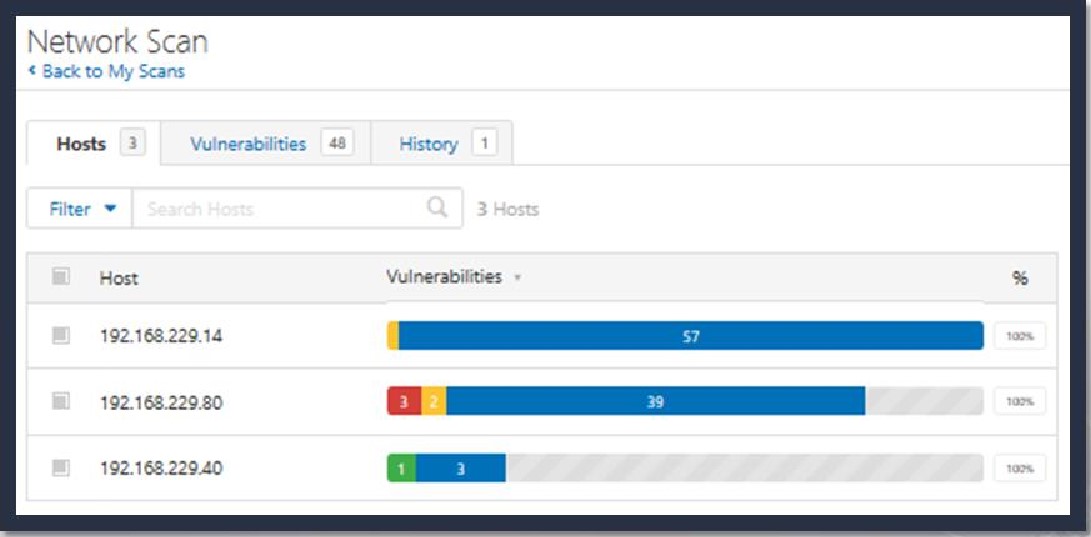
#### Nessus — Configuring a Scan



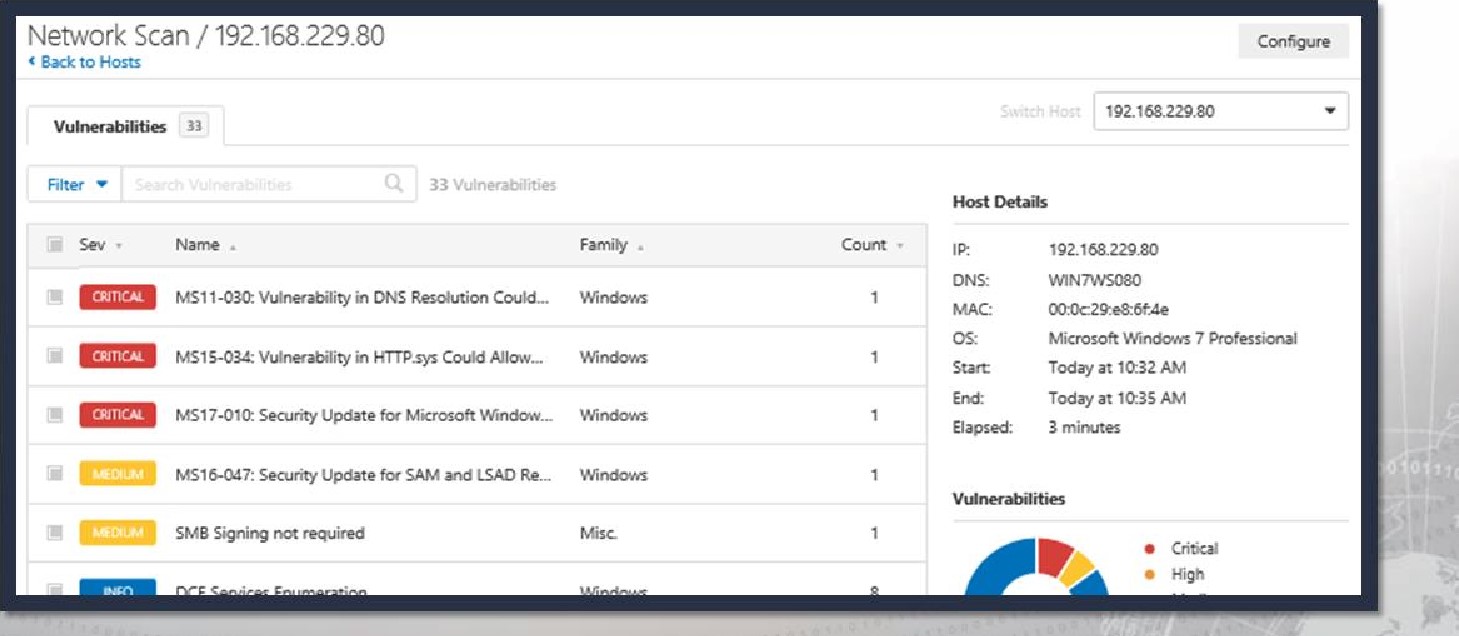
#### Nessus — Launching a Scan

|  |  |  |
| --- | --- | --- |
|  | O New Scan |  |
|  |

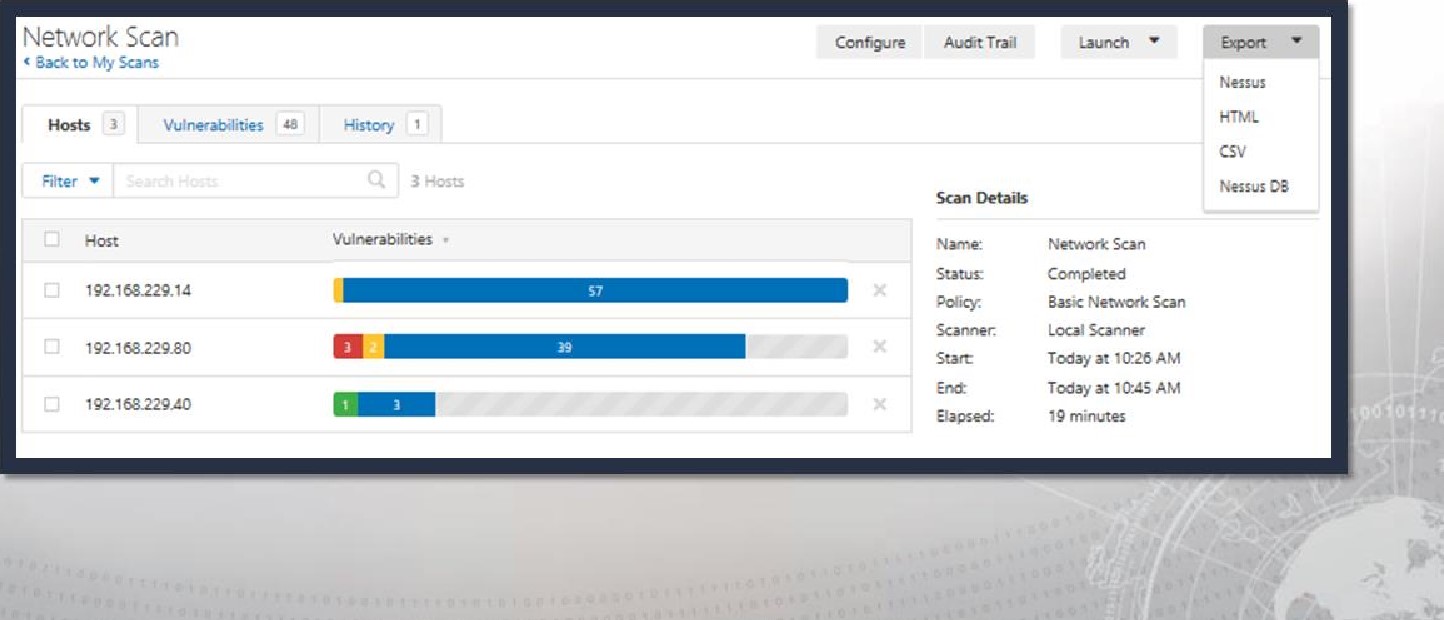
##### Nessus — Reviewing Scan Results



#### Nessus — Reviewing Scan Results



#### Nessus — Reviewing Scan Results



### Exercise: Discovery Scanning & Enumerating Hosts

Objectives

After completing this exercise, students will be able to:

* Conduct active reconnaissance
* Develop mission reports from results of exploitation

Duration

This exercise will take approximately 2 hours to complete.

#### Debrief

Specific Questions

• What are some other ways in which Scapy or a similar tool could be used?

#### Debrief

General Questions

* How did you feel about this procedure?
* Were there any areas in particular where you had difficulty?
* Do you understand how this relates to the work you will be doing?

### Exercise: Advanced Scanning & Evasion Techniques

Objectives

After completing this exercise, students will be able to:

* Conduct active reconnaissance
* Develop mission reports from results of exploitation

#### Duration

This exercise will take approximately 2.5 hours to complete.

#### Debrief

General Questions

* How did you feel about this procedure?
* Were there any areas in

particular where you had difficulty?

* Do you understand how this relates to the work you will be doing?

Specific Questions

* Which other options did you use along with your scans and why did you choose to use them?

#### Exercise: Vulnerability Scanning

Objectives

After completing this exercise, students will be able to:

* Conduct active reconnaissance
* Develop mission reports from results of exploitation

Duration

This exercise will take approximately 1 hour to complete.

#### Debrief

General Questions

* How did you feel about this procedure?
* Were there any areas in

particular where you had difficulty?

* Do you understand how this relates to the work you will be doing?

Specific Questions

* What is the difference between credentialed and non-credentialed scans?
* How do the Nessus and OpenVAS vulnerability scans compare to the results of previous port scans using Nmap?

#### Lesson Summary

In this lesson we learned about:

* Preparing custom packets for scanning
* Using Nmap scans to target ports, detect services, versions of operating systems and applications on a remote host and interpret the results
* Using available scripts to automate networking tasks (such as identifying vulnerabilities, testing controls and detecting backdoors)
* Using Nmap utilities (ncat, ndiff or nping) to analyze a network, generate network packets, connect to other hosts, or compare existing scans
* Performing suitable Nmap scans designed to evade the basic rules of firewalls or Intrusion detection systems
* Completing a vulnerability scan using Nessus and OpenVAS
* Assessing the vulnerability risks to a system and assemble results for inclusion in reporting

|  |
| --- |
| End of Module 2, Lesson 2 |