

Name: Cristian Barreno

## EXERCISE 3 – Vulnerability Scanning and Management

### Task 1 – Conduct your first Vulnerability Scan – Home Network

We are going to start from the dashboard of Tenable Nessus.

Next click on “New Scan”

The screenshot shows the Tenable Nessus interface. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans' (1), 'All Scans', and 'Trash'. Under 'RESOURCES', there are 'Policies', 'Plugin Rules', and 'Terrascan'. The main area is titled 'My Scans' with a search bar showing '1 Scan'. Below it is a table with columns 'Name', 'Schedule', and 'Last Scanned'. One entry, 'Default gateway', is listed with 'On Demand' as the schedule and 'Today at 9:30 AM' as the last scan time. At the top right, there are 'Import' and 'New Folder' buttons, and a prominent blue 'New Scan' button with a plus sign, which is highlighted with a red box.

### Select Basic Network Scan

This screenshot shows the 'Scanner' section of the Tenable Nessus dashboard. On the left, the sidebar includes 'Tenable News' about Microsoft's April 2024 Patch Tuesday. The main area has tabs for 'Scanner' and 'Discovery'. Under 'DISCOVERY', there's a card for 'Host Discovery'. Under 'VULNERABILITIES', there are several cards: 'Basic Network Scan' (selected, shown with a red box), 'Advanced Scan', 'Advanced Dynamic Scan', 'Malware Scan', 'Mobile Device Scan' (with an 'UPGRADE' banner), 'Web Application Tests', 'Credentialated Patch Audit', and 'Intel AMT Security Bypass'. Each card has a small icon and a brief description.

Fill out all the information required, like name, description, and target. In the Target box we are going to put the IP or IP ranges that we are going to scan.

New Scan / Basic Network Scan

Back to Scan Templates

Settings Credentials Plugins

BASIC General Schedule Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Default Gateway

Description: Vulnerability Scan

Folder: My Scans

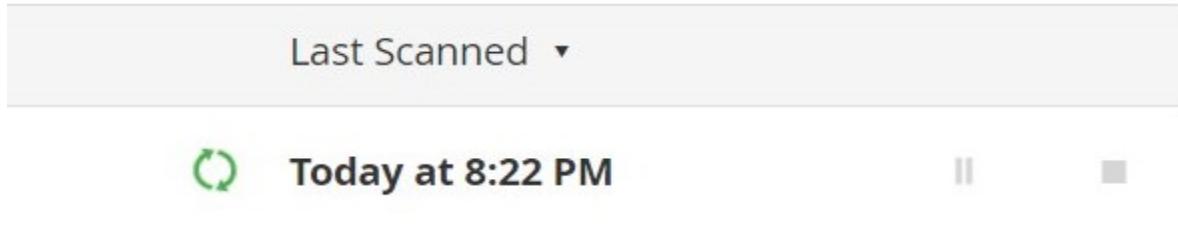
Targets: 192.168.0.1

Upload Targets Add File

My Scans		
Search Scans		1 Scan
<input type="checkbox"/> Name	Schedule	Last Scanned
<input type="checkbox"/> Default gateway	On Demand	✓ Today at 9:30 AM

In the screenshot above we can see the name of the configured scan, if it's going to run in an automated schedule, when was the last scan run, start the scan button, and delete the scan button.

Start the scan.



Run htop from the CLI, you will get a view of all the cores, and memory used for Nessus.

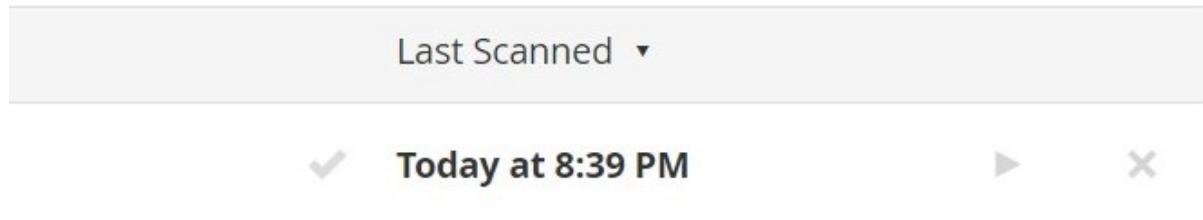
```

0[ ] Tasks: 31, 45 thr; 1 running
1[ ] Load average: 0.13 0.06 0.04
2[ ] Uptime: 00:11:57
Mem[ 392M/7.75G] 2.0% 392M/7.75G
Swap[ 0K/3.82G] 2.0% 0K/3.82G

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
687 root 20 0 381M 190M 14204 S 1.3 2.4 0:26,22 nessusd -q
1303 ajay 20 0 8604 4680 3572 R 0.7 0.1 0:00,05 htop
1 root 20 0 163M 12808 8664 S 0.0 0.2 0:01,86 /sbin/init
404 root 19 -1 48164 17640 16540 S 0.0 0.2 0:00,18 /lib/systemd/systemd-journald
442 root RT 0 282M 27236 9872 S 0.0 0.3 0:00,15 /sbin/multipathd -d -s
445 root RT 0 11752 6248 4168 S 0.0 0.1 0:00,17 /lib/systemd/systemd-udevd
447 root RT 0 282M 27236 9872 S 0.0 0.3 0:00,00 /sbin/multipathd -d -s
448 root RT 0 282M 27236 9872 S 0.0 0.3 0:00,00 /sbin/multipathd -d -s
449 root RT 0 282M 27236 9872 S 0.0 0.3 0:00,00 /sbin/multipathd -d -s
450 root RT 0 282M 27236 9872 S 0.0 0.3 0:00,00 /sbin/multipathd -d -s
451 root RT 0 282M 27236 9872 S 0.0 0.3 0:00,07 /sbin/multipathd -d -s
452 root RT 0 282M 27236 9872 S 0.0 0.3 0:00,00 /sbin/multipathd -d -s
619 systemd-t 20 0 89364 6584 5780 S 0.0 0.1 0:00,09 /lib/systemd/systemd-timesyncd
631 systemd-t 20 0 89364 6584 5780 S 0.0 0.1 0:00,00 /lib/systemd/systemd-timesyncd
659 systemd-n 20 0 16252 8512 7472 S 0.0 0.1 0:00,19 /lib/systemd/systemd-networkd
661 systemd-r 20 0 25540 12660 8464 S 0.0 0.2 0:00,28 /lib/systemd/systemd-resolved
674 root 0 -20 2788 1644 1516 S 0.0 0.0 0:00,03 /usr/sbin/atopacctd
676 root 0 6896 3040 2792 S 0.0 0.0 0:00,00 /usr/sbin/cron -F -P
678 messagebus 20 0 8764 5028 4206 S 0.0 0.1 0:00,16 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
684 root 20 0 82700 4120 3772 S 0.0 0.1 0:00,05 /usr/sbin/irqbalance --foreground
685 root 20 0 2816 996 888 S 0.0 0.0 0:00,00 /opt/nessus/sbin/nessus-service -q
686 root 20 0 32732 18964 10348 S 0.0 0.2 0:00,08 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
688 root 20 0 230M 9860 6876 S 0.0 0.1 0:00,03 /usr/libexec/polkitd --no-debug
689 syslog 20 0 217M 5448 4364 S 0.0 0.1 0:00,01 /usr/sbin/rsyslogd -n -1NONE
691 root 20 0 13600 29676 19116 S 0.0 0.4 0:03,19 /usr/lib/snapd/snapd
693 root 20 0 23540 7644 6620 S 0.0 0.1 0:00,09 /lib/systemd/systemd-logind
694 root 20 0 383M 12980 10796 S 0.0 0.2 0:00,08 /usr/libexec/udisks2/udisksd
697 syslog 20 0 217M 5448 4364 S 0.0 0.1 0:00,00 /usr/sbin/rsyslogd -n -1NONE
698 syslog 20 0 217M 5448 4364 S 0.0 0.1 0:00,00 /usr/sbin/rsyslogd -n -1NONE
699 syslog 20 0 217M 5448 4364 S 0.0 0.1 0:00,00 /usr/sbin/rsyslogd -n -1NONE
709 root 0 -20 10324 10296 4068 S 0.0 0.1 0:00,05 /usr/bin/atop -R -w /var/log/atop/atop_20240417_600
712 root 20 0 230M 9860 6876 S 0.0 0.1 0:00,00 /usr/libexec/polkitd --no-debug
714 root 20 0 383M 12980 10796 S 0.0 0.2 0:00,00 /usr/libexec/udisks2/udisksd
722 root 20 0 15440 8616 7084 S 0.0 0.1 0:00,01 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
733 root 20 0 230M 9860 6876 S 0.0 0.1 0:00,00 /usr/libexec/polkitd --no-debug
F1 Help F2 Setup F3 Search F4 Filter F5 Tree F6 Sort By F7 Nice F8 Kill F9 Kill F10 Quit

```

We can see a date stamp telling us when it finished scanning



Default gateway

Configure Audit Trail Launch Report Export

Folders My Scans All Scans Trash

Resources Policies Plugin Rules Terrascan

Tenable News

Path Traversal Affecting Multiple CData Products Read More

Hosts 1 Vulnerabilities 22 Notes 1 History 2

Filter ▾ Search Hosts 1 Host

Host	Vulnerabilities
192.168.0.1	3 37

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 8:22 PM  
End: Today at 8:39 PM  
Elapsed: 18 minutes

Vulnerabilities

Critical (dark red), High (orange), Medium (light blue)

In the screenshot above we can see the vulnerabilities from the IP address that we selected.

Click on the IP to see more details.

Default gateway / 192.168.0.1

Vulnerabilities 22

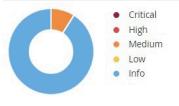
Filter Search Vulnerabilities 22 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	Actions
MEDIUM	6.5	4.9	IP Forwarding Enabled	Firewalls	1	🔗
MIXED	...	...	SSL (Multiple Issues)	General	7	🔗
INFO	...	...	HTTP (Multiple Issues)	Web Servers	6	🔗
INFO	...	...	IETF Md5 (Multiple Issues)	General	2	🔗
INFO	...	...	TLS (Multiple Issues)	General	2	🔗
INFO			Nessus SYN scanner	Port scanners	3	🔗
INFO			Service Detection	Service detection	3	🔗
INFO			DNS Server Detection	DNS	2	🔗
INFO			Common Platform Enumeration (CPE)	General	1	🔗
INFO			Device Type	General	1	🔗
INFO			Ethernet Card Manufacturer Detection	Misc.	1	🔗

Host Details

IP: 192.168.0.1  
MAC: E4:BF:FA:A7:16:90  
OS: Linux Kernel 2.6  
Start: April 17 at 12:22 AM  
End: April 17 at 12:39 AM  
Elapsed: 18 minutes  
KB: Download

Vulnerabilities



Critical  
High  
Medium  
Low  
Info

Explore more of a vulnerability by clicking on it.

Default gateway / Plugin #50686

Vulnerabilities 22

MEDIUM IP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Solution

Unless the remote host is a router, it is recommended that you disable IP forwarding.

On Linux, you can disable IP forwarding by doing:

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command:

```
sysctl -w net.inet.ip.forwarding=0
```

For other systems, check with your vendor.

Output

```
IP forwarding appears to be enabled on the remote host.
```

Plugin Details

Severity: Medium  
ID: 50686  
Version: 1.16  
Type: remote  
Family: Firewalls  
Published: November 23, 2010  
Modified: October 17, 2023

VPR Key Drivers

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: Unproven  
Age of Vuln: 730 days +  
Product Coverage: Low  
CVSSv3 Impact Score: 3.7  
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 4.9  
Risk Factor: Medium  
CVSS v2.0 Base Score: 6.5

To generate a report click on the report button on the top right corner. It will download to your downloads folder.

The screenshot shows the Tenable Nessus web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main area is titled 'Default gateway' and shows a summary of the scan: 1 Host, 22 Vulnerabilities, 1 Note, and 2 History entries. A search bar and filter dropdown are available. To the right, 'Scan Details' provide information about the scan: Policy (Basic Network Scan), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (Today at 8:22 PM), End (Today at 8:39 PM), and Elapsed (18 minutes). Below this is a 'Vulnerabilities' section with a pie chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).



The screenshot above shows an easy to read report of the vulnerabilities scanned.

If you pick a host you can see different columns for the severity, CVSS, Plugin, and name.

Severity	CVSS v3.0	VPR Score	Plugin	Name
MEDIUM	6.5	4.9	50686	IP Forwarding Enabled
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	15901	SSL Certificate Expiry
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
...				

Screenshot of detailed information about a vulnerability.

DETECTIONS

- Plugins
  - Overview
  - Plugins Pipeline
  - Release Notes
  - Newest
  - Updated
  - Search
  - Nessus Families
  - WAS Families
- NNM Families
- LCE Families
- Tenable OT Security Families
- About Plugin Families
- Audits >
- Policies >
- Indicators >
- ANALYTICS
  - CVEs >
  - Attack Path Techniques >

Plugins / Nessus / 50686

## IP Forwarding Enabled

MEDIUM Nessus Plugin ID 50686

Language: English ▾

Information Dependencies Dependents Changelog

**Synopsis**  
The remote host has IP forwarding enabled.

**Description**  
The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.  
Unless the remote host is a router, it is recommended that you disable IP forwarding.

**Solution**  
On Linux, you can disable IP forwarding by doing :  
`echo 0 > /proc/sys/net/ipv4/ip_forward`  
On Windows, set the key 'IPEnableRouter' to 0 under  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  
On Mac OS X, you can disable IP forwarding by executing the command :  
`sysctl -w net.inet.ip.forwarding=0`  
For other systems, check with your vendor.

**Plugin Details**  
Severity: Medium  
ID: 50686  
File Name: ip\_forwarding\_enabled.nasl  
Version: 1.16  
Type: remote  
Family: Firewalls  
Published: 11/23/2010  
Updated: 10/17/2023  
Supported Sensors: Nessus

**Risk Information**

**VPR**  
Risk Factor: Medium  
Score: 4.0

**CVSS v2**  
Risk Factor: Medium  
Base Score: 5.8  
Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P  
CVSS Score Source: CVE-1999-0511

**CVSS v3**  
Risk Factor: Medium  
Base Score: 6.5  
Vector: CVSS3.0#AV:A/AC:L/PR:L/U:N/S/C:L/I:L/A:L  
CVSS Score Source: CVE-1999-0511

**Vulnerability Information**  
Vulnerability Publication Date: 1/1/1997

**Reference Information**  
CVE: CVE-1999-0511

## Task 2 – Conduct your first Vulnerability Scan – DVL

The first step is to have Damn Vulnerable Linux (DVL) powered on. DVL is a Linux VM that contains vulnerabilities for training purposes.

Click new scan.

My Scans

Import New Folder + New Scan

Name	Schedule	Last Scanned
Default gateway	On Demand	Today at 8:39 PM

Click on Basic Network Scan.

Scan Templates

Scanner

DISCOVERY

VULNERABILITIES

Host Discovery

A simple scan to discover live hosts and open ports.

Basic Network Scan

A full system scan suitable for any host.

Advanced Scan

Configure a scan without using any recommendations.

Advanced Dynamic Scan

Configure a dynamic plugin scan without recommendations.

Malware Scan

Scan for malware on Windows and Unix systems.

Mobile Device Scan

Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests

Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialated Patch Audit

Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass

Remote and local checks for CVE-2017-5752, CVE-2017-5715, and CVE-2017-5754.

Spectre and Meltdown

Remote and local checks for CVE-2017-5752, CVE-2017-5715, and CVE-2017-5754.

WannaCry Ransomware

Remote and local checks for MS17-010.

Ripple20 Remote Scan

A remote scan to fingerprint hosts potentially running the Trekk stack in the network.

Zerologon Remote Scan

A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Configure a new basic network scan with the DVL IP address.

Next, launch the scan against the DVL.

The screenshot below shows the vulnerabilities scanned.

The screenshot displays the Tenable.io web interface. On the left, a sidebar shows 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is present. The main content area is titled 'DVL' and shows a scan summary for 'Host 192.168.0.226'. The 'Scan Details' pane indicates a 'Basic Network Scan' was completed. The 'Vulnerabilities' section includes a pie chart showing the distribution of severity levels: Critical (black), High (red), Medium (orange), Low (yellow), and Info (blue).

DVL

Back to My Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 13 Notes 1 History 1

Filter Search Hosts 1 Host

Host Vulnerabilities

192.168.0.226 16

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0 ✓  
Scanner: Local Scanner  
Start: Today at 9:11 PM  
End: Today at 9:13 PM  
Elapsed: 2 minutes

Vulnerabilities

Critical  
High  
Medium  
Low  
Info