

Assignment 9:

TASK-1:

TITLE: A. Perform different scans on your network using the Nessus tool and generate a report.

OBJECTIVE OF THE TASK: HERE WE DONE THE HOST DISCOVERY SCAN AND BASIC NETWORK SCANS TO FIND VULNERABILITY IN WEBSITES AND GENERATE REPORT.

STEP BY SETP PROCEDURE:


- Host discovery scan


1. NOW OPEN THE NESSES TOOL AND SELECT THE TARGETS TO SCAN.
2. Now we go to Nessus tool to done the above mentioned scans.
3. Here we select host discovery scanning.
4. Now add the domain of the target to scan
5. Now we done the Nessus host discovery and get the respected vulnerabilities.


- Basic Network Scan

1. NOW OPEN THE NESSES TOOL AND SELECT THE TARGETS TO SCAN.
2. Now we go to Nessus tool to done the above mentioned scans.
3. Here we select basic networking scanning.
4. Now add the domain of the target to scan
5. Now we done the basic networking scanning and get the respected vulnerabilities.


FOLDERS


 My Scans


 All Scans

 Trash

RESOURCES

 Policies

 Plugin Rules


 Terrascan

Scan Templates

[← Back to Scans](#)

Scanner


DISCOVERY





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

VULNERABILITIES


FOLDERS


 My Scans


 All Scans

 Trash

RESOURCES

 Policies

 Plugin Rules

 Terrascan

New Scan / Host Discovery

[← Back to Scan Templates](#)

Settings Plugins

BASIC

- General
- [Schedule](#)
- Notifications

DISCOVERY

REPORT

ADVANCED

Name

Description

Folder

Targets

Upload Targets [Add File](#)

[Save](#)  [Cancel](#)

Hosts 1

Vulnerabilities 2

History 1

Filter ▼

Search Hosts



1 Host

<input type="checkbox"/>	Host ▼	FQDN
<input type="checkbox"/>	testphp.vulnweb.co...	testphp.vulnweb.com

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:05 PM
End: Today at 3:07 PM
Elapsed: 2 minutes

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

Hosts 1

Vulnerabilities 2

History 1

Filter ▼

Search Vulnerabilities



2 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	INFO			Nessus Scan Information	Settings	1		
<input type="checkbox"/>	INFO			Ping the remote host	Port scanners	1		

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:05 PM
End: Today at 3:07 PM
Elapsed: 2 minutes

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

Basic Network Scan:



Basic Network Scan

A full system scan suitable for any host.

tenable

Nessus Essentials

Scans

Settings

lingamalluvasu143@gm...

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

http://testphp.vulnweb.com/

Configure

Audit Trail

Launch

Report

Export

Hosts

Vulnerabilities

History

Filter

Search Hosts

1 Host

Host

Vulnerabilities

testphp.vulnweb.com

1

16

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 3:18 PM

End:

Today at 3:33 PM

Elapsed:

15 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Task Manager

Taskbar settings

TASK-2:

TITLE: A. Perform different scans on your network using the Nessus tool and generate a report.

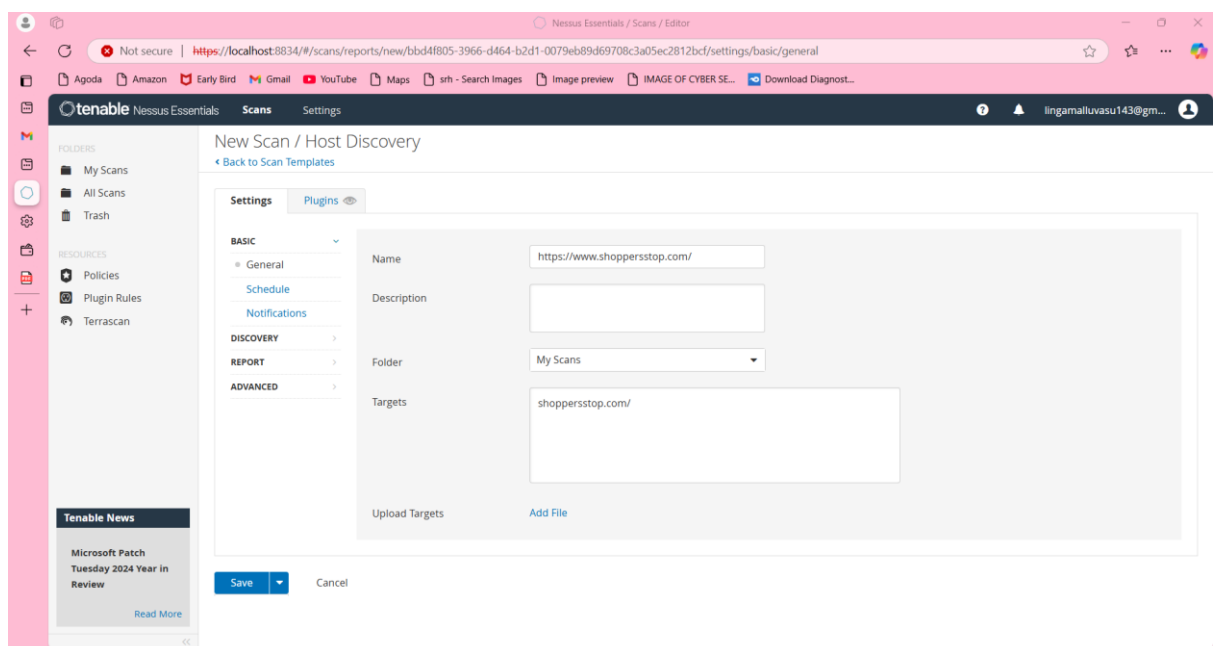
OBJECTIVE OF THE TASK: HERE WE DONE THE HOST DISCOVERY SCAN AND BASIC NETWORK SCANS TO FIND VULNERABILITY IN WEBSITES AND GENERATE REPORT.

STEP BY SETP PROCEDURE:

1. NOW OPEN THE NESSES TOOL AND SELECT THE TARGETS TO SCAN.
2. Now we go to Nessus tool to done the above mentioned scans.
3. Here we select host discovery scanning.
4. Now add the domain of the target to scan
5. Now we done the Nessus host discovery and get the respected vulnerabilities.

Targets: a) <http://testasp.vulnweb.com/>

b) <https://www.shoppersstop.com/>



Tenable

Nessus Essentials

Scans

Settings

lingamalluvasu143@gm...

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

SQL Injection in WordPress Project Manager Plugin

Read More

https://www.shoppersstop.com/

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 2

History 1

Filter

Search Hosts

1 Host

Host

FQDN

☐

shoppersstop.com

shoppersstop.com

Scan Details

Policy: Host Discovery

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 7:30 PM

End: Today at 7:32 PM

Elapsed: 2 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Tenable

Nessus Essentials

Scans

Settings

lingamalluvasu143@gm...

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Scan Templates

Back to Scans

Scanner

DISCOVERY

Host Discovery

A simple scan to discover live hosts and open ports.

VULNERABILITIES

Tenable

Nessus Essentials

Scans

Settings

lingamalluvasu143@gm...

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

New Scan / Host Discovery

Back to Scan Templates

Settings

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

REPORT

ADVANCED

Name

http://testphp.vulnweb.com

Description

Folder

My Scans

Targets

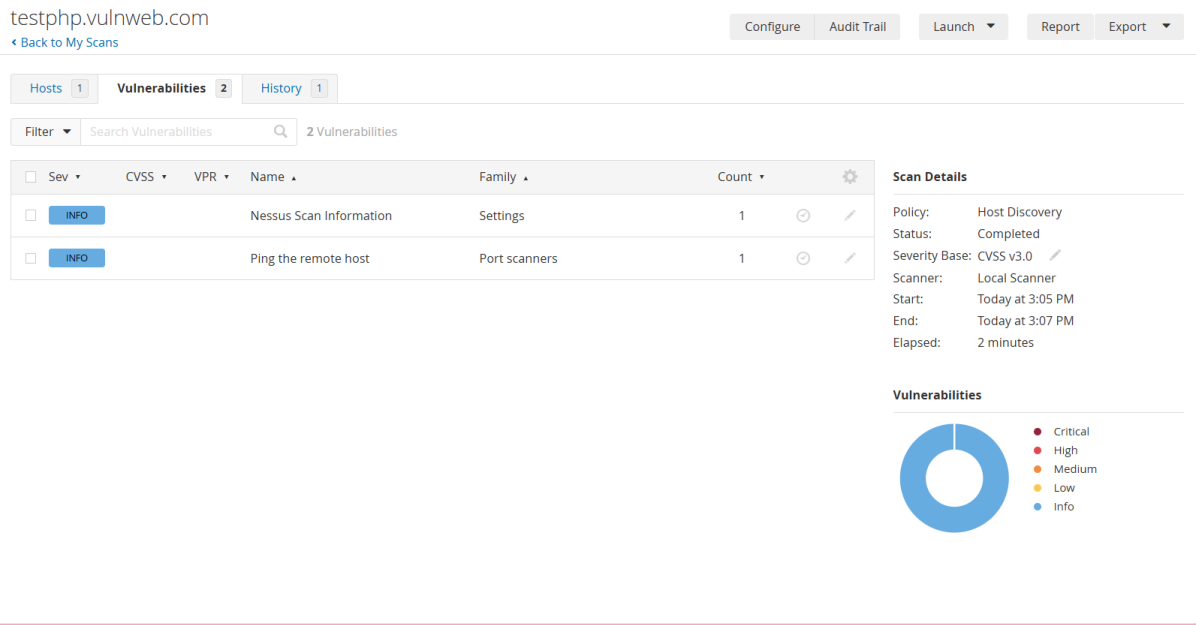
http://testphp.vulnweb.com

Upload Targets

Add File

Save

Cancel



TASK-3:

TITLE: Scan the below-mentioned targets using the Acunetix Vulnerability scanner

OBJECTIVE OF THE TASK: HERE WE DONE THE HOST DISCOVERY SCAN AND BASIC NETWORK SCANS TO FIND VULNERABILITY IN WEBSITES AND GENERATE REPORT.

STEP BY SETP PROCEDURE:

1. NOW OPEN THE ACUNETIX TOOL AND SELECT THE TARGETS TO SCAN.
2. Now we go to ACUNETIX tool to done the above mentioned scans.
3. Now we add the target on the scan details and then select intensiveness of the scan.
4. Now we add the fastness of the scan to get results.
5. Now it scans the whole website using the different types test and results the scanning results and highlight the vulnerability.

acunetix

Administrator

Dashboard

Targets

Vulnerabilities

Scans

Reports

Settings

< Back

Stop Scan

Generate Report

WAF Export...

LOW

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Activity

Completed

Overall progress100%

Scanning of www.ebay.com started

Dec 10, 2024 8:36:35 PM

Scanning of www.ebay.com completed

Dec 10, 2024 8:40:36 PM

Scan Duration4m 4s

Requests2,160

Avg. Response Time255ms

Locations0

Target Information

Addresswww.ebay.com

ServerUnknown

Operating SystemUnknown

Identified Technologies—

Latest Alerts

0020

Clickjacking: X-Frame-Options header missing

Dec 10, 2024 8:36:40 PM

Cookie(s) without HttpOnly flag set

Dec 10, 2024 8:40:33 PM

© 2017 Acunetix Ltd.

Add Target

Address

https://www.ebay.com/

Description

Add Target

Close

< Back

Scan

Save

General

Crawl

HTTP

Advanced

Target Info

https://www.ebay.com/

Description

Business CriticalityNormal

Scan Speed

SlowerSlowModerateFast

Continuous Scanning

Site Login

© 2017 Acunetix Ltd.

×

Add Target

Address

https://shopping.rediff.com/

Description

Add Target

Close

acunetix

Administrator

Dashboard

Targets

Vulnerabilities

Scans

Reports

Settings

Back

Stop Scan

Generate Report

WAF Export...

Scan Stats & Info

Vulnerabilities

Site Structure

Events

LOW

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Activity

Completed

Overall progress

100%

Scanning of shopping.rediff.com started

Dec 10, 2024 8:57:42 PM

Scanning of shopping.rediff.com completed

Dec 10, 2024 9:01:41 PM

Scan Duration

4m 1s

Requests

1,742

Avg. Response Time

616ms

Locations

0

Target Information

Address

shopping.rediff.com

Latest Alerts

Clickjacking: X-Frame-Options header missing

Dec 10, 2024 8:57:47 PM

© 2017 Acunetix Ltd.

Se...	Vulnerability	URL	Parameter	Status	Last Seen
✓	Clickjacking: X-Frame-Options header missing	https://www.ebay.com/		Open	Dec 10, 2024 8:36:40 PM
✓	Clickjacking: X-Frame-Options header missing	https://shopping.rediff.com/		Open	Dec 10, 2024 8:57:47 PM
✓	Cookie(s) without HttpOnly flag set	https://www.ebay.com/		Open	Dec 10, 2024 8:40:32 PM