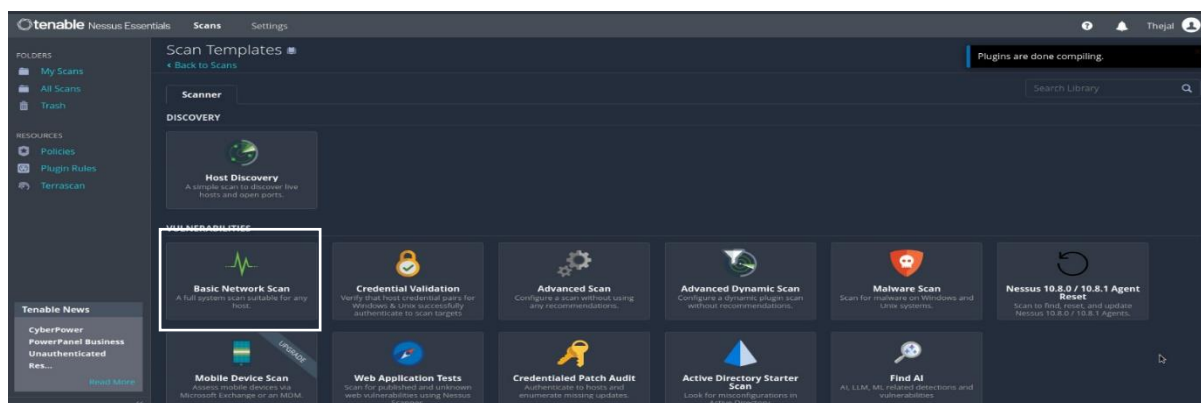


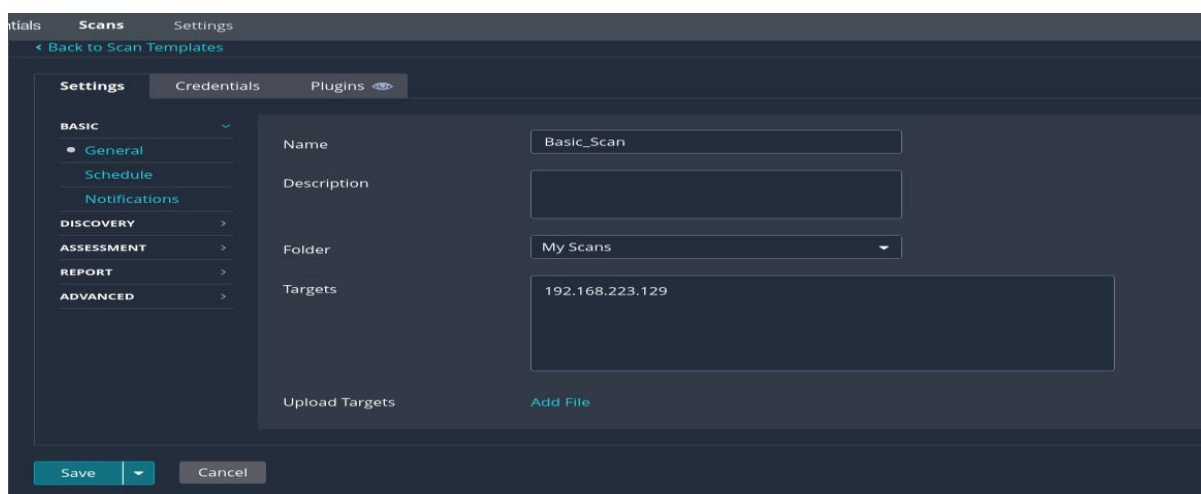
# FAMILIARISING NESSUS ESSENTIALS

## Basic scanning from Nessus to Metasploit

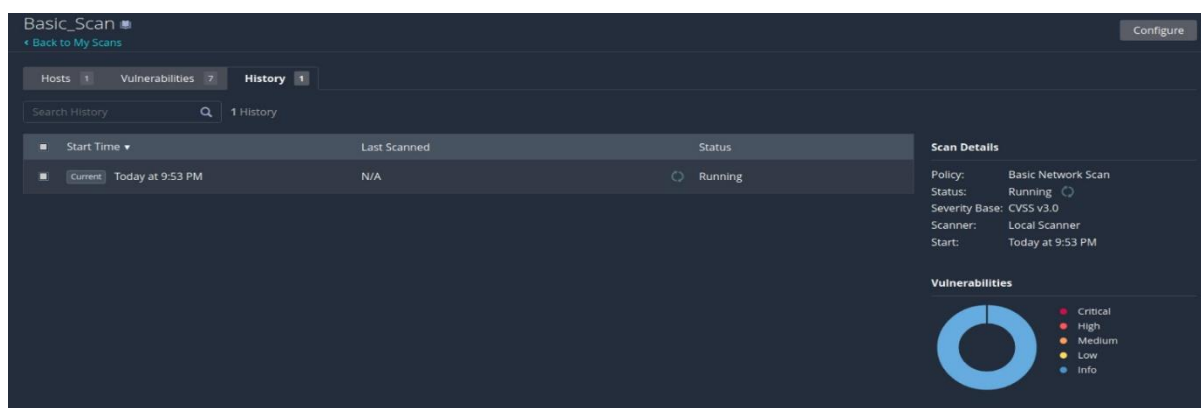
1. Start Nessus service and access the web interface.
2. Go to Scans tab and click on 'Create new scan'.



3. Configure the scan.



4. Click save to store the configuration.
5. Navigate to scans page and click the created scan.
6. Click launch option and monitor the progress.



Filter

Search Vulnerabilities

71 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count		
<div>CRITICAL</div>	10.0 *	7.4	0.6956	UnrealIRCd Backdoor Detection	Backdoors	1		
<div>CRITICAL</div>	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1		
<div>CRITICAL</div>	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2		
<div>CRITICAL</div>	9.8			Bind Shell Backdoor Detection	Backdoors	1		
<div>MIXED</div>	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4		
<div>CRITICAL</div>	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		
<div>HIGH</div>	7.5 *	7.4	0.015	rlogin Service Detection	Service detection	1		
<div>HIGH</div>	7.5 *	7.4	0.015	rsh Service Detection	Service detection	1		
<div>HIGH</div>	7.5	5.9	0.0489	Samba Badlock Vulnerability	General	1		
<div>HIGH</div>	7.5			NFS Shares World Readable	RPC	1		
<div>MIXED</div>	...	...	...	SSL (Multiple Issues)	General	28		

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 9:53 PM

End:

Today at 10:06 PM

Elapsed:

13 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

- The report lists 71 vulnerabilities identified in the scan.
- Vulnerabilities are categorized by severity,
  1. Critical – Immediate attention needed.
  2. High – Significant risk.
  3. Mixed – Combination of multiple severity levels.
- CVSS (Common Vulnerability Scoring System) quantifies the risk on a scale of 0 to 10.
- VPR (Vulnerability Priority Rating) prioritizing the vulnerabilities.
- EPSS (Exploit Prediction Scoring System) indicates likelihood of the exploitation.

Basic\_Scan

Configure

Audit Trail

Launch

Report

Export

Back to My Scans

Hosts1

Vulnerabilities71

Remediations3

History1

Search Actions

3 Actions

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 9:53 PM

End:

Today at 10:06 PM

Elapsed:

13 minutes

Remediation section provides actionable steps to mitigate the identified vulnerabilities.