


Vulnerability Assessment



A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed

After the port scan, we need to find the vulnerabilities for each port and Vulnerability assessment can help us



Vulnerability Assessment

Searchsploit

- Simple command line utility (Kali) to search through **exploit DB**

Nessus

- Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use. It is available for both Windows as well as Kali
(Paid tool)



**searchsploit Comes Pre-
installed with Kali**

Searchsploit

- ❖ Run the scan and check for vulnerabilities

```
>searchsploit vsftpd 2.3.4
```

```
(kali@kali)-[~]
└─$ searchsploit vsftpd 2.3.4
```

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb



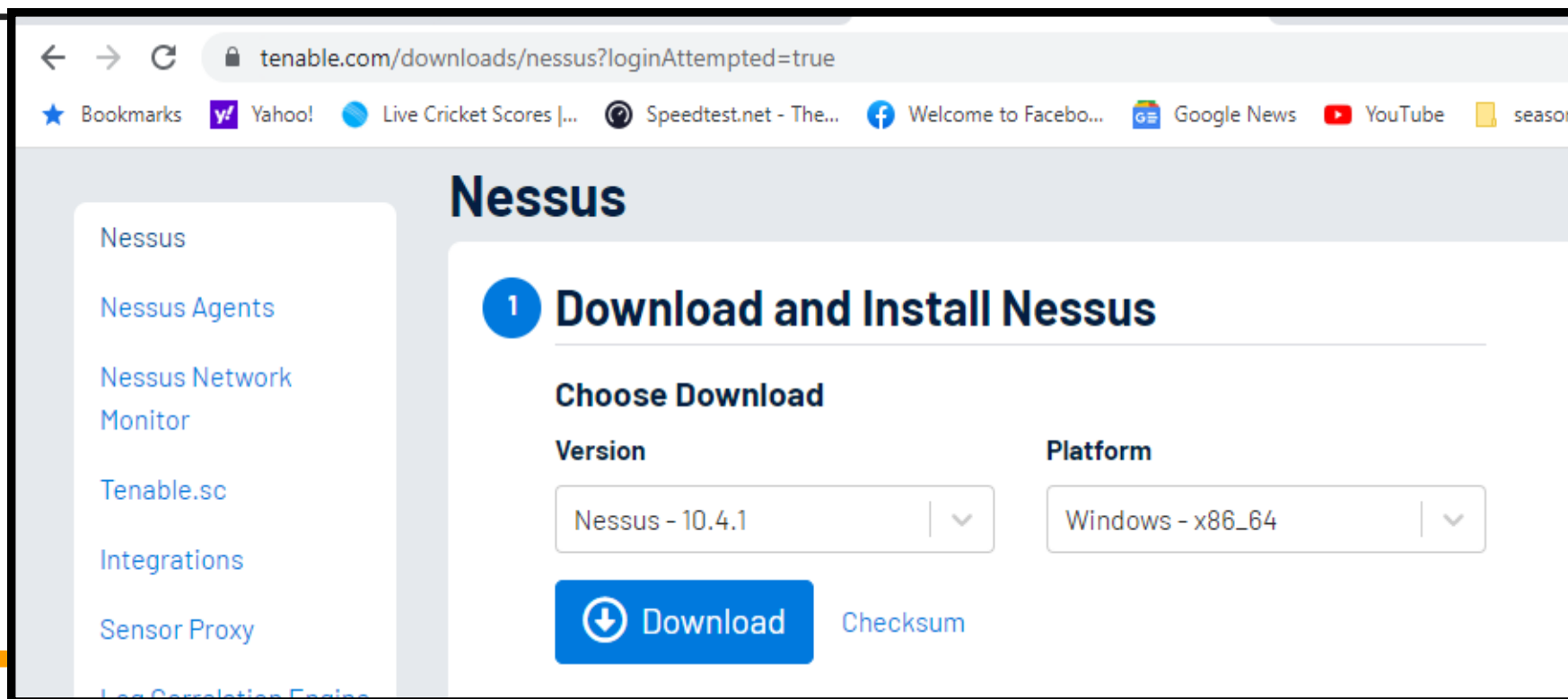
Nessus

**(Trial Version allows scanning
for 16 Ips)**

Step- 1

- ❖ Visit the official Nessus Website, download it and install it

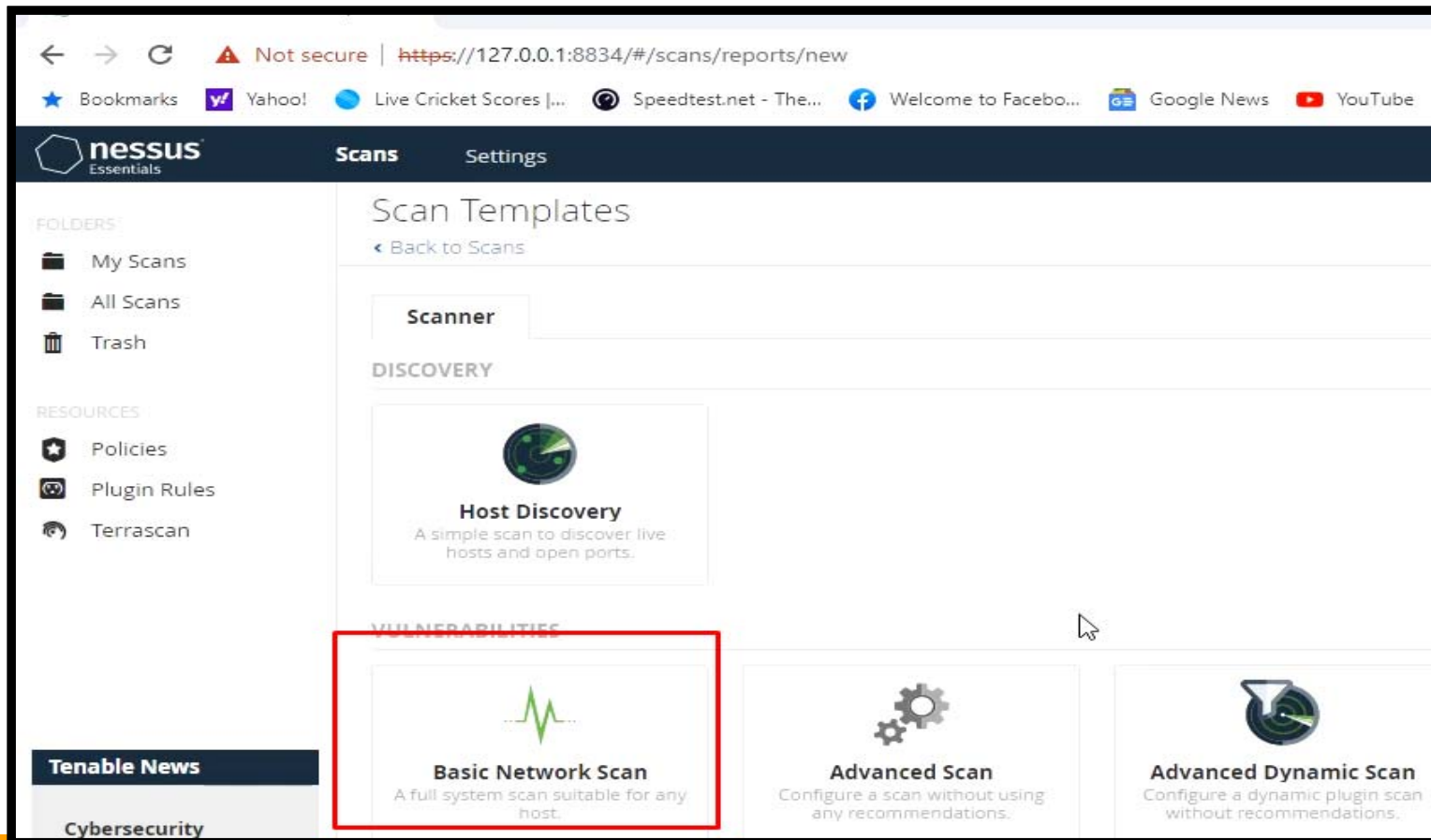
<https://www.tenable.com/downloads/nessus>



The screenshot shows a web browser window displaying the Nessus download page. The address bar shows the URL `tenable.com/downloads/nessus?loginAttempted=true`. The page features a navigation menu on the left with links for Nessus, Nessus Agents, Nessus Network Monitor, Tenable.sc, Integrations, and Sensor Proxy. The main content area is titled "Nessus" and contains a section "1 Download and Install Nessus". Under the heading "Choose Download", there are two dropdown menus: "Version" set to "Nessus - 10.4.1" and "Platform" set to "Windows - x86_64". Below these menus is a blue "Download" button with a downward arrow icon and a "Checksum" link.

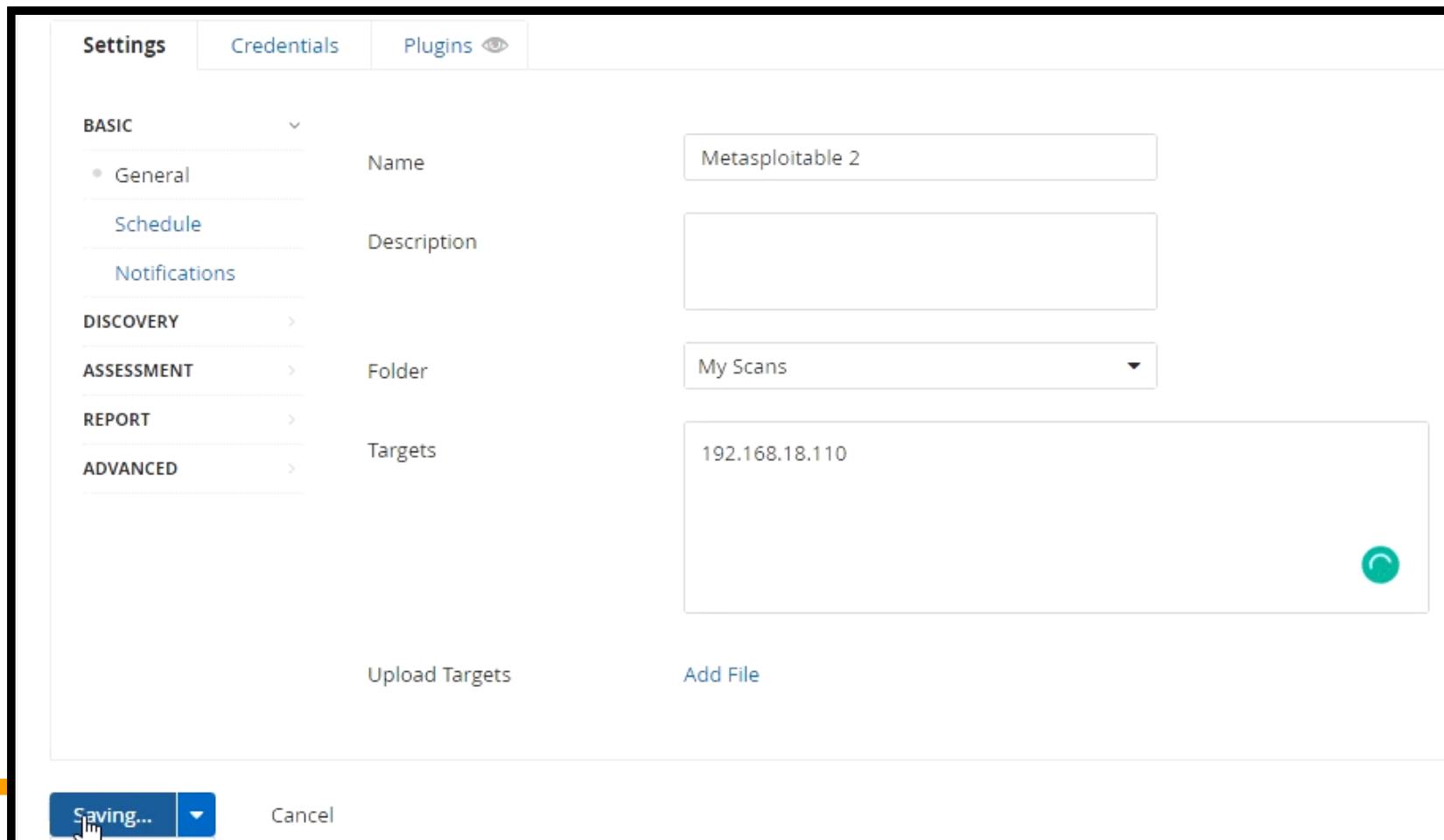
Step- 2

❖ Select to conduct a basic Network scan



Step- 3

❖ Give a target and start the scan



The screenshot shows the Metasploit web interface with the 'Settings' tab selected. The 'BASIC' section is expanded to show 'General' settings. The 'Name' field is filled with 'Metasploitable 2'. The 'Description' field is empty. The 'Folder' dropdown menu is set to 'My Scans'. The 'Targets' field contains the IP address '192.168.18.110'. At the bottom of the form, there are buttons for 'Upload Targets', 'Add File', 'Saving...', and 'Cancel'. A mouse cursor is pointing at the 'Saving...' button.

Section	Field	Value
BASIC	Name	Metasploitable 2
	Description	
	Folder	My Scans
	Targets	192.168.18.110

Step- 4

❖ Nessus will scan the target and provide a complete report

The screenshot shows the Nessus interface for a scan titled 'Metasploitable 2'. At the top, there are links for 'Configure' and 'Audit Tra'. Below the scan title, there are summary boxes for 'Hosts 1', 'Vulnerabilities 69', 'Remediations 3', 'VPR Top Threats' (with a warning icon), and 'History 1'. A search bar is present with the text 'Search Vulnerabilities' and a magnifying glass icon, followed by the text '69 Vulnerabilities'. Below this is a table of vulnerabilities with columns for 'Sev', 'Score', 'Name', 'Family', and 'Count'. Each row includes a checkbox, a severity label (all 'CRITICAL'), a score, a vulnerability name, a family name, and a count of 1. The first six vulnerabilities are listed, with a hand cursor hovering over the 'Service detection' entry.

<input type="checkbox"/>	Sev ▾	Score ▾	Name ▾	Family ▾	Count ▾	⚙
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Inf...	RPC	1	⊖ / ✎
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Det&on	Service detection	1	⊕ / ✎
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System ...	General	1	⊖ / ✎
<input type="checkbox"/>	CRITICAL	10.0 *	UnrealIRCd Backdoor D...	Backdoors	1	⊖ / ✎
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' ...	Gain a shell remotely	1	⊖ / ✎
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor De...	Backdoors	1	⊖ / ✎



DEMO



THANKS