


# 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
<b>vsftpd 2.3.4</b> - Backdoor Command Execution	unix/remote/49757.py
<b>vsftpd 2.3.4</b> - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb



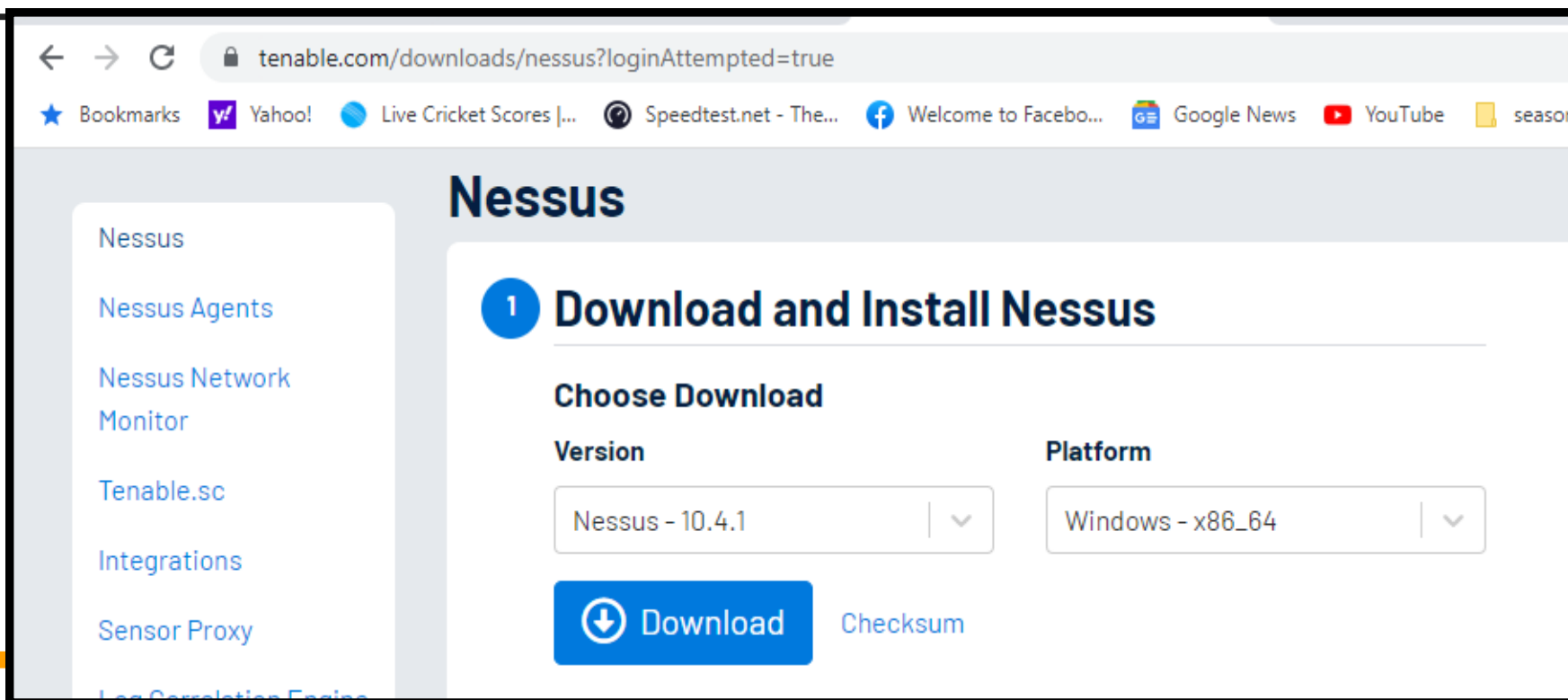
**Nessus**

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

# Step- 1

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

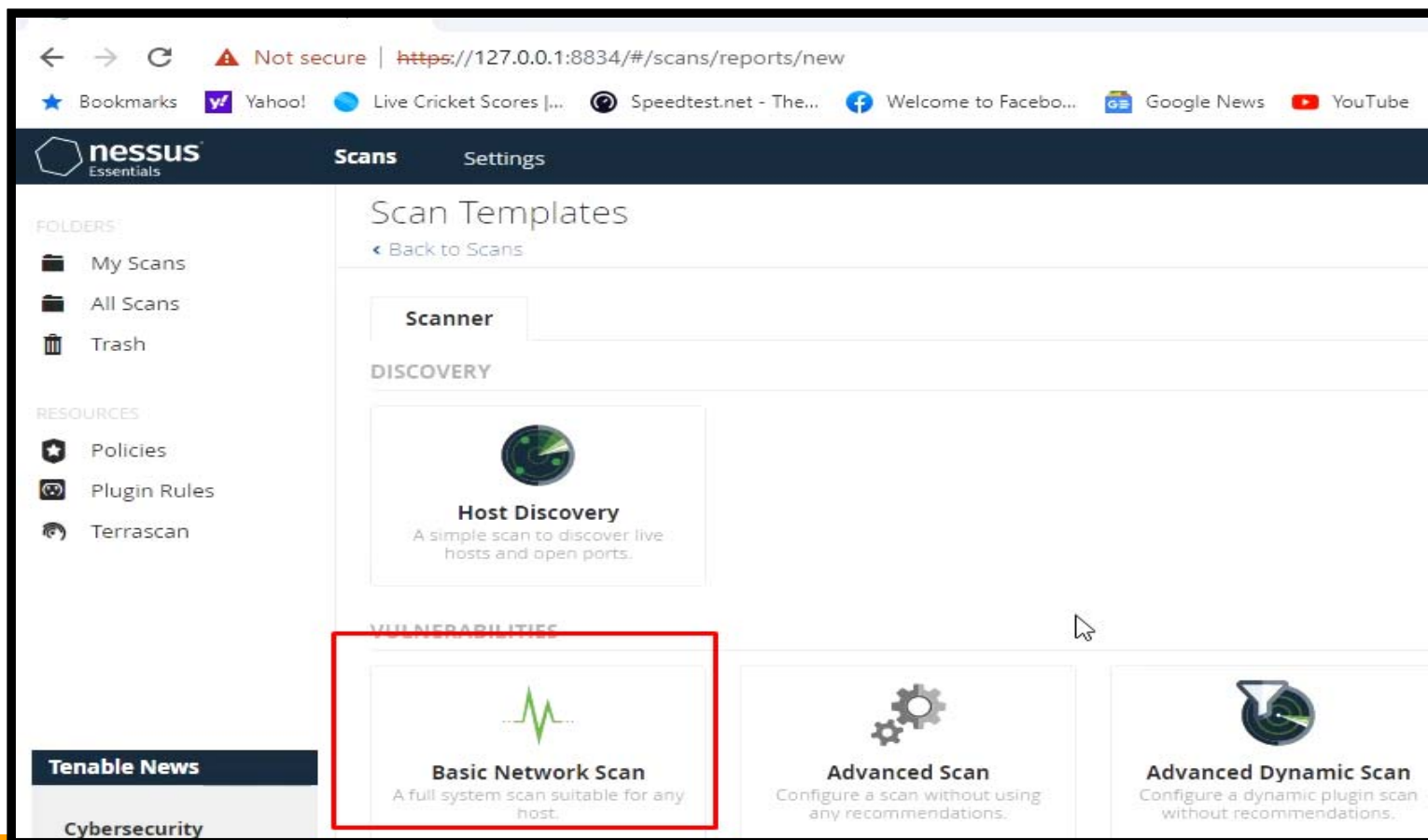
<https://www.tenable.com/downloads/nessus>



The screenshot shows a web browser window with the URL `tenable.com/downloads/nessus?loginAttempted=true`. The browser's address bar and bookmarks are visible. The main content area features the heading "Nessus" and a section titled "1 Download and Install Nessus". Underneath, there is a "Choose Download" section with two dropdown menus: "Version" set to "Nessus - 10.4.1" and "Platform" set to "Windows - x86\_64". A blue "Download" button with a downward arrow icon is prominently displayed, along with 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 Settings interface. The 'Settings' tab is active, with sub-tabs for 'Credentials' and 'Plugins'. The 'BASIC' section is expanded, showing 'General', 'Schedule', and 'Notifications'. The 'Name' field is set to 'Metasploitable 2'. The 'Description' field is empty. The 'Folder' dropdown is set to 'My Scans'. The 'Targets' field contains the IP address '192.168.18.110'. At the bottom, 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
DISCOVERY	Targets	192.168.18.110
	Upload Targets	
ASSESSMENT	Add File	

# 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 right, there are links for 'Configure' and 'Audit Tra'. Below the title, there is a 'Back to My Scans' link. A navigation bar shows 'Hosts 1', 'Vulnerabilities 69', 'Remediations 3', 'VPR Top Threats', and 'History 1'. A search bar is present with the text 'Search Vulnerabilities' and a magnifying glass icon, followed by '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 (CRITICAL), a score, a truncated name, a family name, and a count of 1. Action icons (refresh and edit) are visible for each row.

<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