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
```

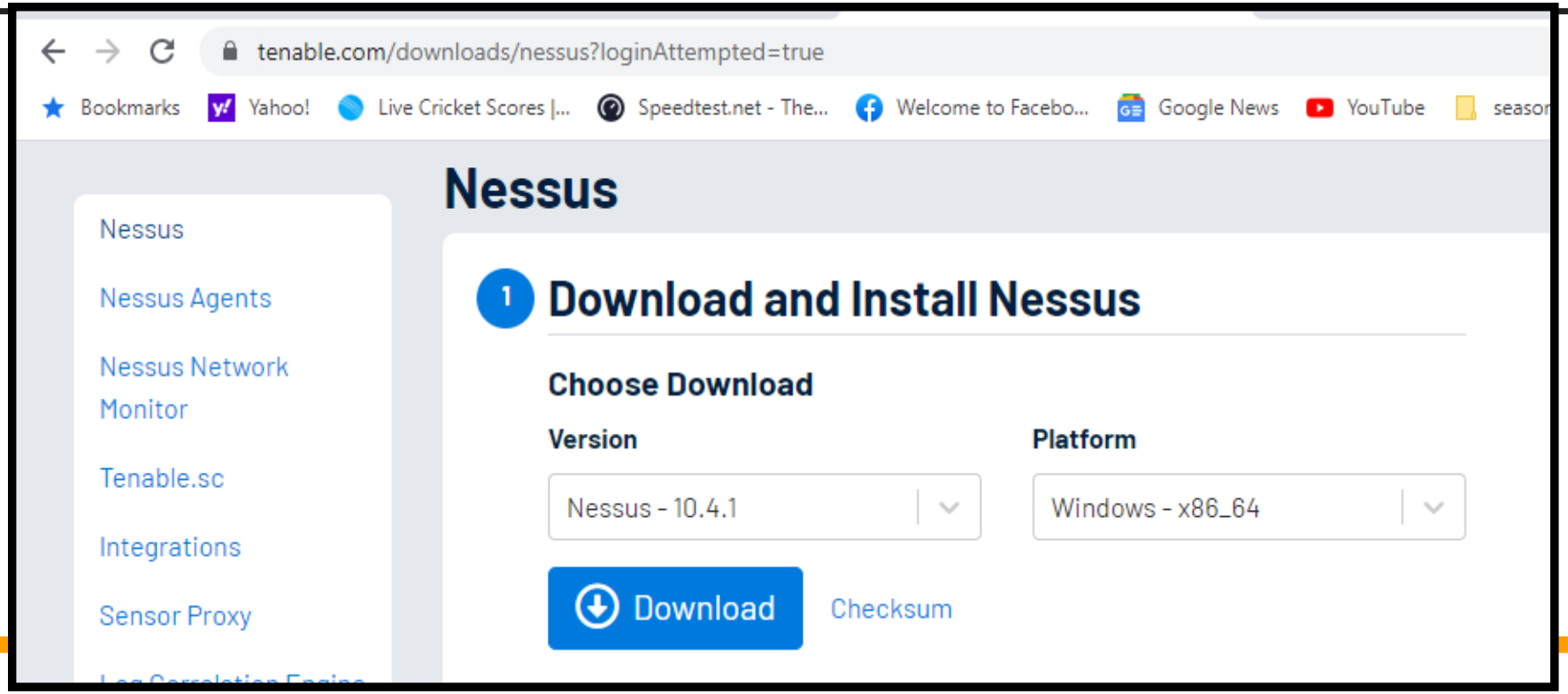
Nessus

(Trial Version allows scanning for 16 Ips)

Step- 1

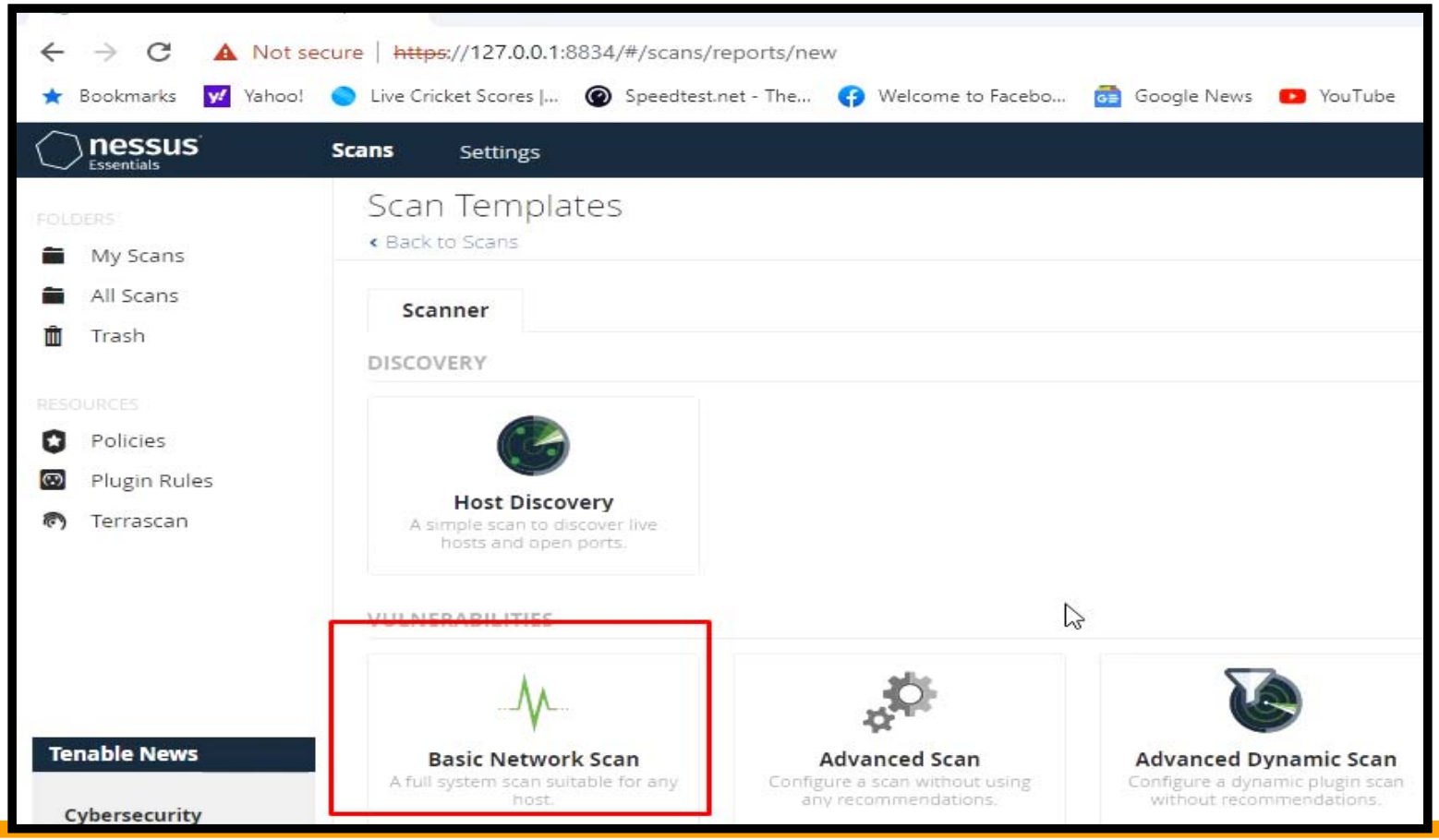
- Visit the official Nessus Website, download it and install it

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



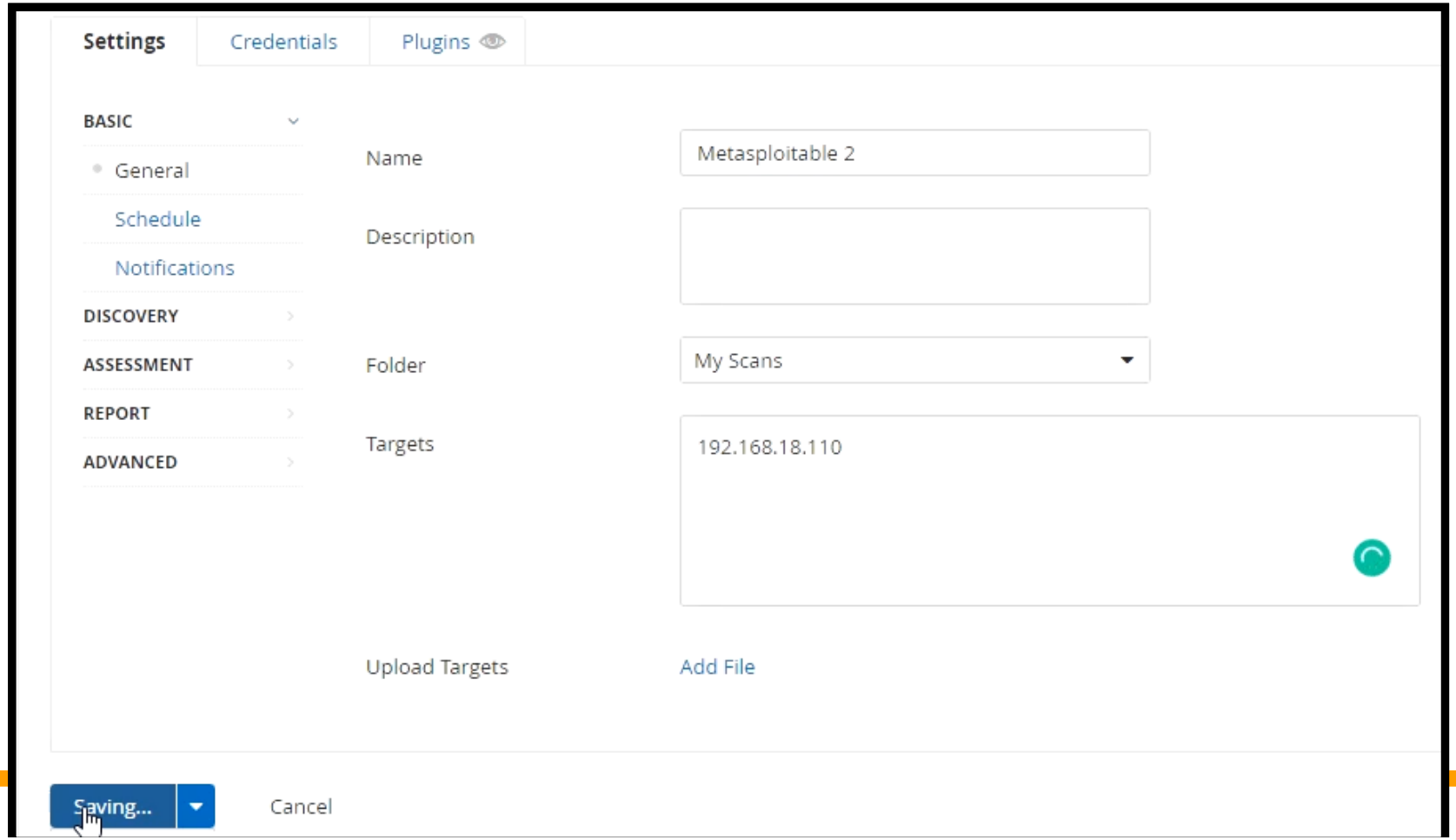
Step- 2

- Select to conduct a basic Network scan



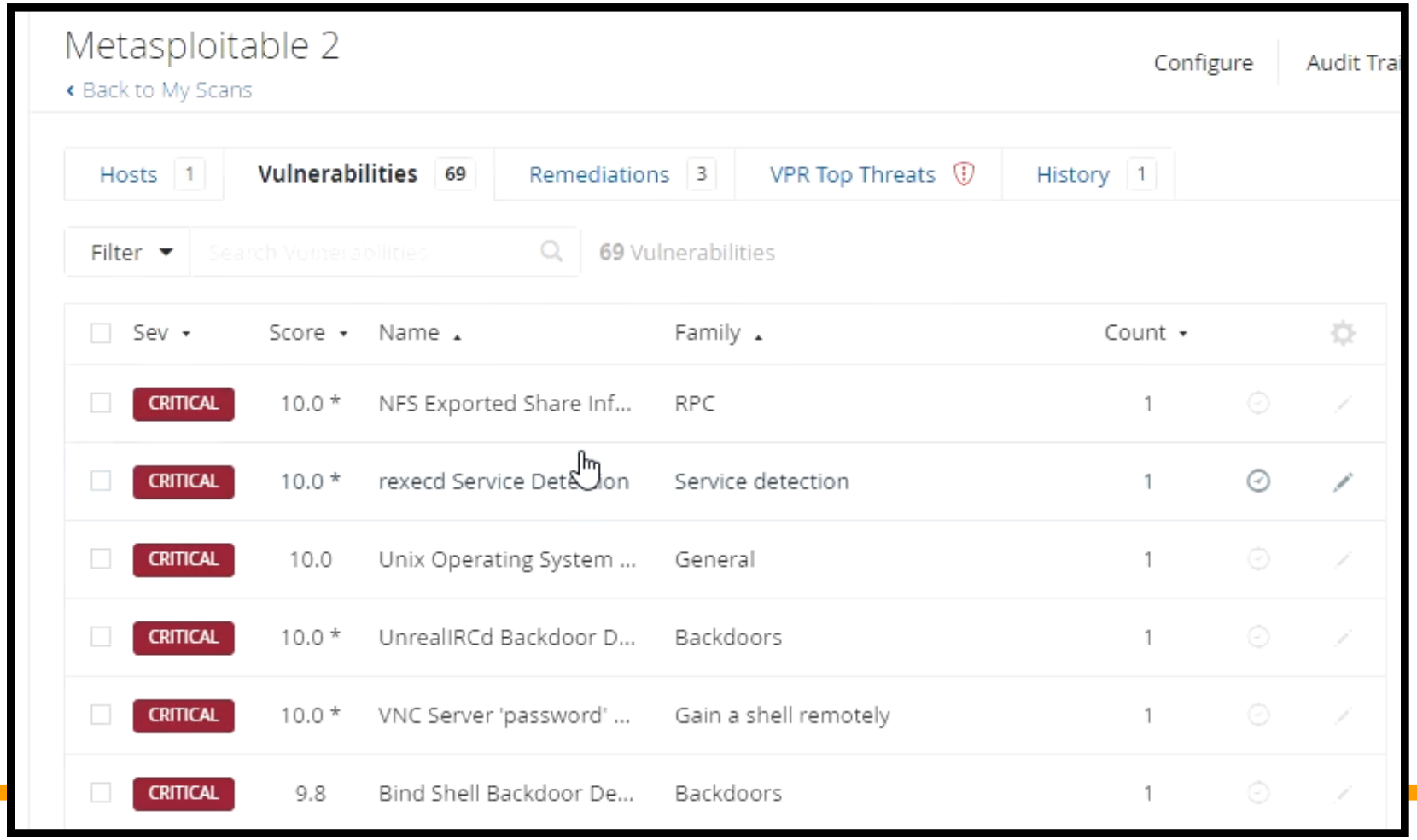
Step- 3

- Give a target and start the scan



Step- 4

- Nessus will scan the target and provide a complete report



DEMO

THANKS