-Sadiq S.

Practical 4

Aim: Practical on vulnerability scanning and assessment

Our Target Machine will be metasploitable2 and target live hosts will be theresianz.in

Vulnerability Scanning using Nmap

1. Navigate to nmap scripts folder and view all the scripts in that folder

```
┌──(kali㉿kali)-[/]
└─$ cd usr/share/nmap/scripts

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls -la | more
total 4972
drwxr-xr-x 2 root root 32768 Mar 10  2023 .
drwxr-xr-x 4 root root  4096 Mar 10  2023 ..
-rw-r--r-- 1 root root  3901 Jan  9  2023 acarsd-info.nse
-rw-r--r-- 1 root root  8749 Jan  9  2023 address-info.nse
-rw-r--r-- 1 root root  3345 Jan  9  2023 afp-brute.nse
-rw-r--r-- 1 root root  6463 Jan  9  2023 afp-ls.nse
-rw-r--r-- 1 root root  7001 Jan  9  2023 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 Jan  9  2023 afp-serverinfo.nse
-rw-r--r-- 1 root root  2621 Jan  9  2023 afp-showmount.nse
-rw-r--r-- 1 root root  2262 Jan  9  2023 ajp-auth.nse
-rw-r--r-- 1 root root  2983 Jan  9  2023 ajp-brute.nse
-rw-r--r-- 1 root root  1329 Jan  9  2023 ajp-headers.nse
-rw-r--r-- 1 root root  2590 Jan  9  2023 ajp-methods.nse
-rw-r--r-- 1 root root  3051 Jan  9  2023 ajp-request.nse
-rw-r--r-- 1 root root  6719 Jan  9  2023 allseeingeye-info.nse
-rw-r--r-- 1 root root  1678 Jan  9  2023 amqp-info.nse
-rw-r--r-- 1 root root 15024 Jan  9  2023 asn-query.nse
-rw-r--r-- 1 root root  2054 Jan  9  2023 auth-owners.nse
-rw-r--r-- 1 root root   870 Jan  9  2023 auth-spoof.nse
-rw-r--r-- 1 root root  9050 Jan  9  2023 backorifice-brute.nse
-rw-r--r-- 1 root root 10193 Jan  9  2023 backorifice-info.nse
-rw-r--r-- 1 root root 53137 Jan  9  2023 bacnet-info.nse
-rw-r--r-- 1 root root  6136 Jan  9  2023 banner.nse
-rw-r--r-- 1 root root  2012 Jan  9  2023 bitcoin-getaddr.nse
-rw-r--r-- 1 root root  1812 Jan  9  2023 bitcoin-info.nse
-rw-r--r-- 1 root root  4437 Jan  9  2023 bitcoinrpc-info.nse
-rw-r--r-- 1 root root  4079 Jan  9  2023 bittorrent-discovery.nse
-rw-r--r-- 1 root root  1344 Jan  9  2023 bjnp-discover.nse
-rw-r--r-- 1 root root  4428 Jan  9  2023 broadcast-ataoe-discover.nse
-rw-r--r-- 1 root root  2964 Jan  9  2023 broadcast-avahi-dos.nse
-rw-r--r-- 1 root root  4786 Jan  9  2023 broadcast-bjnp-discover.nse
-rw-r--r-- 1 root root  2438 Jan  9  2023 broadcast-db2-discover.nse
-rw-r--r-- 1 root root  3217 Jan  9  2023 broadcast-dhcp6-discover.nse
-rw-r--r-- 1 root root 10151 Jan  9  2023 broadcast-dhcp-discover.nse
-rw-r--r-- 1 root root  1499 Jan  9  2023 broadcast-dns-service-discovery.nse
-rw-r--r-- 1 root root  3866 Jan  9  2023 broadcast-dropbox-listener.nse
-rw-r--r-- 1 root root 12202 Jan  9  2023 broadcast-eigrp-discovery.nse
-rw-r--r-- 1 root root  3472 Jan  9  2023 broadcast-hid-discoveryd.nse
-rw-r--r-- 1 root root 14655 Jan  9  2023 broadcast-igmp-discovery.nse
-rw-r--r-- 1 root root  3184 Jan  9  2023 broadcast-jenkins-discover.nse
-rw-r--r-- 1 root root 10449 Jan  9  2023 broadcast-listener.nse
-rw-r--r-- 1 root root  3813 Jan  9  2023 broadcast-ms-sql-discover.nse
-rw-r--r-- 1 root root  1909 Jan  9  2023 broadcast-netbios-master-browser.nse
-rw-r--r-- 1 root root  2330 Jan  9  2023 broadcast-networker-discover.nse
-rw-r--r-- 1 root root  2005 Jan  9  2023 broadcast-novell-locate.nse
mouse pointer inside or press Ctrl+G.
```

2. Update scripts: Before Nmap can be used to perform a vulnerability scan, penetration testers must update the Nmap script database to see whether there are any new scripts added to the database, so that they do not miss the vulnerability identification.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 00:31 EDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 4.05 seconds
```

-Sadiq S.

My Metasploitable 2 IP Address: 192.168.117.128

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:8a:27:84
          inet addr:192.168.117.128  Bcast:192.168.117.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe8a:2784/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3406 (3.3 KB)  TX bytes:5954 (5.8 KB)
          Interrupt:17 Base address:0x2000
```

3. Run Nmap to check vulnerability services running on metasploitable2.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sC 192.168.117.128
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 00:34 EDT
```

mouse pointer inside or press Ctrl+G.

```
Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m03s, deviation: 2h00m00s, median: 2s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-10-10T00:34:55-04:00

Nmap done: 1 IP address (1 host up) scanned in 76.68 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$
```

mouse pointer inside or press Ctrl+G.

4. Let us find available scripts to find vulnerability for ssh. And get information on any one

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | grep ssh
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help ssh2-enum-algos.nse
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 00:38 EDT

ssh2-enum-algos
Categories: safe discovery
https://nmap.org/nsedoc/scripts/ssh2-enum-algos.html
  Reports the number of algorithms (for encryption, compression, etc.) that
  the target SSH2 server offers. If verbosity is set, the offered algorithms
  are each listed by type.

  If the "client to server" and "server to client" algorithm lists are identical
  (order specifies preference) then the list is shown only once under a combined
  type.
```

5. Get more info on ssh-run script

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help ssh-run.nse
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 00:39 EDT

ssh-run
Categories: intrusive
https://nmap.org/nsedoc/scripts/ssh-run.html
  Runs remote command on ssh server and returns command output.
```

6. Let's run the ssh-run script on our target (msf2 IP = 192.168.117.128)

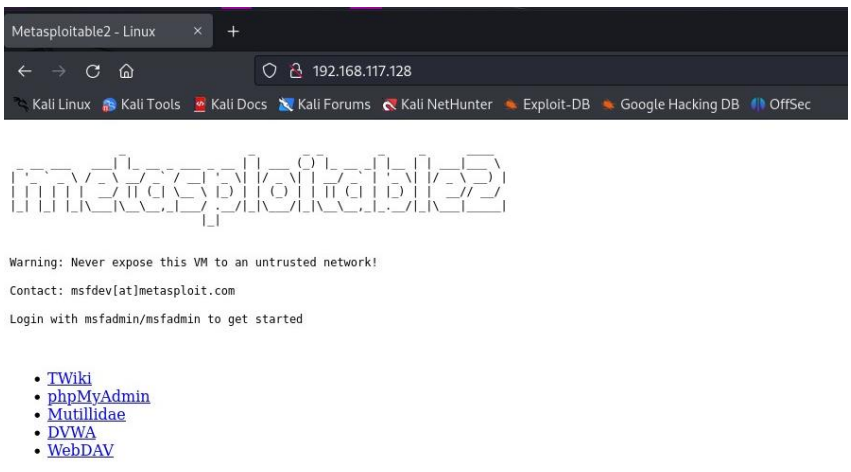
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=ssh-run 192.168.117.128
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 00:41 EDT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for 192.168.117.128
Host is up (0.036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
|_ssh-run: Failed to specify credentials and command to run.
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

Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
```

6. Get available scripts for http

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | grep http
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-cakephp-version.nse
```

Web Server Vulnerability Scanning:

1. Run metasploitable2 website on Firefox in kali linux



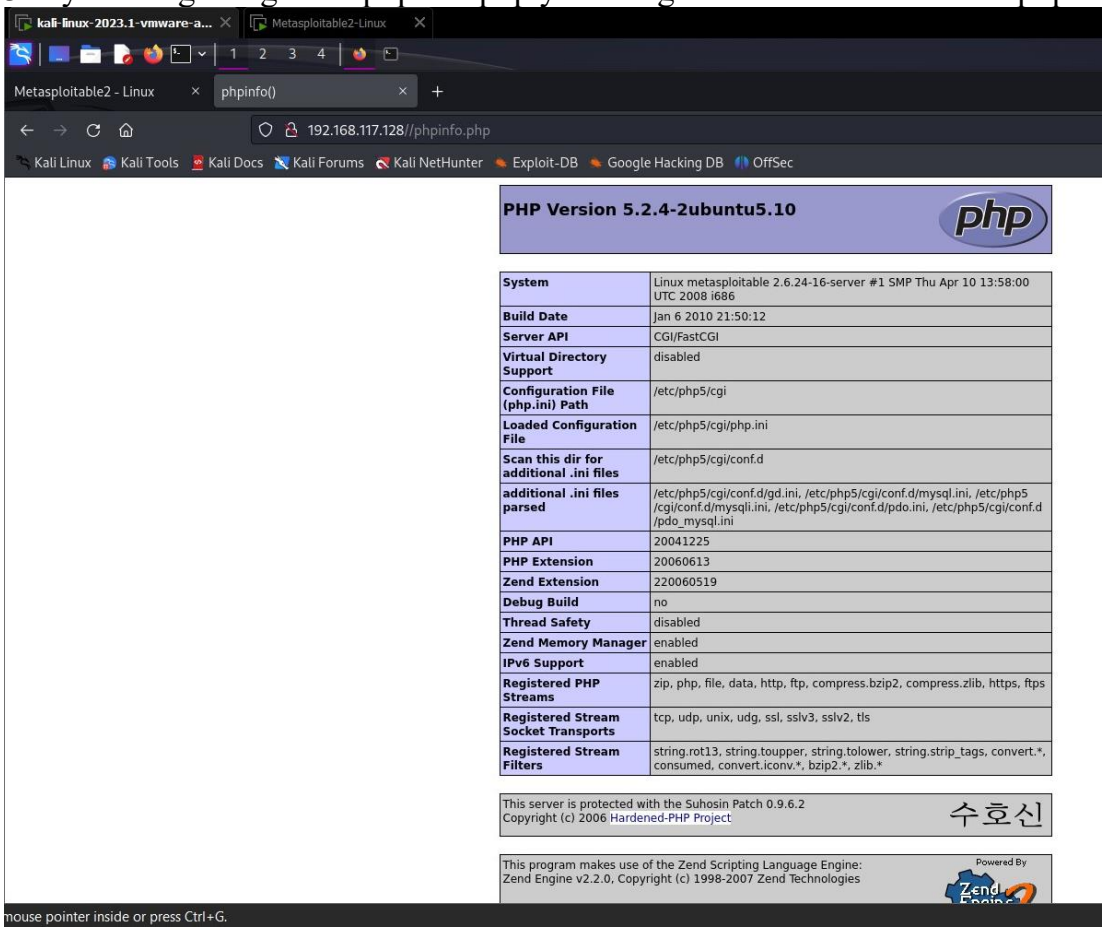
-Sadiq S.

2. Using Nikto tool scan the target for vulnerabilities “nikto -host 192.168.117.128”

```
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http
me.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2023-10-10 00:46:55 (GMT-4) (55 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

As you can see, PHP5 has many vulnerabilities when installed on a server.

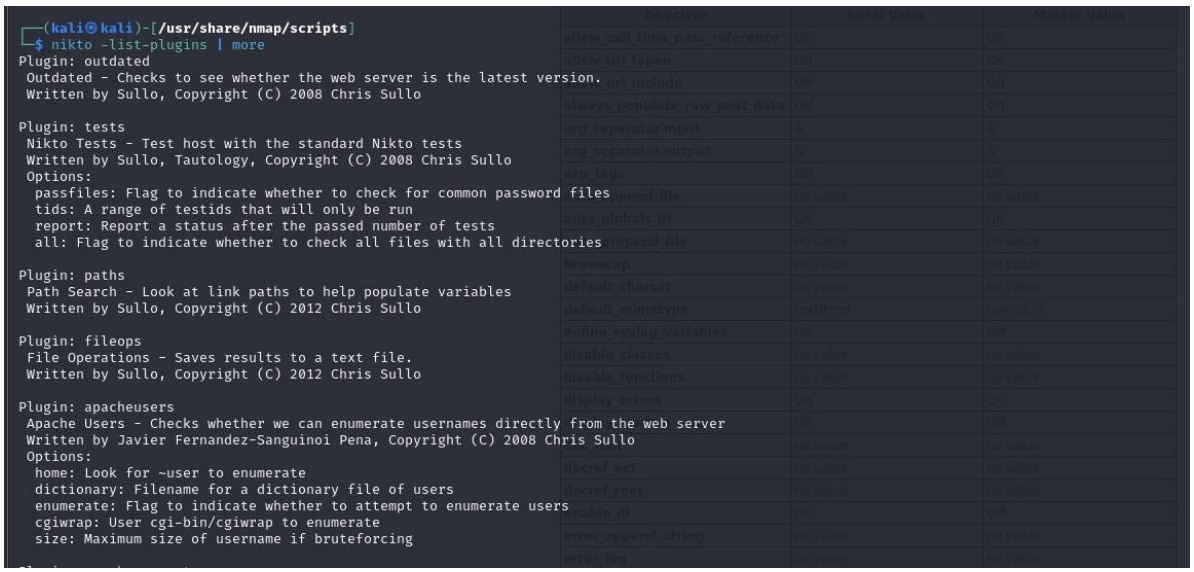
3. By running <targetIP>/phpinfo.php you can get information about the php version



-Sadiq S.

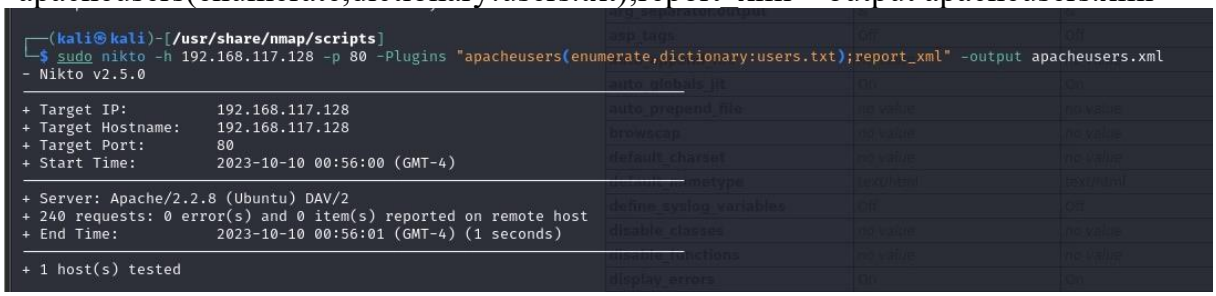
Customizing Nikto

1. List all the plugins in the Nikto tool



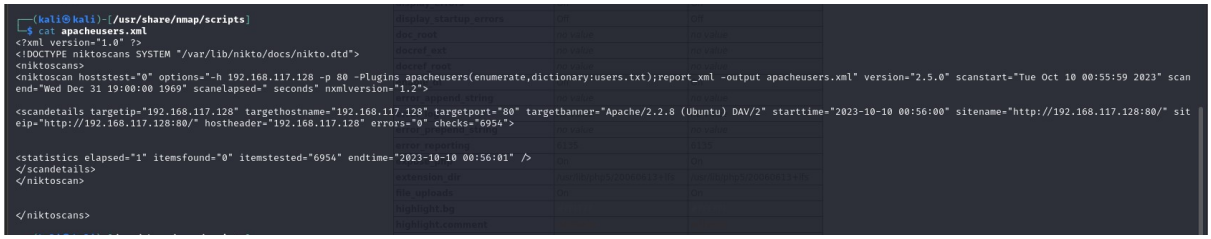
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nikto -list-plugins | more
Plugin: outdated
 Outdated - Checks to see whether the web server is the latest version.
 Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: tests
 Nikto Tests - Test host with the standard Nikto tests
 Written by Sullo, Tautology, Copyright (C) 2008 Chris Sullo
 Options:
  passfiles: Flag to indicate whether to check for common password files
  tids: A range of testids that will only be run
  report: Report a status after the passed number of tests
  all: Flag to indicate whether to check all files with all directories

Plugin: paths
 Path Search - Look at link paths to help populate variables
 Written by Sullo, Copyright (C) 2012 Chris Sullo

Plugin: fileops
 File Operations - Saves results to a text file.
 Written by Sullo, Copyright (C) 2012 Chris Sullo

Plugin: apacheusers
 Apache Users - Checks whether we can enumerate usernames directly from the web server
 Written by Javier Fernandez-Sanguinoi Pena, Copyright (C) 2008 Chris Sullo
 Options:
  home: Look for ~user to enumerate
  dictionary: Filename for a dictionary file of users
  enumerate: Flag to indicate whether to attempt to enumerate users
  cgiwrap: User cgi-bin/cgiwrap to enumerate
  size: Maximum size of username if bruteforcing
```

2. Running Nikto with specific plugin to find active users on the target server "sudo nikto -h 192.168.204.128 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" -output apacheusers.xml"



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nikto -h 192.168.117.128 -p 80 -Plugins "apacheusers(enumerate,dictionary:users.txt);report_xml" -output apacheusers.xml
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.117.128
+ Target Hostname:    192.168.117.128
+ Target Port:        80
+ Start Time:         2023-10-10 00:56:00 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ 240 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2023-10-10 00:56:01 (GMT-4) (1 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Also type "cat apacheusers.xml" to see the output file we got using the above command.



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ cat apacheusers.xml
<?xml version="1.0" ?>
<!DOCTYPE niktoscans SYSTEM "/var/lib/nikto/docs/nikto.dtd">
<niktoscans>
<niktoscan hoststest="0" options="-h 192.168.117.128 -p 80 -Plugins apacheusers(enumerate,dictionary:users.txt);report_xml -output apacheusers.xml" version="2.5.0" scanstart="Tue Oct 10 00:55:59 2023" scanend="Wed Dec 31 19:00:00 1969" scanelapsed=" seconds" nxmlversion="1.2">

<scandetails targetip="192.168.117.128" targethostname="192.168.117.128" targetport="80" targetbanner="Apache/2.2.8 (Ubuntu) DAV/2" starttime="2023-10-10 00:56:00" sitename="http://192.168.117.128:80/" siteip="http://192.168.117.128:80/" hostheader="192.168.117.128" errors="0" checks="6954">


<statistics elapsed="1" itemsfound="0" itemstested="6954" endtime="2023-10-10 00:56:01" />
</scandetails>
</niktoscan>


</niktoscans>
```

-Sadiq S.

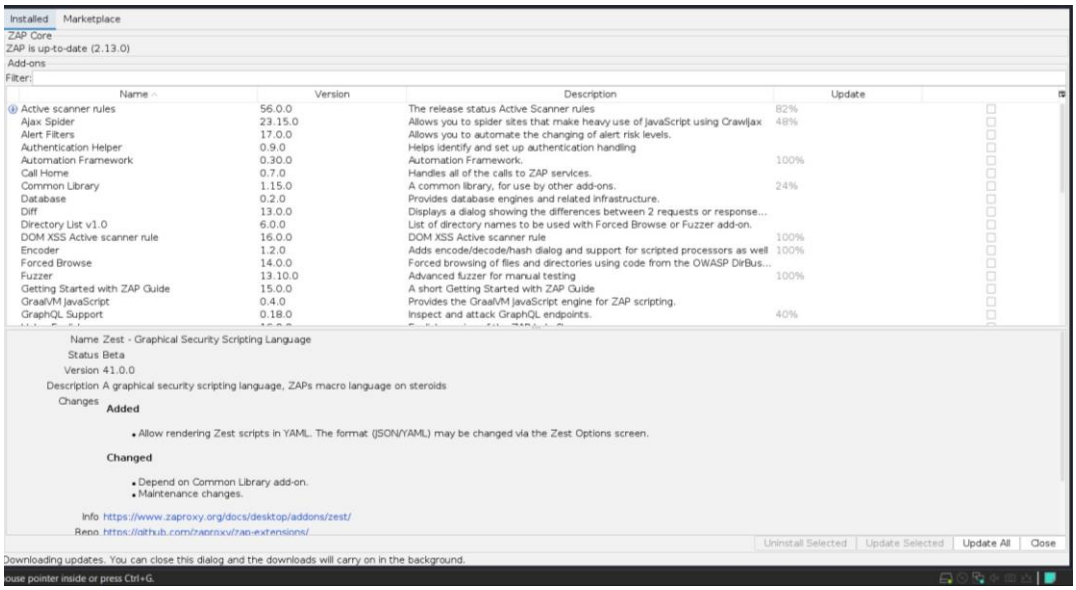
OWASP ZAP

One of the most effective scanners based on the number of verified vulnerabilities discovered is OWASP ZAP. This tool is not preinstalled in Kali Linux 2021.

1. Install the latest version of OWASP ZAP

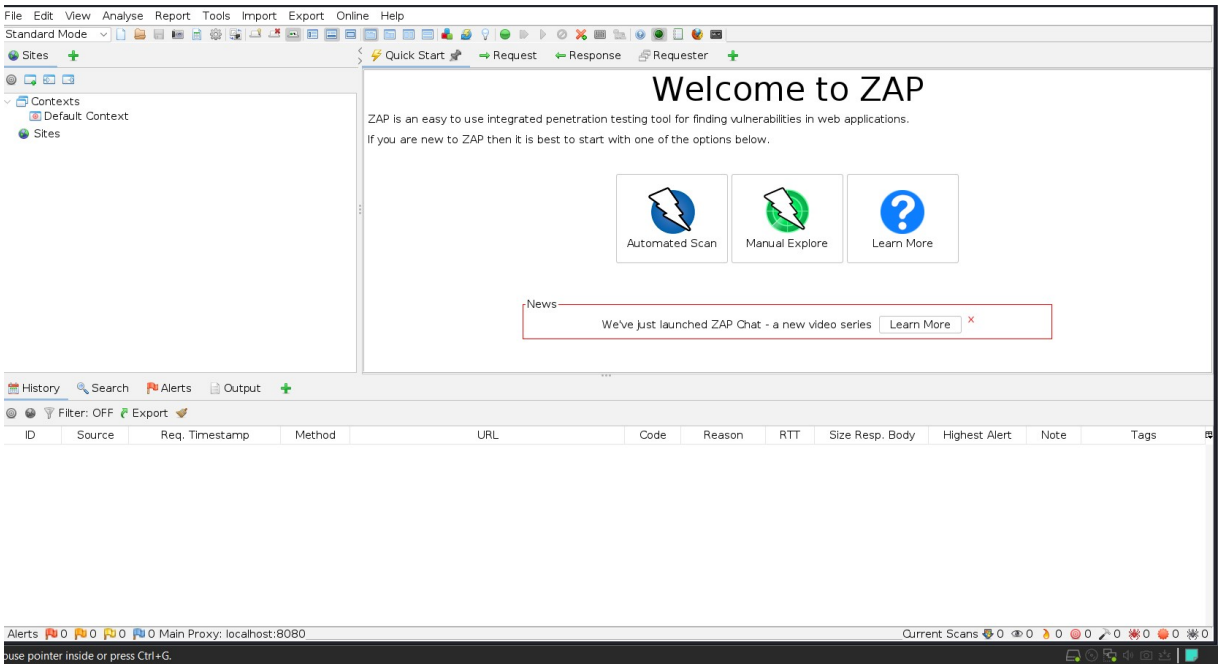
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install zaproxy
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  python3-cryptography37
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  zaproxy
0 upgraded, 1 newly installed, 0 to remove and 1050 not upgraded.
Need to get 186 MB of archives.
After this operation, 246 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.13.0-0kali1 [186 MB]
Fetched 186 MB in 49s (3,778 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 394019 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.13.0-0kali1_all.deb ...
Unpacking zaproxy (2.13.0-0kali1) ...
Setting up zaproxy (2.13.0-0kali1) ...
Processing triggers for kali-menu (2023.1.7) ...
```

2. Run the tool. And on start-up make the appropriate selections and update the plugins

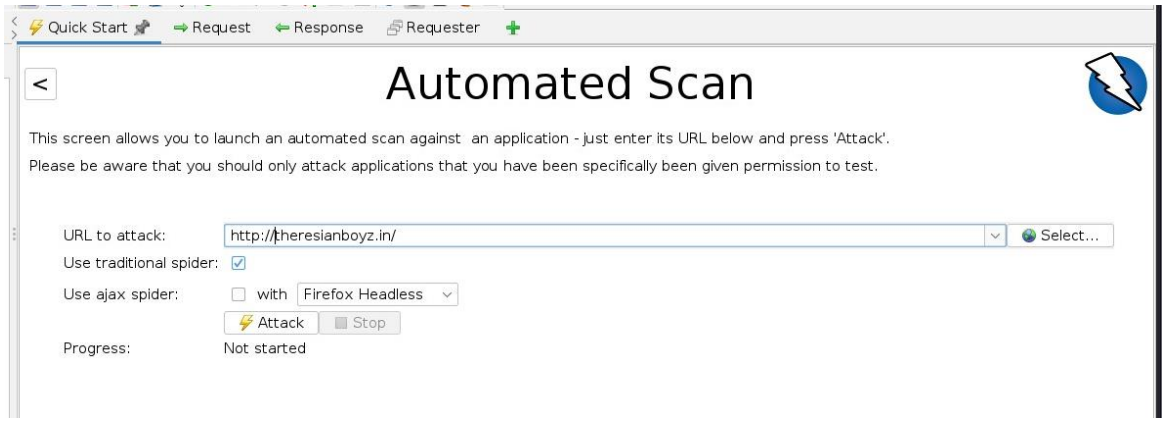


-Sadiq S.

This is the homepage after all steps are followed.



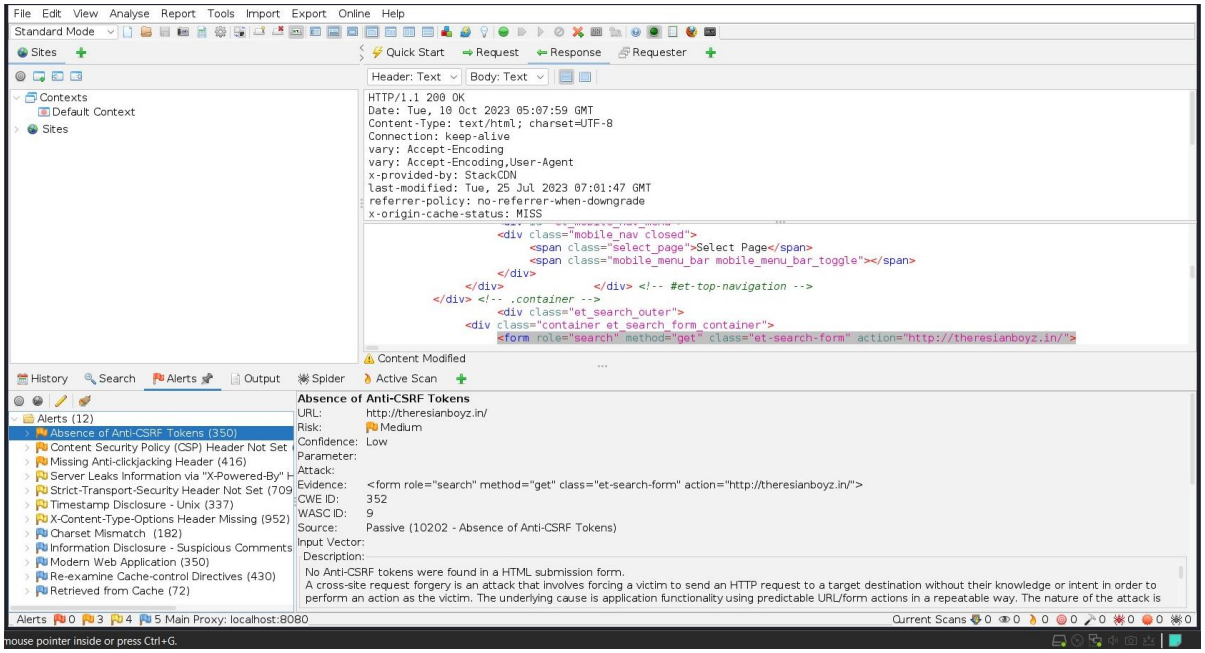
Click on Automated scan and enter the URL to scan



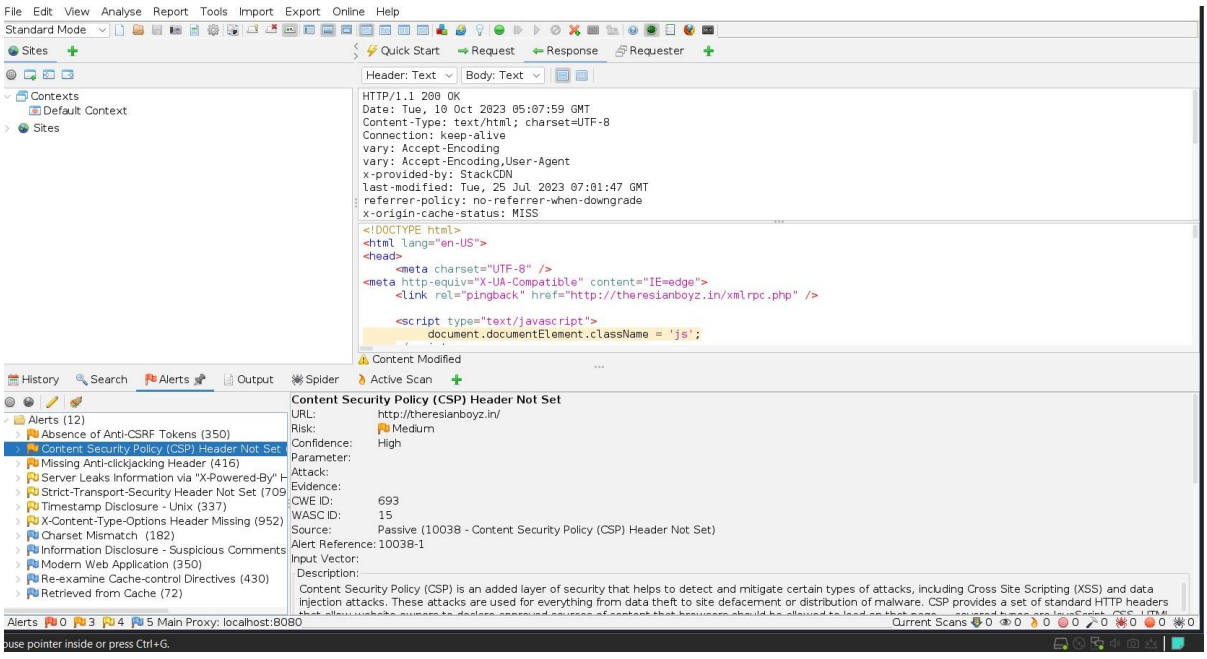
-Sadiq S.

3. After the scan you can click on the identified results to drill down to specific findings. OWASP ZAP can help you find vulnerabilities such as reflected cross-site scripting, stored cross-site scripting, SQL injection, and remote OS command injection.

We got 12 alert out of which 3 are medium, 4 are low and 5 are Informational

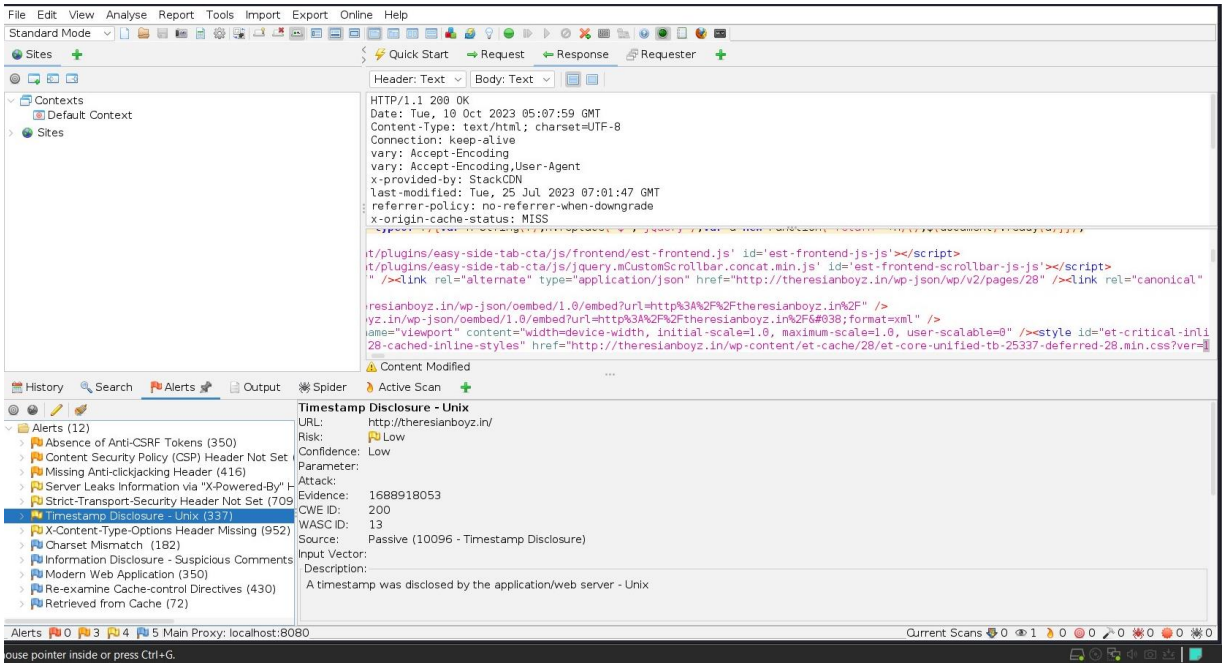


CWE ID: 352 with risk as medium.

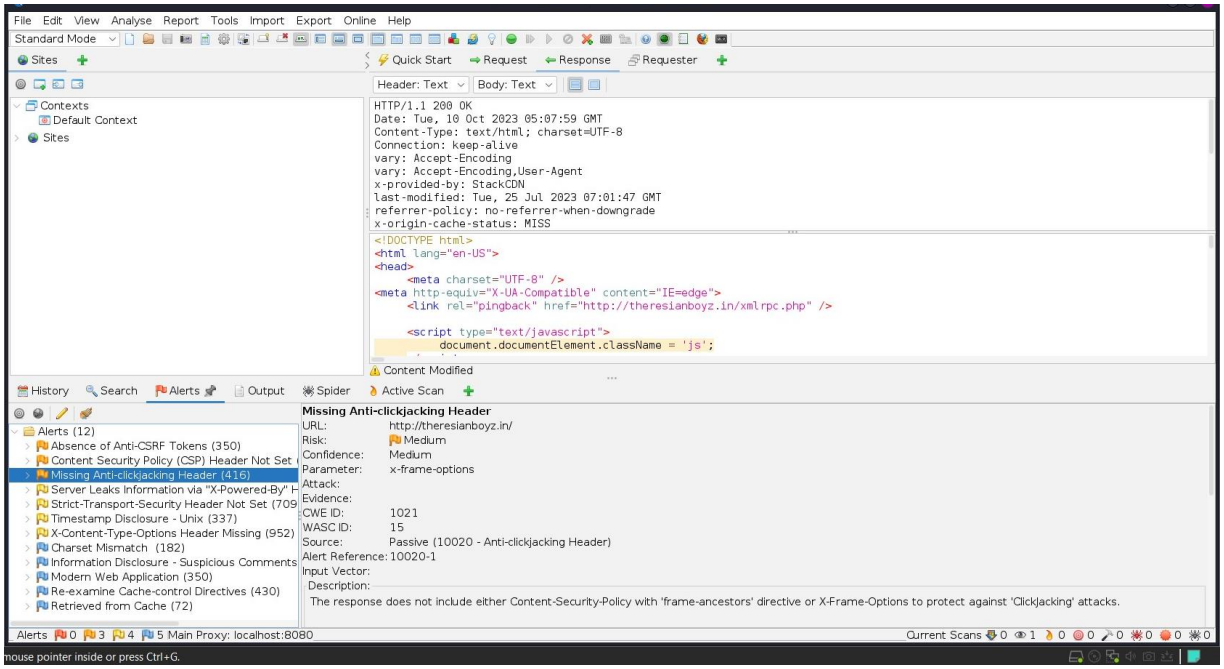


CWE ID: 693 with risk as medium.

-Sadiq S.



CWE ID: 200 with risk as Low.



CWE ID: 1021 with risk as medium.

-Sadiq S.

WPScan:

WPScan is a security tool designed specifically for WordPress sites. It is used to identify vulnerabilities in WordPress plugins, themes, and the core WordPress installation itself. The tool scans for vulnerabilities using a database of known issues, and provides information on how to patch those vulnerabilities.

Just enter the command : **wpscan --url <Target URL>** to scan the wordpress website for vulnerabilities.