Ethical Hacking

The Culture for the Curious

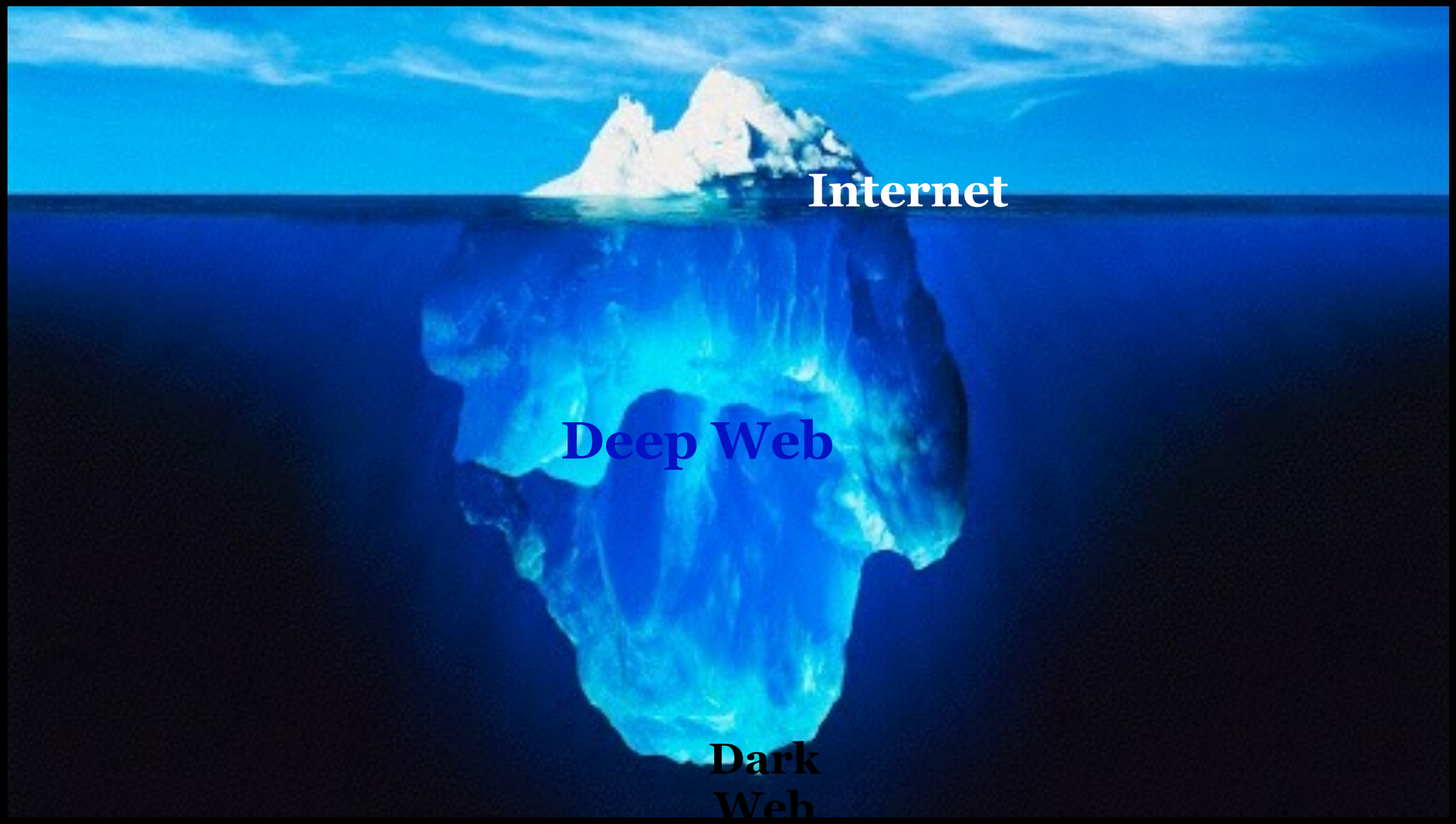
Jayashree S Kumar, IBM

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 types of Penetration Testing :
  > Network Hacking
    - Pre-Connection, Gaining Access, Post-Connection
  > Gaining Access
  > Post Exploitation
  > Website Hacking
- Conclusion


Internet
Deep Web
Dark
Web


I-LOVE-YOU
Virus
YEAR OF ATTACK
2000


Wanna Cry


RANSOMWARE ATTACK
YOUR FILES ARE ENCRYP


YOUR FILES ARE ENCR
Your photos, documents and othe
files have been encrypted with u
generated for this comput
NEXT


CICADA 3301

WHAT ?

Hacking - Gaining Unauthorised Access

X Permission
STEAL
HARM

Permission
ETHICAL

X Permission
X STEAL
X HARM

WHY LEARN?

Disclaimer: Its 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

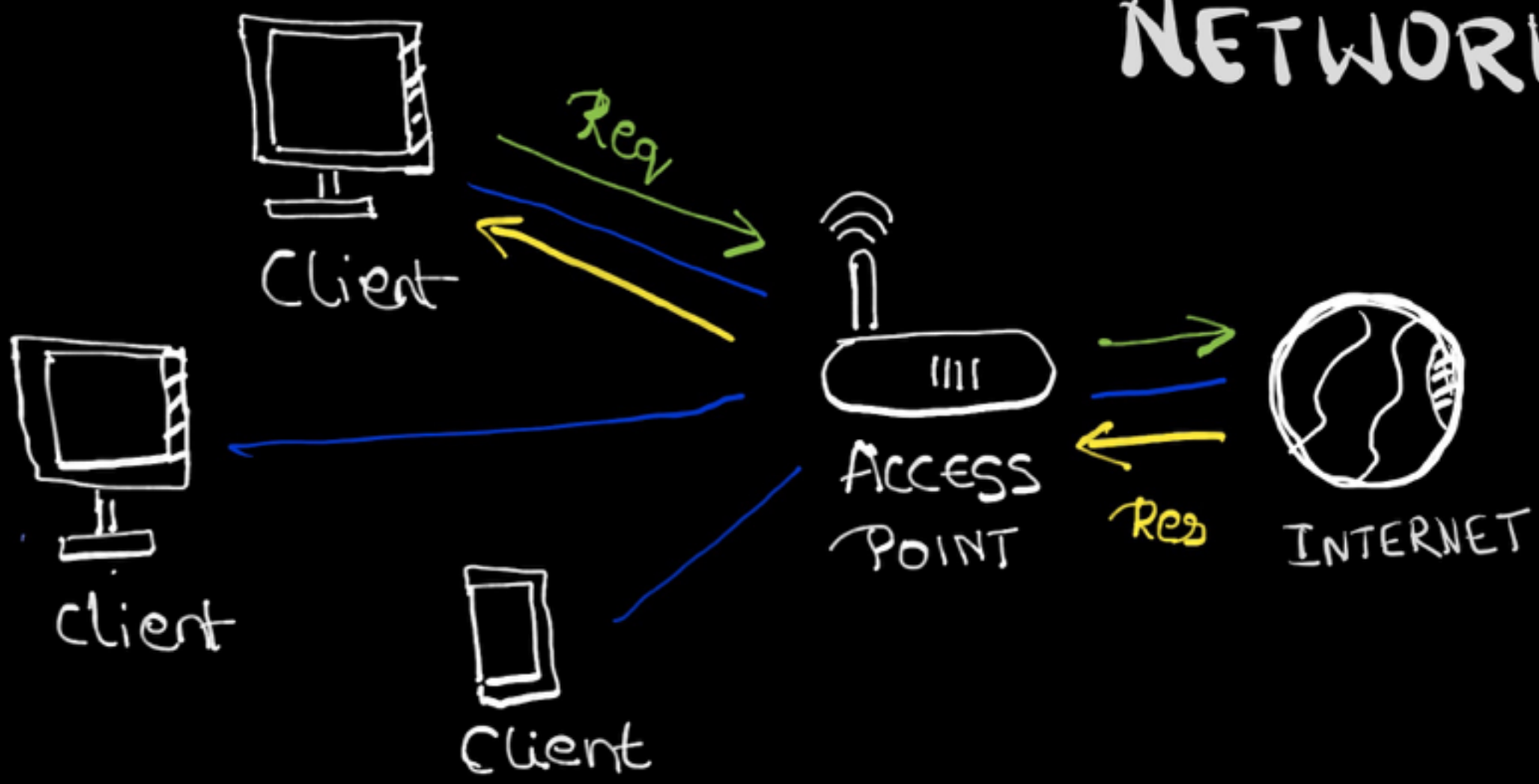
Place to experiment and practice hacking and pen testing.

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

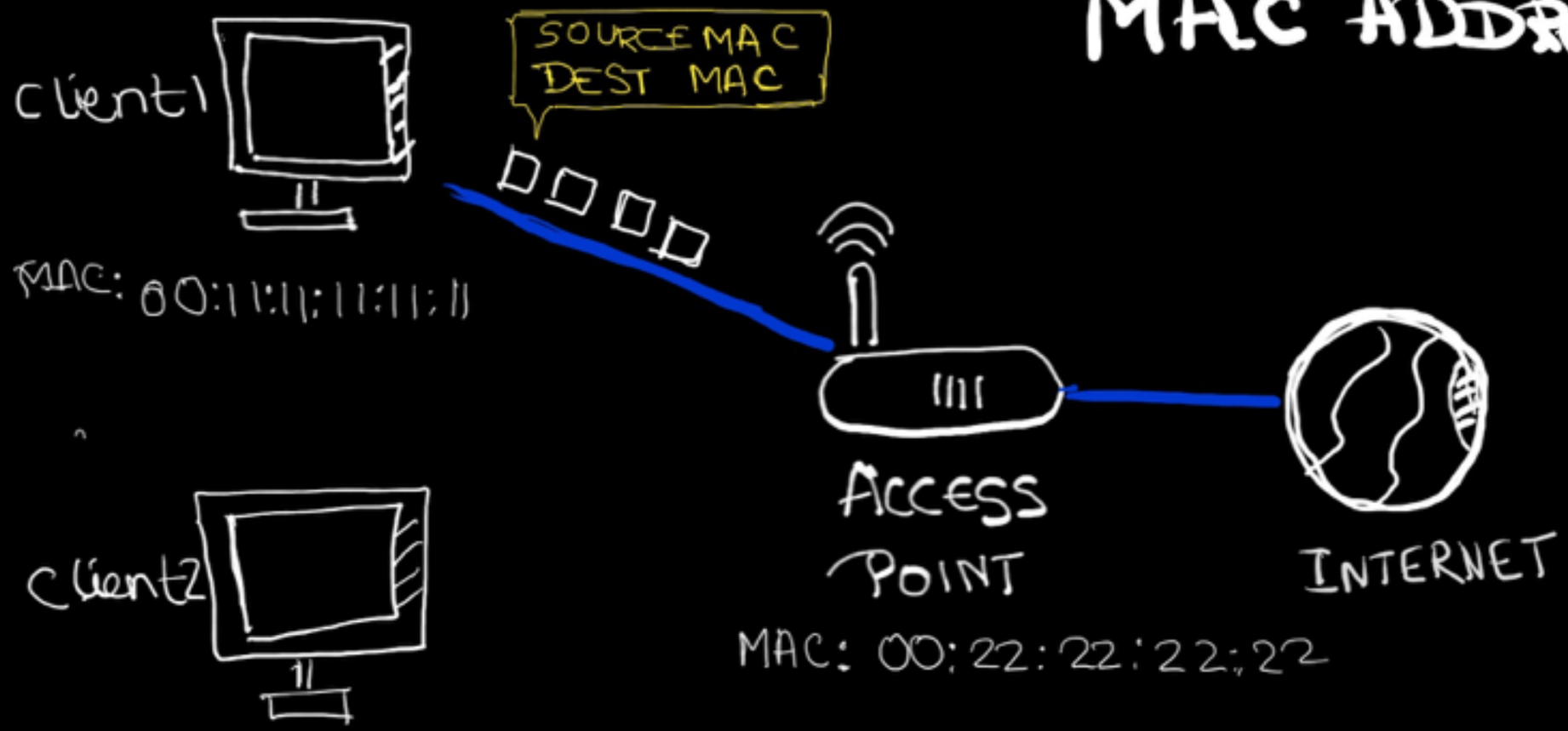
(All In your Host - VirtualBox)

NETWORK HACKING

NETWORK



MAC ADDRESS


Client1
SOURCE MAC
DEST MAC
MAC: 00:11:11:11:11:11
Client2
ACCESS POINT
MAC: 00:22:22:22:22:22
INTERNET

NH: Pre-connection attacks

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_

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

NH: Gaining access

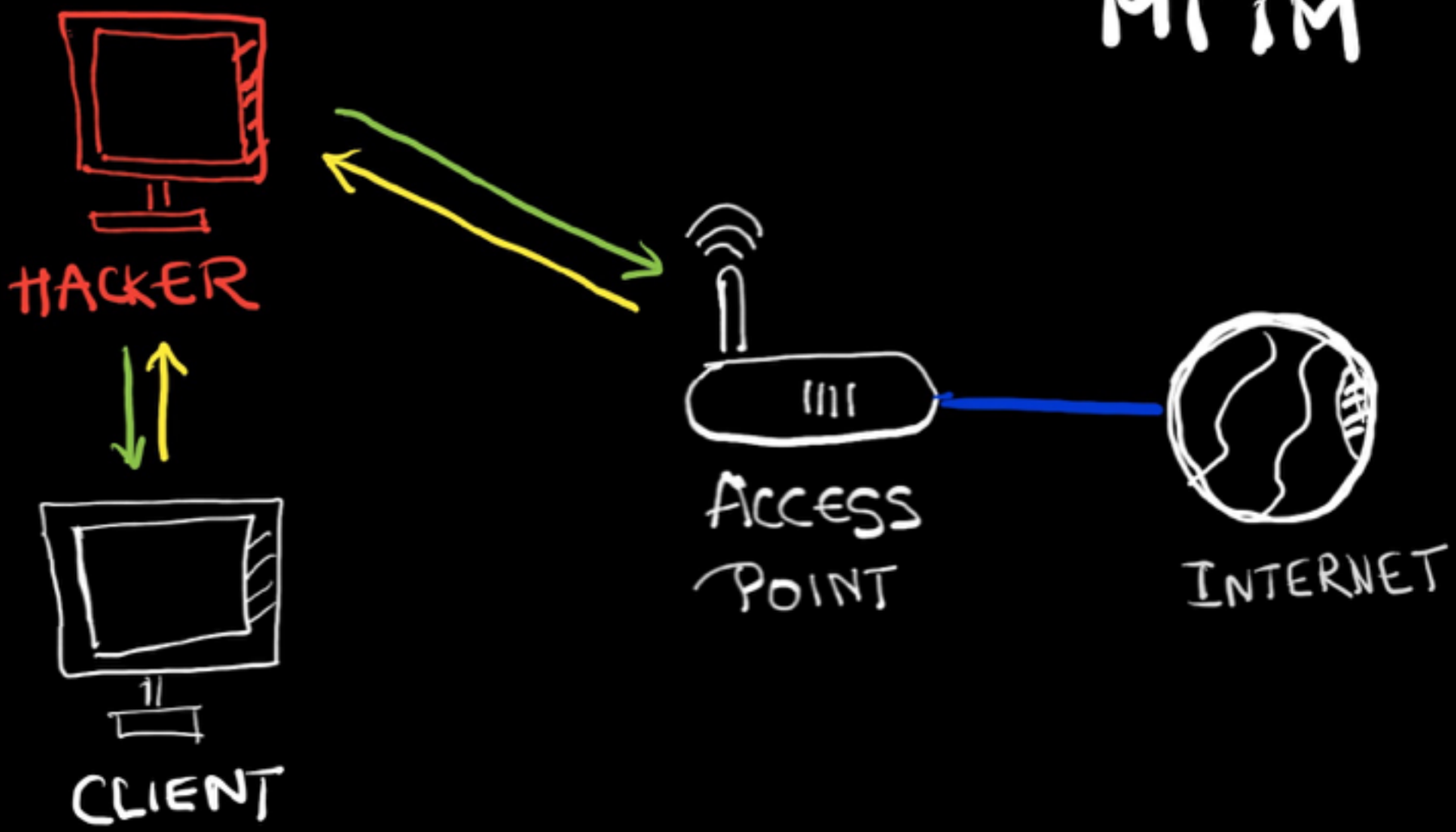
aircrack-ng : Analyse the captured packets to get password

WEP Cracking
aircrack-ng basic_wep.cap

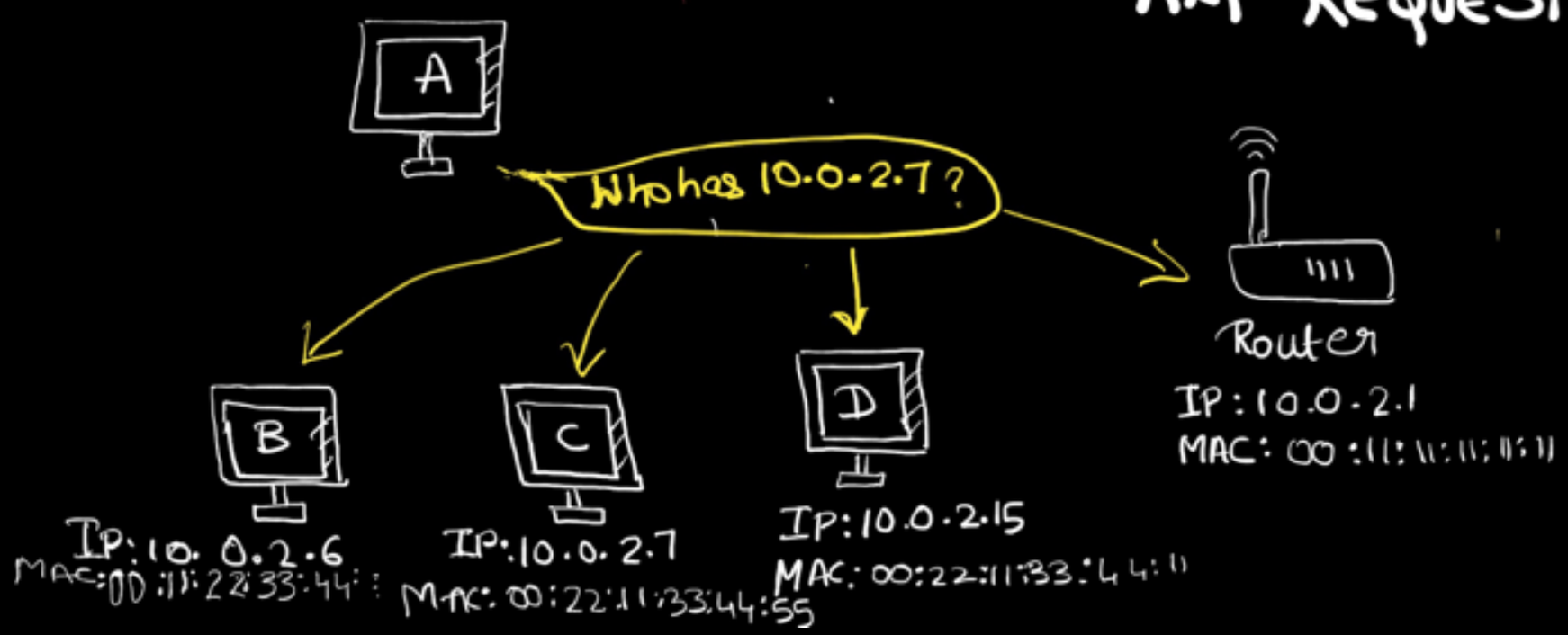
crunch: Creating wordlist
crunch [min][max][characters] -t[pattern]- o[FileName]

WPA / WPA2 cracking
aircrack-ng handshake_wpa.cap -w wordlist.txt

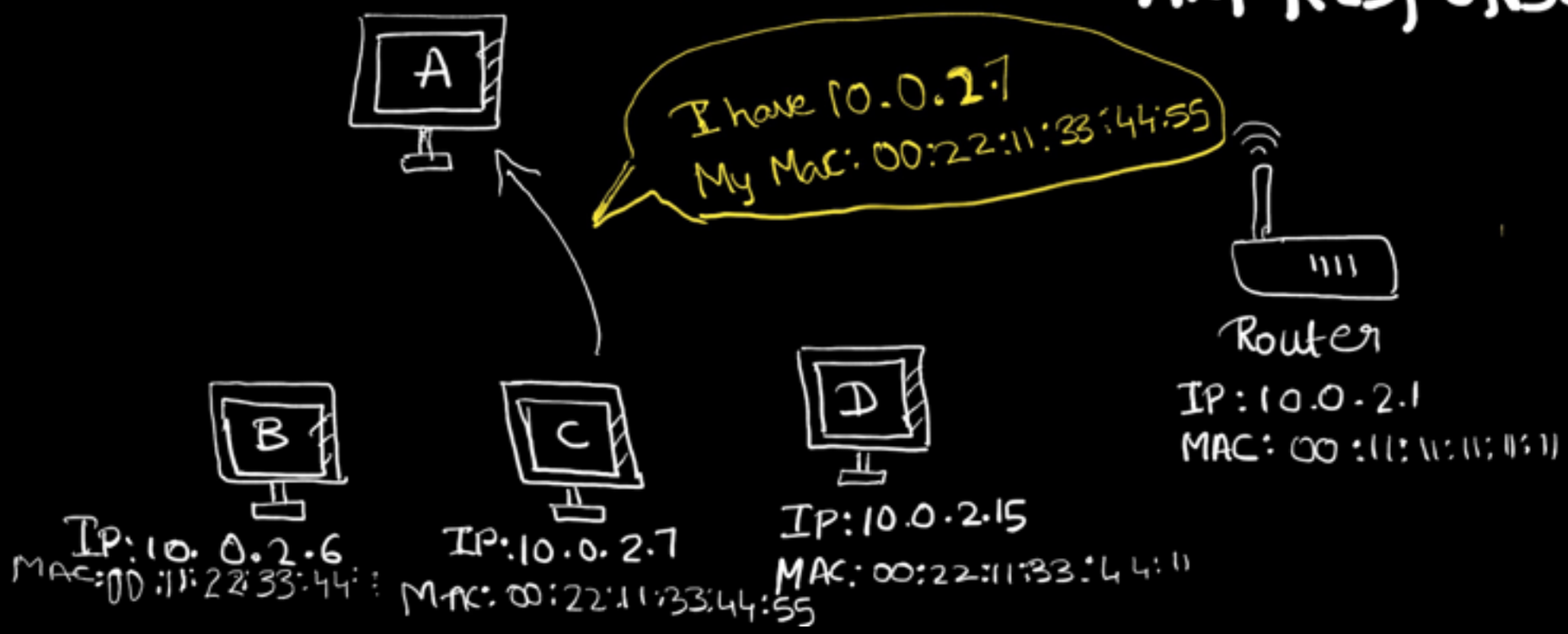
MITM



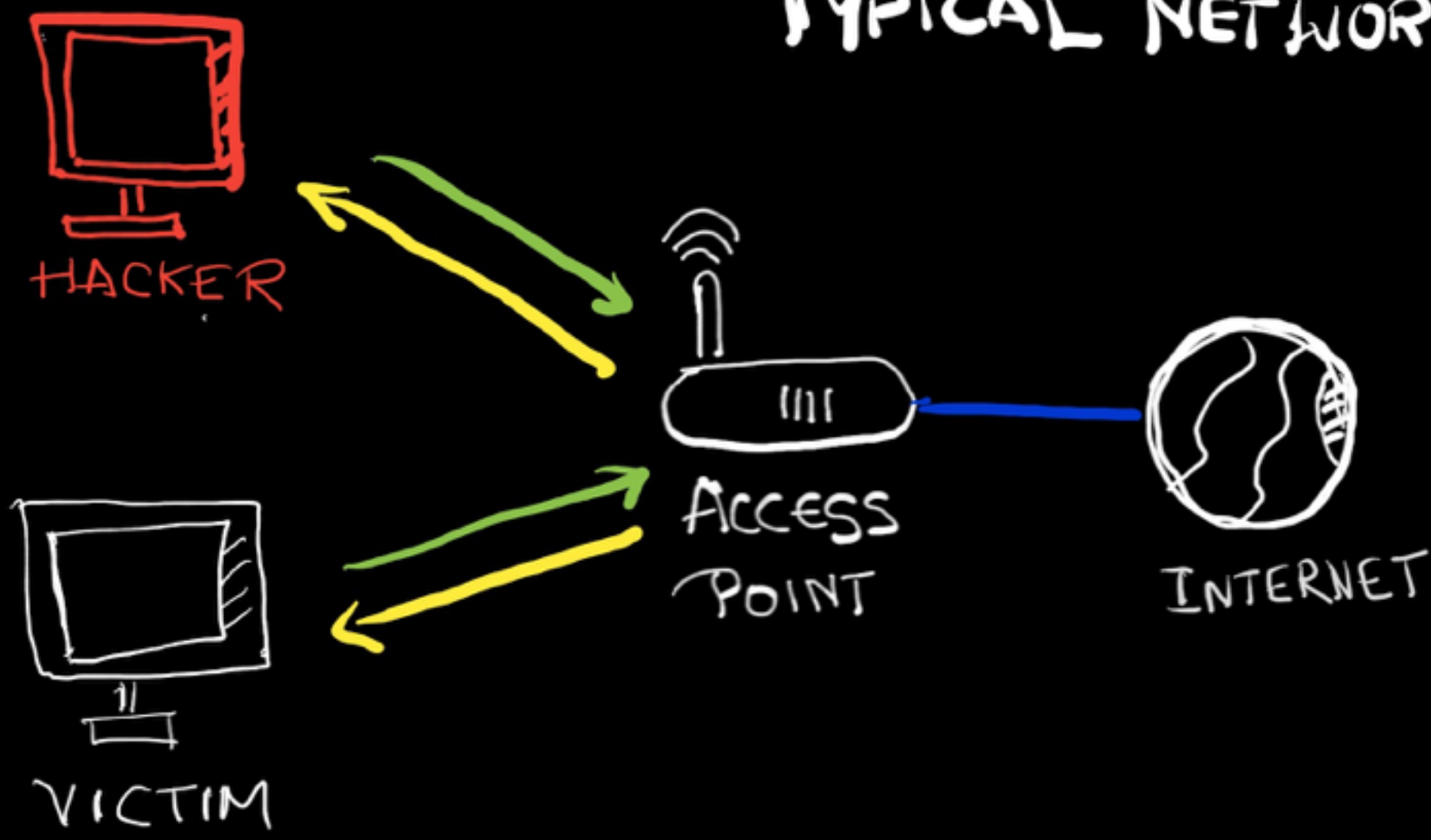
ARP REQUEST


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

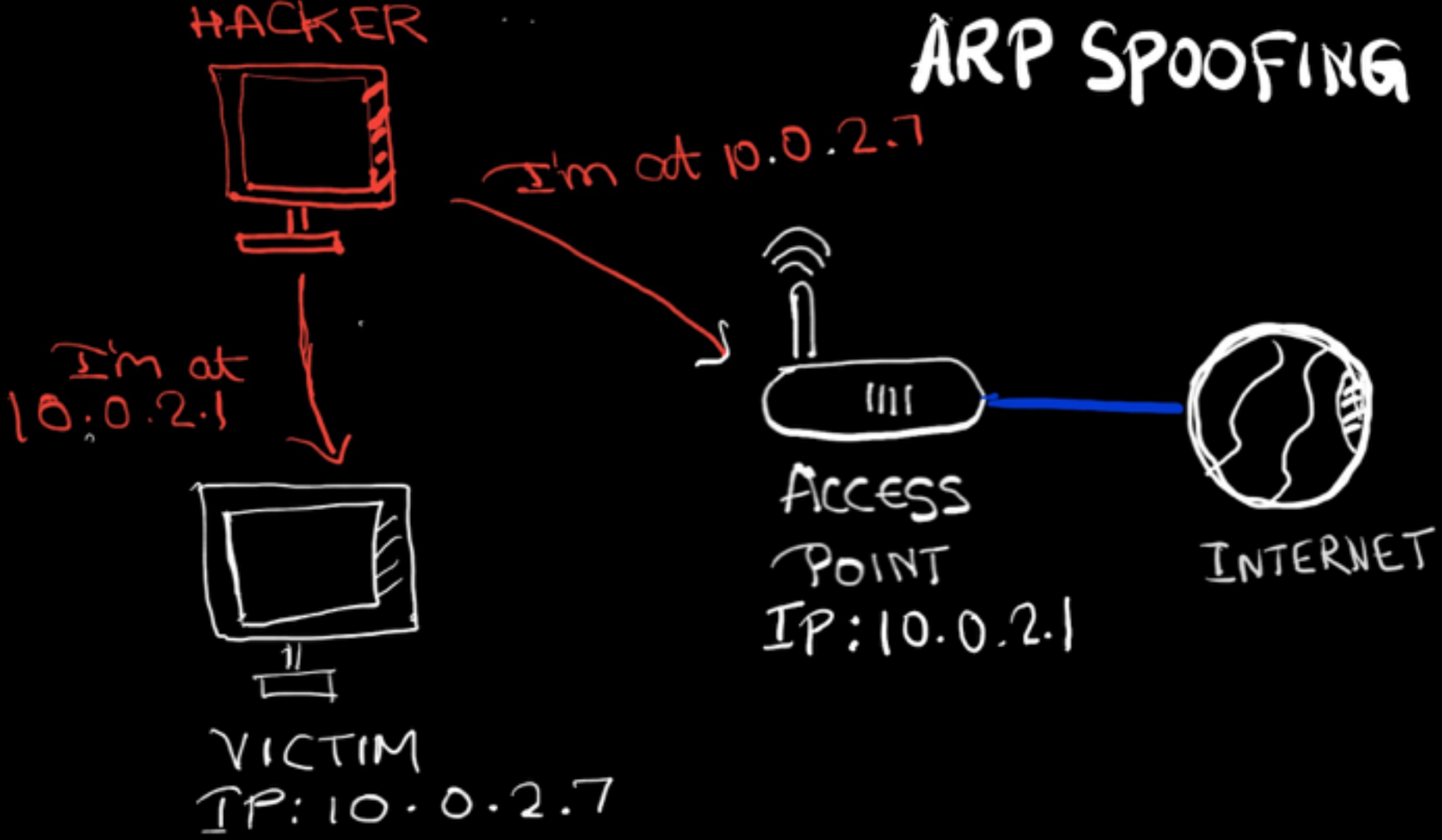
ARP RESPONSE



TYPICAL NETWORK



ARP SPOOFING



NH: Post-connection attacks

arpspoof: Basic ARP spoofing tool
arpspoof -i [inerface] -t [clientIP] [gatewayIP]
arpspoof -i [inerface] -t [gatewayIP][clientIP]

bettercap
buttercup -iface interface

Use **HTTPs** instead of HTTP <— Can be bypassed - by downgrading
Use **HSTS** - Http Strict Transport Security <— Can be Manipulated

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
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

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

GA : Client side

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

TooL: Veil Framework — Create Backdoors

Github:
Veil-Evasion
Veil- Odesion

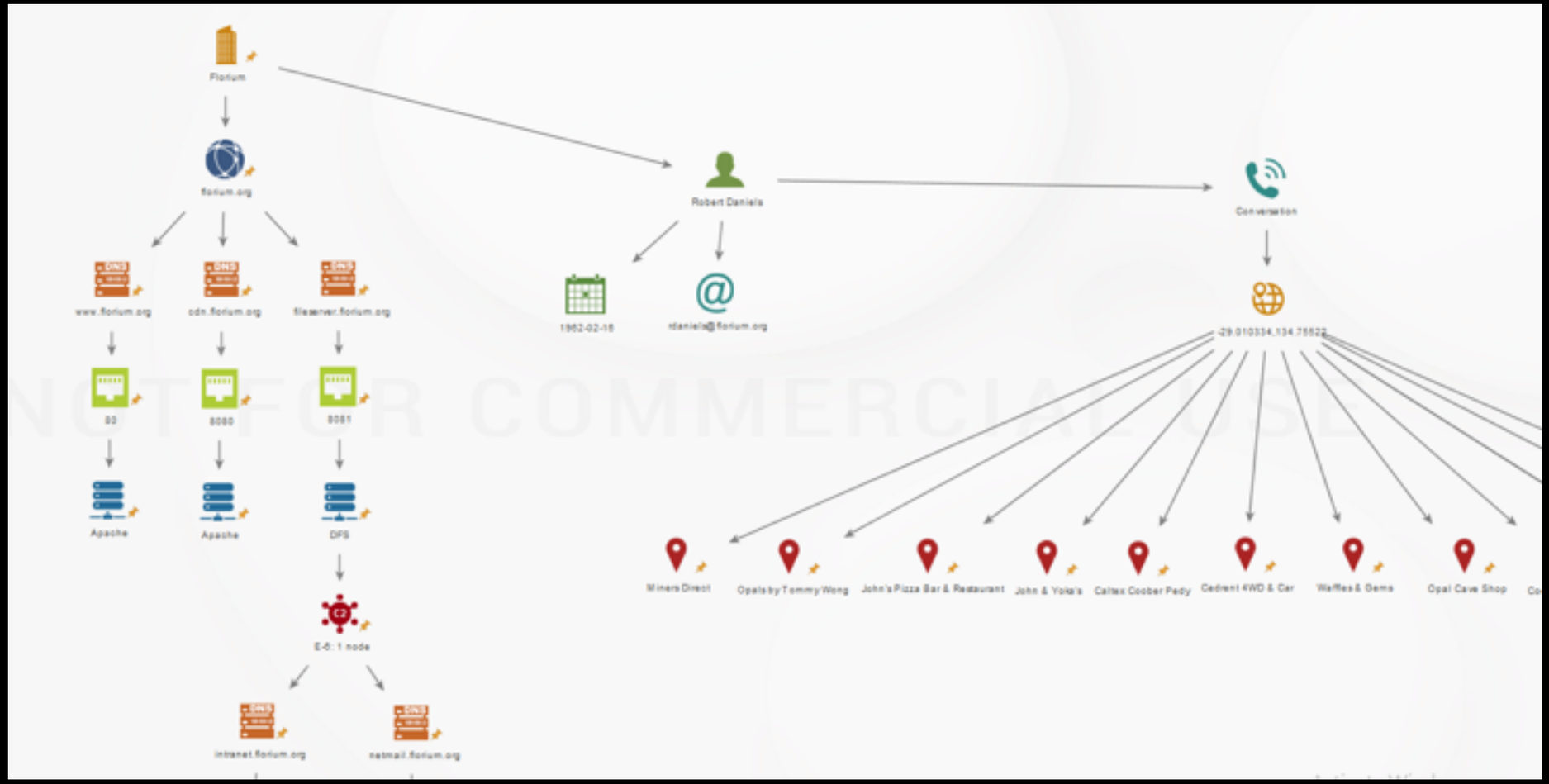
Each having their own Payloads,
written by Meterpreter developers

GA : Socail Engineering

Information Gathering: Users

Very crucial, To build strategy accordingly.

TooL: Maltego



Fake EMAIL

TooL : SendEmail

```
sendemail -s smtp.sendgrid.net:25
-xu apikey
-xp SG.W3s4IQzvSQaz7AG39WtT3w.
2CulbFCiqR5Pk7P7aJbyhZsYzpftbqXwgoPhfnXjm_0
-f "pratik@gmail.com"
-t "jskethhac@gmail.com"
-u “Cloud Native Reception"
-m "Did you register for Cloud Native Yet?, Check this
picture to getting  the mood  https_dropboxlink_?dl=1"
-o message-header="From : Pratik Patel
<pratik@gmail.com>"
```

POST EXPLOITATION

Open WebCam
Capture KeyStokes
Use the machine as Pivot to hack other machines

Blackmail /Ransomeware
Steal Information, Money & Privacy

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!

WEBSITE HACKING