Module 6

Network Security Mechanism

Goals for Day

- Intrusion Detection and Prevention Systems: IDS Concepts, IDS Types and Detection Models, IDS Features, IDS Deployment Considerations, Security Information and Event Management (SIEM)
- Voice over IP (VoIP) and PBX Security: Background, VoIP Components, VoIP Vulnerabilities and Countermeasures, PBX, TEM: Telecom Expense Management. Virtual Private Networks
- Firewalls, DMZ
- Honeypot
- Transport Layer Security (TLS/SSL)
- TLS Programming

Introduction to | Snort

- Snort is an open source software which helps in monitor network traffic in real-time
- It can also be considered as a packet sniffer
- It examines each and every data packet in depth to see if there are any malicious payloads

SName | RegX
Addx
statex
emailx

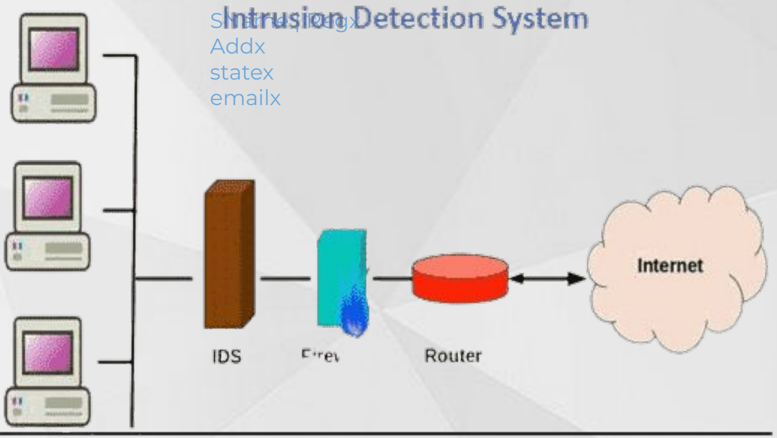
- It is capable of detecting various attacks like port scans, buffer overflow, etc.
- It's available for all platforms i.e. Windows, Linux, etc.

Intrusion Detection System | IDS

- IDS Stands for Intrusion Detection System
- It is used to monitor and reveal malicious activities both on the host and network level
- It can be hardware or software or a combination of both; depends on the requirement

Two Types of IDS

- NIDS: Network Intrusion Detection System
- HIDS: Host Intrusion Detection System



Categories Of | IDS

Signature based IDS

- This IDS verifies signatures of data packets in the network traffic
- It finds the data packets and uses their signatures to confirm whether they are a threat or not
- Intruders such as computer viruses, etc, always have a signature, therefore, it can be easily detected by software IDS
- As it uses signatures to identify the threats

Anomaly IDS

- This IDS models the normal usage of the network as a noise characterization.
- Anything distinct from the noise is assumed to be an intrusion activity.
- E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.

Installation | Snort

Steps to install the Snort in Ubuntu OS

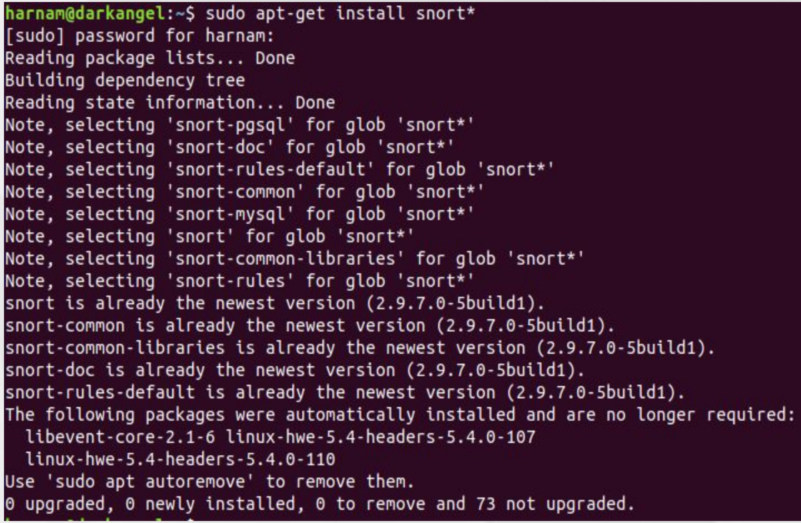
1. Use the ifconfig command in your Ubuntu to check the interface

2. Now, let’s install snort by using the following command :

   ○ *# sudo apt-get install snort**

3. Once the installation starts, it will ask you the interface that we previously checked. Give its name and press enter

4. Then it will ask you about your network IP, provide a single IP or the range of IPs



```
harnam@darkangel:~$ sudo apt-get install snort*
[sudo] password for harnam:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'snort-pgsql' for glob 'snort*'
Note, selecting 'snort-doc' for glob 'snort*'
Note, selecting 'snort-rules-default' for glob 'snort*'
Note, selecting 'snort-common' for glob 'snort*'
Note, selecting 'snort-mysql' for glob 'snort*'
Note, selecting 'snort' for glob 'snort*'
Note, selecting 'snort-common-libraries' for glob 'snort*'
Note, selecting 'snort-rules' for glob 'snort*'
snort is already the newest version (2.9.7.0-5build1).
snort-common is already the newest version (2.9.7.0-5build1).
snort-common-libraries is already the newest version (2.9.7.0-5build1).
snort-doc is already the newest version (2.9.7.0-5build1).
snort-rules-default is already the newest version (2.9.7.0-5build1).
The following packages were automatically installed and are no longer required:
  libevent-core-2.1-6 linux-hwe-5.4-headers-5.4.0-107
  linux-hwe-5.4-headers-5.4.0-110
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 73 not upgraded.
```

Configuration | Snort

Snort is successfully installed

Step 5: Use the following command to open configuration file:

a. sudo nano /etc/snort/snort.conf

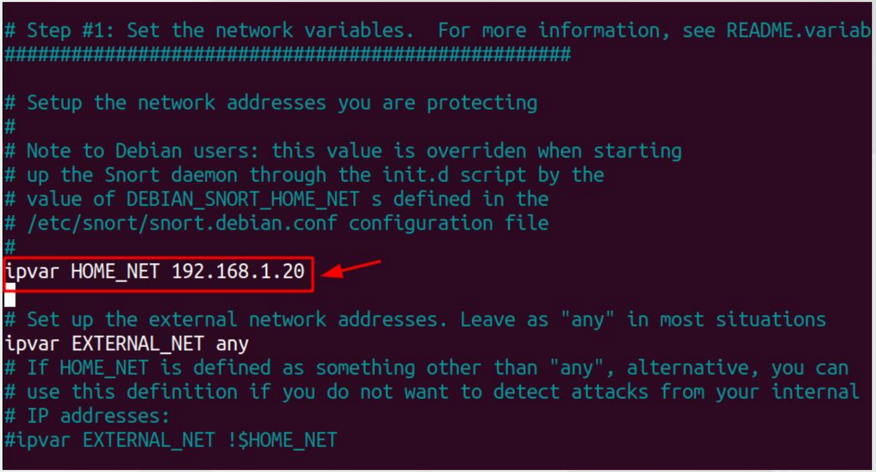
Step 6: Scroll down the text file near line number 45 to specify your network for protection

Step 7: Setup the network addresses you are protecting:

b. # ipvar HOME_NET 192.168.1.21

Step 8: Run this command to enable IDS mode of snort :

```
sudo snort -A console -i ens33 -c /etc/snort/snort.conf
```



```
# Step #1: Set the network variables.  For more information, see README.variab
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.1.20

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

Snort Rule Syntax

- **Action:** It informs Snort what kind of action to be performed when it discovers a packet that matches the rule description
- **Protocol:** We need to describe specific Protocol (IP, TCP, UDP, ICMP, any) on which this rule will be applicable
- **Source IP:** It describes the sender network interface from which traffic is coming
- **Source Port:** It describes the source Port from which traffic is coming
- **Direction operator** (“->”, “<>”): It denotes the direction of traffic flow between sender and receiver networks
- **Destination IP**: It describes the destination network interface in which traffic is coming for establishing the connection
- **Destination Port**: It describes the destination Port on which traffic is coming for establishing the connection

IDS | Demo

We need to add rules for filtering malicious packets:

Step 9: Go to directory *# cd /etc/snort/rules*

Step 10: Open the icmp.rules file and add your rule and save it

Eg:

```
alert icmp any any -> 192.168.2.49 any (msg: "ICMP Packet found"; sid:10000001; )
```

If someone do ping scan it will create a alert “**ICMP Packet found**”

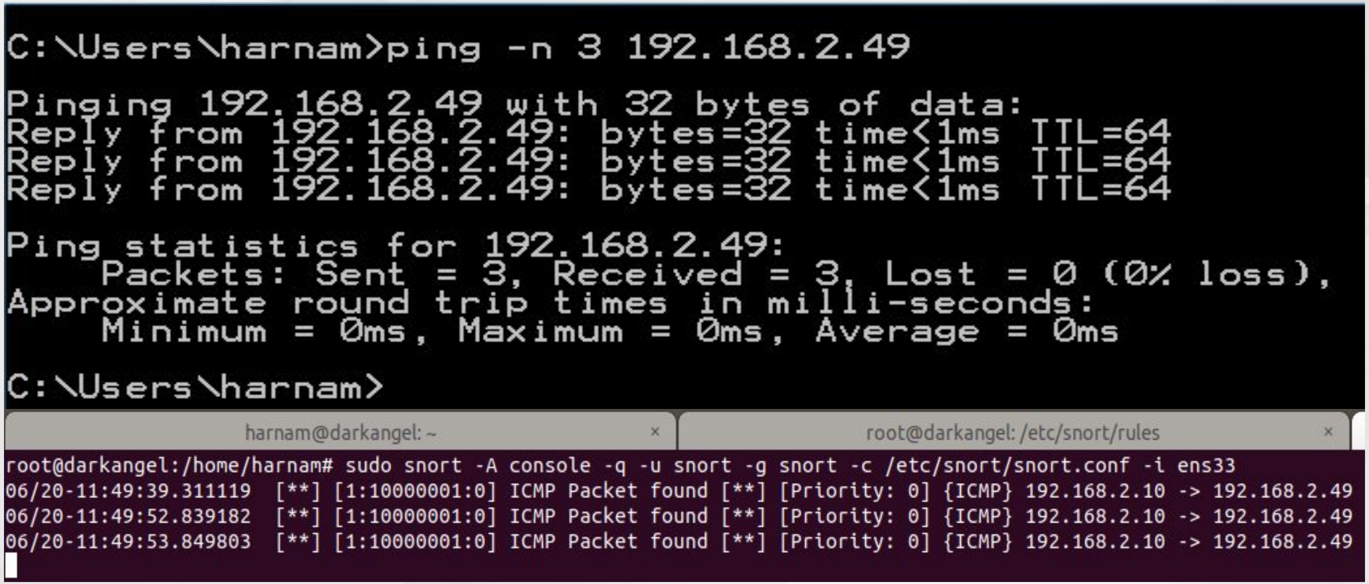
Step 11: Run this command to activate snort to catch the malicious packets

```
# sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
```

IDS | Demo

Run this command to activate snort to catch the malicious packets

# sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33



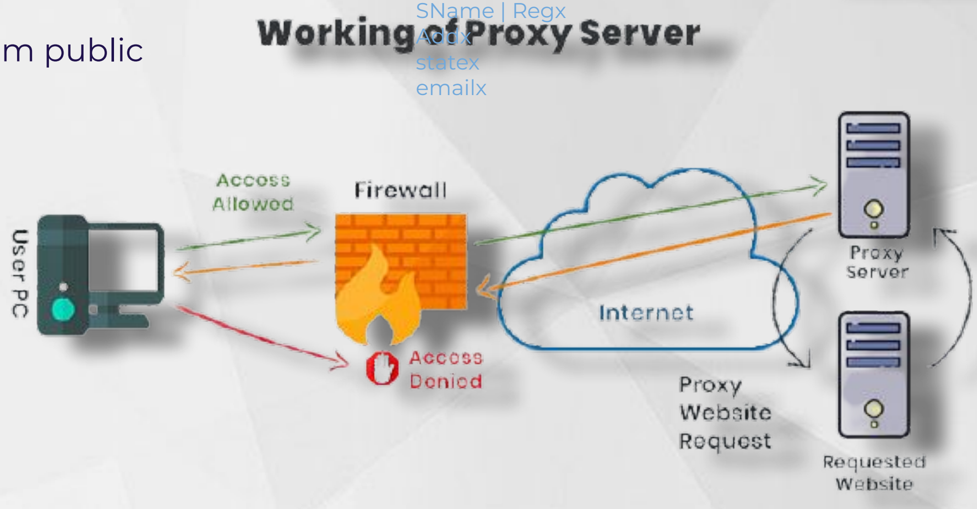
```
C:\Users\harnam>ping -n 3 192.168.2.49

Pinging 192.168.2.49 with 32 bytes of data:
Reply from 192.168.2.49: bytes=32 time<1ms TTL=64
Reply from 192.168.2.49: bytes=32 time<1ms TTL=64
Reply from 192.168.2.49: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.49:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\harnam>
```

```
root@darkangel:/home/harnam# sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
06/20-11:49:39.311119  [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.2.10 -> 192.168.2.49
06/20-11:49:52.839182  [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.2.10 -> 192.168.2.49
06/20-11:49:53.849803  [**] [1:10000001:0] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.2.10 -> 192.168.2.49
```

Proxy Server | About

Proxy Server allow you to Hide your IP Address from public disclosure & can surf the **Internet Anonymously**

- **Hides** your real IP address
- Effectively **Masking** your online identity
- Allowing you to **Bypass** Geo-Blocks



Proxy Server | Tools

Popular Tools for Proxy Server Set-Up

- **CyberGhost**
- KProxy
- Anonymox
- UltraSurf
- Psiphon
- SafeIP

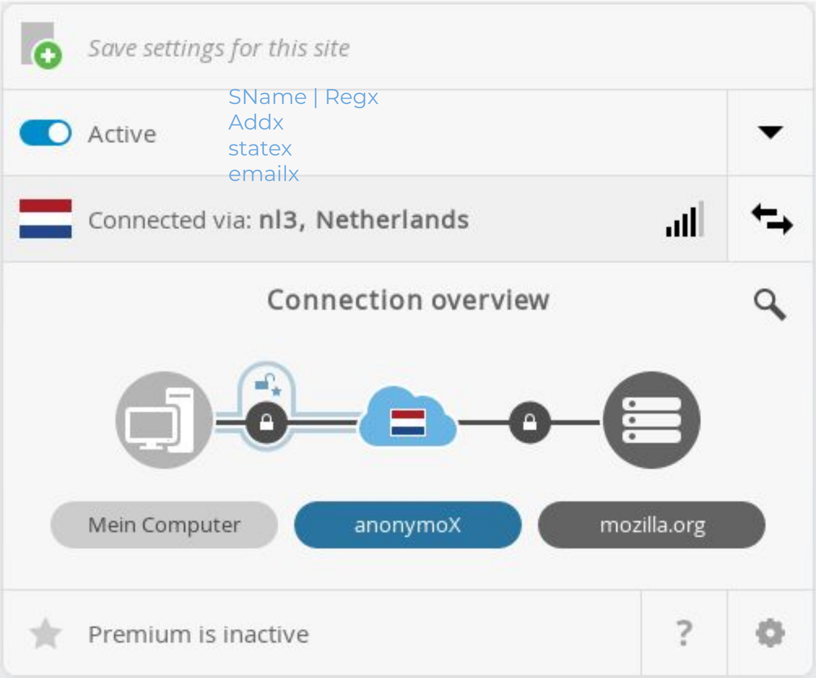
SName | RegX
Addx
statex
emailx

Proxy Server | Set-Up

Steps to Follow :

- **Google : AnonymoX Extension Chrome/FIrefox**
- Add to Browser
- Check new Extension : AnonymoX
- Click Active as **ON**
- Verify new IP Address :
  - Google : My IP

SName | Regx
Addx
statex
emailx



Save settings for this site

SName | Regx
Addx
statex
emailx

Active

Connected via: nl3, Netherlands

Connection overview

Premium is inactive

Virtual Private Network | VPN

About

- Protects your real IP Address
- Effectively masking your Online Identity
- Allowing you to Bypass Geo-blocks
- Protecting your data from hackers and ISP or any surveillance

Virtual Private Network | Working

YES v/s NO

- Are VPN : **Legal.?**

SName | Regx
Addx
statex
emailx

- Are VPN **Secure.?**
- Am I Safe When Using **Public Wi-Fi** Hotspots with a VPN?

Watch Video
→

SName | Regx
Addx
statex
emailx

Virtual Private Network | Tools

Online Services

Hidemyass

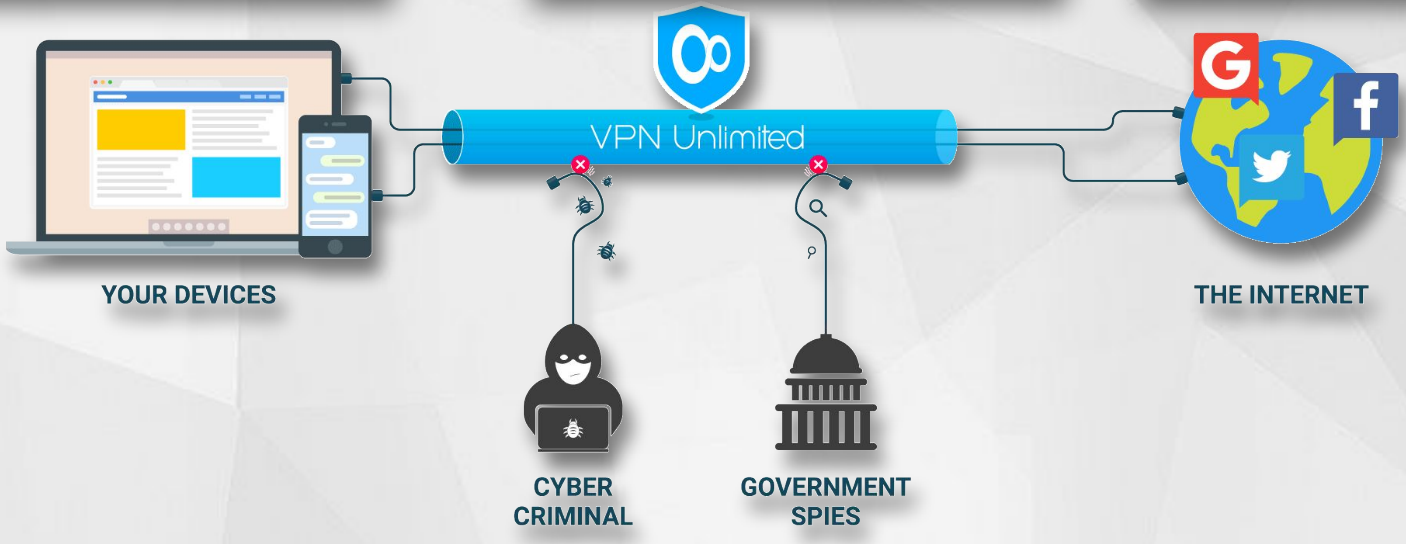
Extension based

Hoxx VPN
Anonymox

SName | Regx
Addx
statex
emailx

Stand Alone Services

Psiphon



Virtual Private Network | Set-Up - I

Fly Vpn is available for Windows, linux, Mac os and Android, iOs

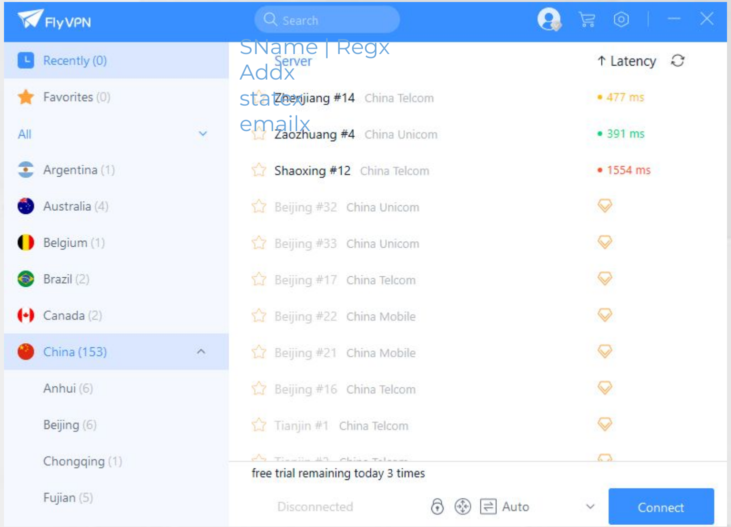
- Download **Flyvpn** and Install it
- Open the VPN signup it
- Use the credential and click on login
- New Dashboard will open

Download Here : Click Here

Virtual Private Network | Set-Up - II

Steps to Follow ;

- Select the server if any available in trial vpn
- Also we can connect the **TCP/UDP** Global proxy or Manual proxy
- After connected check your ip address it will show you the another location



Recently (0)
Favorites (0)
All
Argentina (1)
Australia (4)
Belgium (1)
Brazil (2)
Canada (2)
China (153)
Anhui (6)
Beijing (6)
Chongqing (1)
Fujian (5)

Server		↑ Latency
Zhenjiang #14	China Telcom	477 ms
Zaozhuang #4	China Unicom	391 ms
Shaoxing #12	China Telcom	1554 ms
Beijing #32	China Unicom	
Beijing #33	China Unicom	
Beijing #17	China Telcom	
Beijing #22	China Mobile	
Beijing #21	China Mobile	
Beijing #16	China Telcom	
Tianjin #1	China Telcom	

free trial remaining today 3 times

Disconnected

Auto

Virtual Private Network | Verify IP

- Connect With Any server
- Connected with China server

Check Here : www.whatismyipaddress.com

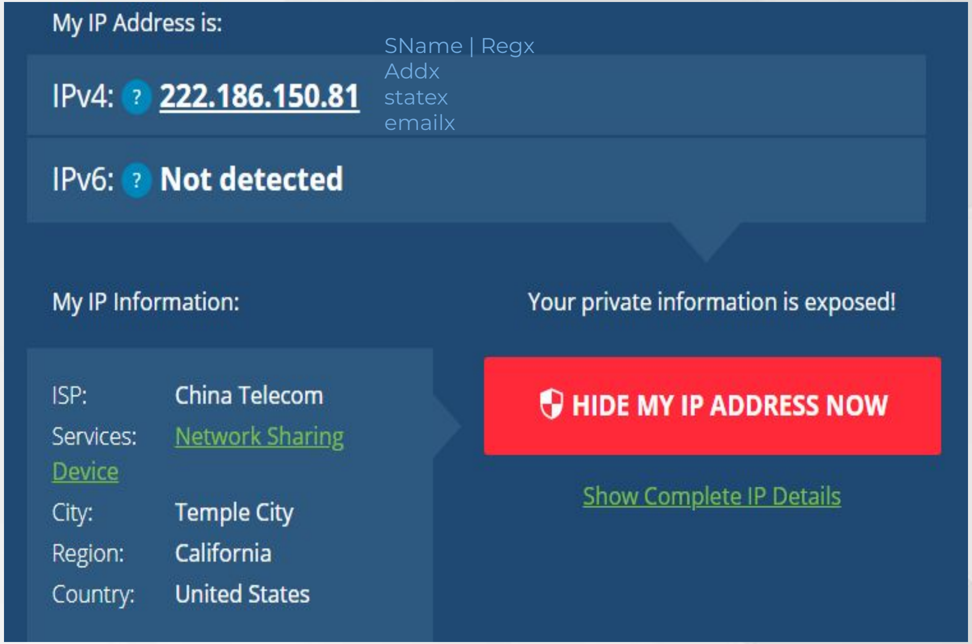
ISP: China Telecom

Services: Network Sharing Device

City: Temple City

Region: California

Country: United States



My IP Address is:

IPv4: ? 222.186.150.81

IPv6: ? Not detected

My IP Information:

Your private information is exposed!

ISP: China Telecom
Services: Network Sharing Device
City: Temple City
Region: California
Country: United States

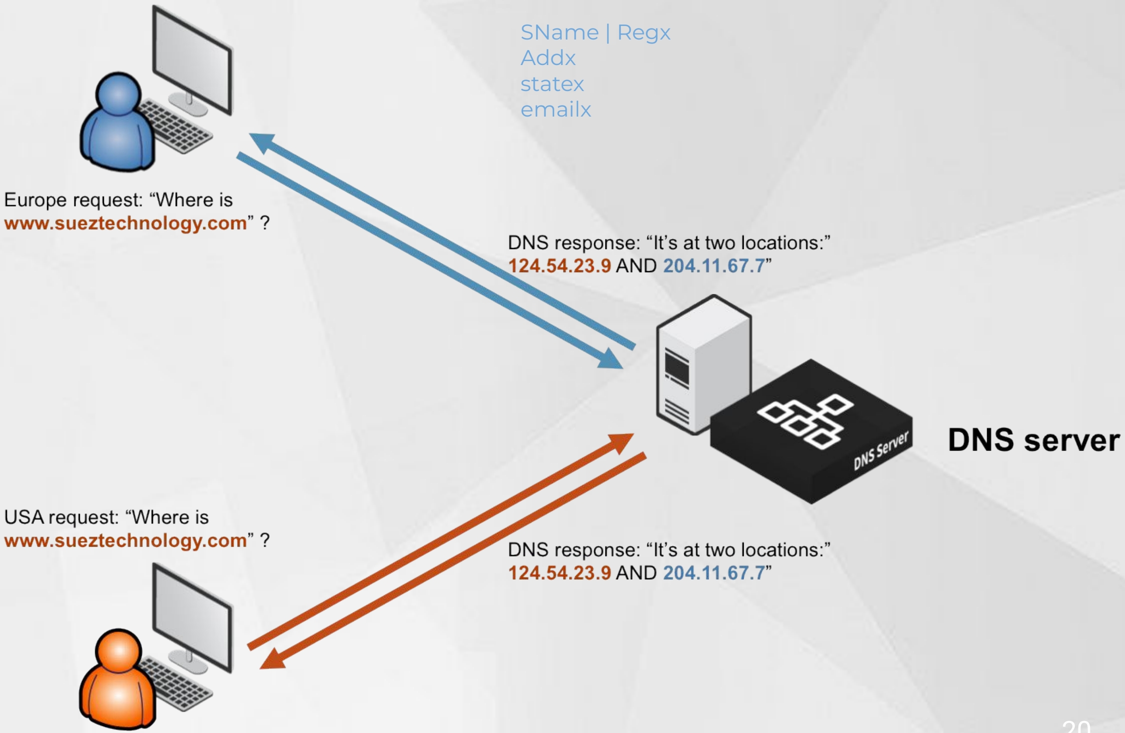
Domain Name System | About

DNS : Domain Name System

A Phonebook of the Internet

SName | RegX
Addx
statex
emailx

SName | Regx
Addx
statex
emailx



Europe request: “Where is www.sueztechnology.com” ?

DNS response: “It’s at two locations:” 124.54.23.9 AND 204.11.67.7”

DNS server

USA request: “Where is www.sueztechnology.com” ?

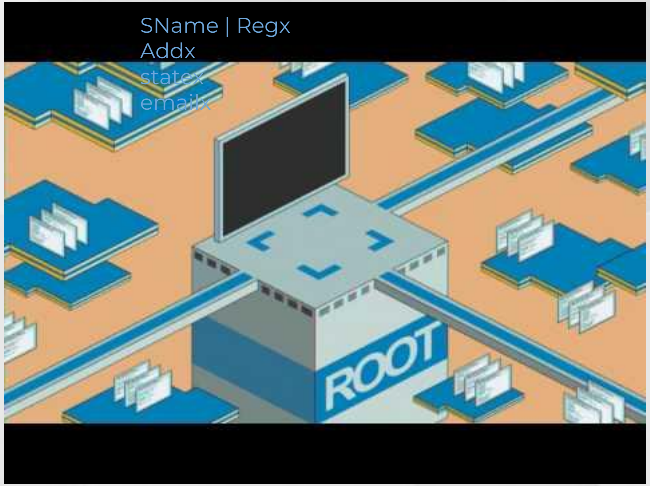
DNS response: “It’s at two locations:” 124.54.23.9 AND 204.11.67.7”

Domain Name System | Working

- DNS **translate domain** names into IP Addresses, which computers can understand

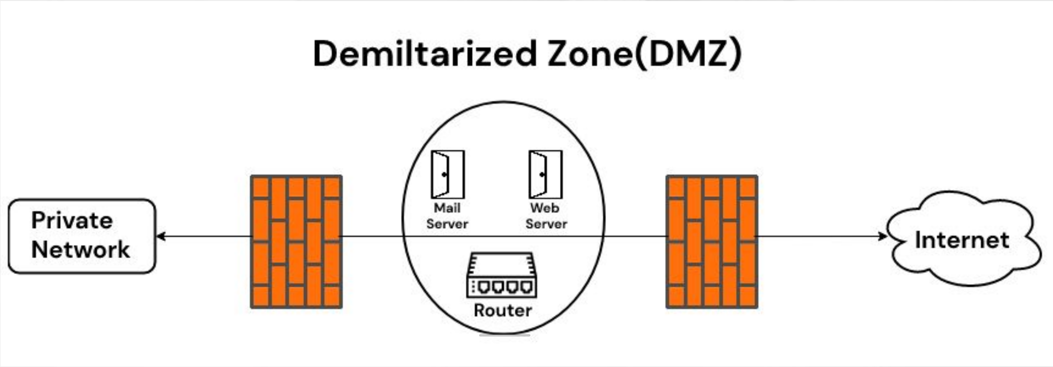
Browser Request IP Address against the Domain Name

- Send a Request to **Resolve a Domain Name**
- Search for an IP Locally
- Contact **ISP** and its Recursive DNS Server to Resolve a Domain Name
- Ask Outside DNS Servers to Provide an IP Address
- Receive the IP Address



Firewall, DMZ

- A DMZ or demilitarized zone is a perimeter network
- that protects and adds an extra layer of security
- To an organization’s internal local-area network from untrusted traffic
- The end goal of a demilitarized zone network is to allow an organization
- To access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure

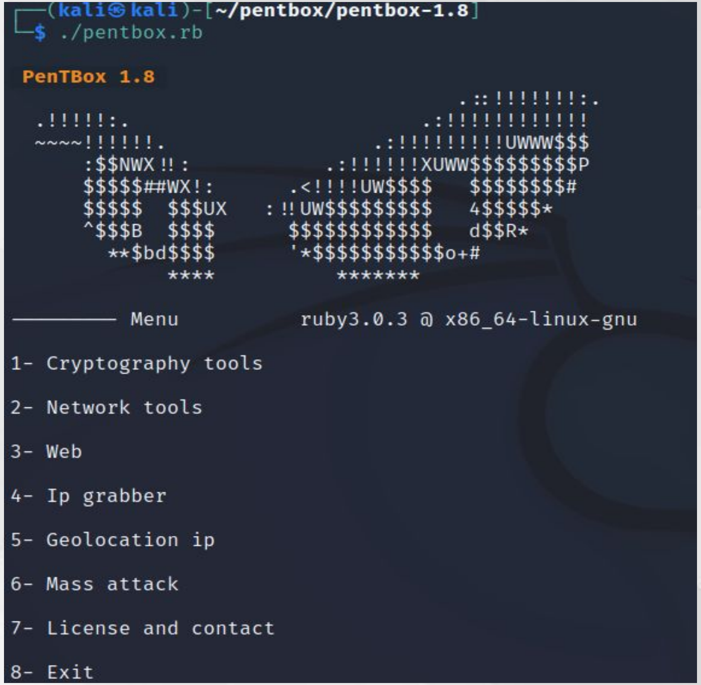


Introduction to Honeypot

- Honeypot is a network-attached system used as a trap for cyber-attacker
- It helps cybersecurity researchers to learn about the different type of attacks used by attackers
- It acts as a potential target on the internet and informs the defenders about any unauthorized attempt
- It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information

Automated Tool | Pentbox

- To set up honeypot in Kali Linux system we need to download a tool from github it called Pentbox
- This tool is written in ruby language
- To install this use the below commands:
  - *git clone https://github.com/technicaldada/pentbox*
  - *tar -zxvf pentbox.tar.gz*
  - *cd pentbox*
  - *./pentbox.rb*



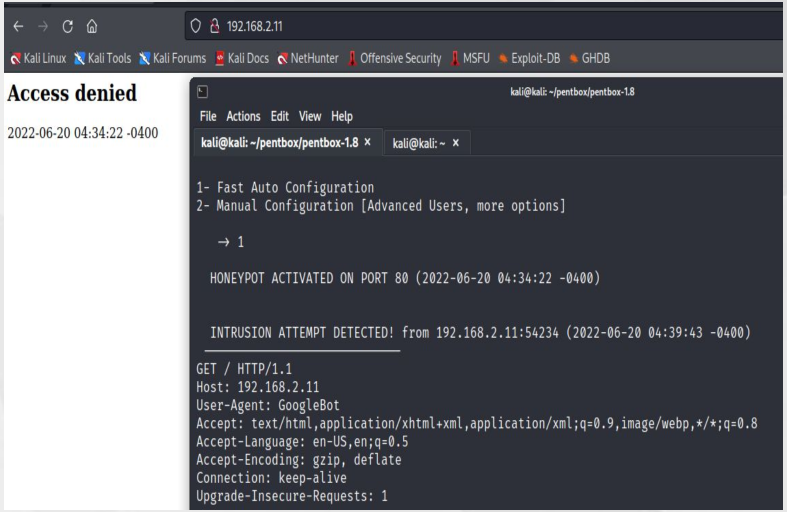
```
┌──(kali㉿kali)-[~/pentbox/pentbox-1.8]
└─$ ./pentbox.rb

 PenTBox 1.8
                                     .::!!!!!!!:.
  .!!!!!:.                        .:!!!!!!!!!!!!
  ~~~~!!!!!!.                 .:!!!!!!!!!UWWW$$$
      :$$NWX!!:           .:!!!!!!XUWW$$$$$$$$$P
      $$$$$##WX!:      .<!!!!UW$$$$   $$$$$$$$#
      $$$$$  $$$UX   :!!UW$$$$$$$$$   4$$$$$*
      ^$$$B  $$$$      $$$$$$$$$$$$   d$$R*
        **$bd$$$$      '*$$$$$$$$$$$o+#
             ****          *******

———————— Menu           ruby3.0.3 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit
```

Automated Tool | Pentbox

Lets create a honeypot on port 80

Steps to configure Honeypot

- Use the command to run the pentbox tool
- Press 2 for network tool
- Press 3 for honeypot
- Choose 1 for auto configuration
- Honeypot is successfully activated on port 80
- To check how it work open the ip address in attacker browser
- Check the terminal where we started honeypot it will show the attacker ip address and more detail.



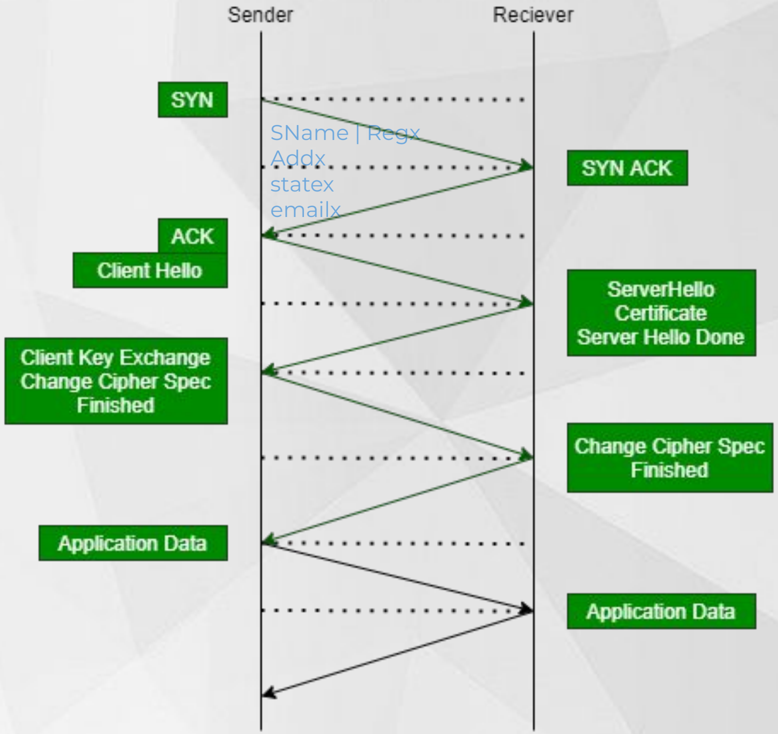
Access denied

2022-06-20 04:34:22 -0400

```
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 1

  HONEYPOT ACTIVATED ON PORT 80 (2022-06-20 04:34:22 -0400)


  INTRUSION ATTEMPT DETECTED! from 192.168.2.11:54234 (2022-06-20 04:39:43 -0400)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.2.11
User-Agent: GoogleBot
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Transport Layer Security (TLS/SSL)

- Transport Layer Security, or TLS, is a widely adopted security protocol
- Designed to facilitate privacy and data security for communications over the Internet
- A primary use case of TLS is encrypting the communication between web applications and servers
- Such as web browsers loading a website



TLS Programing

- Transport Layer Security (TLS) is a cryptographic protocol
- Designed to provide communications security over a computer network
- The protocol is widely used in applications such as email, instant messaging, and voice over IP
- But its use in securing HTTPS remains the most publicly visible

SName | Regx
Addx
statex
emailx

SName | Regx
Addx
statex

Time for Queries..!