



LAB MANUAL ON ZENMAP & HONEYBOT



**ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY
TRAINING TO TECHNICAL TEACHERS
DEPARTMENT OF INFORMATION MANAGEMENT AND COORDINATION
SPONSORED BY MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA**

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Mr. Vipul Mandhar (Project Assistant)

Table of Contents

MANUAL-1:3

A Practical Approach to make a trap for the Attacker.....3

What is a Computer Network?4

What is Information Technology (IT)?4

 Computer Technologies5

 Communication Technology5

 Network Essentials5

What is a Port?6

 Types of ports6

 Hardware Ports6

 Software Ports6

.....8

**INSTALLATION OF KALI LINUX OPERATING SYSTEM IN
VMWARE WORKSTATION.....10**

 Basics Requirements10

What is Zenmap.....13

 Types of scanning done by Zenmap.....13

 Steps to run Zenmap.....15

WHAT ARE HONEYPOTS?.....21

 Classification of Honeypots21

 High interaction21

 Low interaction.....22

 Physical Honeypots22

 Virtual Honeypots22

 Production Honeypots22

Research Honeypots22

What is HoneyBOT23

How does it works?23

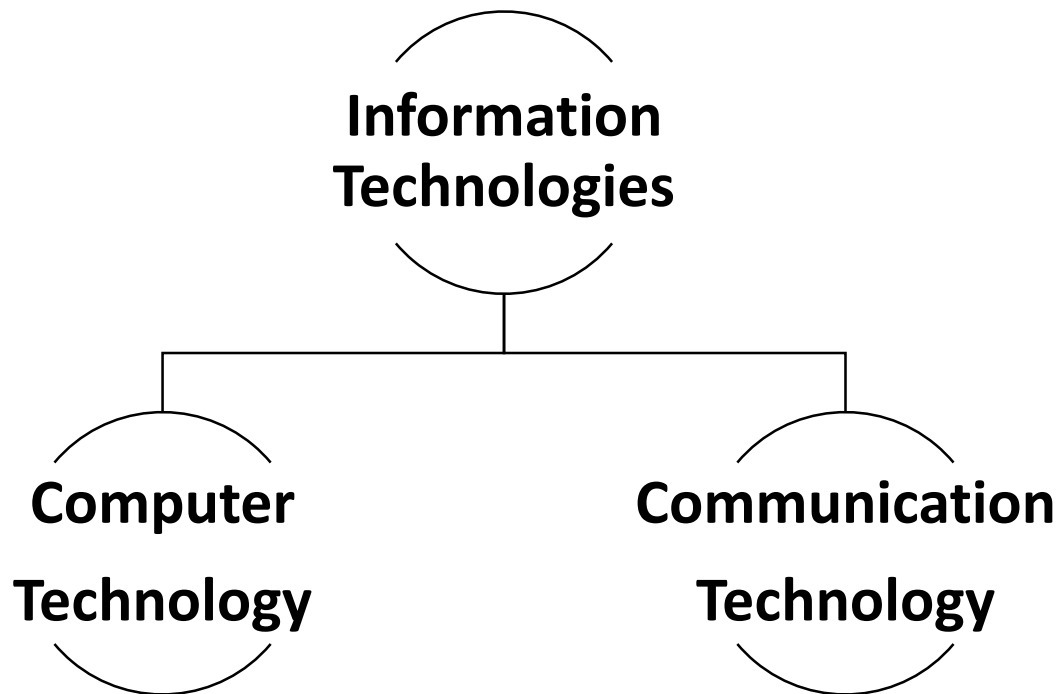
Steps to download and run Honey bot24

MANUAL-1:
**A Practical
Approach to
make a trap
for the
Attacker**

What is a Computer Network?

When two or more computers or communications devices are connected together by transmission media and channels and guided by a set of rules for communication purposes that allow users to communicate with each other and share information and data.

What is Information Technology (IT)?



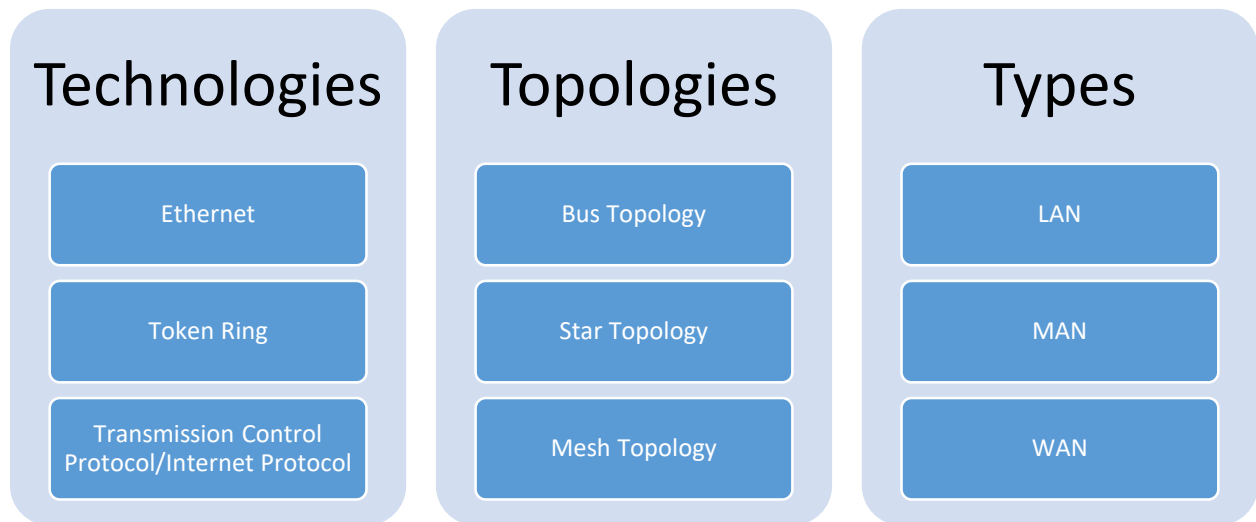
Computer Technologies

To collect, store, process, search, retrieve, and present electronic information to meet the needs of various kinds of users, e.g., computer hardware & software, PDAs, printers, groupware, smart cards....

Communication Technology

To deliver, disseminate, exchange, transmit, and receive electronic information in local, regional or global contexts, e.g., networks, fax machines, cell phones, email, satellites, GPS, Internet, telephony,

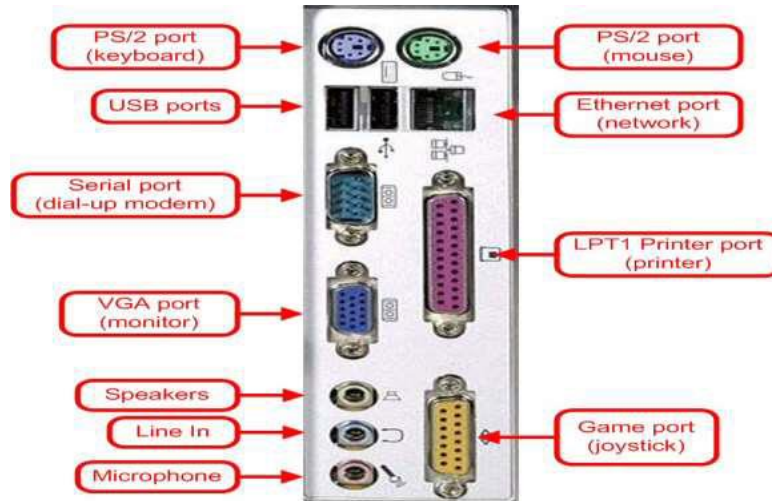
Network Essentials



What is a Port?

In computer hardware, a “port” serves as an interface between the computer and other computer or peripheral devices.

The term “PORT” is derived from a latin word “porta” meaning (gate, entrance, door)



Types of ports

1. Hardware Ports
2. Software Ports

Hardware Ports

It is a port serves as an interface between the computer and other computers or peripheral devices. In computer terms, a port generally refers to the female part of connection. Computer ports have many uses, to connect a monitor, webcam, speakers, or other peripheral devices. On the physical layer, a computer port is a specialized outlet on a piece of equipment to which a plug or cable connects.

Software Ports

A software port (usually just called a 'port') is a virtual/logical data connection that can be used by programs to exchange data directly.

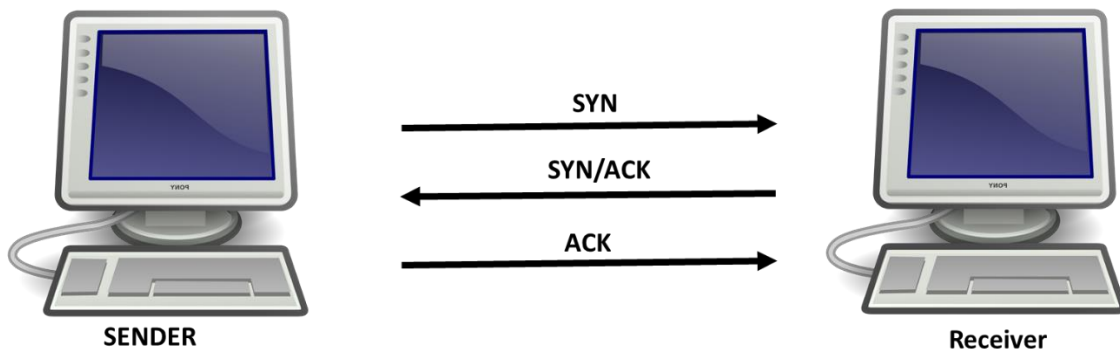
The most common of these are TCP and UDP ports, which are used to

exchange data between computers on the Internet.

Types of Software ports

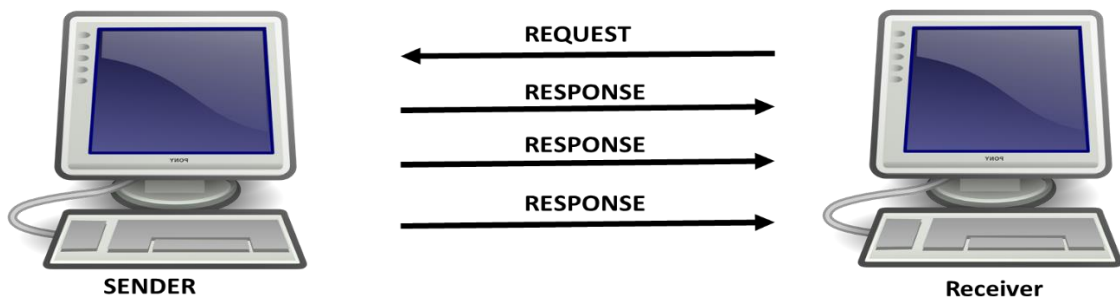
1. TCP (Transmission control Protocol) :-

TCP is a connection-oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.



2. UDP (User Datagram Protocol):-

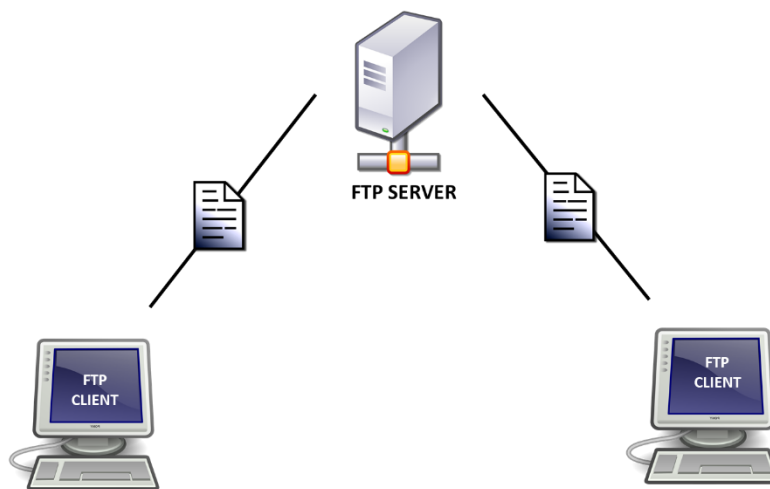
The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication.



3. FTP (File Transfer Protocol):-

Protocol for transferring files over a network. It supports both anonymous and password-mediated access.

FTP is one of the most commonly used file transfer protocols on the Internet and within private networks. An FTP server can easily be set up with little networking knowledge and provides the ability to easily relocate files from one system to another. FTP control is handled on TCP port 21 and its data transfer can use TCP port 20 as well as dynamic ports depending on the specific configuration.



Some basic Port no:

Port	Service name	Transport protocol
20, 21	File Transfer Protocol (FTP)	TCP
22	Secure Shell (SSH)	TCP and UDP
23	Telnet	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
50, 51	IPSec	
53	Domain Name System (DNS)	TCP and UDP

67, 68	Dynamic Host Configuration Protocol (DHCP)	UDP
69	Trivial File Transfer Protocol (TFTP)	UDP
80	HyperText Transfer Protocol (HTTP)	TCP
110	Post Office Protocol (POP3)	TCP
119	Network News Transport Protocol (NNTP)	TCP
123	Network Time Protocol (NTP)	UDP
135-139	NetBIOS	TCP and UDP
143	Internet Message Access Protocol (IMAP4)	TCP and UDP
161, 162	Simple Network Management Protocol (SNMP)	TCP and UDP
389	Lightweight Directory Access Protocol	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	TCP and UDP
3389	Remote Desktop Protocol	TCP and UDP

INSTALLATION OF KALI LINUX OPERATING SYSTEM IN VMWARE WORKSTATION

Basics Requirements

- Minimum requirements in Computer: 8 GB RAM, 500 GB internal memory
- VMware must be installed in main OS.
- Microsoft Windows 7/8/10 must be installed in VMware.
- Kali OS must be installed in VMware.

Step 1: Download VMware workstation 15.5 on Windows Operating system.

- To download, navigate to the following link:
<https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html>

Step 2: Install VMware workstation 15.5 on Windows Operating system desktop by:

- Start the installer by double clicking it.
- Click the next button after reading the instructions to move on to the next screen.
- Select the folder in which you want to install the application and create shortcuts for the desktop.
- Wait for installation to complete and restart the computer after successful installation.

- Click the VMware workstation shortcut and run the program.
- When you will be asked for license, you can select the option- “I want to try 30 days for free” and click continue.

Step 3: Download Kali Linux (32 or 64 bit iso file according to requirements).

- To download, navigate to the following link: <https://www.kali.org/downloads/> and select first or second option according to the requirements (i.e. 32 or 64bit).

Step 4: Installation of Kali Linux in VMware workstation.

- Open VMWare Workstation and click on “create a new virtual machine”. Select Kali Linux Operating system.
- Select Graphical Install using the down arrow key and click continue.
- A dialog box will appear to select a language. Select English Language and click continue.
- A dialog box will appear to select a location. Select India and click continue.
- A dialog box will appear to select a keyboard layout. Select American English and click continue.
- A dialog box will appear to select a location. Select India and click continue.
- A dialog box will appear to enter the host name of system. Enter Kali and click continue.
- A dialog box will appear to enter the domain name of system. Write example.com and click continue.
- Set username and password and click continue.
- A dialog box will appear to partition your disk. Enter Kali and continue. Select Guided – Use entire disk and click continue. Select sda, VMware Virtual disk and click continue. Select all files in one partition and click Continue.

- Select the Finish Partitioning and write changes to disk which should be selected by default.
- A dialog box will appear to confirm changes to disk. Select yes and click continue.
- Wait for the installation to complete.
- A dialog box will appear to configure network mirror for Package manager. Select yes.
- A dialog box will appear to install the GRUB boot loader. Select yes. Select /dev/sda and click Continue.
- Wait for the installation to complete.
- Login with username: root, Password: what you entered during the installation process earlier (or toor if you have not entered any password).

What is Zenmap

Zenmap is the official Nmap Security Scanner GUI. It is a multi- platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

Types of scanning done by Zenmap

Intense scan: It is a fast, comprehensive and accurate scan utilizes all TCP ports and evaluates the operating system, version ,script scanning and trace route running on a host and provides the detailed results. It does not need root information. The result gives information about how many live hosts are present, find open TCP ports and for remote system IP path is addressed.

Intense scan plus UDP: It is an intense scan which scans UDP ports a well. The UDP scan is a connectionless protocol. It scans if UDP ports are open by sending UDP packets on ports on the target host and analyses the feedback packets to verify the openness of service on the host. The UDP scan sends an UDP packet with an empty header to the target port.

Ping Scan: This is basic type of scan observes network to locates target hosts which are live utilizing ping such as ICMP echo and waiting for

reply. It can be utilized for testing and troubleshooting the network connectivity.

Quick scan: This Scan faster than the intense scan as it scans limited numbers of TCP ports that are common utilizing timing templates. It scans common places in the network that are vulnerable.

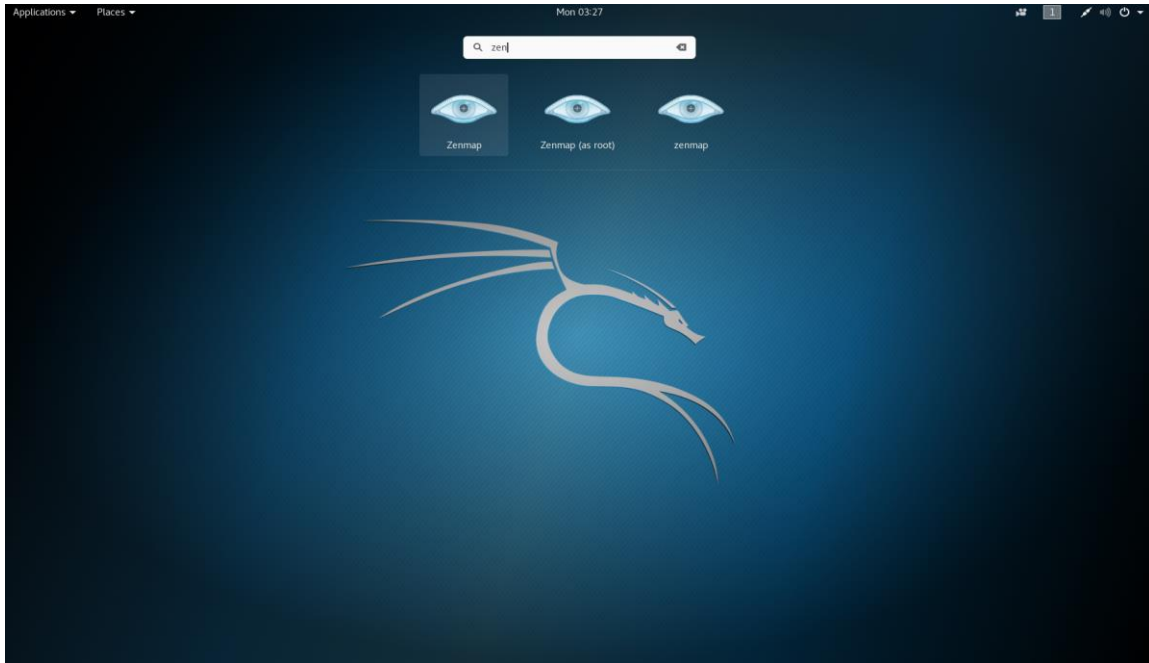
Quick scan plus: It is a quick scan with addition of Operating System and version detection.

Regular scan: This scans everything by default. This is a simple mechanism helps in making the network functioning healthy. This is The TCP SYN scan for common 1000 TCP ports utilizing the ICMP Echo ping for host detection is done.

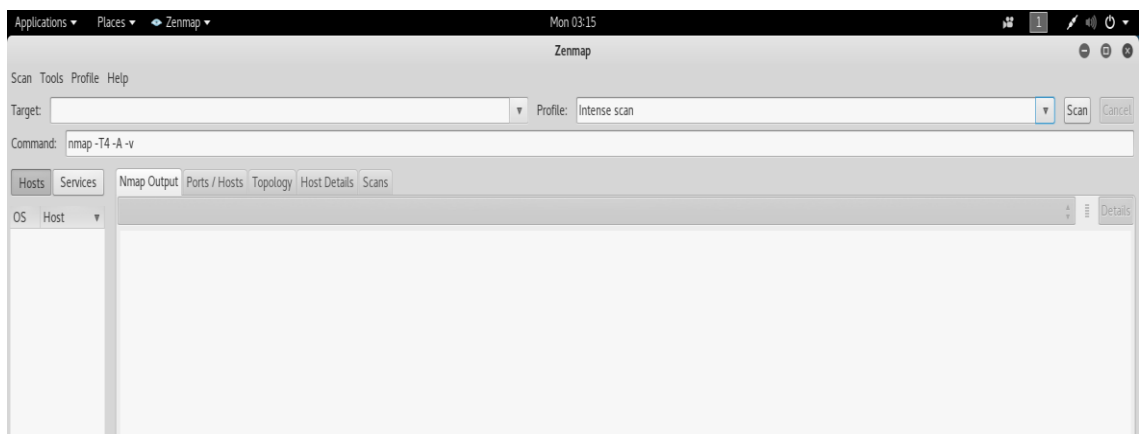
Slow comprehensive scan: It is a prominent and accurate scan that relies on different protocols i.e. TCP, UDP and SCTP to evaluate the hosts. If a host is detected then it identifies the Operating System, services and versions the host is running.

Steps to run Zenmap

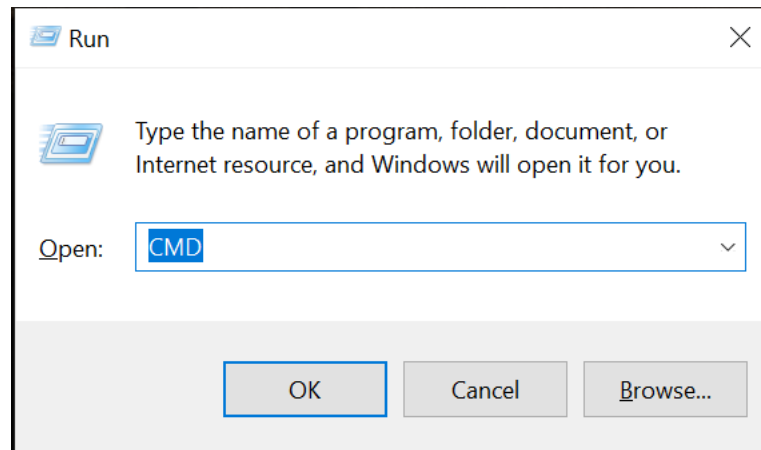
Step 1: Click on application in Kali OS and type zenmap and press Enter.



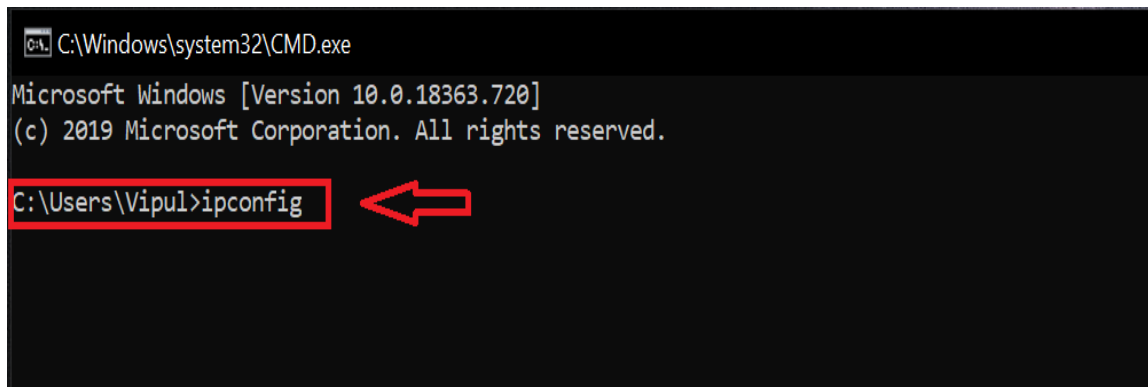
Step 2: Zenmap will open like this as shown in figure.



Step 3: Open cmd to get the IP Address



Step 4: In cmd type IPCONFIG to get the IP address of Main Machine i.e. Windows.



Step 5: Here we get the IP Address of main OS. i.e. 192.168.43.88

```
C:\Windows\system32\CMD.exe
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

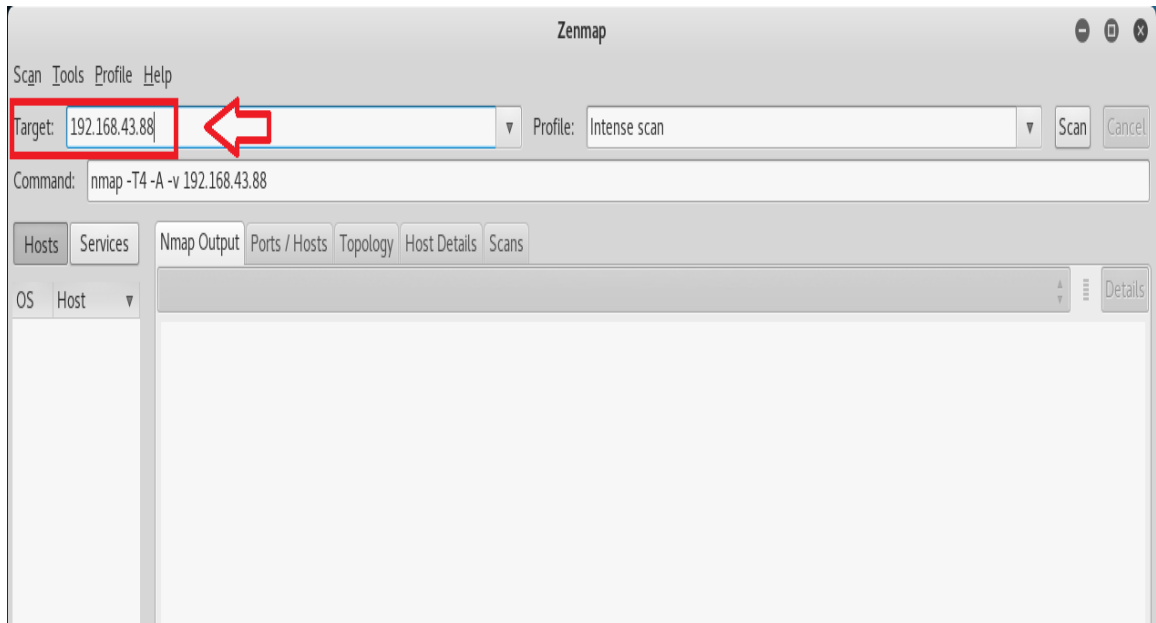
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2401:4900:c80:f9ba:d495:1075:8bfc:995b
Temporary IPv6 Address. . . . . : 2401:4900:c80:f9ba:b556:70bf:98f6:ce65
Link-local IPv6 Address . . . . . : fe80::d495:1075:8bfc:995b%10
IPv4 Address. . . . . : 192.168.43.88
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::3094:35ff:fe07:8ad5%10
                            192.168.43.107

Ethernet adapter Bluetooth Network Connection:

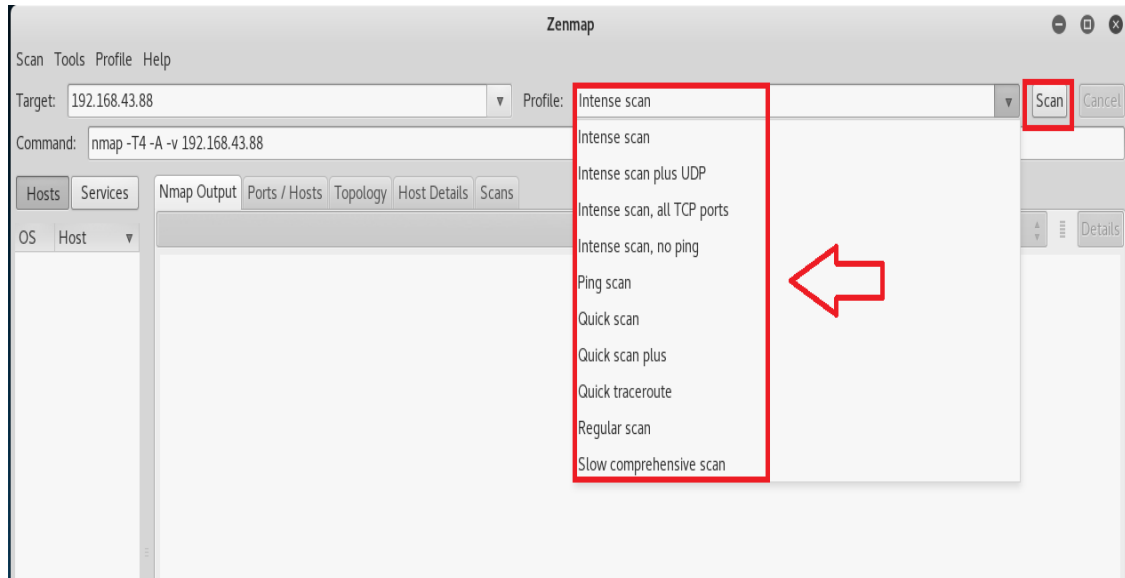
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\Vipul>
```

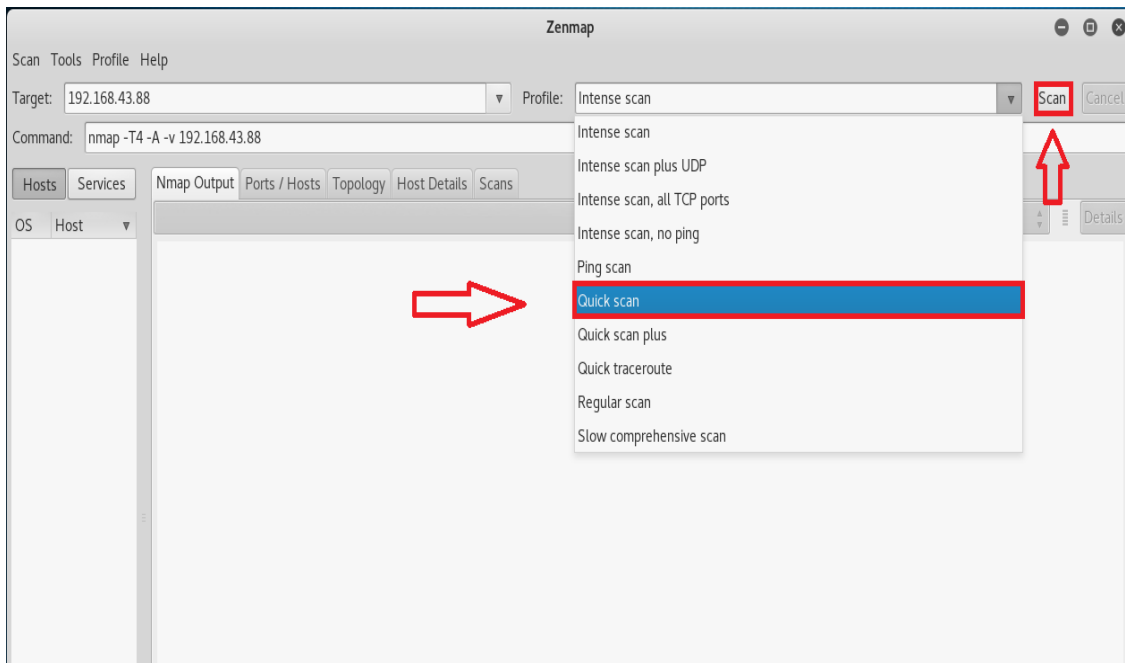
Step 6: In Attackers machine i.e Kali just type the IP address of main machine to scan the open ports. As shown in fig.



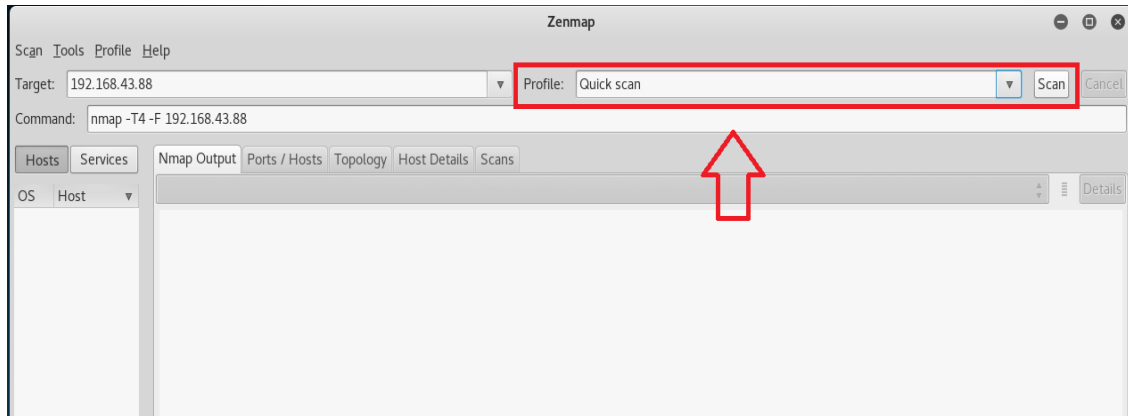
Step 7: We have so many different options to scan an particular IP Address as shown in fig. given below.



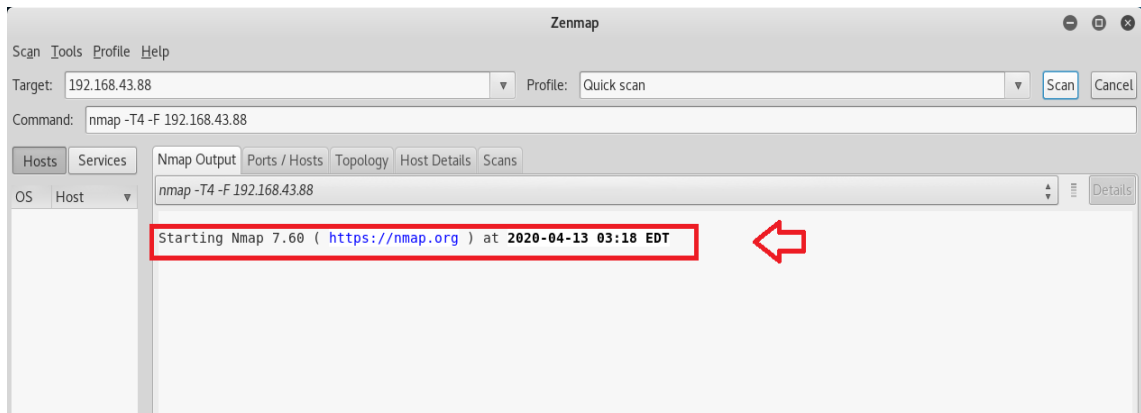
Step 8: From the following scanning type we choose Quick scan to get the information of Main Machine.



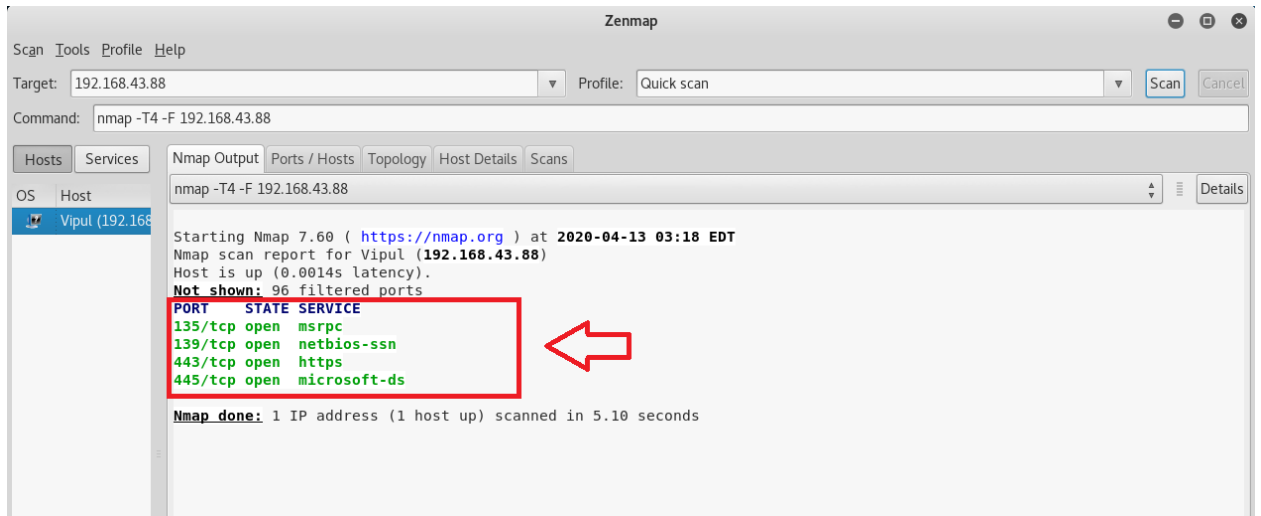
Step 9: After selecting the scan type i.e Quick scan the click on Scan button.



Step 10: Scanning process will start



Step 11: After the scanning process it will show results like this, that following ports are open on the Operating system whose IP address is 192.168.43.88 (main machine).



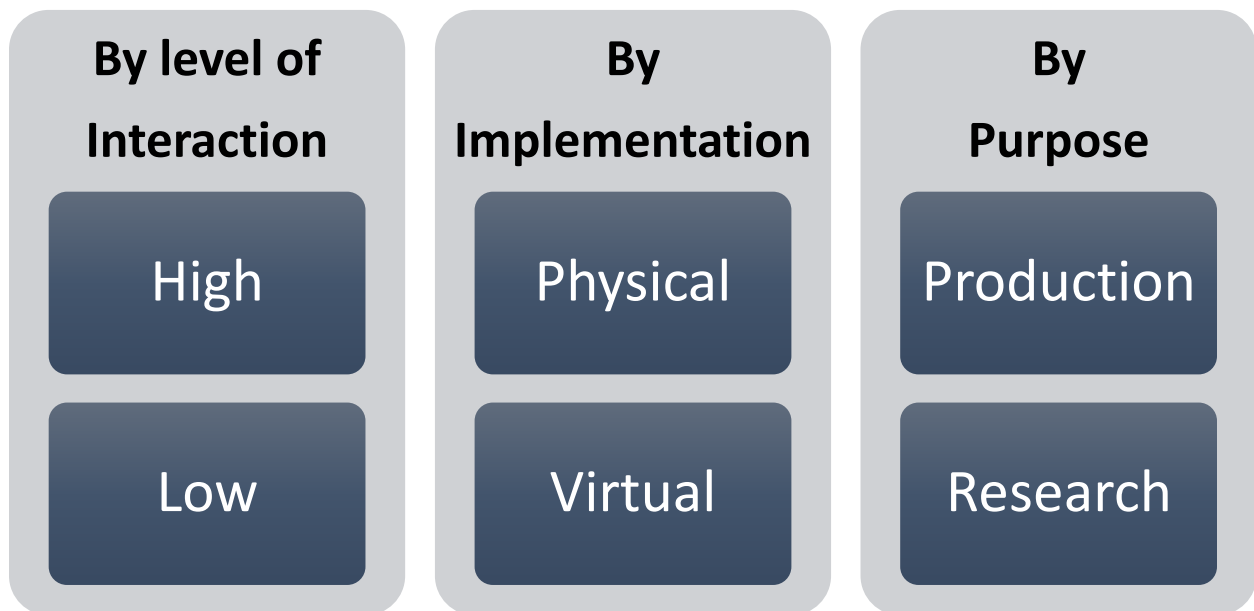
WHAT ARE HONEYPOTS?

Honeypot is an exciting new technology with enormous potential for the security community.

According to Lance Spitzner, founder of honeypot project: “A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.”

Used for monitoring, detecting and analyzing attacks.

Classification of Honeypots



High interaction

- Simulates all aspects of the OS: real systems.
- Can be compromised completely, higher risk.
- Provide More Information

- Eg:-Honeynet

Low interaction

- Simulates some aspects of the system.
- Easy to deploy, minimal risk
- Provide Limited Information

Physical Honeypots

- Real machines
- Own IP Address
- High Intractive

Virtual Honeypots

- Simulated by other machines that:
 - Respond to the network traffic sent to the honeypots.
 - May simulate a lot of (different) virtual honeypots at the same time.

Production Honeypots

- Help to mitigate risk in your organizations

It is further classified in 3 categories.

1. Prevention

- Keeping the bad guys out
- Mechanism such as encryption prevent attackers from accessing critical information.

2. Detection

- Detecting the attacker when he breaks in.
- Challenges: False positive, False negative

3. Response

- Can easily be pulled offline.

Research Honeypots

- Capture extensive information.
- Used primarily by research, military, government organization.

What is HoneyBOT

HoneyBOT is a medium interaction honeypot for windows.

A honeypot creates a safe environment to capture and interact with unsolicited and often malicious traffic on a network. HoneyBOT is an easy to use solution ideal for network security research or as part of an early warning IDS. The logging capability of a honeypot is far greater than any other network security tool and captures raw packet level data even including the keystrokes and mistakes made by hackers. The captured information is highly valuable as it contains only malicious traffic with little to no false positives. Honeypots are becoming one of the leading security tools used to monitor the latest tricks and exploits of hackers by recording their every move so that the security community can more quickly respond to new exploits.

How does it works?

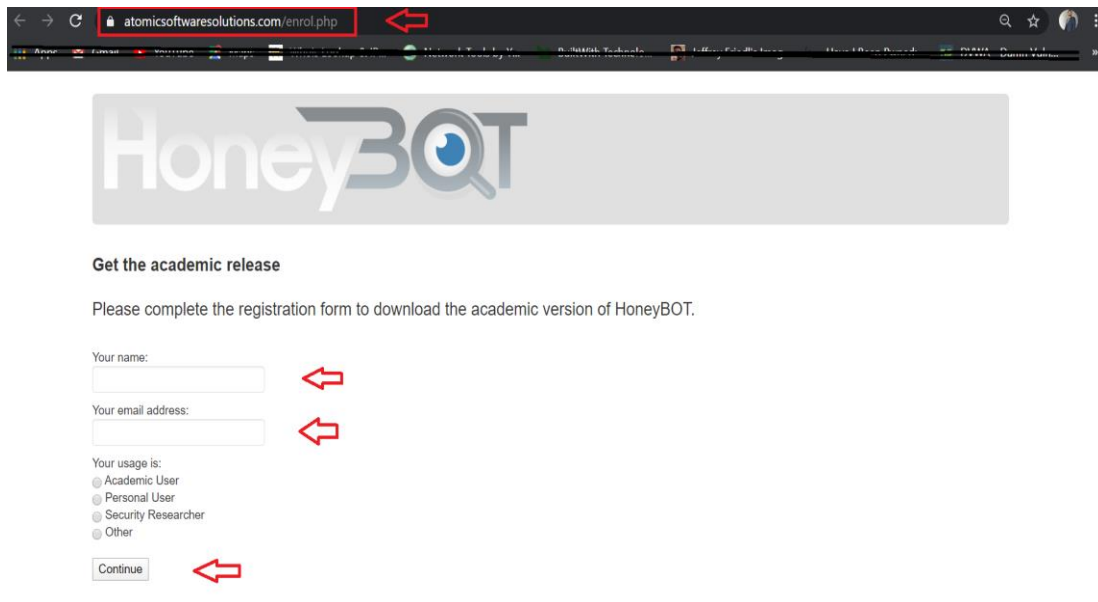
HoneyBOT works by opening a range of listening sockets on your computer which are designed to mimic vulnerable services. When an attacker connects to these services they are fooled into thinking they are attacking a real server. The honeypot safely captures all communications with the attacker and logs these results for future analysis. Should an attacker attempt an exploit or upload a rootkit or trojan to the server the honeypot environment can safely store these files on your computer for malware collection and analysis purposes.

Steps to download and run Honey bot

Step 1: To Download the honeybot visit the official web site i.e.

<https://www.atomicsoftwaresolutions.com/>

Step 2: Fill the following information to download the honeybot



atomicsoftwaresolutions.com/enrol.php

HoneyBOT

Get the academic release

Please complete the registration form to download the academic version of HoneyBOT.

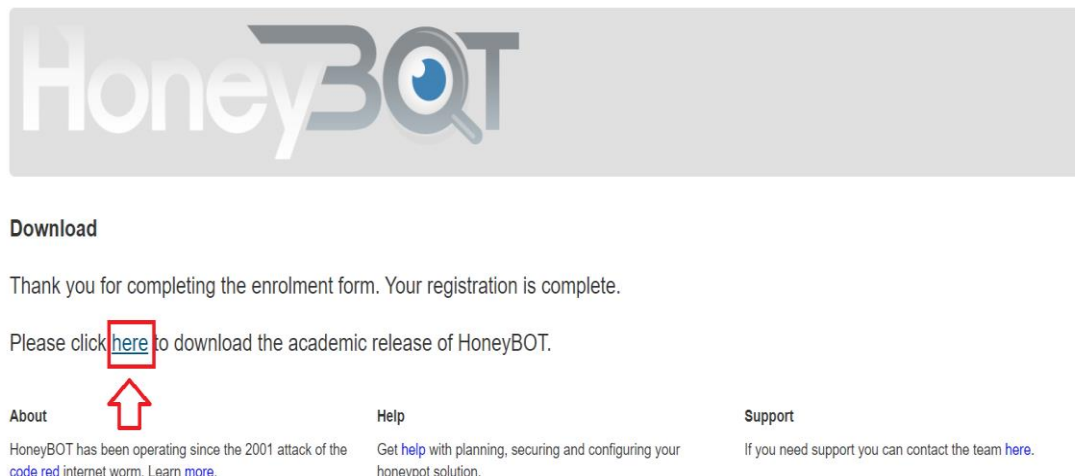
Your name:

Your email address:

Your usage is:

- Academic User
- Personal User
- Security Researcher
- Other

Step 3: After that click on Hyperling i.e. “here” as shown in figure given below.



HoneyBOT

Download

Thank you for completing the enrolment form. Your registration is complete.

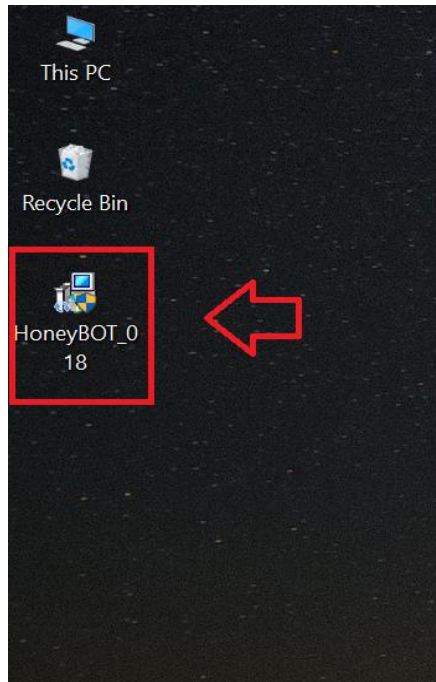
Please click [here](#) to download the academic release of HoneyBOT.

About
HoneyBOT has been operating since the 2001 attack of the code red internet worm. Learn [more](#).

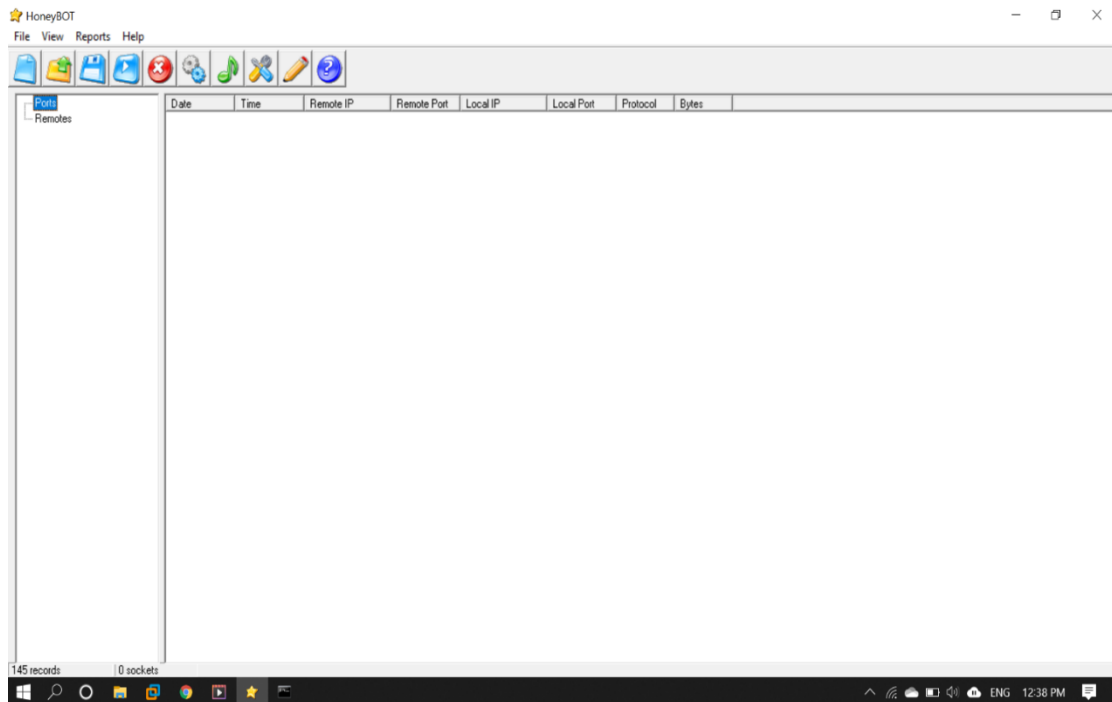
Help
Get [help](#) with planning, securing and configuring your honeypot solution.

Support
If you need support you can contact the team [here](#).

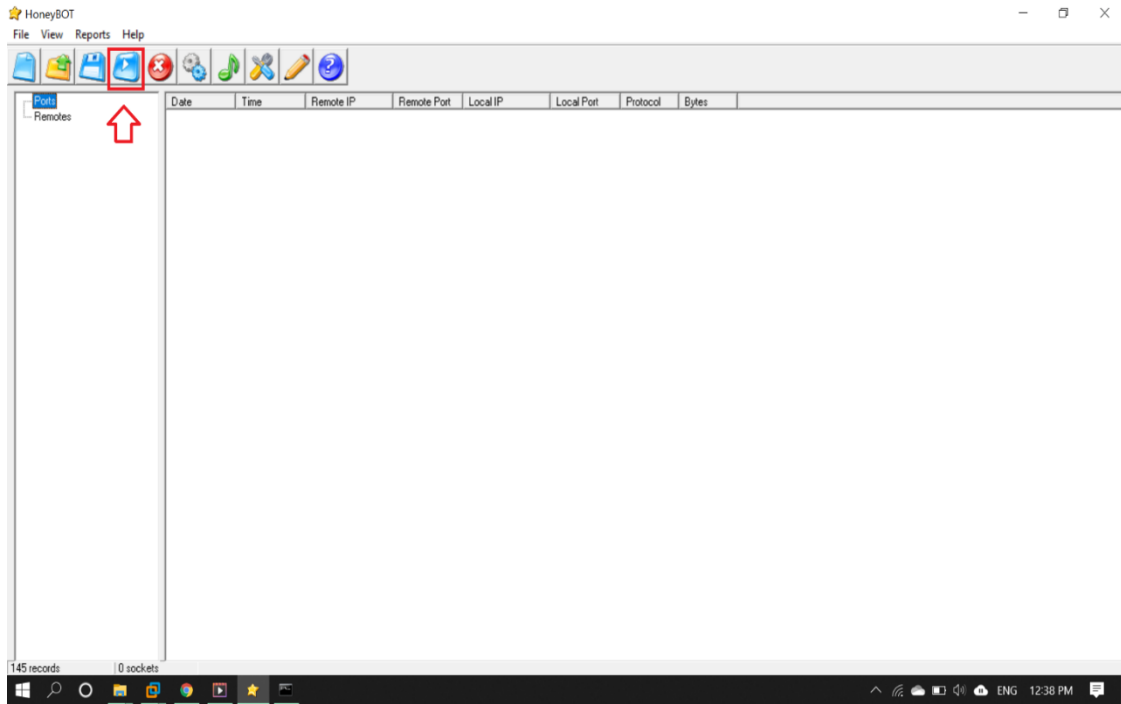
Step 4: After that double click on setup of Honeybots to run.



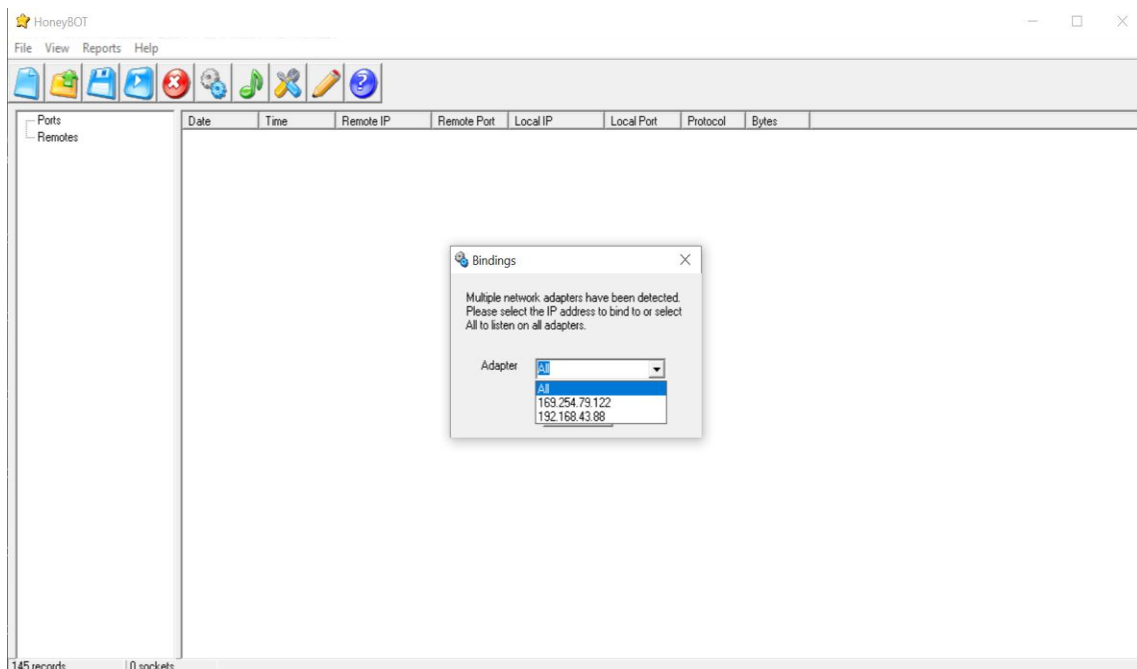
Step 5: This is the view of the honeybot software.



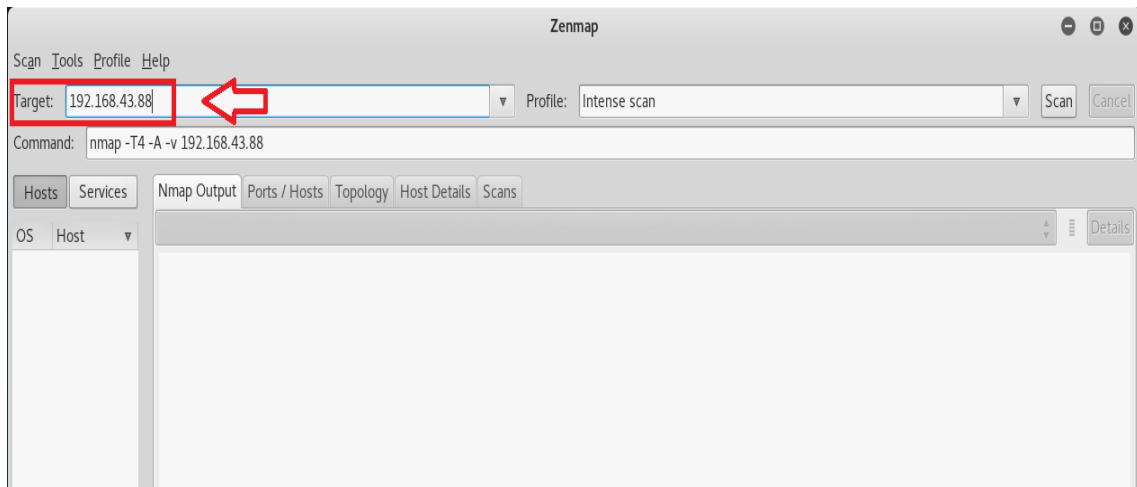
Step 6: Click on start before running the Zenmap in attackers machine.



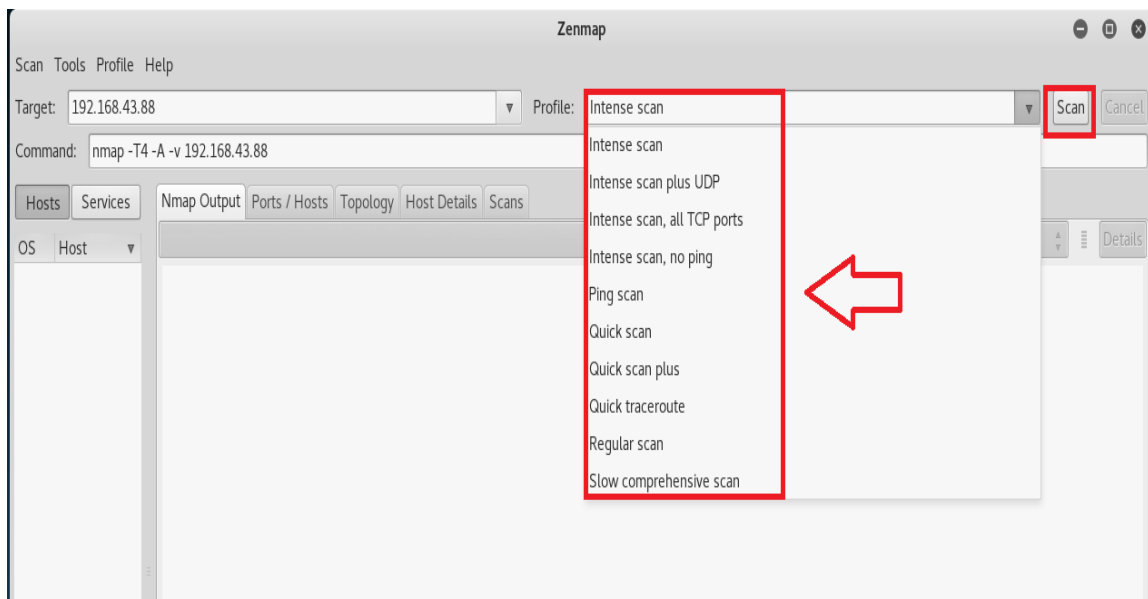
Step 7: Select the IP Address to bind to or to listen on all adapters.



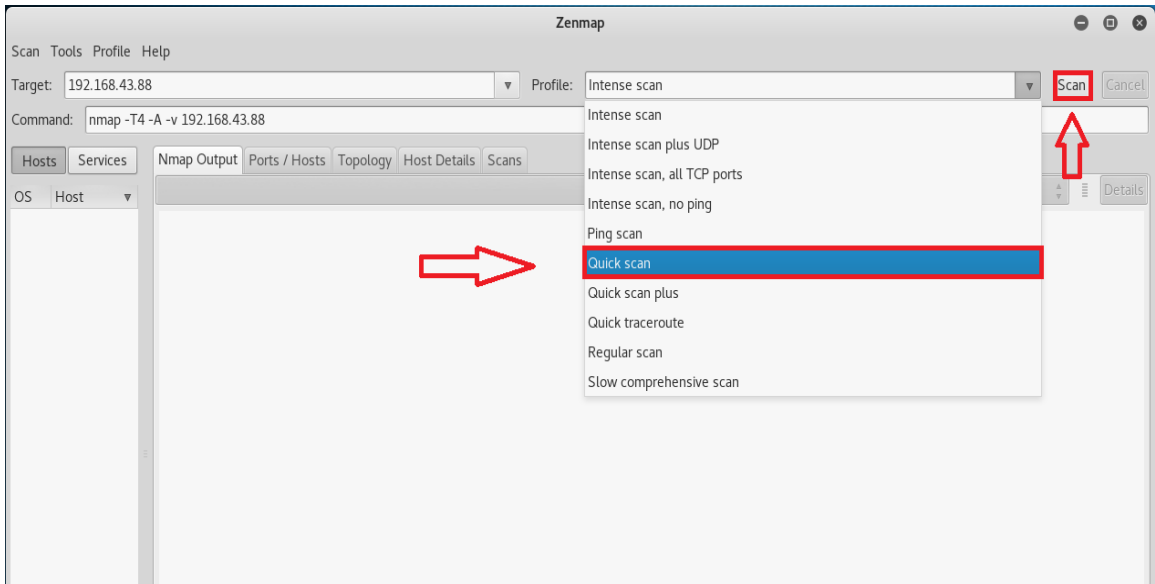
Step 8: After that run Zenmap in attackers OS i.e. Kali



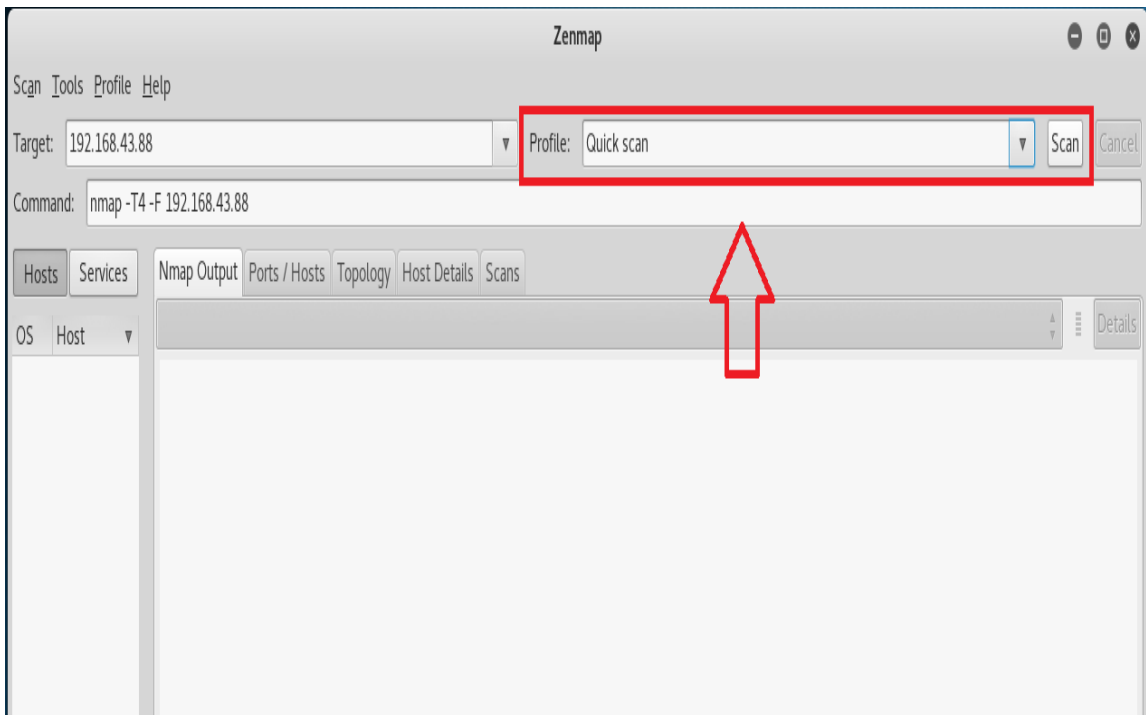
Step 9: We have so many different options to scan an particular IP Address as shown in fig. given below.



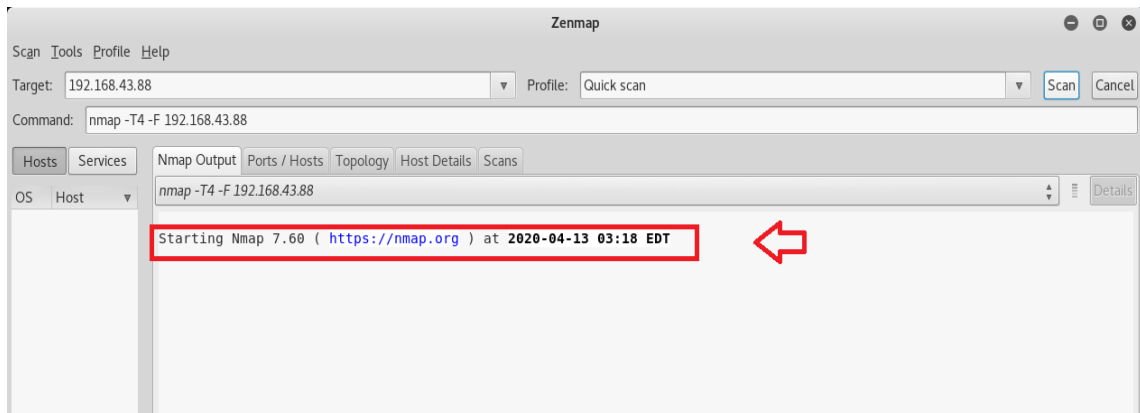
Step 10: From the following scanning type we choose Quick scan to get the information of Main Machine.



Step 11: After selecting the scan type i.e Quick scan the click on Scan button.



Step 12: Scanning process will start



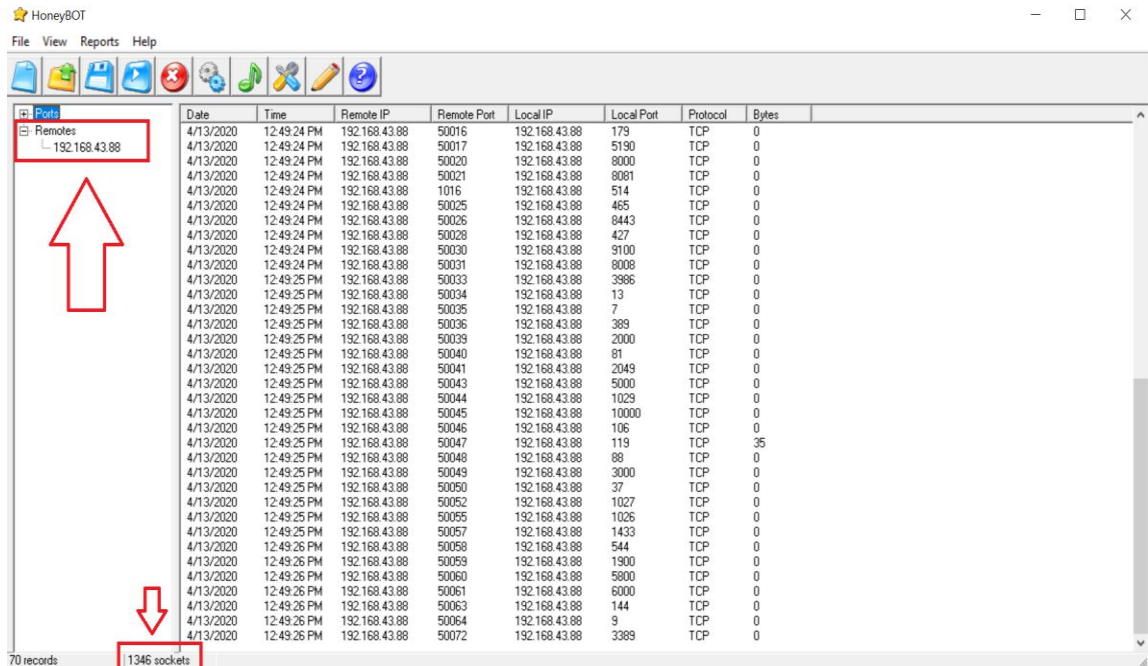
Step 13: After the scanning process it will show results like this, that following ports are open on the Operating system whose IP address is 192.168.43.88 (main machine).

After start the Honeybot it will show some fake open Port to attract the Attacker.

The screenshot shows the HoneyBOT interface with a table of open ports. The table has columns for Date, Time, Remote IP, Remote Port, Local IP, Local Port, Protocol, and Bytes. The data shows a list of open ports on 192.168.43.88, including ports 3389, 5900, 53, 143, 23, 8080, 111, 3306, 22, 80, 1723, 25, 110, 113, 995, 8888, 199, 554, 993, 21, 1720, 1025, 548, 515, 3128, 4899, 543, 513, 5631, 2001, 444, 5432, 79, 6001, 1028, and 179.

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
4/13/2020	12:49:21 PM	192.168.43.88	49966	192.168.43.88	3389	TCP	0
4/13/2020	12:49:21 PM	192.168.43.88	49967	192.168.43.88	5900	TCP	12
4/13/2020	12:49:21 PM	192.168.43.88	49968	192.168.43.88	53	TCP	0
4/13/2020	12:49:21 PM	192.168.43.88	49969	192.168.43.88	143	TCP	77
4/13/2020	12:49:21 PM	192.168.43.88	49970	192.168.43.88	23	TCP	12
4/13/2020	12:49:21 PM	192.168.43.88	49971	192.168.43.88	8080	TCP	0
4/13/2020	12:49:21 PM	192.168.43.88	49972	192.168.43.88	111	TCP	0
4/13/2020	12:49:21 PM	192.168.43.88	49973	192.168.43.88	3306	TCP	51
4/13/2020	12:49:22 PM	192.168.43.88	49974	192.168.43.88	22	TCP	0
4/13/2020	12:49:22 PM	192.168.43.88	49975	192.168.43.88	80	TCP	0
4/13/2020	12:49:22 PM	192.168.43.88	49976	192.168.43.88	1723	TCP	16
4/13/2020	12:49:22 PM	192.168.43.88	49977	192.168.43.88	25	TCP	25
4/13/2020	12:49:23 PM	192.168.43.88	49979	192.168.43.88	110	TCP	22
4/13/2020	12:49:23 PM	192.168.43.88	49980	192.168.43.88	113	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49981	192.168.43.88	995	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49982	192.168.43.88	8888	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49985	192.168.43.88	199	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49986	192.168.43.88	554	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49987	192.168.43.88	993	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49988	192.168.43.88	21	TCP	41
4/13/2020	12:49:23 PM	192.168.43.88	49991	192.168.43.88	1720	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49992	192.168.43.88	1025	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49993	192.168.43.88	548	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49996	192.168.43.88	515	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49997	192.168.43.88	3128	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	49998	192.168.43.88	4899	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	50000	192.168.43.88	543	TCP	0
4/13/2020	12:49:23 PM	192.168.43.88	50001	192.168.43.88	513	TCP	0
4/13/2020	12:49:24 PM	192.168.43.88	50006	192.168.43.88	5631	TCP	0
4/13/2020	12:49:24 PM	192.168.43.88	50007	192.168.43.88	2001	TCP	0
4/13/2020	12:49:24 PM	192.168.43.88	50009	192.168.43.88	444	TCP	0
4/13/2020	12:49:24 PM	192.168.43.88	50010	192.168.43.88	5432	TCP	0
4/13/2020	12:49:24 PM	192.168.43.88	50011	192.168.43.88	79	TCP	0
4/13/2020	12:49:24 PM	192.168.43.88	50013	192.168.43.88	6001	TCP	0
4/13/2020	12:49:24 PM	192.168.43.88	50014	192.168.43.88	1028	TCP	0
4/13/2020	12:49:24 PM	192.168.43.88	50016	192.168.43.88	179	TCP	0

Step 14: We are able to scan different IP addresses by single scan in Honeybot



Step 15: In setting we are also able to ADD, EDIT, or DELETE any Services

