iGNITE Technologies

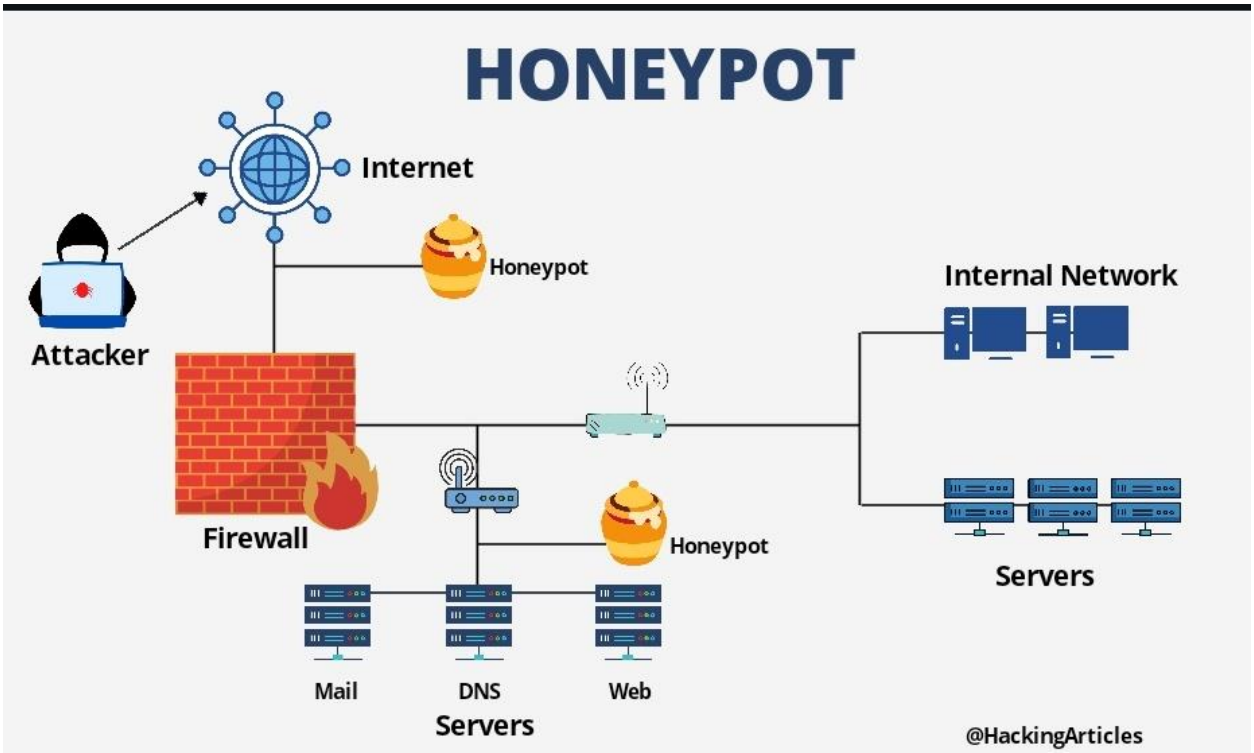
A DETAILED GUIDE ON HONEYPOTS

WWW.HACKINGARTICLES.IN

Contents

Introduction

Honeypots are generally hardware or software that are deployed by the security departments of any organization to examine the threats that are possessed by the attackers. Honeypots usually act as baits for an organization to gather information on the attacker and alongside protect the real target system.



What are honeypots?

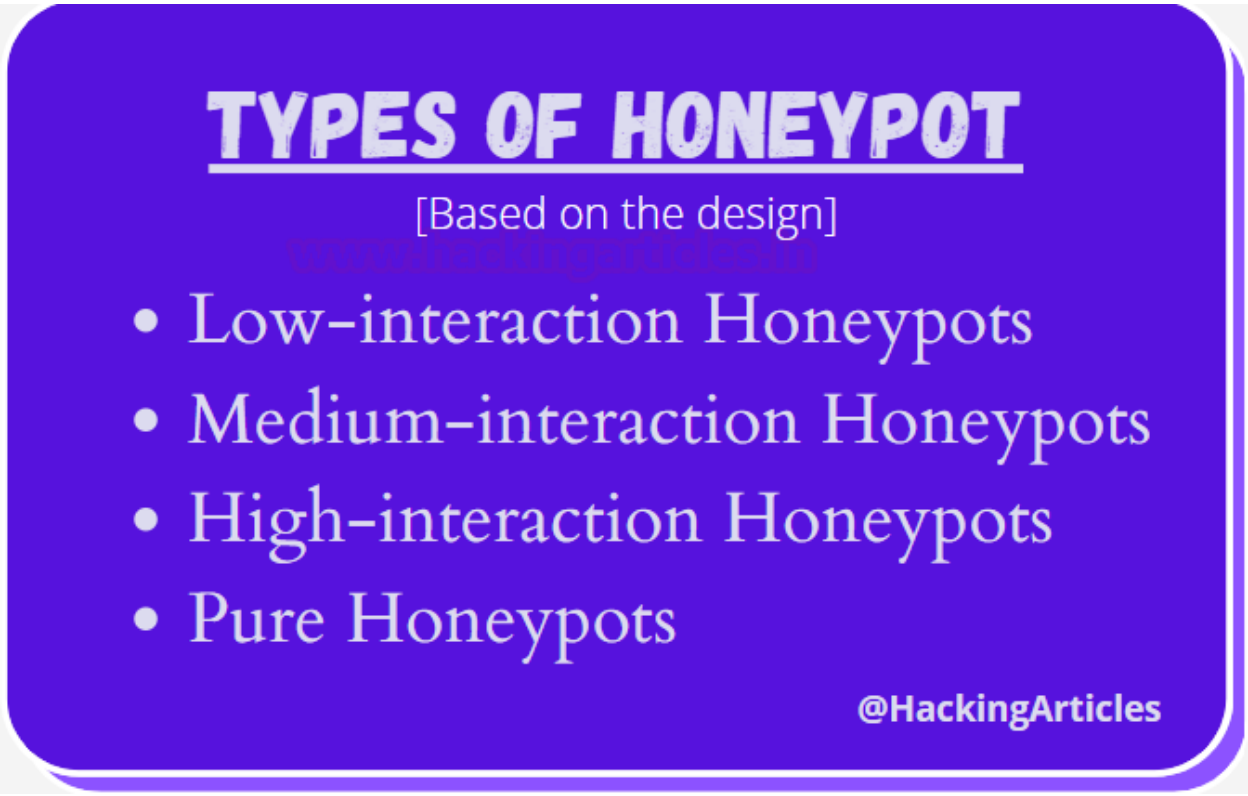
Honeypots are a type of Internet security resource that is used to entice cybercriminals to deceive them when they try to intrude into the network for any illegal use. These honeypots are generally set up to understand the activities of the attacker in the network so that the organisation can come up with stronger prevention methods against these intrusions. The honeypots do not carry any valuable data as they are faked proxies that help in logging the network traffic.

Working of honeypots

As an IT administrator, you would want to set up a honeypot system that might look like a genuine system to the outside world. The kind of data that honeypots generally capture:

- Keystrokes entered and typed by the attacker.
- The IP address of the attacker
- The usernames and different privileges used by the attackers
- The type of data that the attacker had accessed, deleted or that was altered.

Types of Honeypots



Low-Interaction Honeypots:

They match a very limited number of services and applications that are present on the network or on the system. This type of honeypot can be used to keep track of UDP, TCP, and ICMP ports and services. Here we make use of fake databases, data, files, etc. as bait to trap attackers to understand the attacks that would happen in real-time. Examples of a few low-interaction tools are **Honeytrap, Specter, KFsensor,** etc.

Medium-Interaction Honeypots:

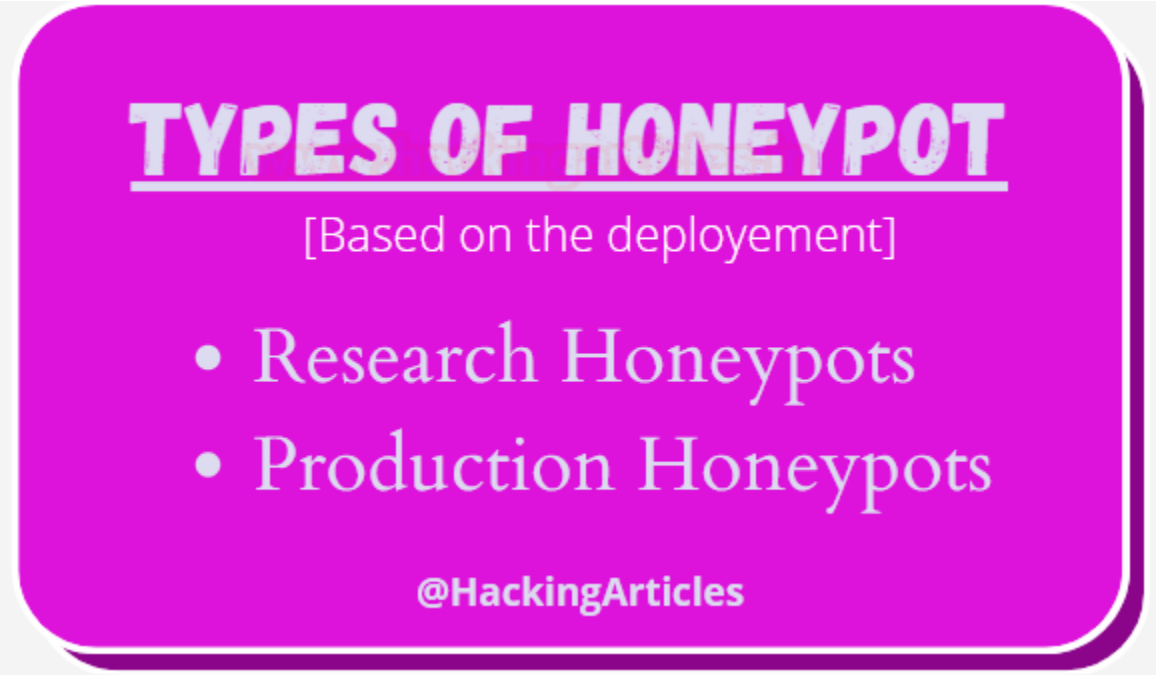
They are based on imitating real-time operating systems and have all the applications and services of a target network. They tend to capture more information as their purpose is to stall the attacker so that the organisation gets more time to respond appropriately to the threat. Examples of a few medium-interaction tools are **Cowrie, HoneyPy, etc.**

High-Interaction Honeypots:

They are genuine vulnerable software that is run on a real operating system with various applications that a production system would generally have. The information gathered using these honeypots is more resourceful, but they are difficult to maintain. An example of a high-interaction tool is the **honeynet.**

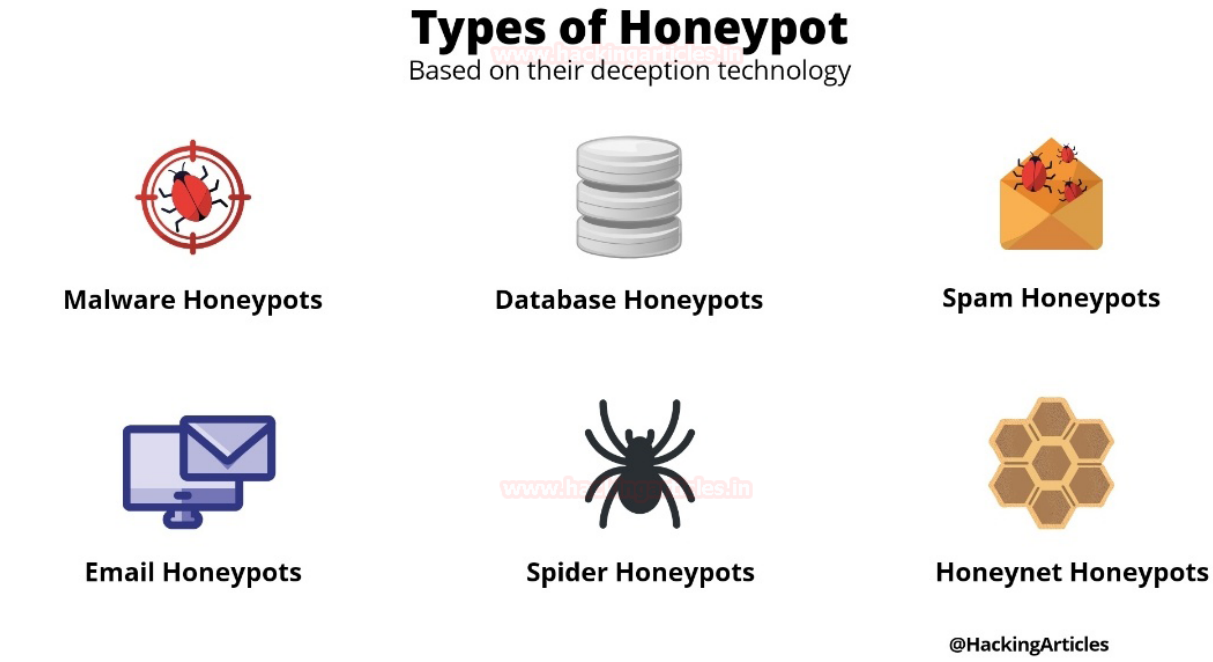
Pure Honeypots:

These honeypots usually imitate the actual production environment of an organization, which makes an attacker assume it to be a genuine one and invest more time exploiting it. Once the attacker tries to find the vulnerabilities, the organisation will be alerted, and hence any kind of attack can be prevented earlier.



Production Honeypots:
These honeypots are usually installed in the organization's actual production network. They also help in finding any internal vulnerabilities or attacks as they are present in the network internally.

Research Honeypots:
They are high-interaction honeypots, but they are set up with a focus of research in the areas of various governmental or military organisations to gain more knowledge about the behaviour of the attackers.



Malware Honeypots:

They are the kind of honeypots that are used to trap malware in a network. Their purpose is to attract the attacker or any malicious software and allow them to perform certain attacks that can be used to understand the pattern of the attack.

Email Honeypots:

These honeypots are hoax email addresses that are used to attract attackers across the internet. The emails that are received by any malicious actor can be monitored and examined and can be used to help the fall for phishing email scams.

Database Honeypots:

These honeypots pose as actual databases that are vulnerable in name and usually attract attacks like SQL injections. They are meant to lure the attackers into thinking that they might contain sensitive information like credit card details, which will let the organisation understand the pattern of the attacks they have performed.

Spider Honeypots:

These honeypots are installed with the purpose of trapping the various web crawlers and spiders that tend to steal important information from the web applications.

Spam Honeypots:

These honeypots consist of hoax email servers to attract spammers to exploit vulnerable email elements and give details about the activities performed by them.

Honeynets:

these are nothing but a network of honeypots which are installed in a virtual and isolated environment along with various servers to record the activities of the attackers and understand the potential threats.

Honeypots can be deployed in various environments. Today we will see the installation and working of honeypots in the Windows, Android, and Linux environments.

Windows System

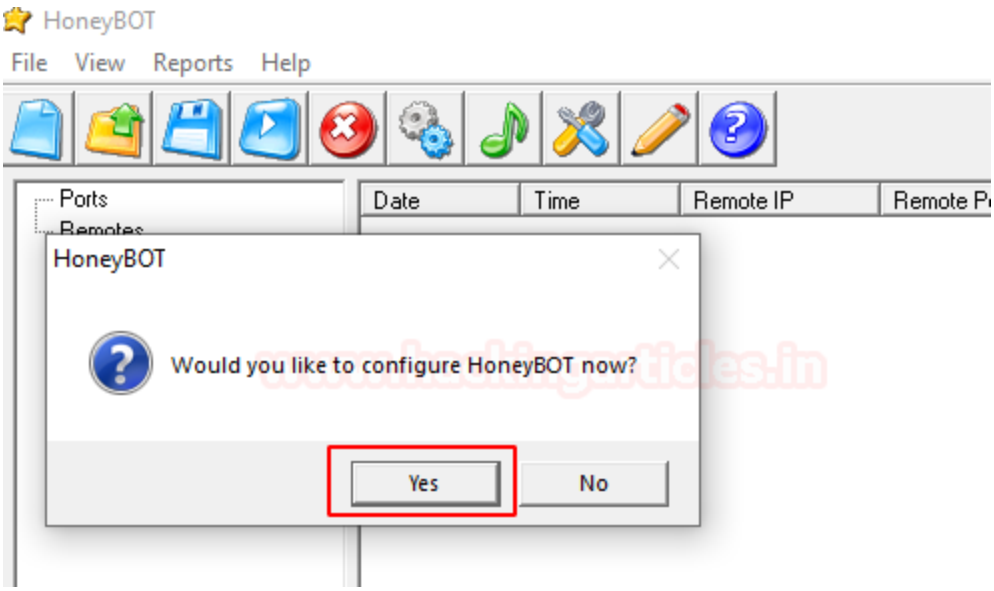
Today we will be looking at the famous honeypot software called HoneyBOT. which can be downloaded **here**. Start Kali Linux as the attacker machine and your Windows system as the host machine.

Let us first do an nmap scan on the host machine when the honeypot is not installed.

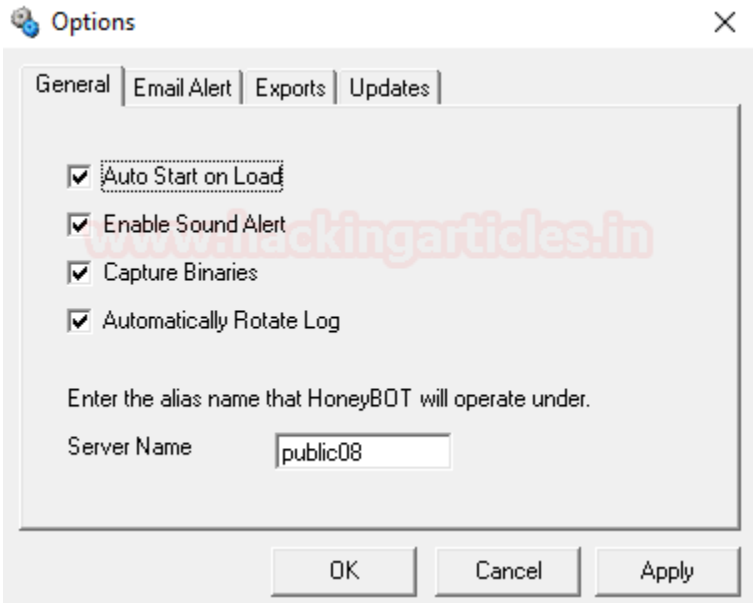
nmap -sV 192.168.1.17

```
root@kali:~# nmap -sV 192.168.1.17
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-13 07:19 EST
Nmap scan report for 192.168.1.17
Host is up (0.00027s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:0C:29:54:91:59 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

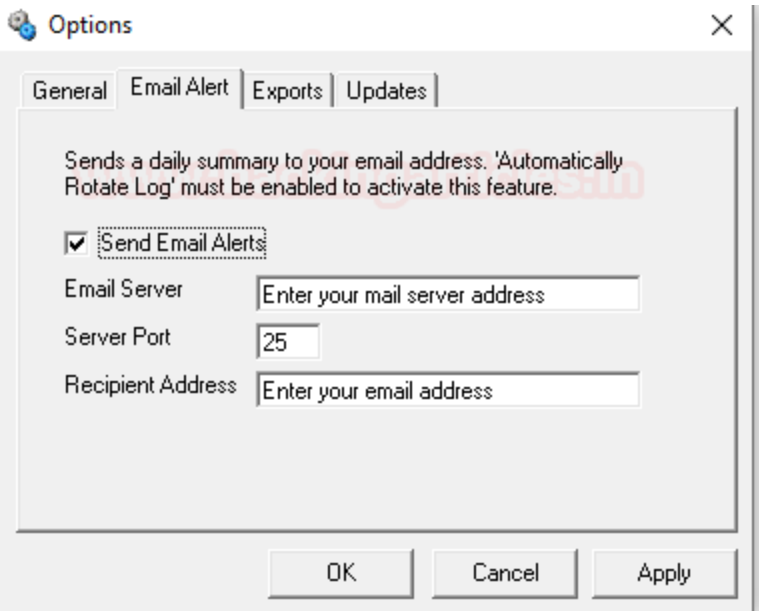
Now on your Windows system, install the HoneyBOT software and configure it. Click on "yes" to proceed.



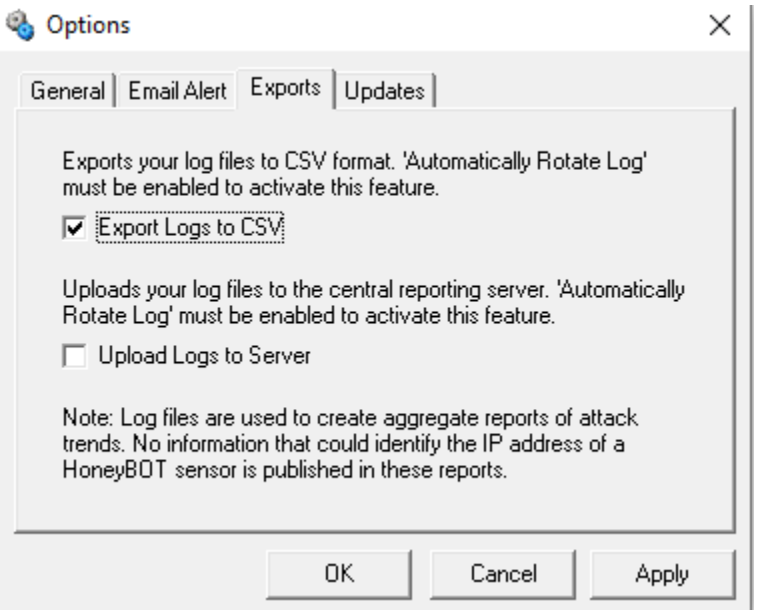
Check all the parameters that you want in your honeypot and click on Apply to proceed.



To get email reports on your honeypot, add the recipient's email address and click on "Apply."



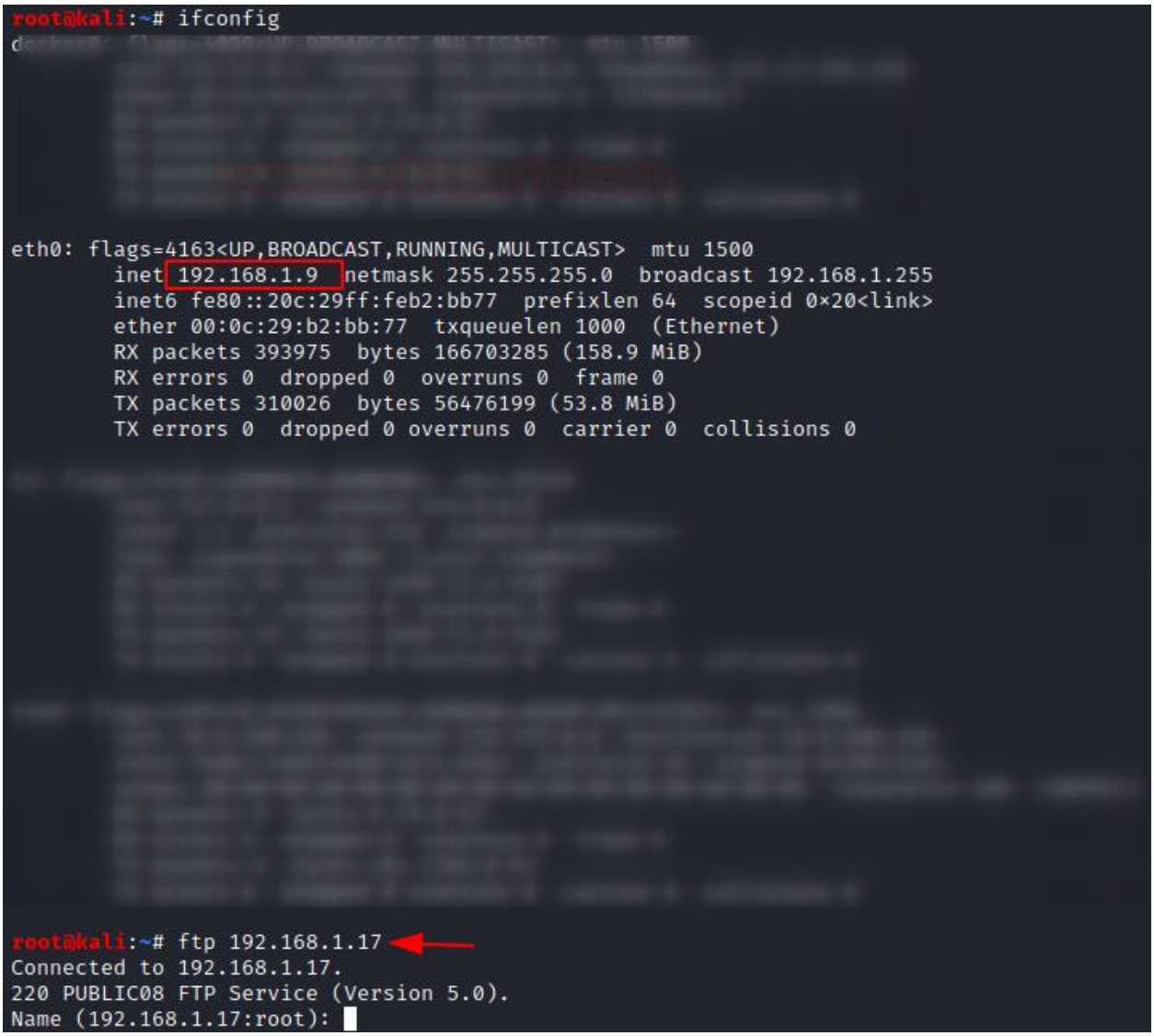
If you want to save the honeypot logs in CSV format, you can use this setting.



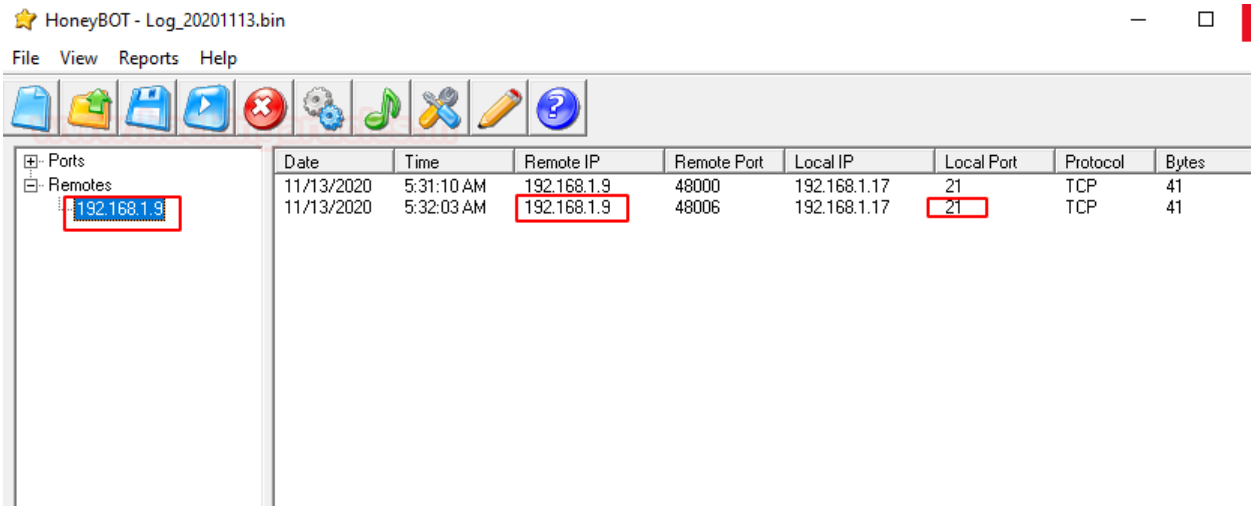
> On the attacker's machine, performs a nmap scan, and there you will see so many fake services that are open due to the presence of the honeypot in the system.

```
root@kali:~# nmap 192.168.1.17
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-13 08:24 EST
Nmap scan report for 192.168.1.17
Host is up (0.00084s latency).
Not shown: 752 closed ports
PORT    STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
33/tcp    open  dsp
37/tcp    open  time
42/tcp    open  nameserver
43/tcp    open  whois
49/tcp    open  tacacs
53/tcp    open  domain
70/tcp    open  gopher
79/tcp    open  finger
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
84/tcp    open  ctf
85/tcp    open  mit-ml-dev
88/tcp    open  kerberos-sec
89/tcp    open  su-mit-tg
90/tcp    open  dnsix
99/tcp    open  metagram
100/tcp   open  newacct
106/tcp   open  pop3pw
109/tcp   open  pop2
110/tcp   open  pop3
111/tcp   open  rpcbind
113/tcp   open  ident
119/tcp   open  nntp
125/tcp   open  locus-map
135/tcp   open  msrpc
```

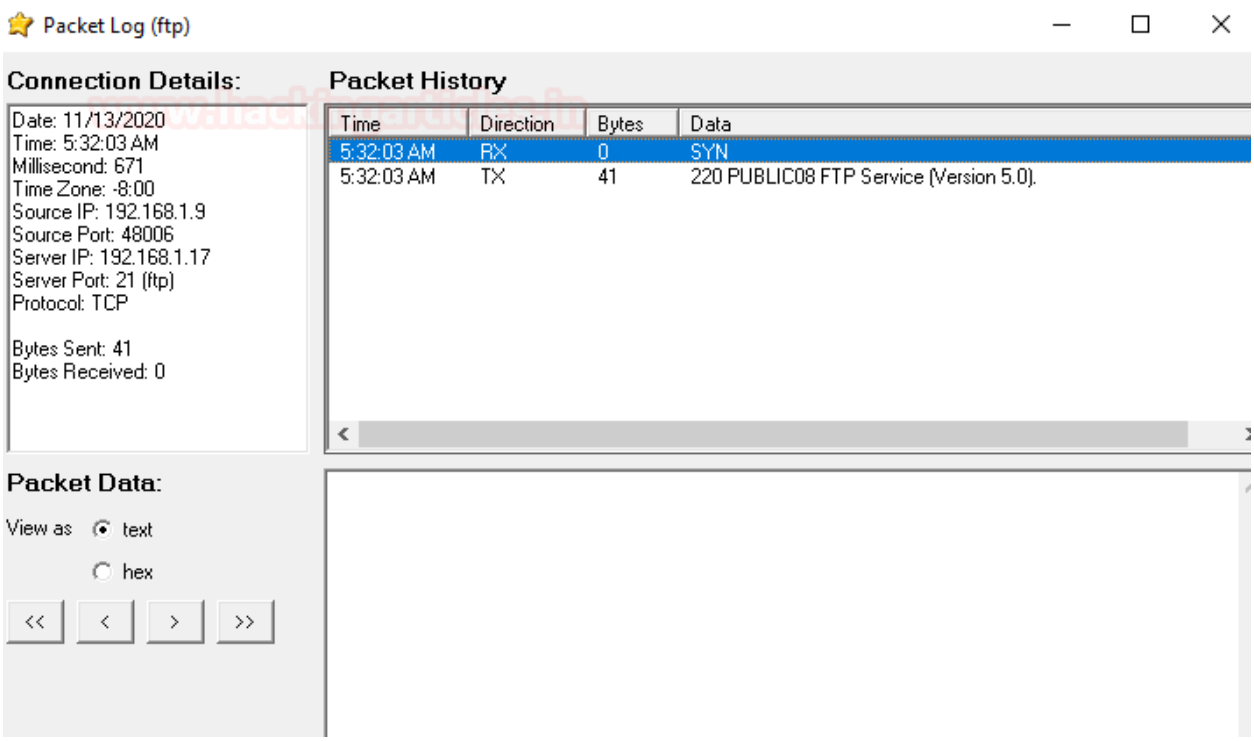
Let us try connecting via FTP from the attacker machine to the host machine.



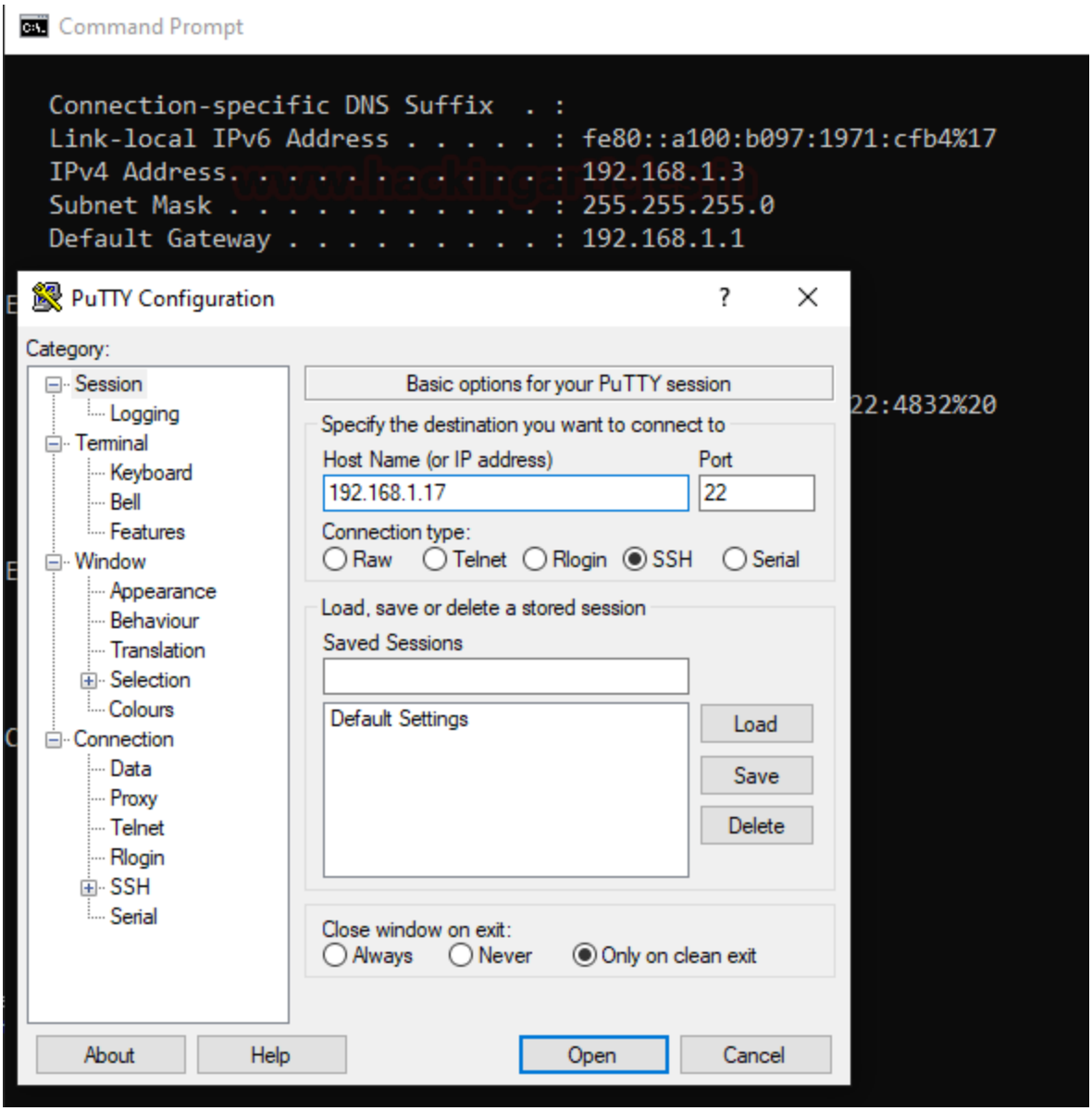
As you see, a log has been generated of the attacker's IP and the port that he was connected to.



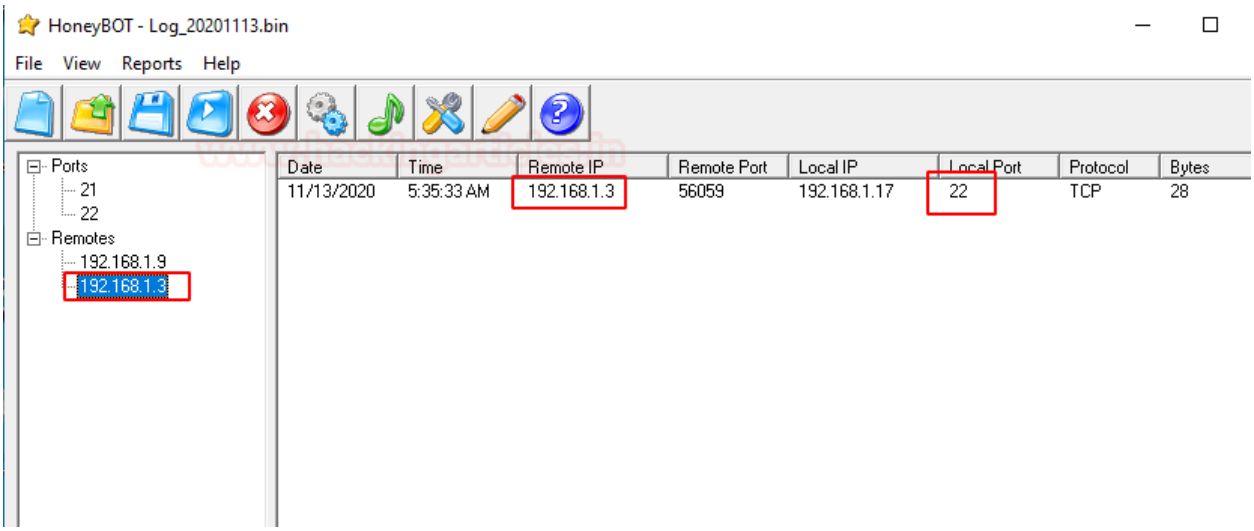
Here you can see a detailed report on the connection that was created by the attacker.



Similarly, an SSH connection was initiated on port 22 from another operating system.

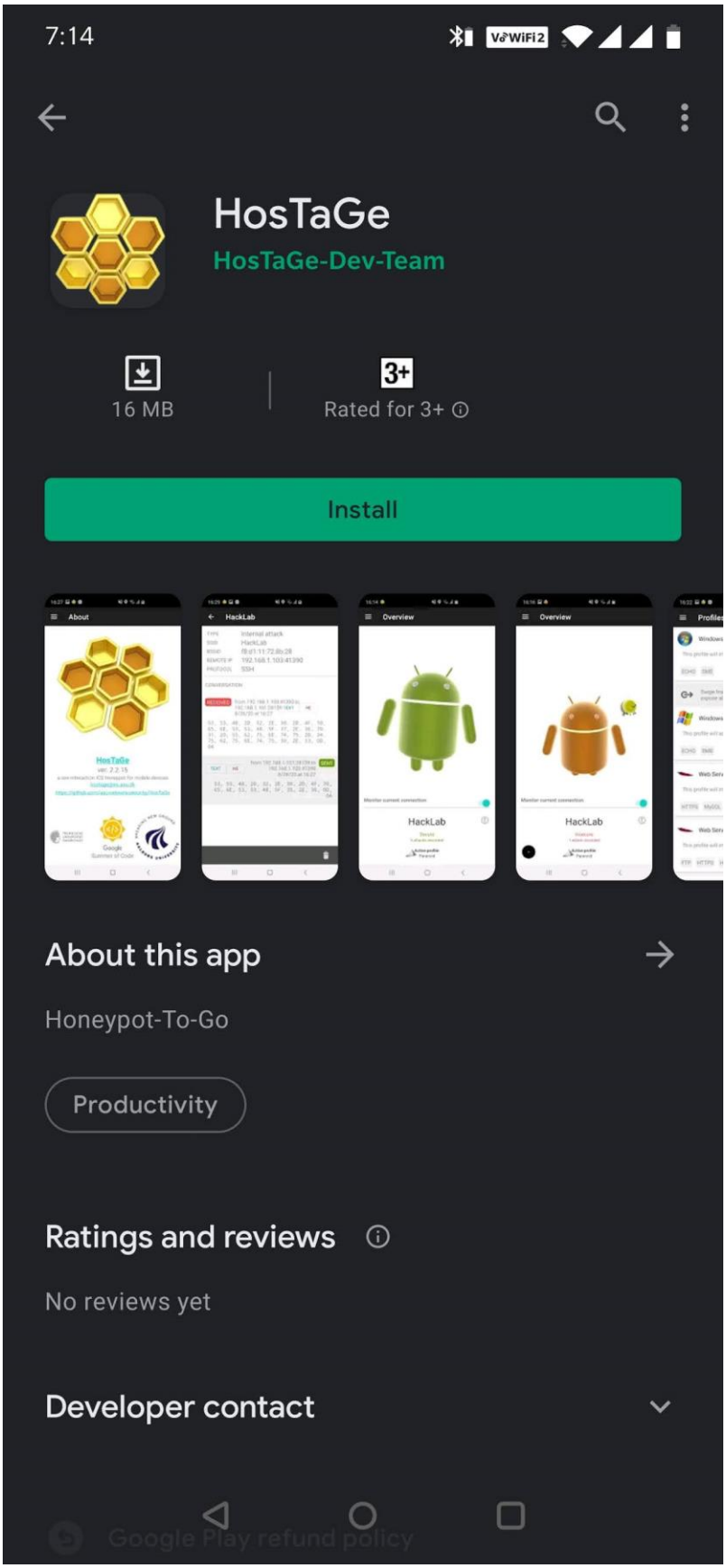


Now you can see that a log for the same has been generated for the connection created on port 22.

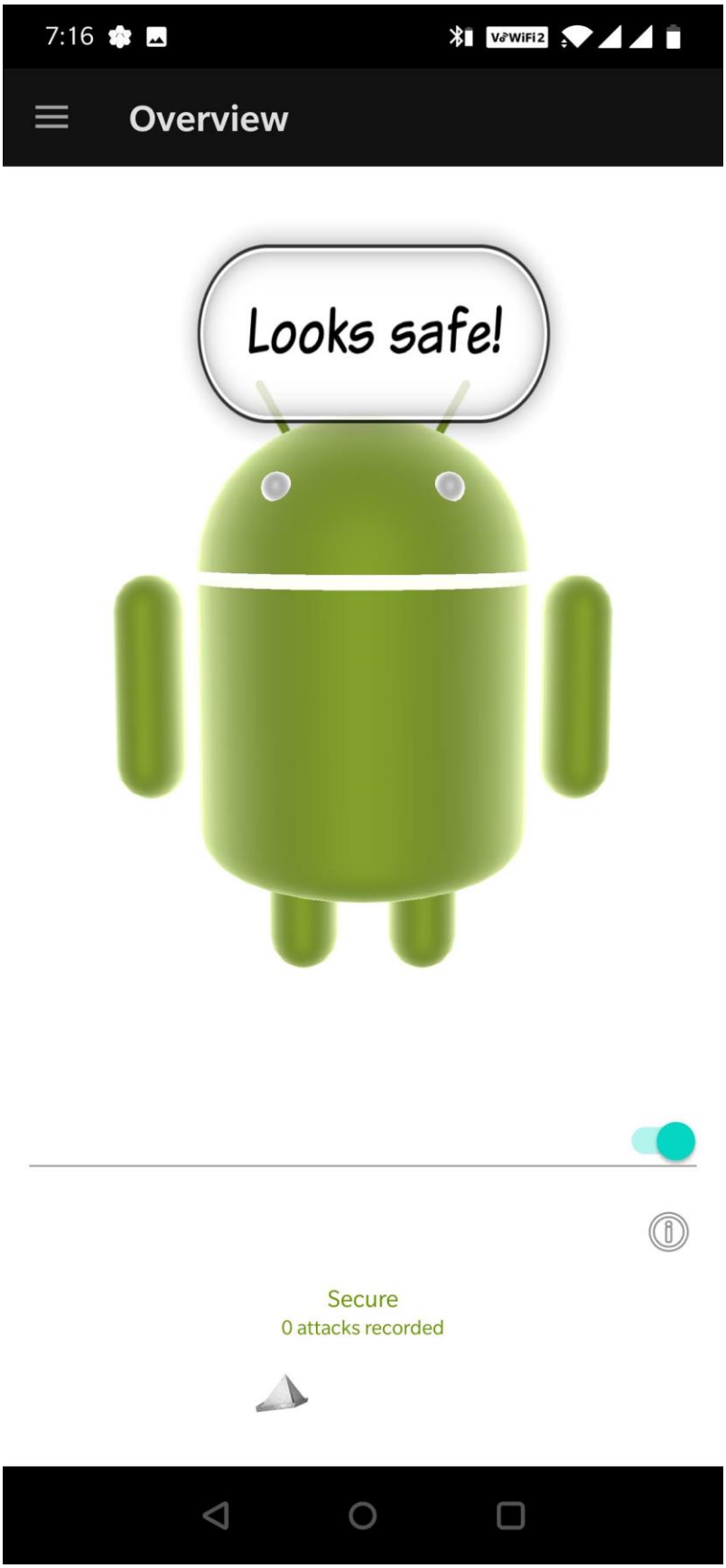


Android Honeypot

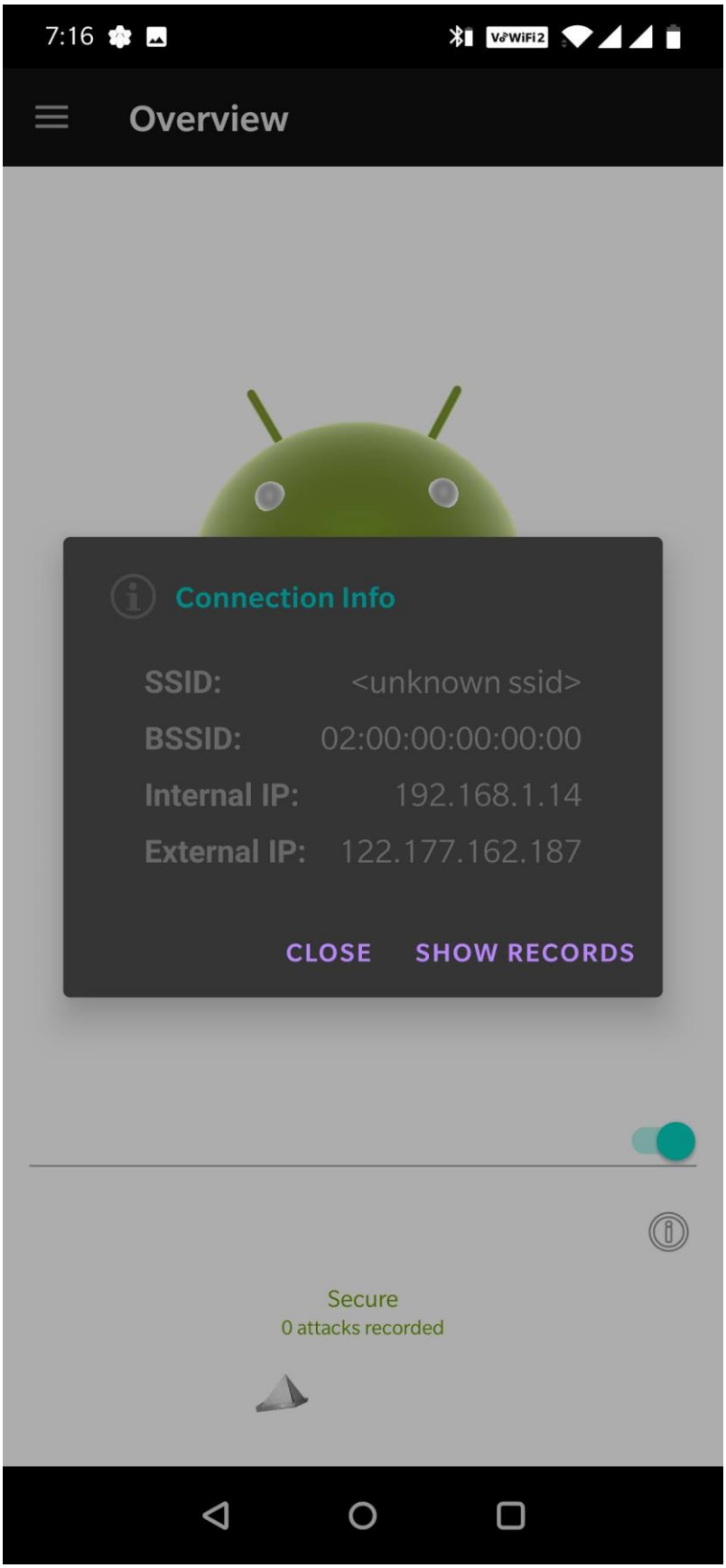
The honeypots can also be installed on Android phones using the Google Play store. Here we have downloaded the Hostage honeypot.


7:14
HosTaGe
HosTaGe-Dev-Team
16 MB
3+
Rated for 3+
Install
About this app
Honeypot-To-Go
Productivity
Ratings and reviews
No reviews yet
Developer contact
Google Play refund policy

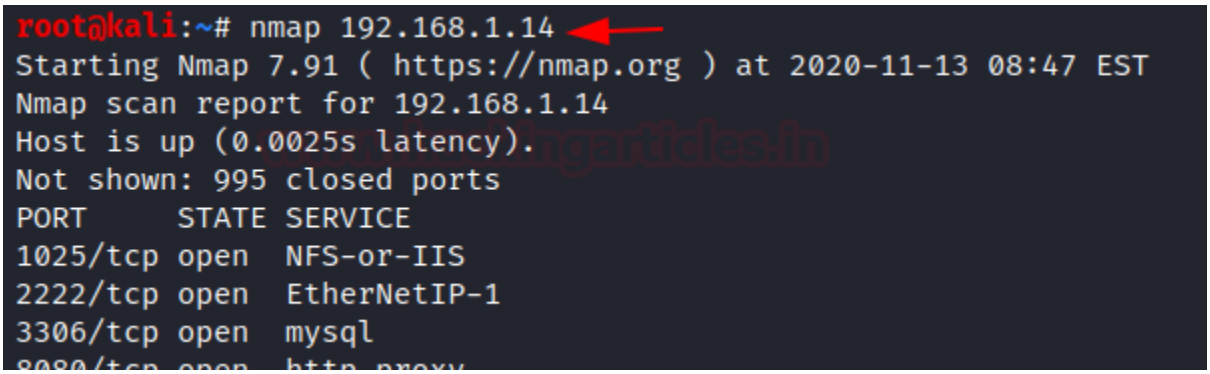
On switching on the application, it looks safe.


7:16
Overview
Looks safe!
Secure
0 attacks recorded

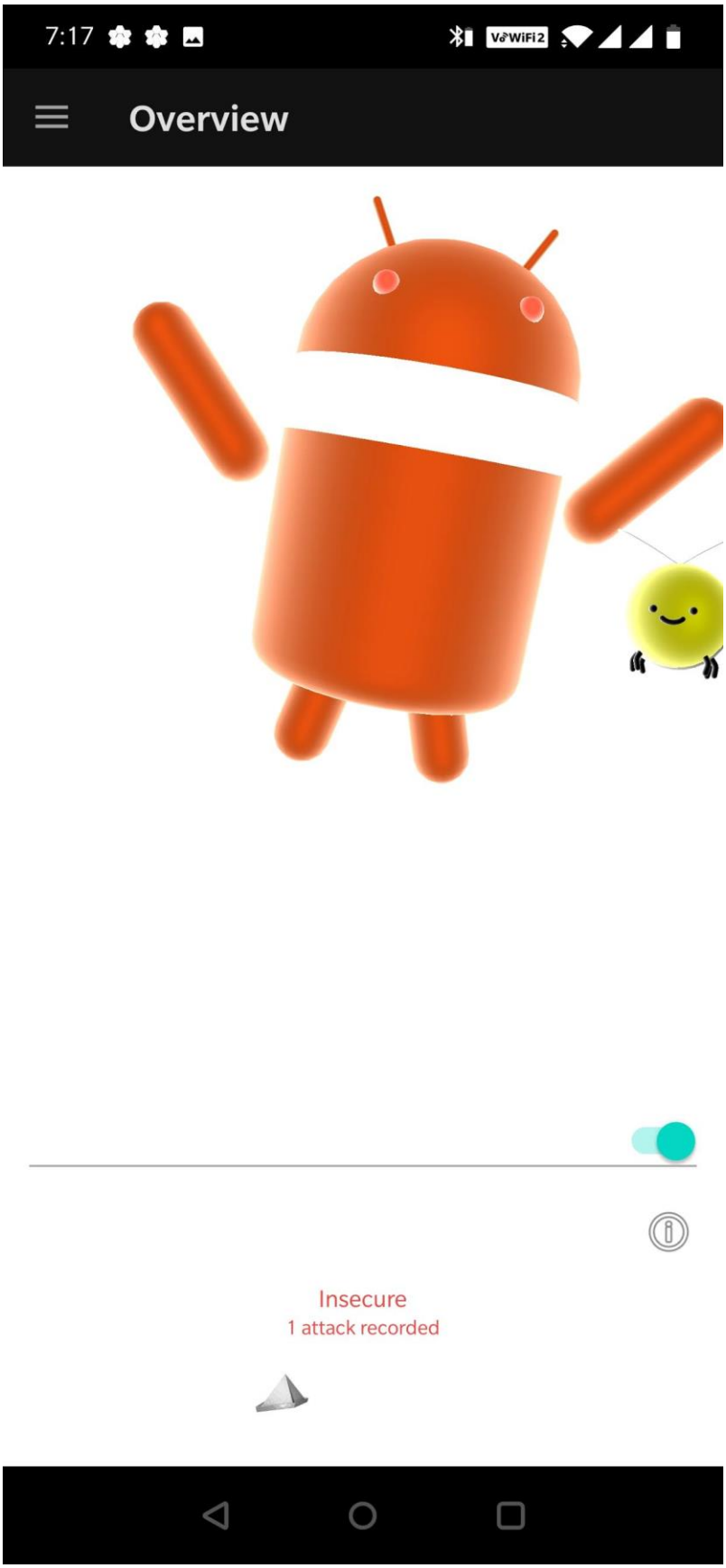
Now let us check the IP address of your android device and let’s proceed.


7:16
Overview
Connection Info
SSID: <unknown ssid>
BSSID: 02:00:00:00:00:00
Internal IP: 192.168.1.14
External IP: 122.177.162.187
CLOSE
SHOW RECORDS
Secure
0 attacks recorded

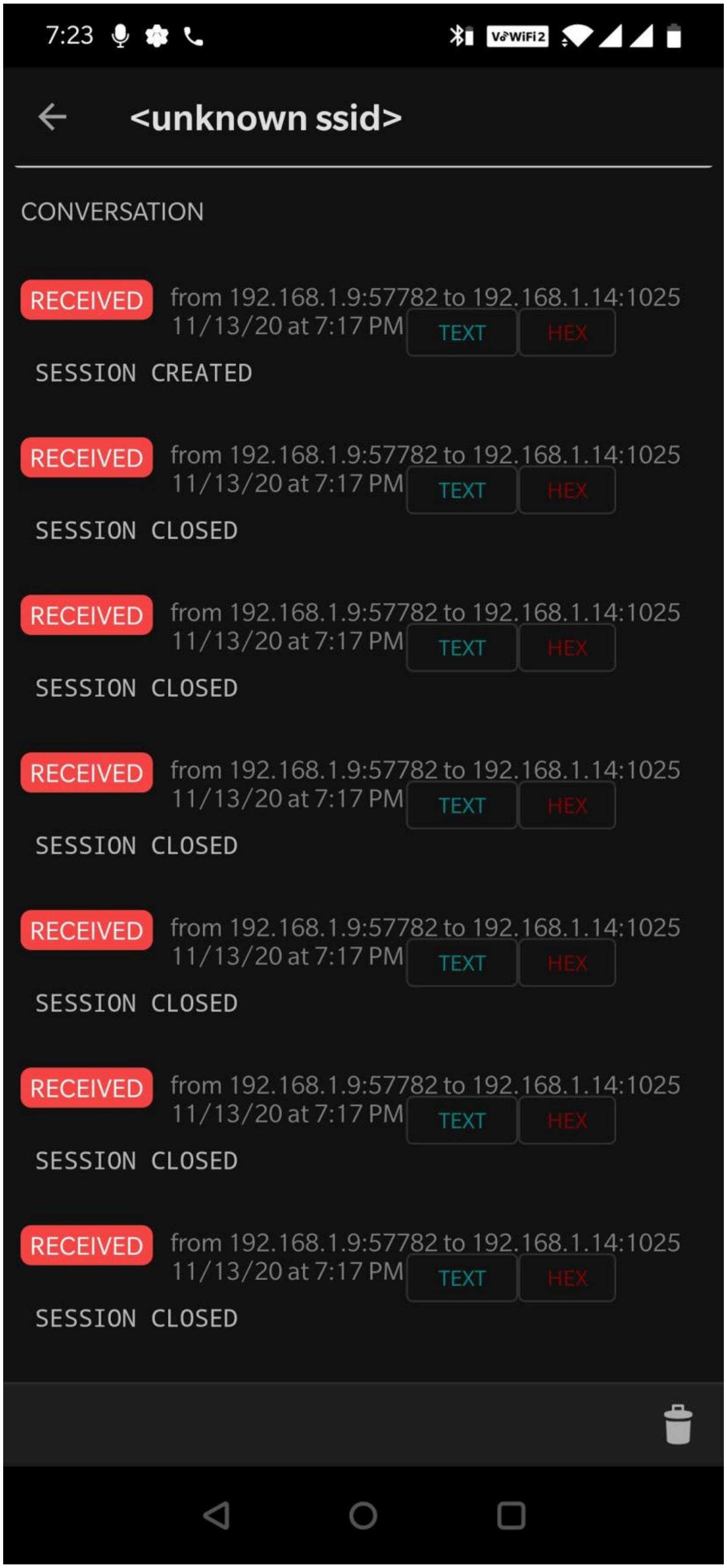
Let’s turn on the attacker's system and let’s conduct an nmap scan on the IP address of the android device.



An alert will be generated on the android device when the nmap scan is connected.


7:17
Overview
Insecure
1 attack recorded

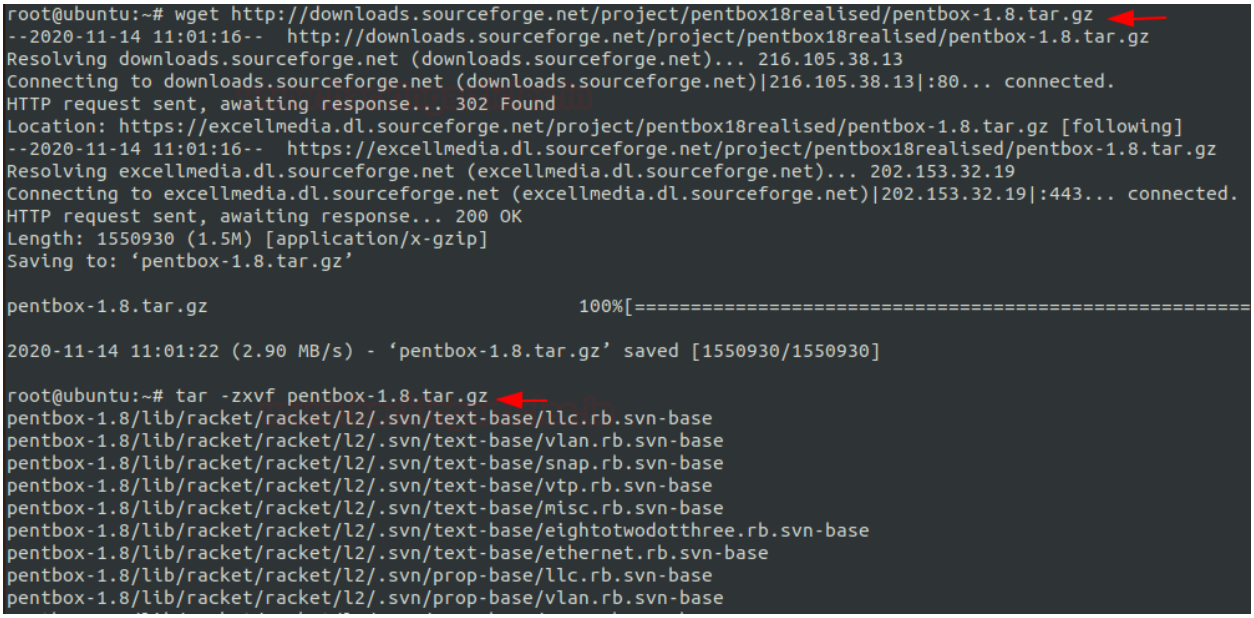
A log will be created and we will see the IP of the attacker system and the ports that were attacked.


7:23
<unknown ssid>
CONVERSATION
RECEIVED
from 192.168.1.9:57782 to 192.168.1.14:1025
11/13/20 at 7:17 PM
TEXT
HEX
SESSION CREATED
RECEIVED
from 192.168.1.9:57782 to 192.168.1.14:1025
11/13/20 at 7:17 PM
TEXT
HEX
SESSION CLOSED
RECEIVED
from 192.168.1.9:57782 to 192.168.1.14:1025
11/13/20 at 7:17 PM
TEXT
HEX
SESSION CLOSED
RECEIVED
from 192.168.1.9:57782 to 192.168.1.14:1025
11/13/20 at 7:17 PM
TEXT
HEX
SESSION CLOSED
RECEIVED
from 192.168.1.9:57782 to 192.168.1.14:1025
11/13/20 at 7:17 PM
TEXT
HEX
SESSION CLOSED
RECEIVED
from 192.168.1.9:57782 to 192.168.1.14:1025
11/13/20 at 7:17 PM
TEXT
HEX
SESSION CLOSED
RECEIVED
from 192.168.1.9:57782 to 192.168.1.14:1025
11/13/20 at 7:17 PM
TEXT
HEX
SESSION CLOSED

Linux Honeypot

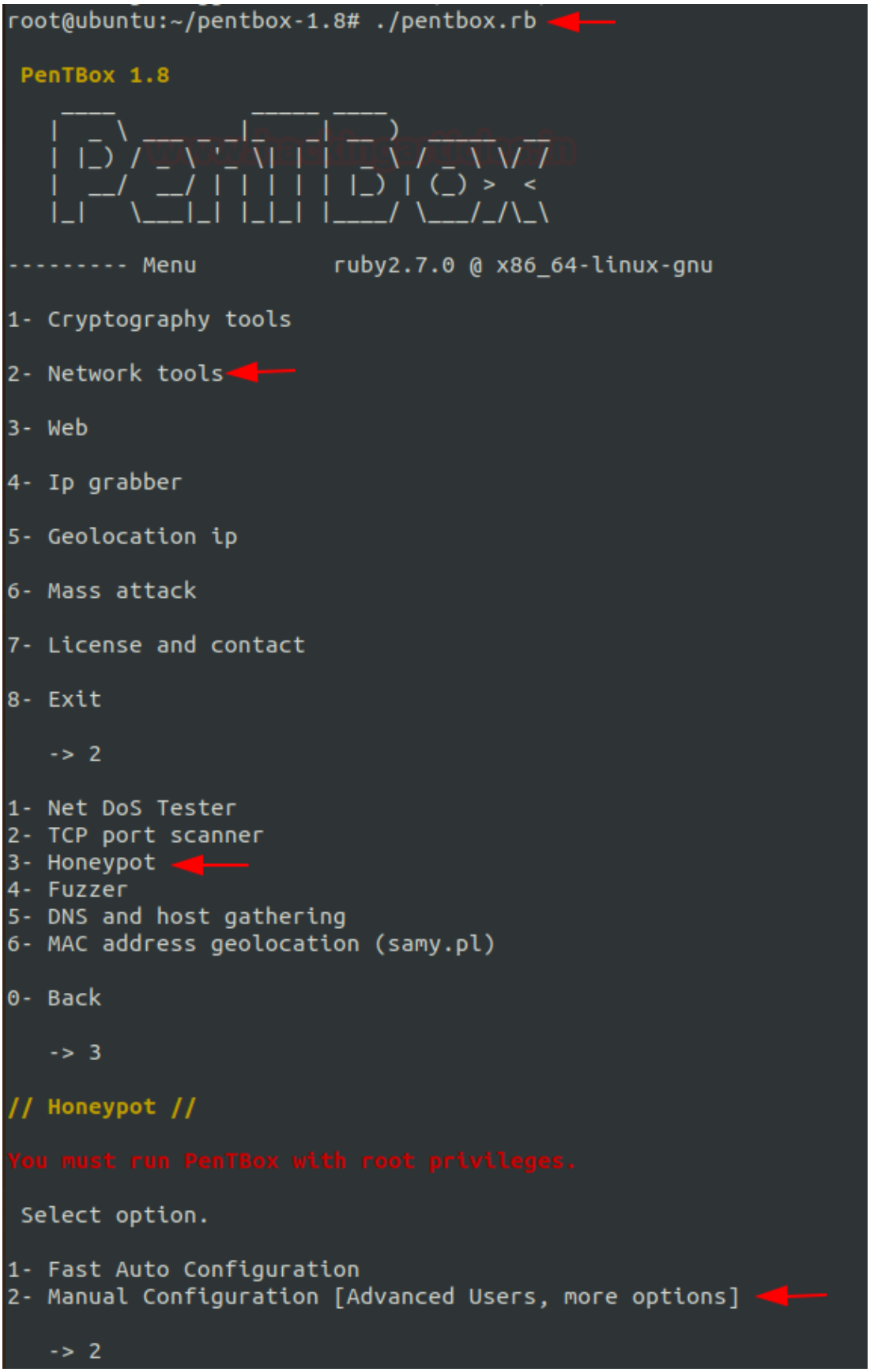
We can install a honeypot on a Linux machine as well. Here we have demonstrated using Pentox, which can be easily installed on Ubuntu.

wget http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz
tar -zxvf pentbox-1.8.tar.gz

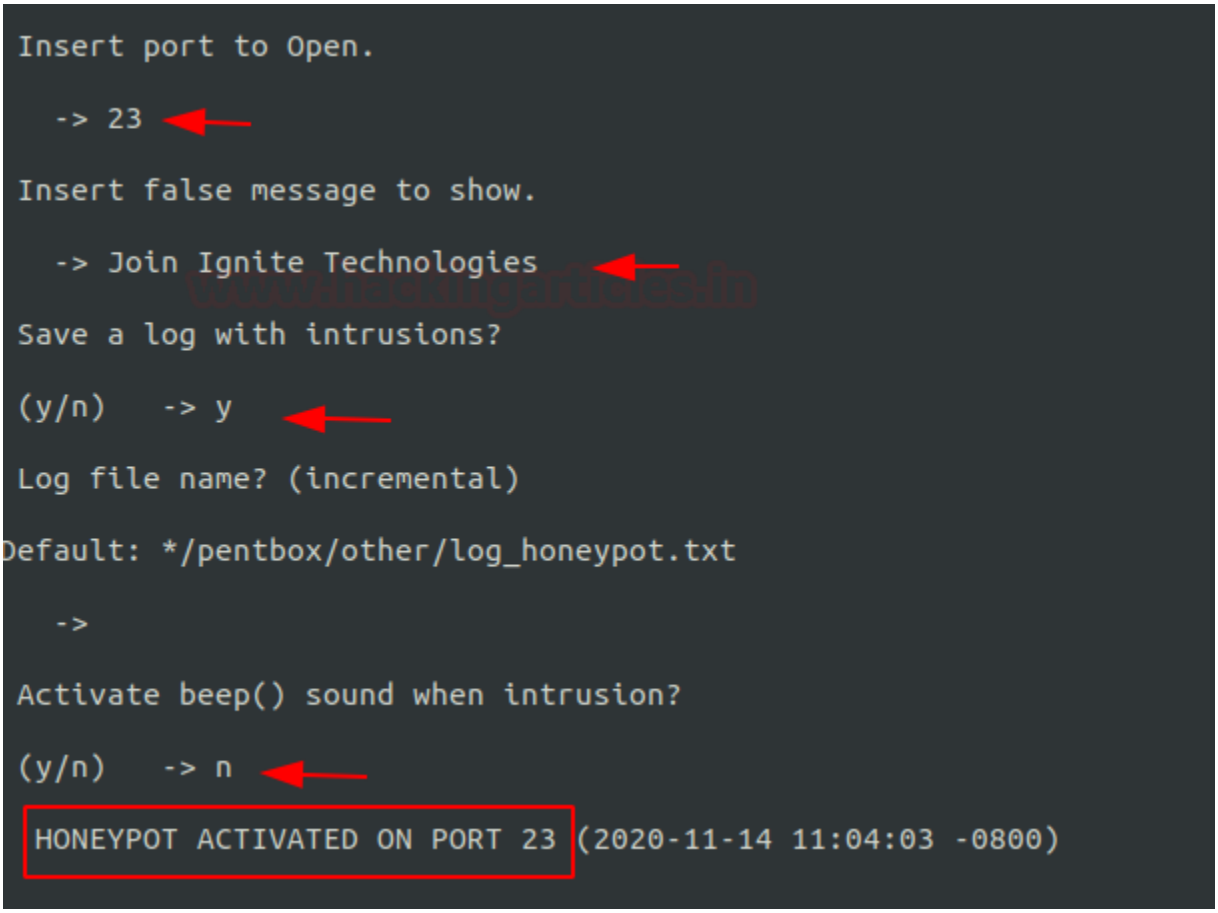


Once it is installed, let us start using the pentbox. Select the network tools and honeypot from the menu to install the honeypot. Go along with the manual configuration to install it according to your preferences for a honeypot.

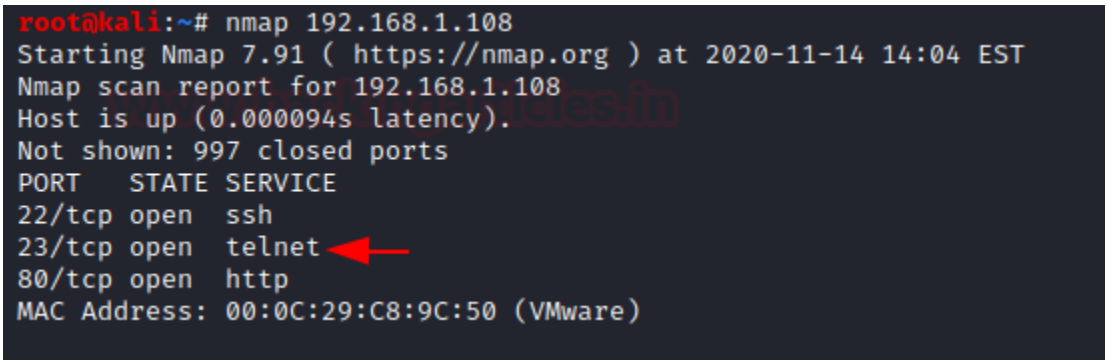
./pentbox.rb


root@ubuntu:~/pentbox-1.8# ./pentbox.rb
PenTBox 1.8
--------- Menu ruby2.7.0 @ 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
-> 2
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)
0- Back
-> 3
// Honeypot //
You must run PenTBox with root privileges.
Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
-> 2

Now you can open the fake port according to your preference and insert a fake message. You can also provide the option to save the log and save the name of the log. You can see that the honeypot is activated on the required port, and similarly, you can manually activate honeypots for other ports.



Turn on the attacker's machine, and scan the host machine using nmap. The results of the open ports and services are displayed below.



Here, the attacker machine is trying to connect with the host machine using telnet.

telnet 192.168.1.108

```
root@kali:~# telnet 192.168.1.108
Trying 192.168.1.108 ...
Connected to 192.168.1.108.
Escape character is '^]'.
Join Ignite TechnologiesConnection closed by foreign host.
root@kali:~#
```

For every attempt of intrusion that is made, it gets alerted and a log is created where the attacker's IP and port are recorded.

```
 INTRUSION ATTEMPT DETECTED! from 192.168.1.9:60492 (2020-11-14 11:04:30 -0800)
 ------------------------------
```

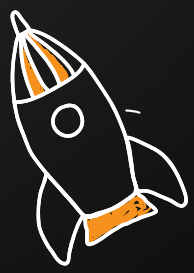
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

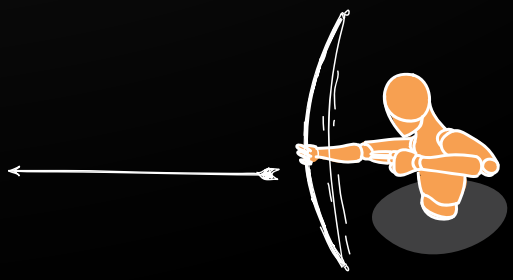
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux