



Honeypots

A Pentesting Guide

Original Author: *Jeenali Kothari*



Table of Contents

Abstract.....	3
What are honeypots?	4
Working of honeypots.....	4
Types of Honeypots.....	5
Windows Honeypot.....	7
Android Honeypot.....	13
Linux Honeypot.....	19
Conclusion	22
References	22



Abstract

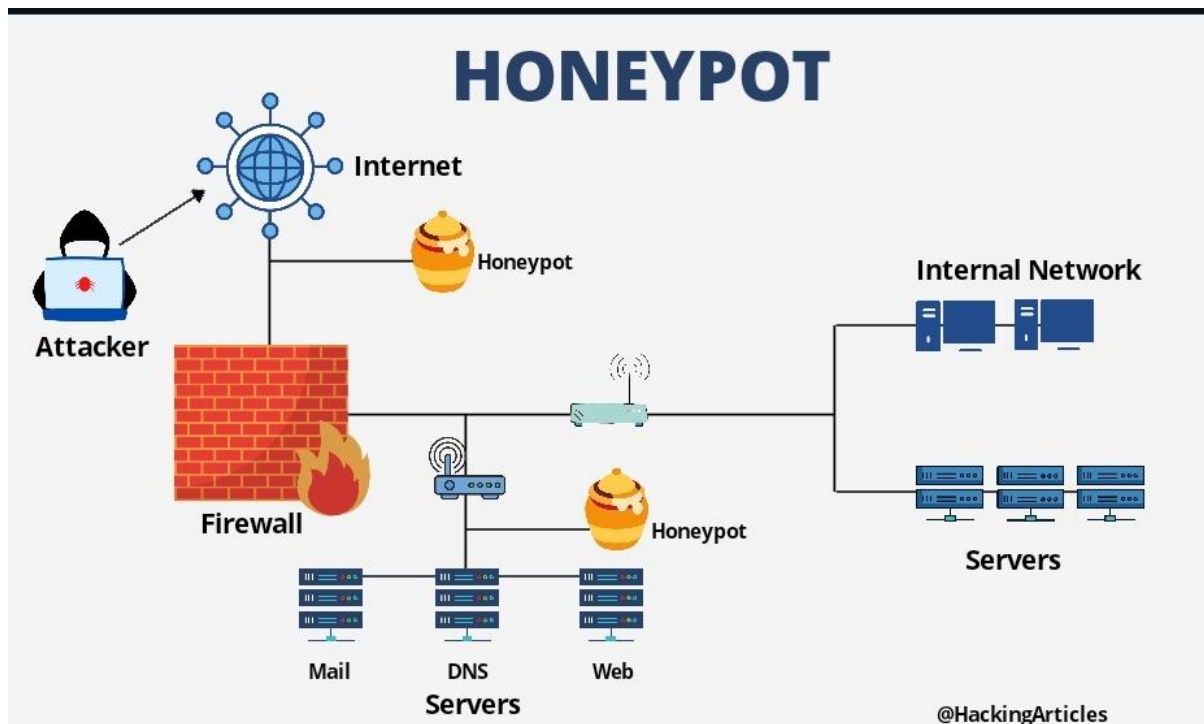
Honeypots are generally hardware or software that are deployed by the security departments of any organization to examine the threats that are possessed by the attackers. Honeypots usually act as baits for an organization to gather information on the attacker and alongside protect the real target system.

The aim of this report is to provide valuable insights on honeypots, including their configuration for various operating systems such as Windows, Linux, and Android, and to equip cybersecurity professionals with the tools to prevent illegal intrusions into organizational networks and systems.

Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.

What are honeypots?

Honeypots are a type of Internet security resource which is used to entice cybercriminals to deceive them when they try to intrude inside the network for any illegal use. These honeypots are generally set up to understand the activity of the attacker in the network so that the organization can come up with stronger prevention methods against these intrusions. The honeypots do not carry any valuable data as it is a fake proxy that helps in logging the network traffic.



Working of honeypots

In an organization 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 Honey pots

TYPES OF HONEYPOT

[Based on the design]

- Low-interaction Honey pots
- Medium-interaction Honey pots
- High-interaction Honey pots
- Pure Honey pots

@HackingArticles

Low-Interaction Honey pots: They match a very limited number of services and applications that are present in the network or on the system. This type of honeypot can be used to keep track on 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 Honey pots: They are based on imitating real-time operating systems, and has all its applications and its services as that of a target network. They tend to capture more information as their purpose is to stall the attacker so that the organization gets more time to respond to the threat appropriately. Examples of a few medium-interaction tools are **Cowrie, HoneyPy**, etc.

High-Interaction Honey pots: 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 **honeynet**.

Pure Honey pots: 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 organization will be alerted and hence any kind of attack can be prevented earlier.

TYPES OF HONEYPOT

[Based on the deployment]

- Research Honeypots
- Production Honeypots

@HackingArticles

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

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

Types of Honeypot

Based on their deception technology



Malware Honeypots



Database Honeypots



Spam Honeypots



Email Honeypots



Spider Honeypots



HoneyNet Honeypots

@HackingArticles



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 where can be used to understand the pattern of the attack.

Email Honeypots: These honeypots are hoax email address which is used to attract the 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 organization understand the pattern of the attacks performed.

Spider Honeypots: These honeypots are installed with the purpose to trap the various web crawlers and spiders which tend to steal important information from the web applications.

Spam Honeypots: These honeypots consist of hoax email servers to attract the 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 the 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 windows, Android and Linux environment.

Windows Honeypot

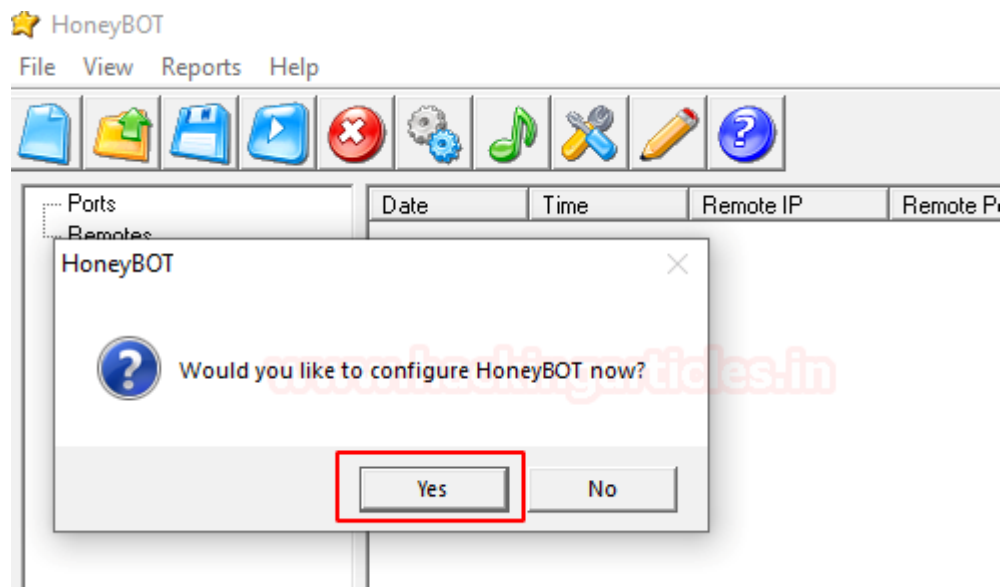
Today we will be looking at the famous honeypot software called HoneyBOT. which can be downloaded from the link provided in the references. Switch on your kali Linux as the attacker machine and the windows system as your host machine.

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

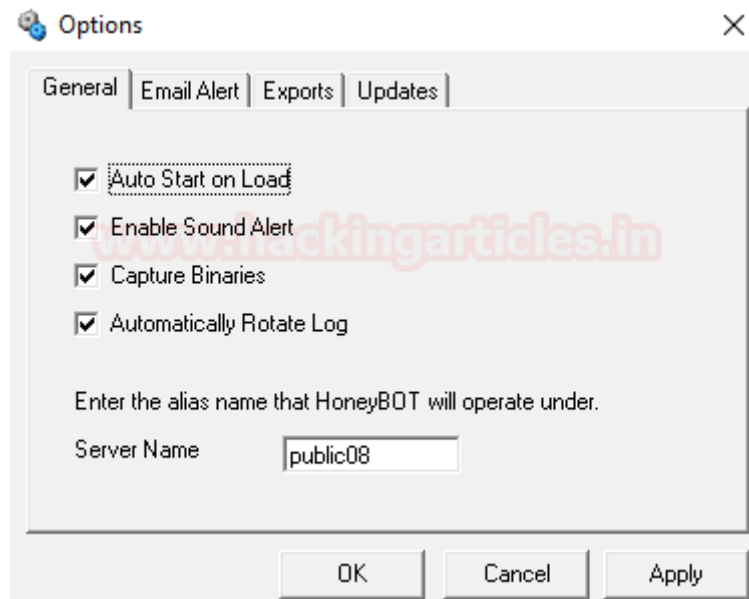
```
nmap -sV 192.168.1.17
```

```
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
```

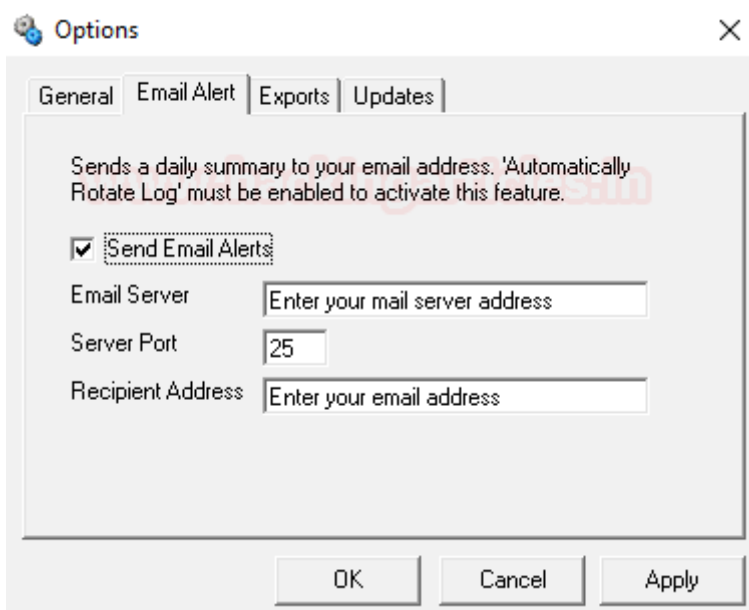
Now in your Windows system install the HoneyBOT software and configure it, click on yes to proceed.



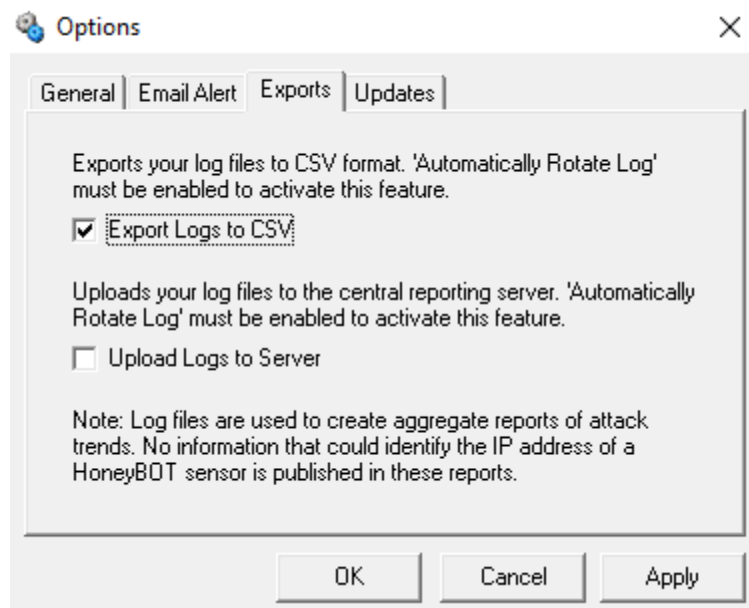
Check all the parameters that you want in your honeypot and click on Apply to proceed.



To get email reports on your honeypot, add the recipient email address and click on apply.



If you want to save the honeypot logs into CSV format, you can apply this setting.



On the attacker, machine performs a nmap scan and there you will see so many fake services that are open due to the presence of 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 to FTP from the attacker machine to the host machine.

```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:feb2:bb77 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b2:bb:77 txqueuelen 1000 (Ethernet)
    RX packets 393975 bytes 166703285 (158.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 310026 bytes 56476199 (53.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ftp 192.168.1.17
Connected to 192.168.1.17.
220 PUBLIC08 FTP Service (Version 5.0).
Name (192.168.1.17:root):

```

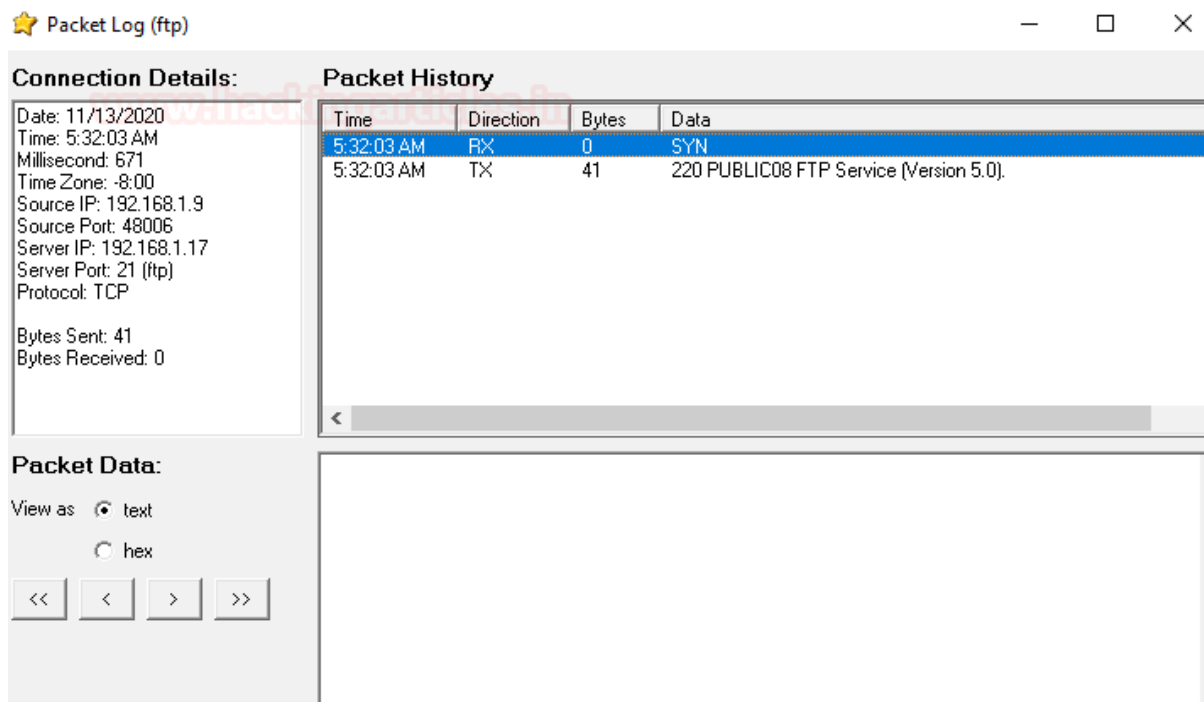
Where you see the log has been generated of the attacker's IP and the port that he was connected on.

★ HoneyBOT - Log_20201113.bin

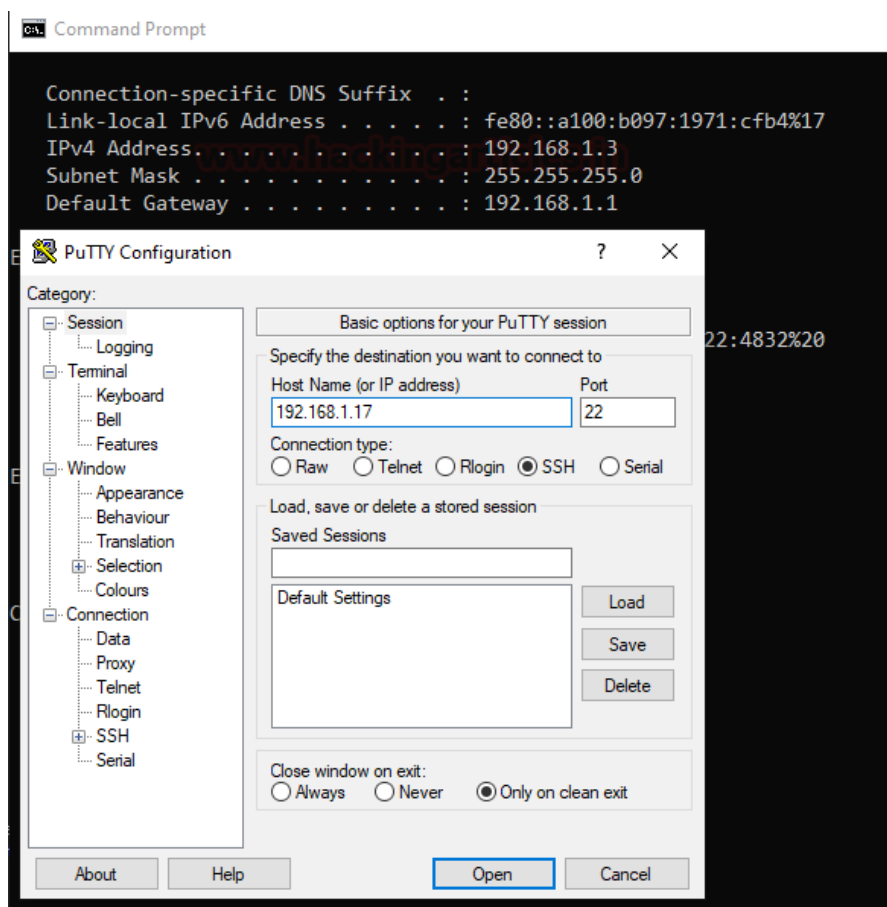
File View Reports Help

	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
Ports	11/13/2020	5:31:10 AM	192.168.1.9	48000	192.168.1.17	21	TCP	41
Remotes	11/13/2020	5:32:03 AM	192.168.1.9	48006	192.168.1.17	21	TCP	41

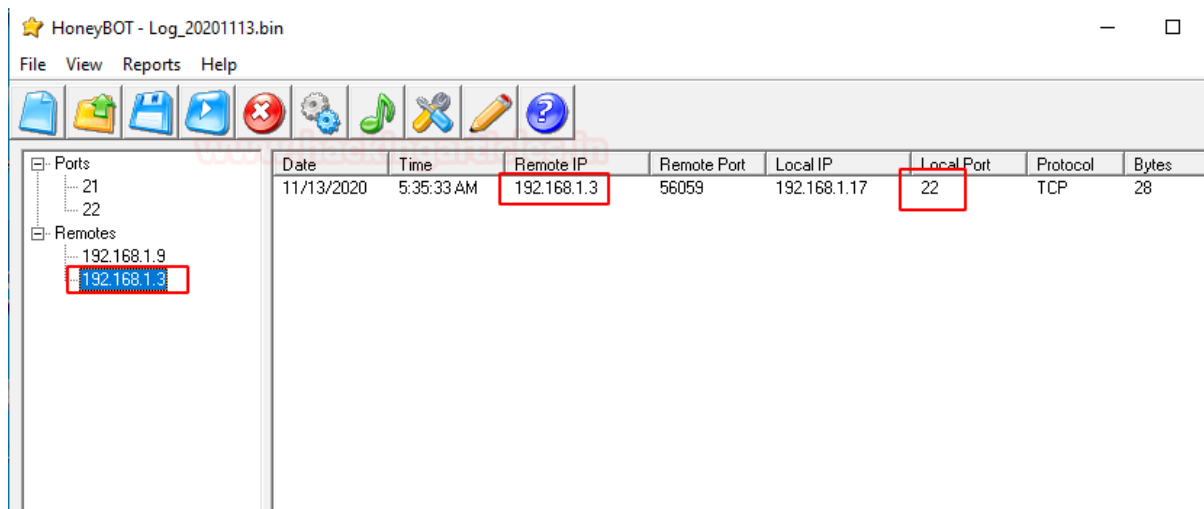
Here you can see a detailed report on the connection that is created by the attacker.



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

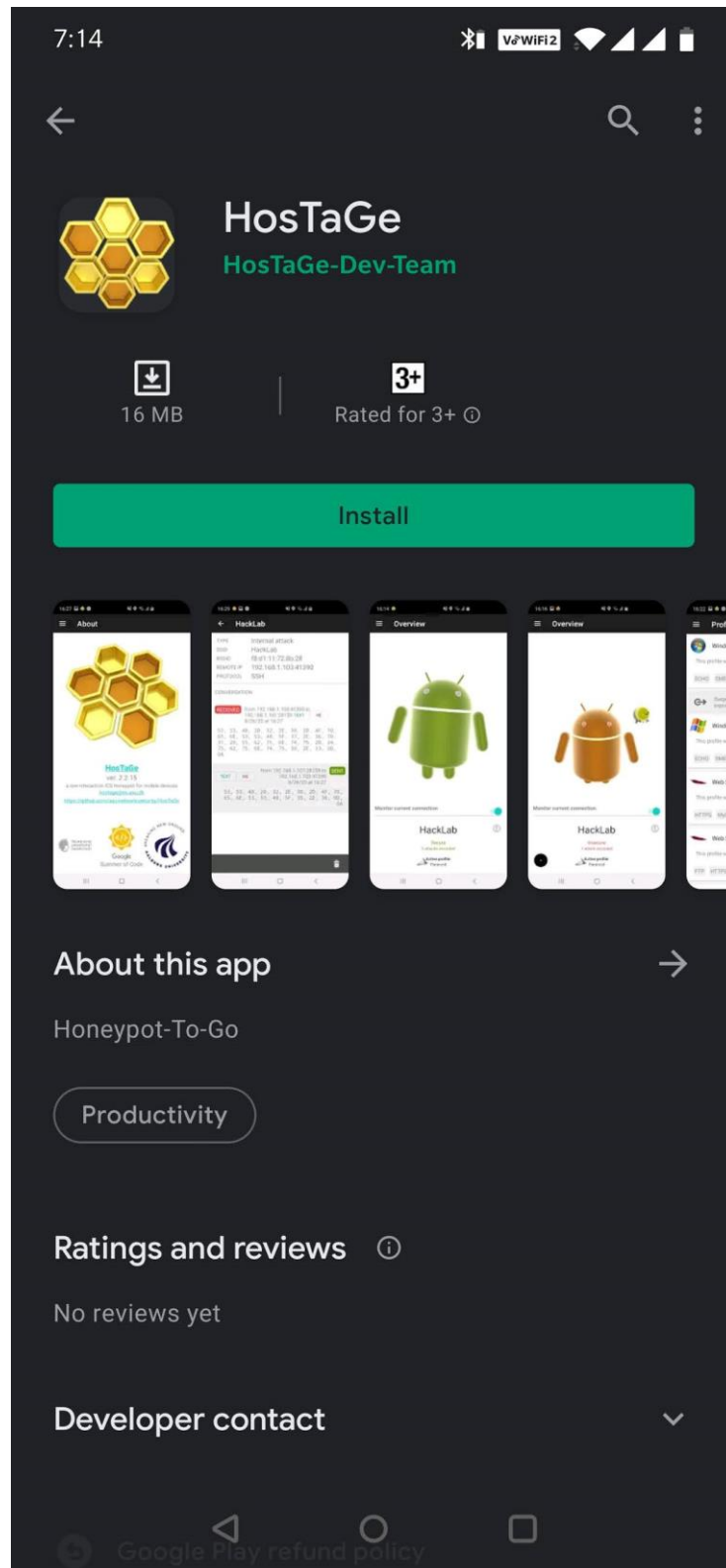


Now you can see that log for the same has been generated for the connection created on port 22.

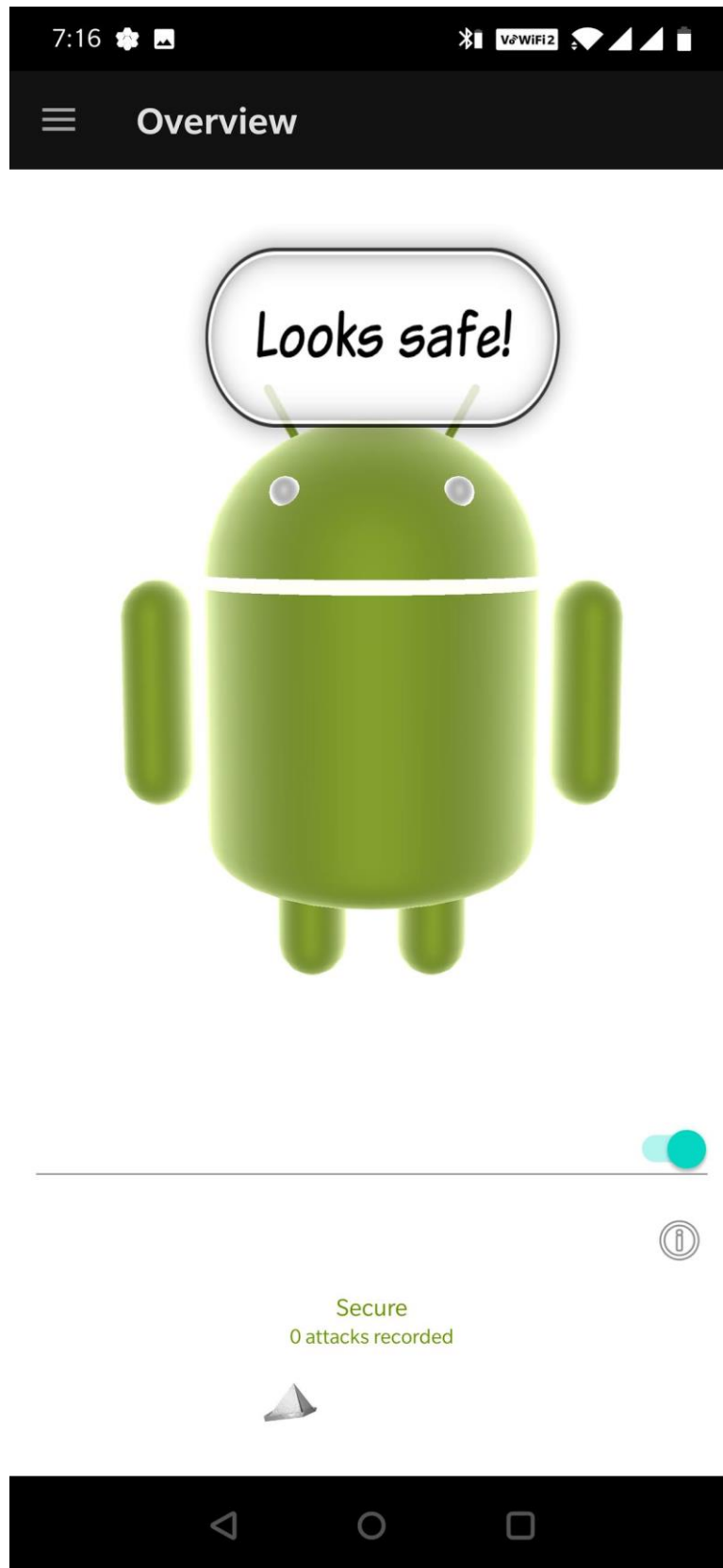


Android Honeypot

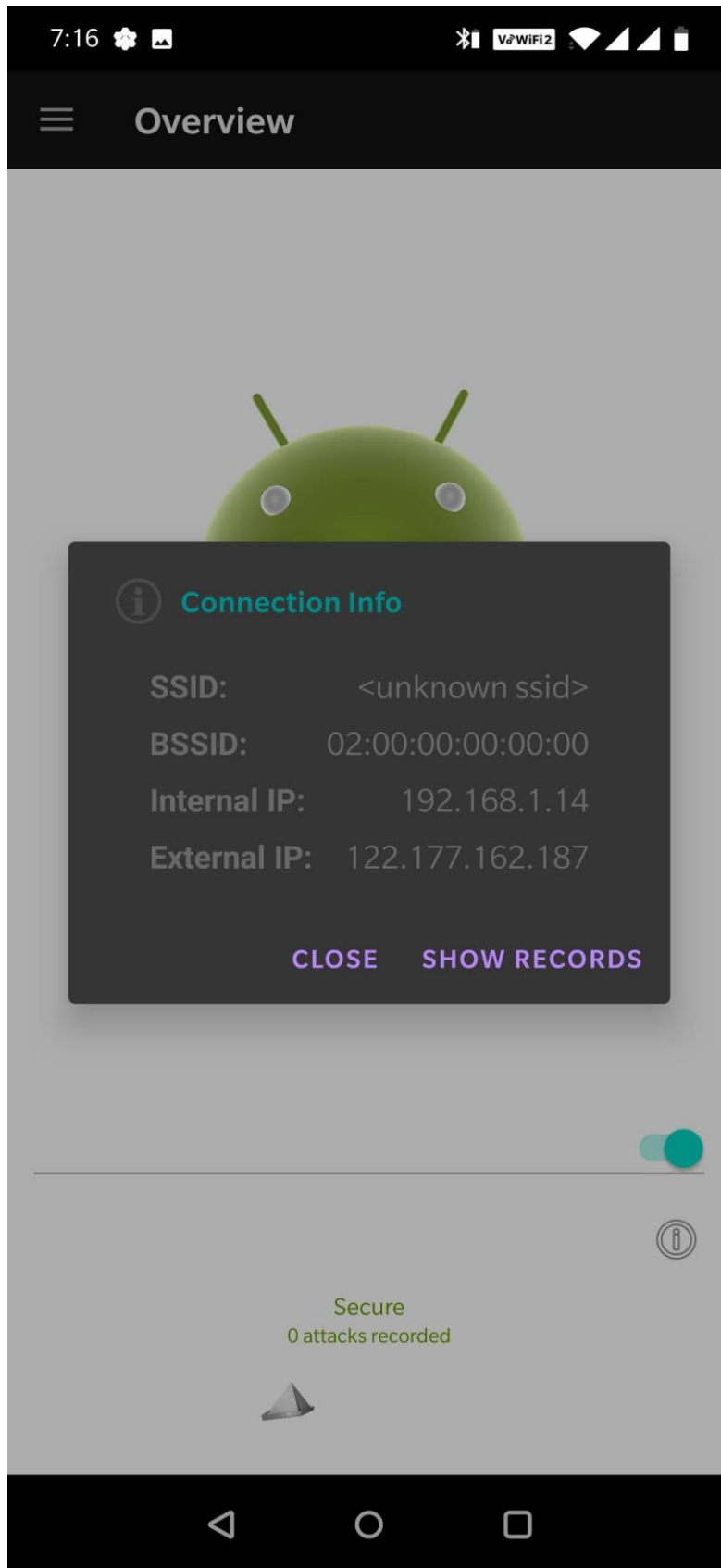
The honeypots can also be installed in android phones using the google play store. Here we have downloaded Hostage honeypot.



On switching on the application, it looks safe.



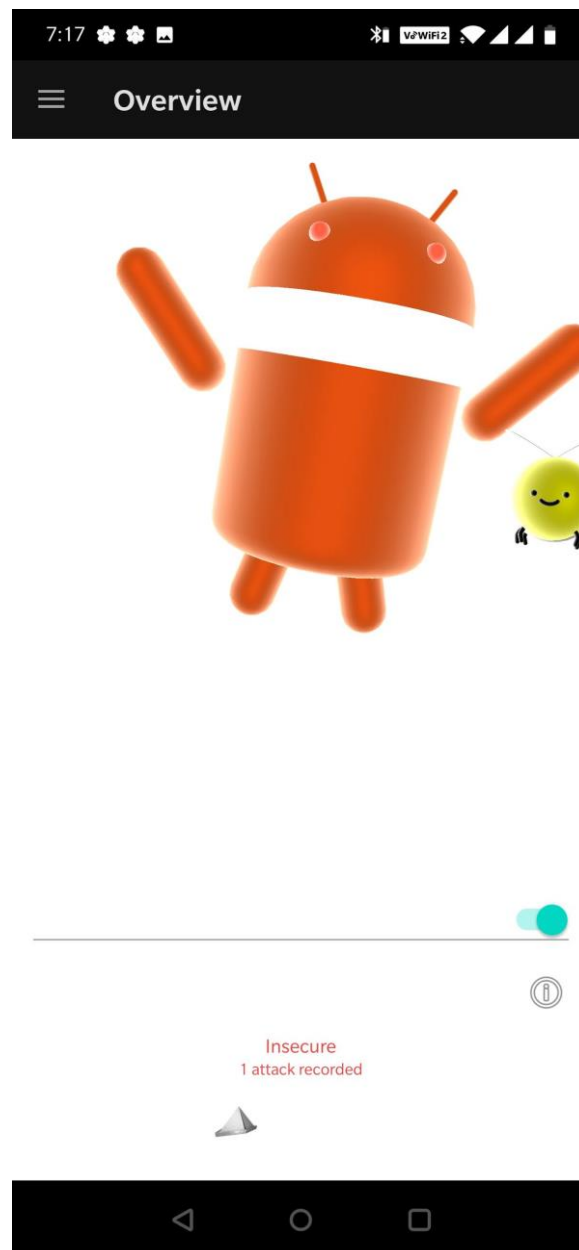
Now let us check the IP address of your android device and let's proceed.



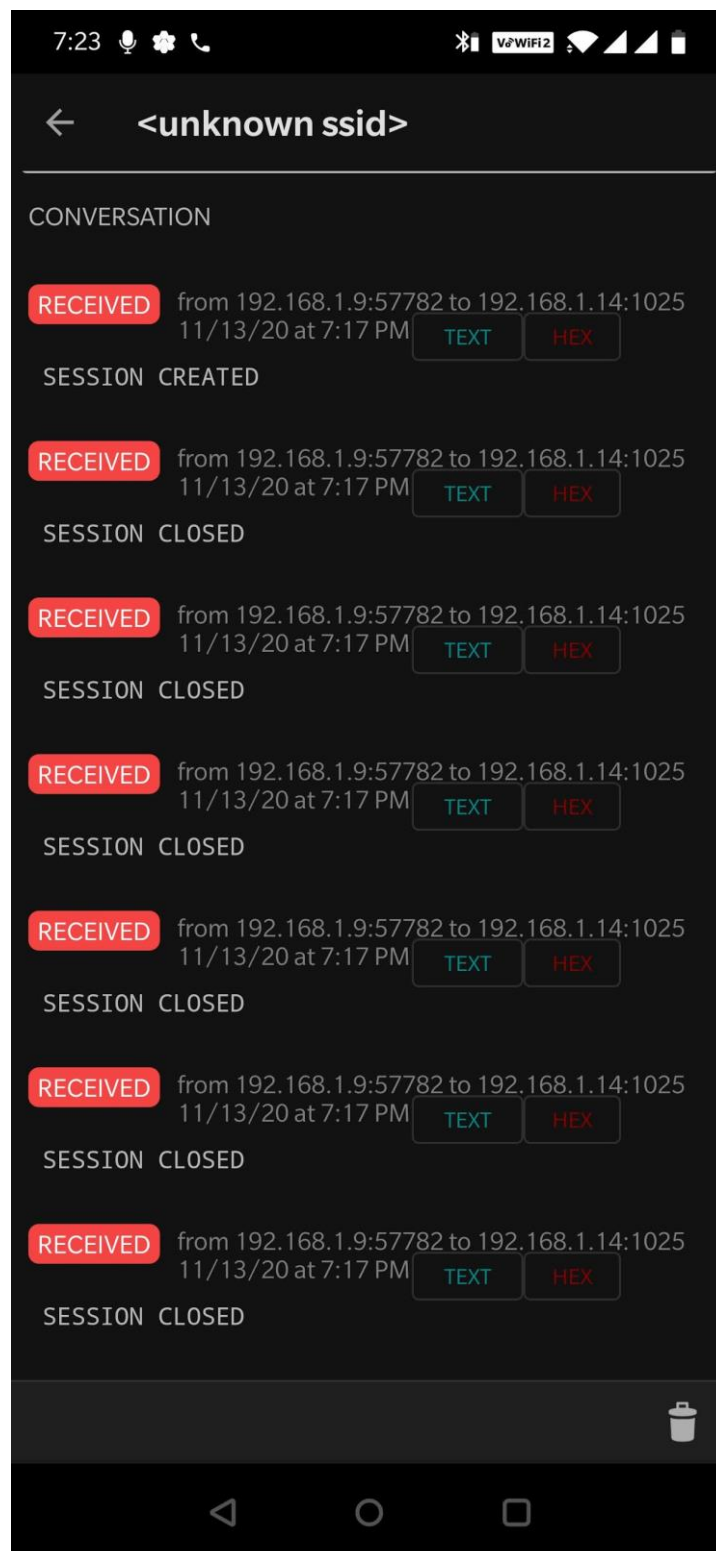
Let's turn on the attacker system and let's conduct a nmap scan on the IP address of the android device.


```
root@kali:~# nmap 192.168.1.14
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-13 08:47 EST
Nmap scan report for 192.168.1.14
Host is up (0.0025s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
1025/tcp   open  NFS-or-IIS
2222/tcp   open  EtherNetIP-1
3306/tcp   open  mysql
8080/tcp   open  http-proxy
```

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



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



Linux Honeypot

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

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

```
tar -zxvf pentbox-1.8.tar.gz
```

```
root@ubuntu:~# wget http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz
--2020-11-14 11:01:16-- http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 216.105.38.13
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)|216.105.38.13|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://excellmedia.dl.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz [following]
--2020-11-14 11:01:16-- https://excellmedia.dl.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz
Resolving excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)... 202.153.32.19
Connecting to excellmedia.dl.sourceforge.net (excellmedia.dl.sourceforge.net)|202.153.32.19|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1550930 (1.5M) [application/x-gzip]
Saving to: 'pentbox-1.8.tar.gz'

pentbox-1.8.tar.gz                               100%[=====]
2020-11-14 11:01:22 (2.90 MB/s) - 'pentbox-1.8.tar.gz' saved [1550930/1550930]

root@ubuntu:~# tar -zxvf pentbox-1.8.tar.gz
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/llc.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/vlan.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/snap.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/vtp.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/misc.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/eighttotwodotthree.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/ethernet.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/llc.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/vlan.rb.svn-base
```

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

```
./pentbox.rb
```

-> 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.

```
Insert port to Open.  
-> 23  
Insert false message to show.  
-> Join Ignite Technologies  
Save a log with intrusions?  
(y/n) -> y  
Log file name? (incremental)  
Default: */pentbox/other/log_honeypot.txt  
->  
Activate beep() sound when intrusion?  
(y/n) -> n  
HONEYPOT ACTIVATED ON PORT 23 (2020-11-14 11:04:03 -0800)
```

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

```
root@kali:~# nmap 192.168.1.108  
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-14 14:04 EST  
Nmap scan report for 192.168.1.108  
Host is up (0.000094s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
23/tcp    open  telnet  
80/tcp    open  http  
MAC Address: 00:0C:29:C8:9C:50 (VMware)
```

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

```
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 was made, it gets alerted and a log is created where the attacker IP and port is recorded.

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

Conclusion

Hence, one can make use of these commands as a cybersecurity professional to assess vulnerabilities on systems and keep these systems away from threat.

References

- <https://www.hackingarticles.in/comprehensive-guide-on-honeypots/>
- <https://honeybot.software.informer.com/>
- <https://sourceforge.net/projects/pentbox18realised/files/>