



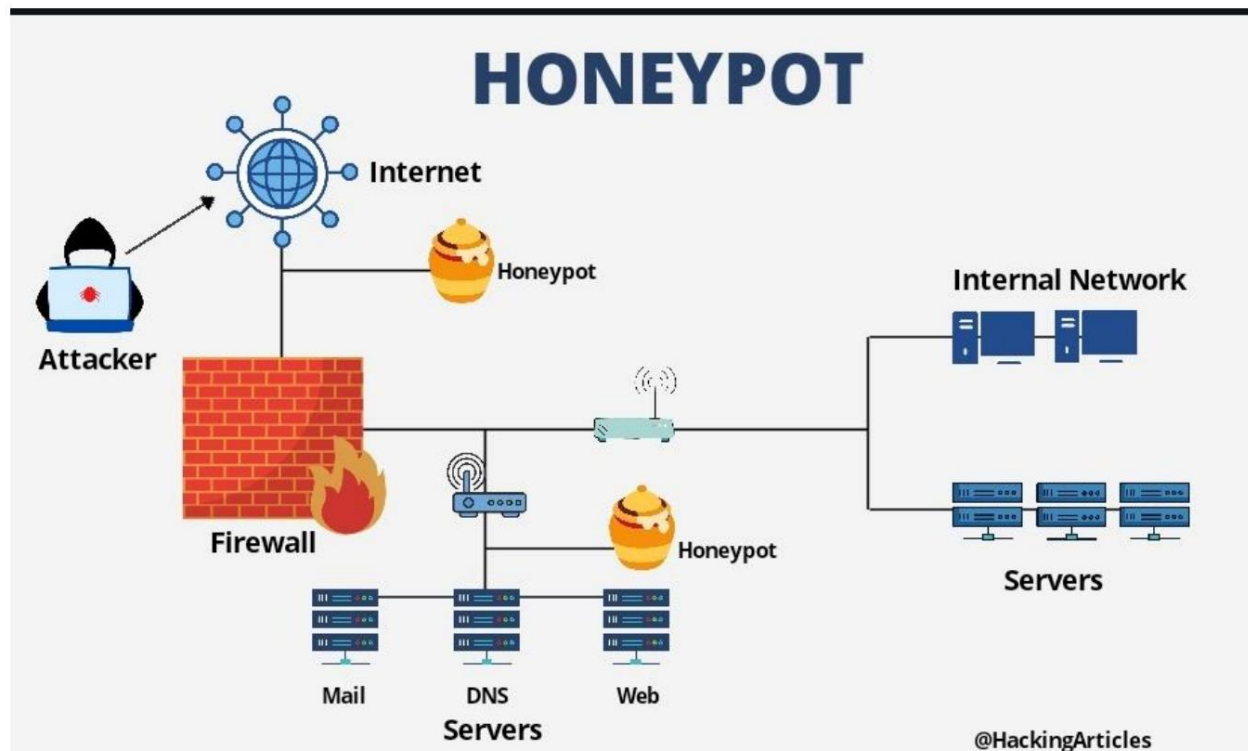
A DETAILED GUIDE ON HONEYPOTS

Contenido

Introducción.....	3
¿Qué son los honeypots?.....	3
Funcionamiento de los honeypots.....	3
Tipos de Honeypots.....	4
Sistema Windows.....	7
Honeypot de Android	14
Honeypot de Linux.....	24

Introducción

Los Honeypots son generalmente hardware o software que implementan los departamentos de seguridad de cualquier organización para examinar las amenazas que poseen los atacantes. Los Honeypots suelen actuar como cebo para que una organización recopile información sobre el atacante y, al mismo tiempo, proteja el sistema objetivo real.



¿Qué son los honeypots?

Los Honeypots son un tipo de recurso de seguridad de Internet que se utiliza para atraer a los ciberdelincuentes y engañarlos cuando intentan invadir la red para cualquier uso ilegal. Estos honeypots generalmente se configuran para comprender las actividades del atacante en la red, de modo que la organización pueda idear métodos de prevención más sólidos contra estas intrusiones. Los honeypots no contienen datos valiosos, ya que son servidores proxy falsos que ayudan a registrar el tráfico de la red.

Trabajo de honeypots

Como administrador de TI, usted querrá configurar un sistema honeypot que pueda parecer un sistema genuino para el mundo exterior. El tipo de datos que generalmente capturan los honeypots:

- Pulsaciones de teclas ingresadas y escritas por el atacante.
- La dirección IP del atacante.
- Los nombres de usuario y los diferentes privilegios utilizados por los atacantes.
- El tipo de datos a los que el atacante había accedido, eliminado o que fueron alterados.

Tipos de Honeypots

TYPES OF HONEYPOT

[Based on the design]

- Low-interaction Honeypots
- Medium-interaction Honeypots
- High-interaction Honeypots
- Pure Honeypots

@HackingArticles

Honeypots de baja interacción:

Corresponden a un número muy limitado de servicios y aplicaciones presentes en la red o en el sistema. Este tipo de honeypot se puede utilizar para realizar un seguimiento de los puertos y servicios UDP, TCP e ICMP.

Aquí utilizamos bases de datos, datos, archivos, etc. falsos como cebo para atrapar a los atacantes y comprender los ataques que ocurrirían en tiempo real. Ejemplos de algunas herramientas de baja interacción son Honeytrap, Spectre, KFSensor, etc.

Honeypots de interacción media:

Se basan en imitar sistemas operativos en tiempo real y cuentan con todas las aplicaciones y servicios de una red objetivo.

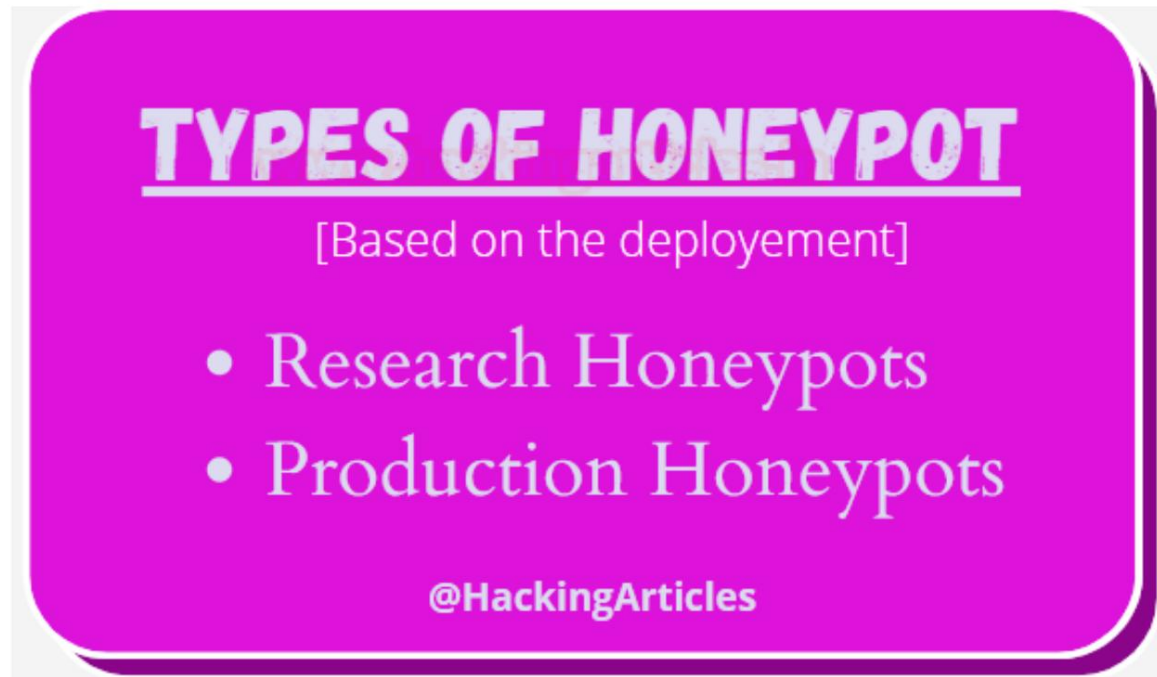
Suelen capturar más información ya que su propósito es detener al atacante para que la organización tenga más tiempo para responder adecuadamente a la amenaza. Ejemplos de algunas herramientas de interacción media son Cowrie, HoneyPy, etc.

Honeypots de alta interacción:

Se trata de software vulnerable genuino que se ejecuta en un sistema operativo real con varias aplicaciones que normalmente tendría un sistema de producción. La información recopilada mediante estos honeypots es más ingeniosa, pero es difícil de mantener. Un ejemplo de herramienta de alta interacción es la red miel.

Puros Honeypots:

Estos honeypots suelen imitar el entorno de producción real de una organización, lo que hace que un atacante asuma que es genuino e invierta más tiempo en explotarlo. Una vez que el atacante intenta encontrar las vulnerabilidades, se alertará a la organización y, por lo tanto, se podrá prevenir cualquier tipo de ataque antes.



Honeypots de producción:

Estos honeypots suelen instalarse en la propia red de producción de la organización. También ayudan a encontrar vulnerabilidades o ataques internos, ya que están presentes internamente en la red.

Honeypots de investigación:

Son honeypots de alta interacción, pero están configurados con un enfoque de investigación en áreas de diversas organizaciones gubernamentales o militares para obtener más conocimiento sobre el comportamiento de los atacantes.

Types of Honeypot

Based on their deception technology



Malware Honeypots



Database Honeypots



Spam Honeypots



Email Honeypots



Spider Honeypots



HoneyNet Honeypots

@HackingArticles

Malware Honeypots: son el tipo de honeypots que se utilizan para atrapar malware en una red. Su propósito es atraer al atacante o cualquier software malicioso y permitirle realizar ciertos ataques que pueden usarse para comprender el patrón del ataque.

Honeypots de correo electrónico: estos honeypots son direcciones de correo electrónico falsas que se utilizan para atraer atacantes a través de Internet. Los correos electrónicos que recibe cualquier actor malicioso pueden monitorearse y examinarse y pueden usarse para ayudar a evitar estafas de phishing por correo electrónico.

Honeypots de bases de datos: estos honeypots se hacen pasar por bases de datos reales que son vulnerables en nombre y generalmente atraen ataques como inyecciones SQL. Su objetivo es hacer que los atacantes piensen que podrían contener información confidencial, como datos de tarjetas de crédito, lo que permitirá a la organización comprender el patrón de los ataques que han realizado.

Spider Honeypots: estos honeypots se instalan con el propósito de atrapar a los distintos rastreadores web y arañas que tienden a robar información importante de las aplicaciones web.

Honeypots de spam: estos honeypots consisten en servidores de correo electrónico engañosos para atraer spammers para explotar elementos vulnerables del correo electrónico y brindar detalles sobre las actividades realizadas por ellos.

Honeynets:

no son más que una red de honeypots que se instalan en un entorno virtual y aislado junto con varios servidores para registrar las actividades de los atacantes y comprender las posibles amenazas.

Los Honeypots se pueden implementar en varios entornos. Hoy veremos la instalación y funcionamiento de honeypots en los entornos Windows, Android y Linux.

Sistema Windows

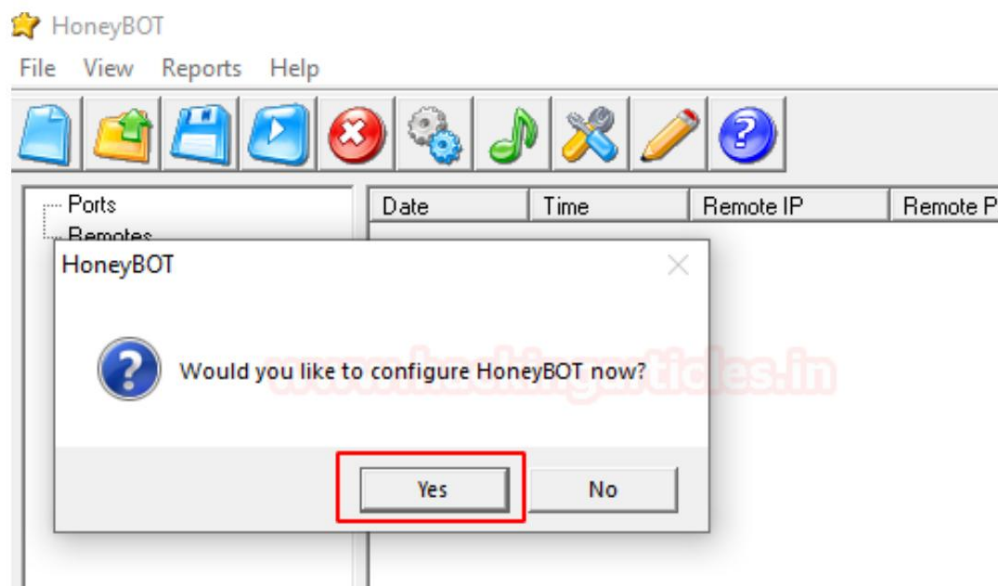
Hoy veremos el famoso software honeypot llamado HoneyBOT. que se puede descargar [aquí](#). Inicie Kali Linux como máquina atacante y su sistema Windows como máquina host.

Primero hagamos un escaneo nmap en la máquina host cuando el honeypot no esté instalado.

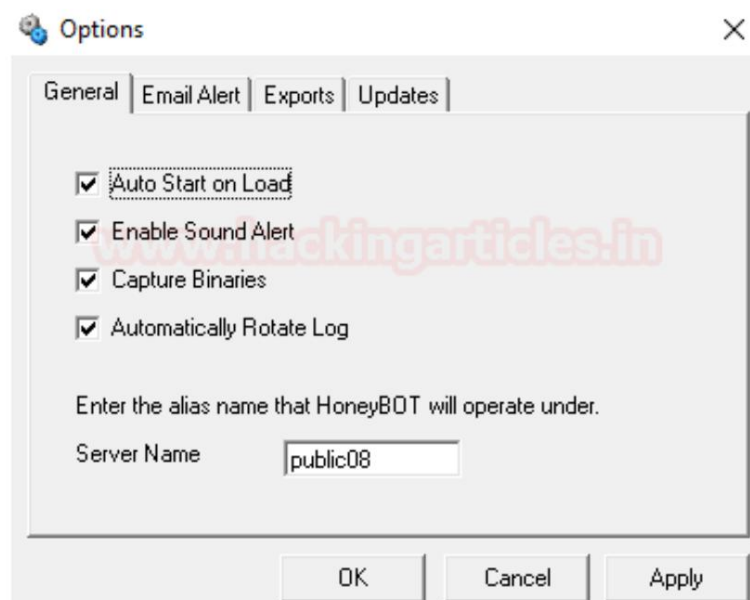
```
nmap -sV 192.168.1.17
```

```
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
```

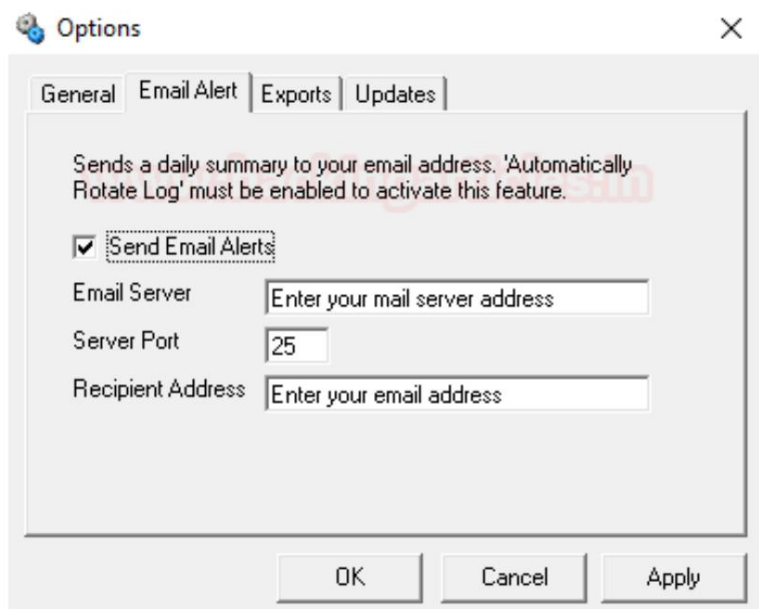
Ahora en su sistema Windows, instale el software HoneyBOT y configúrelo. Haga clic en "sí" para continuar.



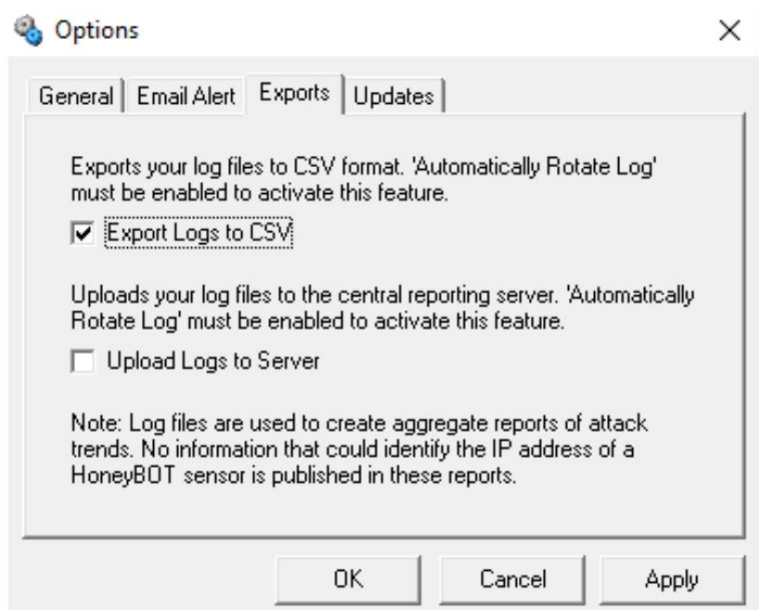
Verifique todos los parámetros que desee en su honeypot y haga clic en Aplicar para continuar.



Para recibir informes por correo electrónico sobre su honeypot, agregue la dirección de correo electrónico del destinatario y haga clic en "Aplicar".



Si desea guardar los registros del honeypot en formato CSV, puede utilizar esta configuración.



En la máquina del atacante, realiza un escaneo nmap y allí verá muchos servicios falsos que están abiertos debido a la presencia del honeypot en el sistema.

```

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

```

Intentemos conectarnos vía FTP desde la máquina atacante a la máquina host.

```
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):
```

Como puede ver, se ha generado un registro de la IP del atacante y del puerto al que estaba conectado.

★ HoneyBOT - Log_20201113.bin

File View Reports Help

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

Aquí puede ver un informe detallado sobre la conexión creada por el atacante.

★ Packet Log (ftp)

Connection Details:

Date: 11/13/2020
 Time: 5:32:03 AM
 Millisecond: 671
 Time Zone: -8:00
 Source IP: 192.168.1.9
 Source Port: 48006
 Server IP: 192.168.1.17
 Server Port: 21 (ftp)
 Protocol: TCP

Bytes Sent: 41
 Bytes Received: 0

Packet History

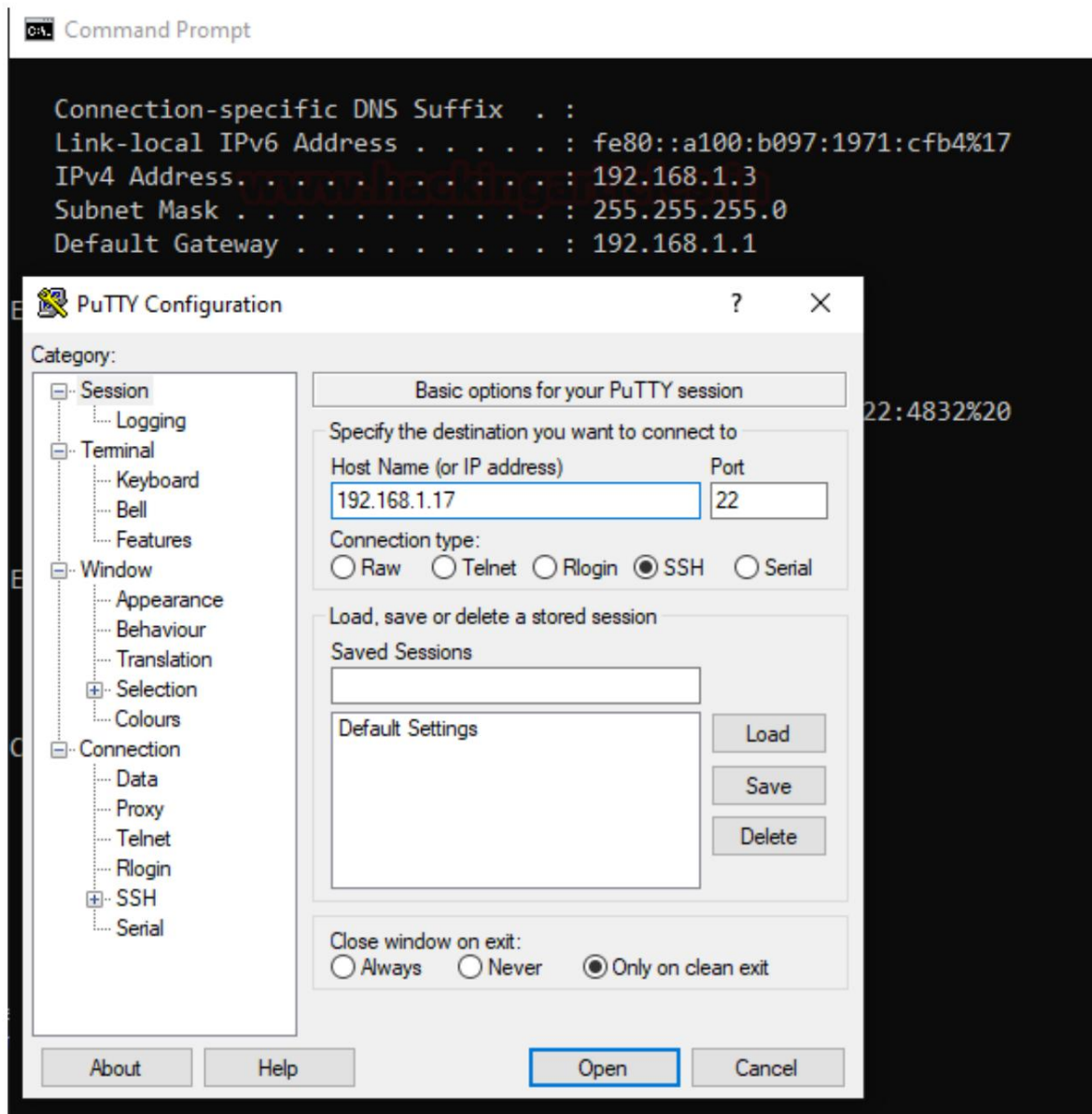
Time	Direction	Bytes	Data
5:32:03 AM	RX	0	SYN
5:32:03 AM	TX	41	220 PUBLIC08 FTP Service (Version 5.0).

Packet Data:

View as: ☒ text ☐ hex

<< < > >>

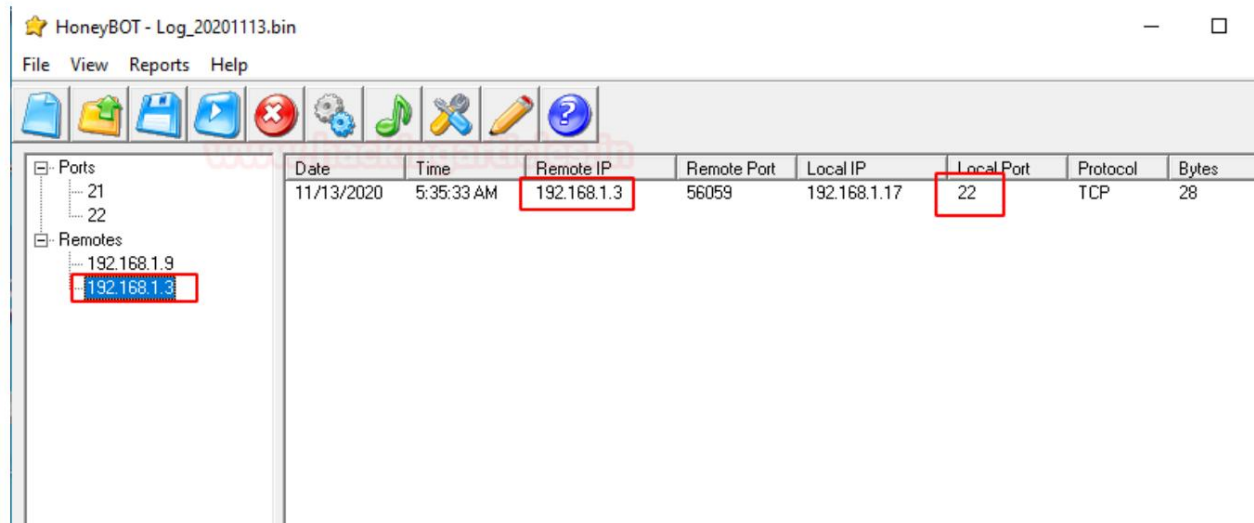
De manera similar, se inició una conexión SSH en el puerto 22 desde otro sistema operativo.



Ahora puede ver que se ha generado un registro del mismo para la conexión creada en el puerto 22.

★ HoneyBOT - Log_20201113.bin

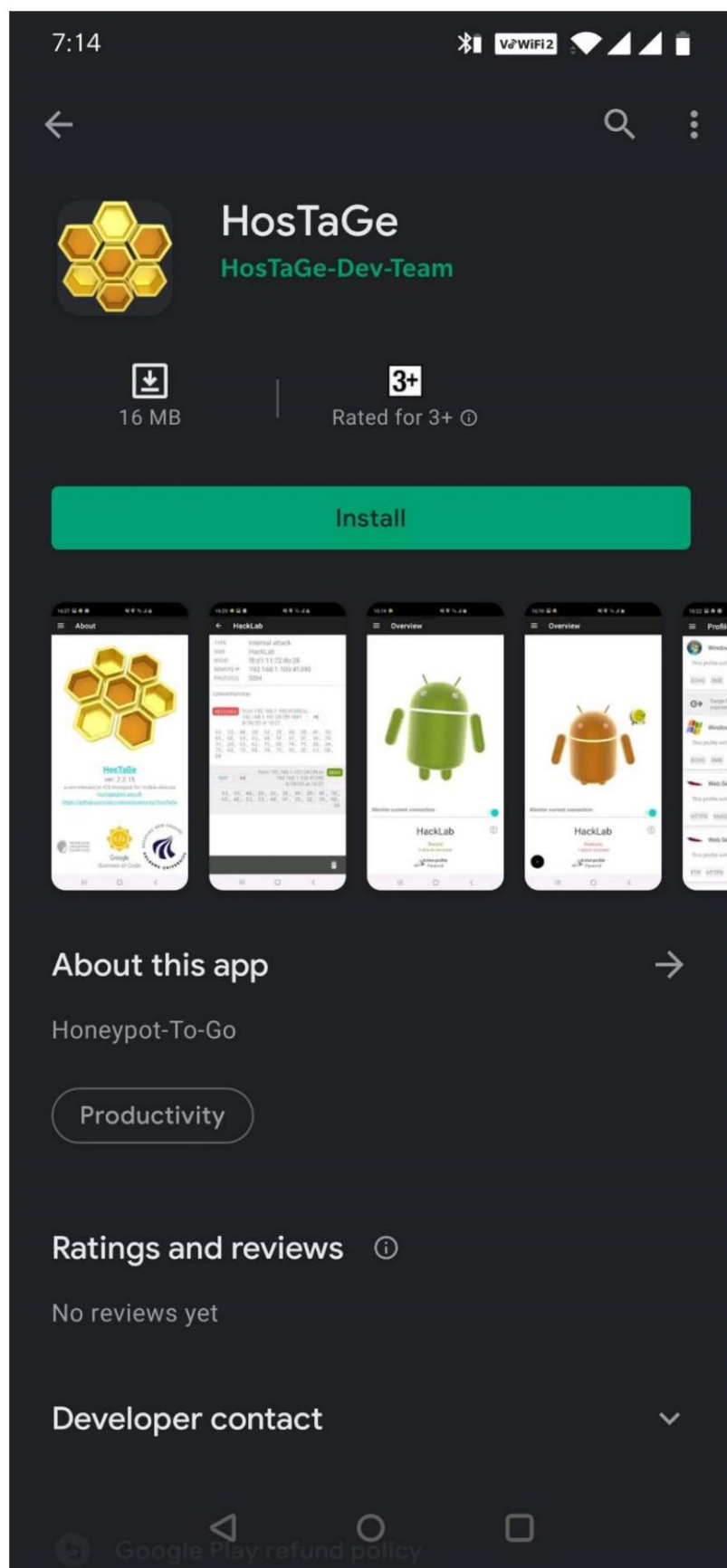
File View Reports Help



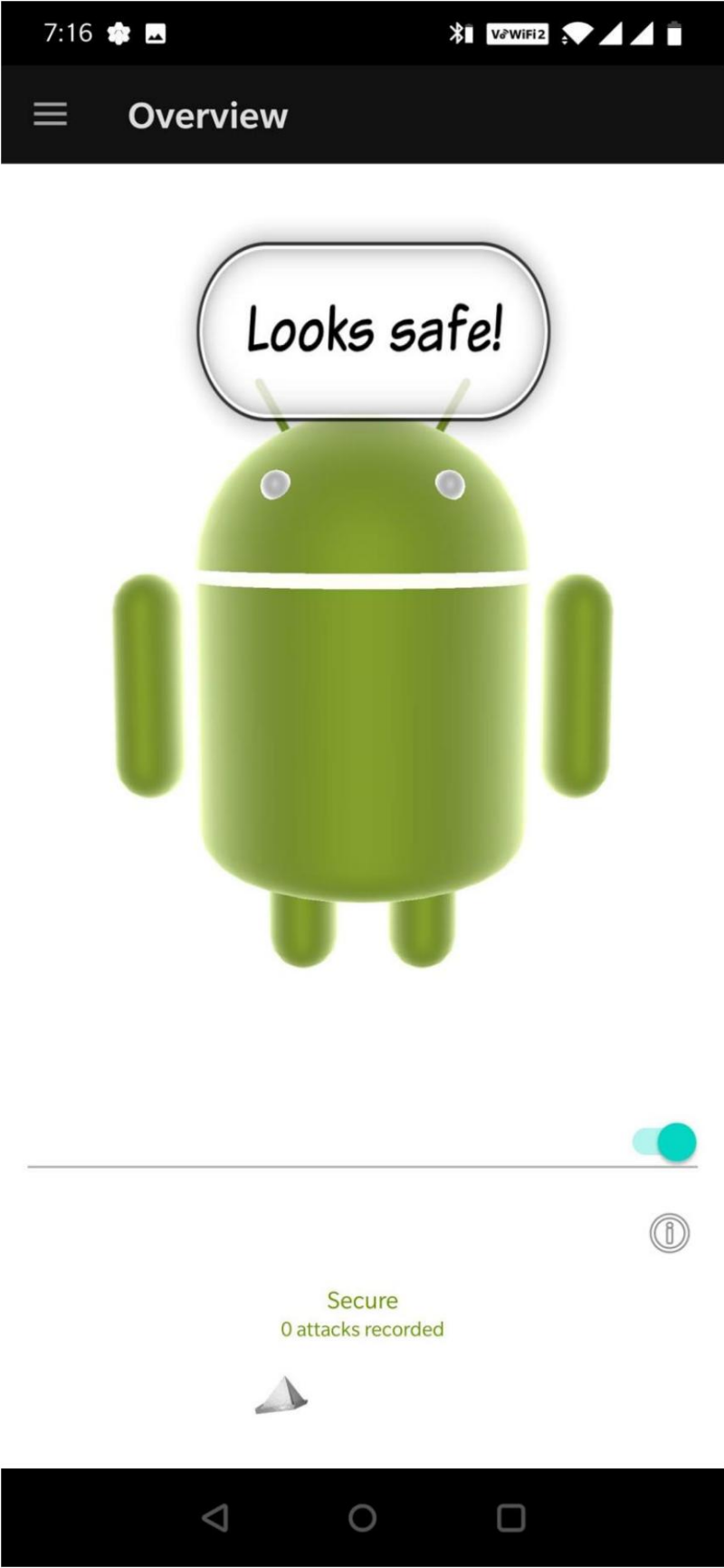
Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
11/13/2020	5:35:33 AM	192.168.1.3	56059	192.168.1.17	22	TCP	28

Android Honeypot

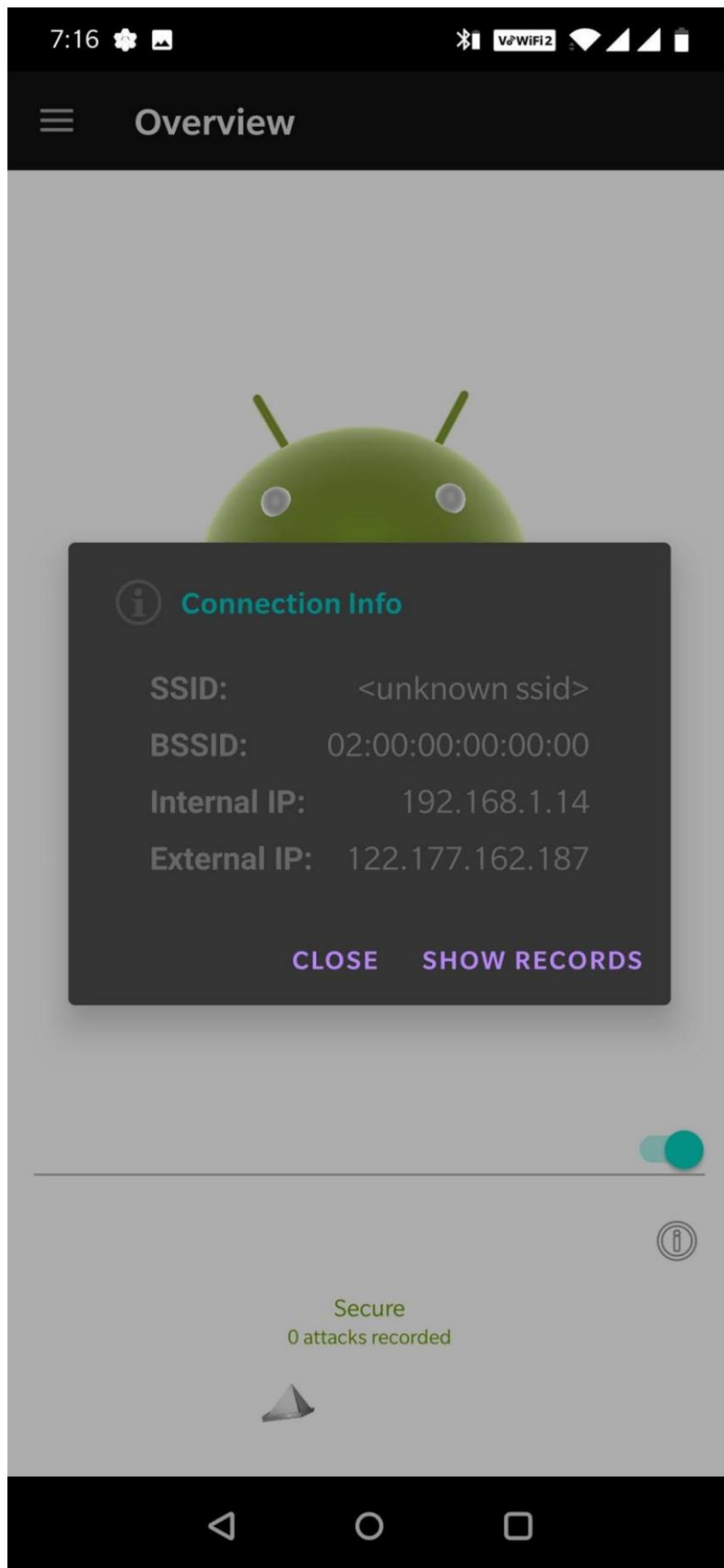
Los honeypots también se pueden instalar en teléfonos Android mediante la tienda Google Play. Aquí hemos descargado el honeypot Hostage.



Al encender la aplicación, parece segura.



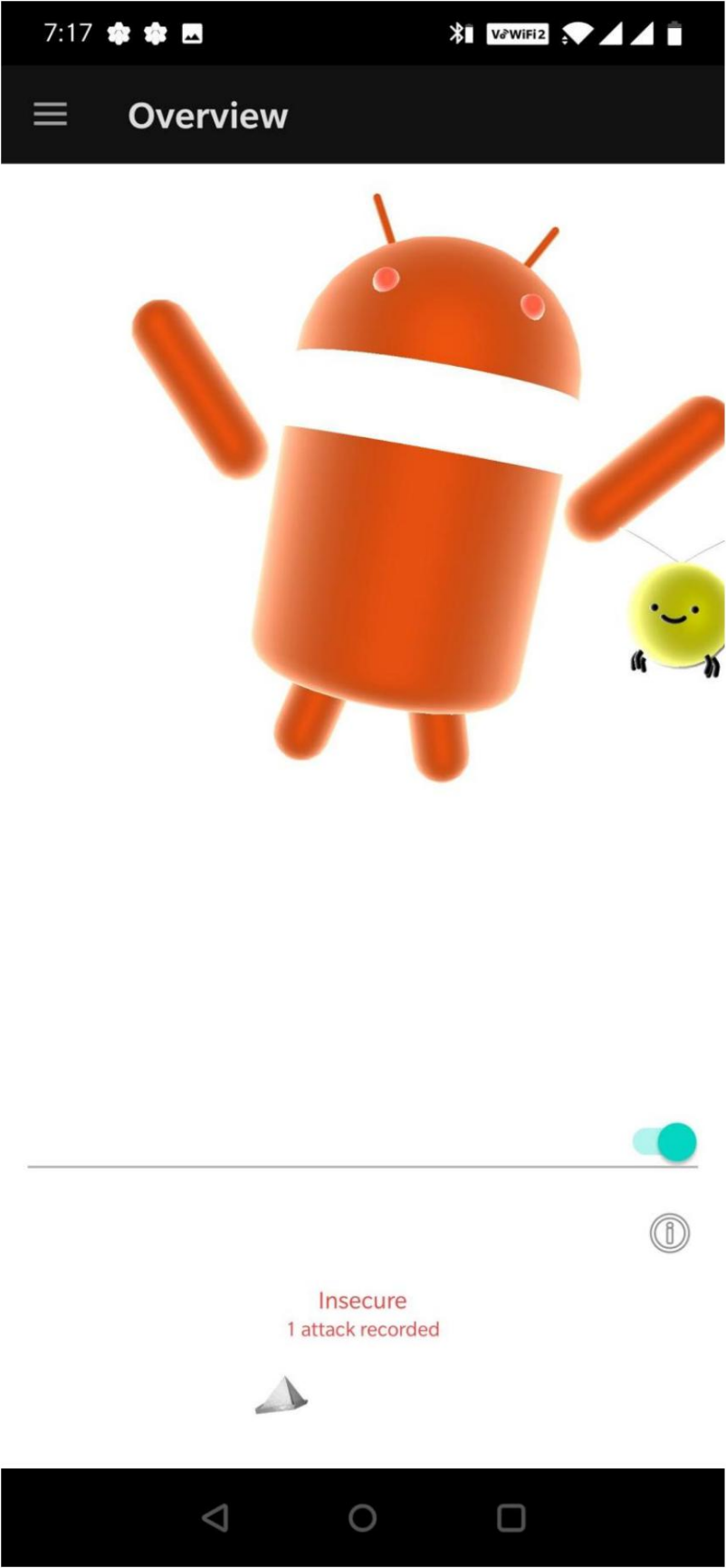
Ahora verifiquemos la dirección IP de su dispositivo Android y procedamos.



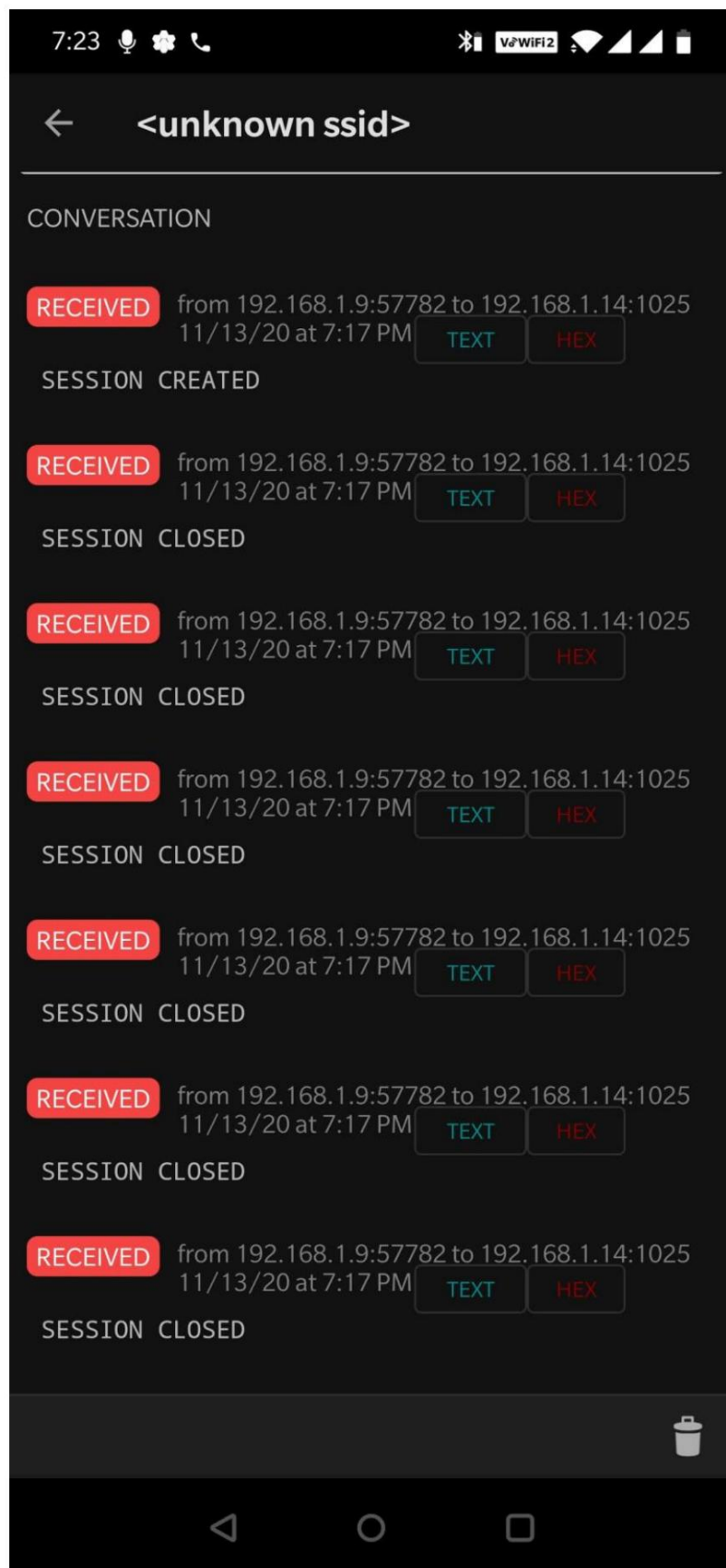
Encendamos el sistema del atacante y realicemos un escaneo nmap en la dirección IP del dispositivo Android.

```
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
```

Se generará una alerta en el dispositivo Android cuando se conecte el escaneo nmap.



Se creará un registro y veremos la IP del sistema atacante y los puertos que fueron atacados.



Pote de miel de Linux

También podemos instalar un honeypot en una máquina Linux. Aquí hemos demostrado el uso de Pentox, que se puede instalar fácilmente en 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
```

Una vez instalado, comencemos a usar pentbox. Seleccione las herramientas de red y el honeypot del menú para instalar el honeypot. Continúe con la configuración manual para instalarlo según sus preferencias para un 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
```

Ahora puedes abrir el puerto falso según tus preferencias e insertar un mensaje falso. También puede proporcionar la opción de guardar el registro y guardar el nombre del registro. Puede ver que el honeypot está activado en el puerto requerido y, de manera similar, puede activar manualmente los honeypots para otros puertos.

```

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)

```

Encienda la máquina del atacante y escanee la máquina host usando nmap. Los resultados de los puertos y servicios abiertos se muestran a continuación.

```

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)

```

Aquí, la máquina atacante intenta conectarse con la máquina host mediante 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:~#
```

Por cada intento de intrusión que se realiza, se alerta y se crea un registro donde se registra la IP y el puerto del atacante.

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

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

