

# “HONEYPOT”

Informe N°7

## Laboratorio de Seguridad en Redes

Melanny Dávila

Ingeniería en Telecomunicaciones  
Facultad de Eléctrica y Electrónica  
Quito, Ecuador  
melanny.davila@epn.edu.ec

Alejandra Silva

Ingeniería en Telecomunicaciones  
Facultad de Eléctrica y Electrónica  
Quito, Ecuador  
alejandra.silva@epn.edu.ec

**Abstract**—En el presente documento se presenta el sustento teórico e implementación de un honeypot es un entorno controlado y seguro para mostrar cómo trabajan los atacantes y examinar diferentes tipos de amenazas.

**Index Terms**—Atacante, HoneyPot, HoneyNet, tráfico, Kali.

### I. INTRODUCCIÓN

Un HoneyPot crea una trampa para los piratas informáticos. Es un sistema informático de sacrificio que está destinado a atraer ciberataques, como un señuelo. Imita un objetivo para los piratas informáticos y utiliza sus intentos de intrusión para obtener información sobre los ciberdelincuentes y la forma en que operan o para distraerlos de otros objetivos [1].

### II. OBJETIVOS

- Instalar, configurar y poner en marcha un honeypot.
- Evaluar el funcionamiento del honeypot, a partir de las interacciones de un atacante simulado desde Kali Linux.

### III. CUESTIONARIO

#### A. Presente la configuración realizada en el laboratorio.

Para la realización del laboratorio se usaron dos máquinas, una atacante y otra que actuará de honeypot de manera que se cuantifique y cualifique los ataques realizados sobre el honeypot. Como configuración inicial se tiene la asignación de direcciones IP estáticas a las distintas máquinas que actúan en la topología, luego la verificación de conexión entre ellas y de ellas al internet. Luego, la configuración del honeypot como tal por medio de la edición del archivo kippo donde se establece la dirección IP a la que se escuchará por una conexión ssh, así como el puerto y el nombre del host del honeypot. En el caso de esta práctica también se definió la versión de ssh que se permitirá usar. Además se habilitó el inicio en modo interactivo del honeypot. Una vez este archivo fue editado con todas las configuraciones requeridas se procedió a iniciarlo con el archivo *start.sh*. Para dar inicio al análisis de datos se hizo un escaneo de puertos desde el atacante, donde se verificó que el puerto 2223 estaba abierto. Luego, desde el atacante, se estableció una conexión ssh al honeypot especificando el puerto desde el cual se desea conectar tal como se estableció al inicio. Se hicieron varias sesiones ssh fallidas para luego

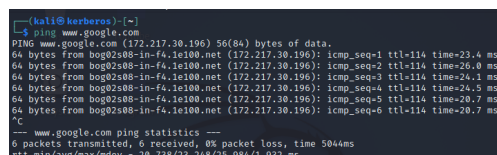
verificar esta información en los logs de honeypot.

Una vez se verificó que se puede establecer una sesión ssh entre el atacante y el honeypot se procedió a agregar usuarios del mismo a través de la edición del archivo *userdb.txt*. En este caso se agrego el usuario *alejandra* con la contraseña 12344. Para aplicar los cambios realizados se procedió a reiniciar el servicio por medio de los archivos *stop.sh* y *start.sh* respectivamente.

Para monitorear la actividad de un atacante en el honeypot se hace uso de el modo interactivo donde se puede ver en tiempo real la actividad de un cliente ssh a través de su ID, además, el modo interactivo permite finalizar la actividad de un cliente ssh de manera inmediata por medio de un comando. Asimismo, en el caso de que se ejecuten ataques de fuerza bruta sobre el honeypot, se pueden obtener gráficas de los intentos realizados y los distintos usuarios probados de manera que se pueden diagnosticar fallas de privacidad de la información de login al honeypot.

#### B. Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados, y el correspondiente análisis de las capturas de tráfico realizadas.

A continuación se presenta la prueba de conectividad a internet en la figura 1.



```
[kali@kerberos: ~]$ ping www.google.com
PING www.google.com (172.217.30.196) 56(84) bytes of data:
64 bytes from bog02s08-in-fa.1e108.net (172.217.30.196): icmp_seq=1 ttl=114 time=23.4 ms
64 bytes from bog02s08-in-fa.1e108.net (172.217.30.196): icmp_seq=2 ttl=114 time=26.0 ms
64 bytes from bog02s08-in-fa.1e108.net (172.217.30.196): icmp_seq=3 ttl=114 time=24.1 ms
64 bytes from bog02s08-in-fa.1e108.net (172.217.30.196): icmp_seq=4 ttl=114 time=24.5 ms
64 bytes from bog02s08-in-fa.1e108.net (172.217.30.196): icmp_seq=5 ttl=114 time=20.7 ms
64 bytes from bog02s08-in-fa.1e108.net (172.217.30.196): icmp_seq=6 ttl=114 time=20.7 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5044ms
rtt min/avg/max/mdev = 20.738/23.248/25.984/1.932 ms
```

Fig. 1. Prueba de conexión a internet

Se cambia el adaptador de la máquina a adaptador sólo-anfitrión como se muestra en la figura 2.

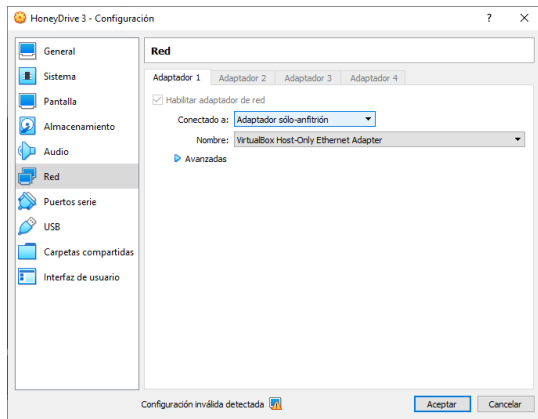


Fig. 2. Cambio del adaptador de la máquina virtual

Se cambia la conexión dentro de una máquina cliente. Esto se puede visualizar en la figura 3.

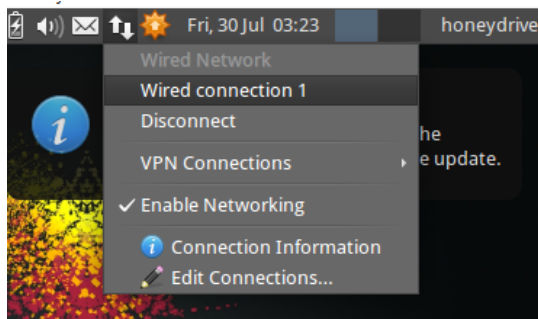


Fig. 3. Cambio de la conexión dentro de una máquina cliente

En la figura 4 se muestran las configuraciones IPv4 de la máquina cliente. Se asigna una dirección IP estática.

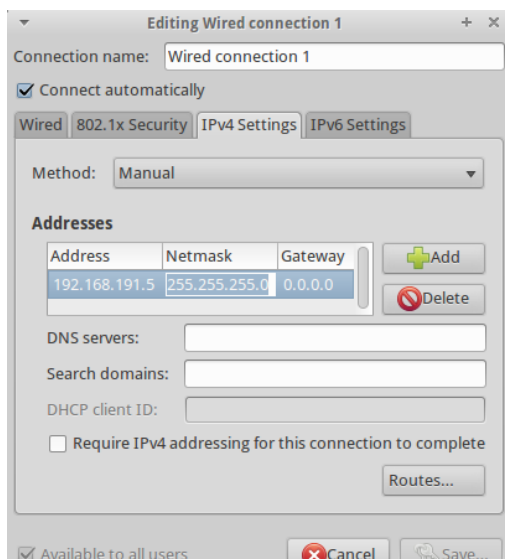


Fig. 4. Asignación de una dirección estática a la máquina cliente.

En la figura 5 se muestra la notificación de conexión establecida.



Fig. 5. Notificación de conexión establecida

En las figuras 6 y 7 se muestran las pruebas de conexión entre todos los miembros de la topología.

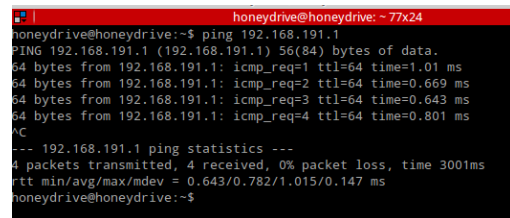


Fig. 6. Ping a la máquina con la dirección 192.168.191.1

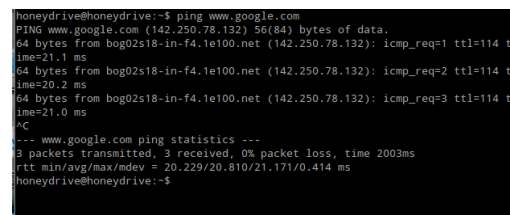


Fig. 7. Ping a google.com

En la figura 8 se presenta el ingreso a al directorio kippo y visualización de todos los archivos y directorios que se encuentran en él.

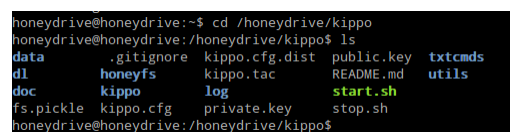


Fig. 8. Ingreso y visualización de los archivos de kippo

Edición del archivo kippo.cfg, en este archivo se encuentran las direcciones, puertos y nombres de usuarios a las que se escucharán por conexiones ssh.

```

honeydrive@honeydrive:/honeydrive/kippo 67x24
#
# Kippo configuration file (kippo.cfg)
#
[honeypot]
# IP addresses to listen for incoming SSH connections.
#
# (default: 0.0.0.0) = any address
ssh_addr = 192.168.191.5
# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 2223
# Hostname for the honeypot. Displayed by the shell prompt of the v
rtual
# environment.
#
# (default: svr03)
hostname = servidor.epn.edu

```

Fig. 9. Configuración de dirección, puerto y nombre de usuario para conexiones ssh

La asignación de la versión de ssh que se va a hacer se muestra en la figura 10

```

# (default: "SSH-2.0-OpenSSH_5.1p1 Debian-5")
ssh_version_string = SSH-2.0-OpenSSH_5.1p1 Debian-5 EPN

```

Fig. 10. Asignación de la versión de ssh

En la figura 11 se activa la interacción y el puerto con el que interactuará.

```

# (default: false)
interact_enabled = true
# (default: 5123)
interact_port = 5123

```

Fig. 11. Activación de la interacción y asignación de su puerto correspondiente

En la figura 12 se muestra el cambio de permisos del archivo stop.sh para poder ser ejecutado por todos.

```

honeydrive@honeydrive:/honeydrive/kippo$ chmod 775 stop.sh

```

Fig. 12. Cambio de permisos del archivo stop.sh

En la figura 12 se muestra el archivo con sus nuevos permisos asignados

```

honeydrive@honeydrive:/honeydrive/kippo$ ls -la
total 2684
drwxr-xr-x 11 honeydrive honeydrive 4096 Jul 30 03:46 .
drwxr-xr-x 20 honeydrive honeydrive 4096 Jul 22 2014 ..
drwxrwxr-x 2 honeydrive honeydrive 4096 Jul 18 2014 data
drwxrwxr-x 2 honeydrive honeydrive 4096 Jul 18 2014 dl
drwxrwxr-x 3 honeydrive honeydrive 4096 Jul 18 2014 doc
-rw-rw-r-- 1 honeydrive honeydrive 2657150 Jul 18 2014 fs.pickle
drwxrwxr-x 8 honeydrive honeydrive 4096 Jul 25 2014 .git
-rw-rw-r-- 1 honeydrive honeydrive 167 Jul 18 2014 .gitignore
drwxrwxr-x 4 honeydrive honeydrive 4096 Jul 18 2014 honeypfs
drwxrwxr-x 5 honeydrive honeydrive 4096 Jul 18 2014 kippo
-rw-rw-r-- 1 honeydrive honeydrive 5361 Jul 30 03:46 kippo.cfg
-rw-rw-r-- 1 honeydrive honeydrive 5344 Jul 18 2014 kippo.cfg.dist
-rw-rw-r-- 1 honeydrive honeydrive 1987 Jul 18 2014 kippo.tac
drwxrwxr-x 3 honeydrive honeydrive 4096 Jul 18 2014 log
-rw-rw-r-- 1 honeydrive honeydrive 886 Jul 18 2014 private.key
-rw-rw-r-- 1 honeydrive honeydrive 212 Jul 18 2014 public.key
-rw-rw-r-- 1 honeydrive honeydrive 2689 Jul 18 2014 README.md
-rwxrwxr-x 1 honeydrive honeydrive 147 Jul 18 2014 start.sh
-rwxrwxr-x 1 honeydrive honeydrive 154 Jul 18 2014 stop.sh

```

Fig. 13. Demostración del cambio de permisos

En la figura 14 se muestra el inicio del archivo start.sh, se puede apreciar que se inicia como un proceso secundario y usar mysql.

```

honeydrive@honeydrive:/honeydrive/kippo$ sudo vi kippo.cfg
honeydrive@honeydrive:/honeydrive/kippo$ ./start.sh
Starting kippo in the background...

Loading dblog engine: mysql
honeydrive@honeydrive:/honeydrive/kippo$

```

Fig. 14. Ejecución del archivo start.sh

Luego de haber configurado la máquina que va a hacer de honetpot se configura la máquina kali para realizar un ataque. Para esto se inicia msfdb. Este proceso se muestra en la figura 15

```

kali@kali:~$ sudo msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization

```

Fig. 15. Inicio de msfdb

Luego se mapean las vulnerabilidades de la base de datos con nmap, se coloca la dirección de la víctima y el puerto que va a ser atacado como se muestra en la figura 16

```

msf6 > db_nmap -sV 192.168.191.5 -p 0-65535
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-29 22:59 EDT
[*] Nmap: Nmap scan report for 192.168.191.5
[*] Nmap: Host is up (0.00020s latency).
[*] Nmap: Not shown: 65533 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 80/tcp    open  http   Apache httpd 2.2.22
[*] Nmap: 2223/tcp  open  ssh     OpenSSH 5.1p1 Debian 5 EPN (protocol 2.0)
[*] Nmap: 5123/tcp  open  telnet
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port5123-TCP:V=7.91%I=7KD=7/29%T=61036B0A3P=x86_64-pc-linux-gnu%r(NU
[*] Nmap: SFL:LL,141,"\xff\xfd"\xff\xfa"\x01\x00\xff\x00\xff\xfb\x01*\
[*] Nmap: SF:20session\x20management\x20console\x20*\r\nList\x20of\x20commands:
[*] Nmap: SF:r\n\x20list\x20\x20\x20\x20\x20\x20\x20\x20\x20list\x20all\x20active\x20s

```

Fig. 16. Lectura de vulnerabilidades en la base de datos del honeypot

Se leen los logs dentro del honeypot y se obtienen los datos mostrados en la figura 17

```

honeydrive@honeydrive:~$ tail -f /honeydrive/kippo/log/kippo.log
return func(*args,**kw)
--- <exception caught here> ---
File "/usr/lib/python2.7/dist-packages/twisted/internet/posixbase.py", line 586, in _doReadOrWrite
why = selectable.doRead()
File "/usr/lib/python2.7/dist-packages/twisted/internet/tcp.py", line 199, in doRead
rval = self.protocol.dataReceived(data)
File "/usr/lib/python2.7/dist-packages/twisted/conch/terminal.py", line 537, in dataReceived
raise ValueError("Stumped", b)
exceptions.ValueError: ('Stumped', '\x01')

```

Fig. 17. Lectura de logs dentro del honeypot

A continuación, se realiza un intento de conexión ssh al usuario "noexiste", este proceso se visualiza en la figura 18.

```
honeydive@honeydive:~$ ssh -p 2223 192.168.191.5 -l noexiste
The authenticity of host '[192.168.191.5]:2223 ([192.168.191.5]:2223)' can't
be established.
RSA key fingerprint is 14:d3:8f:4f:26:37:fd:a:76:06:b9:3f:c5:4b:3c:f1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.191.5]:2223' (RSA) to the list of kno
wn hosts.
Password:
Password:
noexiste@192.168.191.5's password:
Permission denied, please try again.
noexiste@192.168.191.5's password:
```

Fig. 18. Intento de loggeo con el usuario no existe

Para comprobar que los intentos de loggeo han sido registrados se visualiza el archivo de logs nuevamente como se muestra en la figura 19.

```
honeydrive@honeydrive:~$ 65x24
sport,0,192.168.191.5] unauthorized login:
2021-07-30 04:16:52+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] noxistie trying aut keyboard-interactive
2021-07-30 04:16:54+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] login attempt [noxistie/ale] failed
2021-07-30 04:16:54+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] noxistie failed aut keyboard-interactive
2021-07-30 04:16:54+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] unauthorized login:
2021-07-30 04:16:54+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] noxistie trying aut keyboard-interactive
2021-07-30 04:17:02+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] login attempt [noxistie/noxistie] failed
2021-07-30 04:17:02+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] noxistie failed aut keyboard-interactive
2021-07-30 04:17:02+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] unauthorized login:
2021-07-30 04:17:24+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] noxistie trying aut password
2021-07-30 04:17:24+0100 [SSHSERVICE ssh-usrauth on HoneyPotTran
sport,0,192.168.191.5] login attempt [noxistie/11234] failed
2021-07-30 04:17:25+0100 [-] noxistie failed aut password
2021-07-30 04:17:25+0100 [-] unauthorized login:
```

Fig. 19. Registro de intentos de acceso al honeypot

Luego, se muestra el ingreso al directorio /honeydrive/kip-po/data y el inicio de la edición del archivo userdb.txt.

```
honeydrive@honeydrive:~$ cd /honeydrive/kippo/data
honeydrive@honeydrive:/honeydrive/kippo/data$ ls
lastlog.txt  userdb.txt
honeydrive@honeydrive:/honeydrive/kippo/data$ vi userdb.txt
```

Fig. 20. Ingreso y muestra del conetido del directorio /honeydrive/kippo/data

Posteriormente se editó el usuario root y alejandra dentro del archivo userdb.txt

```
root:0:123456
alejandra:0:12344
```

Fig. 21. Edición del usuario root y alejandra dentro del archivo userdb.txt

Con el fin de aplicar los cambios se detiene Kippo con el script stop.sh y luego se lo vuelve a iniciar con el script start.sh como se muestra en la figura 22

```
honeydrive@honeydrive:/honeydrive/kippo$ ./stop.sh
Stopping kippo...

honeydrive@honeydrive:/honeydrive/kippo$ ./start.sh
Starting kippo in the background...

Loading dblog engine: mysql
honeydrive@honeydrive:/honeydrive/kippo$
```

Fig. 22. Reinicio del servicio Kippo

En la figura 23 se muestra el login via ssh en la misma máquina, pero con el usuario y la contraseña antes creados, se puede visualizar que el hostname ha cambiado y que se puede hacer login con éxito.

```
(kali@kerberos)-[~]
$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes256-cbc alejandr
a@192.168.191.5 -p 2223
Password:
alejandra@servidor.epn.edu:~#
```

Fig. 23. Login al usuario previamente creado

Luego, se procede a navegar en los directorios del usuario al que se pudo hacer login y se muestran otros usuarios de la máquina. Esto se puede visualizar en la figura 24

```
(kali@kerberos)-[~]
# cd -> /usr/share/kerberos-libs+diffie-hellman-group1-sha1 -c aes256-cbc alejandra192.168.191.5 -p 2223
Password:
Password:
Password:
alejandra@servidor.epn.edu:~# ls
alejandra@servidor.epn.edu:~# cd /home/
alejandra@servidor.epn.edu:/home# ls
richard
alejandra@servidor.epn.edu:/home#
```

Fig. 24. Navegación entre directorios y visualización de otros usuarios

En la figura 25 se puede visualizar que dentro del honeypot solo se encuentra el usuario honeydrive.

```
honeydrive@honeydrive:/honeydrive/kippo$ cd /home
honeydrive@honeydrive:/home$ ls
honeydrive
honeydrive@honeydrive:/home$
```

Fig. 25. Usuarios del honeypot

Luego, desde otra terminal se accede al usuario jon y al usuario alejandra dentro del honeypot, donde el acceso a jon es denegado hasta el final.

```

kali@kali:~$ ssh -o StrictHostKeyChecking=no root@10.10.10.5
Warning: Permanently added '10.10.10.5' (RSA) to the list of known hosts.
root@kali:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
www:x:34:34:www:/var/www:/usr/sbin/nologin
www-data:x:35:35:www-data:/var/www:/usr/sbin/nologin
www:x:36:36:www:/var/www:/usr/sbin/nologin
www-data:x:37:37:www-data:/var/www:/usr/sbin/nologin
www:x:38:38:www:/var/www:/usr/sbin/nologin
www-data:x:39:39:www-data:/var/www:/usr/sbin/nologin
www:x:40:40:www:/var/www:/usr/sbin/nologin
www-data:x:41:41:www-data:/var/www:/usr/sbin/nologin
www:x:42:42:www:/var/www:/usr/sbin/nologin
www-data:x:43:43:www-data:/var/www:/usr/sbin/nologin
www:x:44:44:www:/var/www:/usr/sbin/nologin
www-data:x:45:45:www-data:/var/www:/usr/sbin/nologin
www:x:46:46:www:/var/www:/usr/sbin/nologin
www-data:x:47:47:www-data:/var/www:/usr/sbin/nologin
www:x:48:48:www:/var/www:/usr/sbin/nologin
www-data:x:49:49:www-data:/var/www:/usr/sbin/nologin
www:x:50:50:www:/var/www:/usr/sbin/nologin
www-data:x:51:51:www-data:/var/www:/usr/sbin/nologin
www:x:52:52:www:/var/www:/usr/sbin/nologin
www-data:x:53:53:www-data:/var/www:/usr/sbin/nologin
www:x:54:54:www:/var/www:/usr/sbin/nologin
www-data:x:55:55:www-data:/var/www:/usr/sbin/nologin
www:x:56:56:www:/var/www:/usr/sbin/nologin
www-data:x:57:57:www-data:/var/www:/usr/sbin/nologin
www:x:58:58:www:/var/www:/usr/sbin/nologin
www-data:x:59:59:www-data:/var/www:/usr/sbin/nologin
www:x:60:60:www:/var/www:/usr/sbin/nologin
www-data:x:61:61:www-data:/var/www:/usr/sbin/nologin
www:x:62:62:www:/var/www:/usr/sbin/nologin
www-data:x:63:63:www-data:/var/www:/usr/sbin/nologin
www:x:64:64:www:/var/www:/usr/sbin/nologin
www-data:x:65:65:www-data:/var/www:/usr/sbin/nologin
www:x:66:66:www:/var/www:/usr/sbin/nologin
www-data:x:67:67:www-data:/var/www:/usr/sbin/nologin
www:x:68:68:www:/var/www:/usr/sbin/nologin
www-data:x:69:69:www-data:/var/www:/usr/sbin/nologin
www:x:70:70:www:/var/www:/usr/sbin/nologin
www-data:x:71:71:www-data:/var/www:/usr/sbin/nologin
www:x:72:72:www:/var/www:/usr/sbin/nologin
www-data:x:73:73:www-data:/var/www:/usr/sbin/nologin
www:x:74:74:www:/var/www:/usr/sbin/nologin
www-data:x:75:75:www-data:/var/www:/usr/sbin/nologin
www:x:76:76:www:/var/www:/usr/sbin/nologin
www-data:x:77:77:www-data:/var/www:/usr/sbin/nologin
www:x:78:78:www:/var/www:/usr/sbin/nologin
www-data:x:79:79:www-data:/var/www:/usr/sbin/nologin
www:x:80:80:www:/var/www:/usr/sbin/nologin
www-data:x:81:81:www-data:/var/www:/usr/sbin/nologin
www:x:82:82:www:/var/www:/usr/sbin/nologin
www-data:x:83:83:www-data:/var/www:/usr/sbin/nologin
www:x:84:84:www:/var/www:/usr/sbin/nologin
www-data:x:85:85:www-data:/var/www:/usr/sbin/nologin
www:x:86:86:www:/var/www:/usr/sbin/nologin
www-data:x:87:87:www-data:/var/www:/usr/sbin/nologin
www:x:88:88:www:/var/www:/usr/sbin/nologin
www-data:x:89:89:www-data:/var/www:/usr/sbin/nologin
www:x:90:90:www:/var/www:/usr/sbin/nologin
www-data:x:91:91:www-data:/var/www:/usr/sbin/nologin
www:x:92:92:www:/var/www:/usr/sbin/nologin
www-data:x:93:93:www-data:/var/www:/usr/sbin/nologin
www:x:94:94:www:/var/www:/usr/sbin/nologin
www-data:x:95:95:www-data:/var/www:/usr/sbin/nologin
www:x:96:96:www:/var/www:/usr/sbin/nologin
www-data:x:97:97:www-data:/var/www:/usr/sbin/nologin
www:x:98:98:www:/var/www:/usr/sbin/nologin
www-data:x:99:99:www-data:/var/www:/usr/sbin/nologin
root@kali:~#

```

Fig. 26. Loggeo en cuentas dentro del honeypot

Como se puede visualizar en la figura 27, se han registrado los intentos de login dentro de las cuentas previamente mencionadas.

Fig. 27. Registro de intentos de loggeo dentro del honeypot

```
honeydrive@honeydrive:~$ telnet -e q 192.168.191.5 5123
Telnet escape character is 'q'.
Trying 192.168.191.5...
Connected to 192.168.191.5.
Escape character is 'q'.
*** kippo session management console ***
List of commands:
list      - list all active sessions
view      - attach to a session in read-only mode
hijack    - attach to a session in interactive mode
disconnect - disconnect a session
help      - this help
exit      - disconnect the console
```

Fig. 28. Ingreso al modo interactivo

```
list
ID      clientIP      clientVersion
2       192.168.191.1 SSH-2.0-OpenSSH_8.4p1 Debian-5
4       192.168.191.1 SSH-2.0-OpenSSH_8.4p1 Debian-5
```

Fig. 29. Lista de clientes conectados por medio de ssh

```
alejandro@servidor.epn.edu:/home# cd richard/
alejandro@servidor.epn.edu:/home/richard# ls
alejandro@servidor.epn.edu:/home/richard# touch asd.txt
alejandro@servidor.epn.edu:/home/richard# cd richard/
bash: cd: richard/: No such file or directory
alejandro@servidor.epn.edu:/home/richard# touch asd.txt
alejandro@servidor.epn.edu:/home/richard#
```

Fig. 30. Comandos ejecutados por el atacante dentro del honeypot

```
view 4
** Attaching to #4, hit ESC to return
cd richard/
bash: cd: richard/: No such file or directory
alejandra@servidor.epn.edu:/home/richard$ touch asd.txt
alejandra@servidor.epn.edu:/home/richard#
** Interactive session closed.
hijack 4
** Attaching to #4, hit ESC to return
```

Fig. 31. Registro de la actividad del atacante dentro del honeypot

```
hijack 4
** Attaching to #4, hit ESC to return
ls
asd.txt
alejandra@servidor.epn.edu:/home/richard# touch hola.txt
alejandra@servidor.epn.edu:/home/richard#
```

Fig. 32. Cierre de la sesión interactiva

```
alejandra@servidor.epn.edu:/home/richard# touch hola.txt
alejandra@servidor.epn.edu:/home/richard#
```

Fig. 33. Creación de un archivo de texto por parte del atacante

```
disconnect 4
** Disconnecting session #4
```

Fig. 34. Cierre de la sesión del atacante desde el honeypot

```
Connection to 192.168.191.5 closed.  
[kali@kerberos]~  
$ 192.168.191.5 2222  
password:
```

Fig. 35. Mensaje de cierre de sesión en el honeypot

```
(kali@kerberos)-[~/pydictor]
$ sudo python3 pydictor.py --head 123 --len 2 2 -base d -o /home/kali/De
pydictor
2.1.5.4#dev

[+] A total of :100 lines
[+] Store in :/home/kali/Desktop/claves.txt
[+] Cost :0.0949 seconds

(kali@kerberos)-[~/pydictor]
```

Fig. 36. Descarga y uso de pydictor



Con la ayuda de medusa se inicia el ataque de fuerza bruta al honeypot, al usuario alejandr con el diccionario claves.txt haciendo uso de ssh.

```

(kali@kerberos)-[~/Desktop]
$ medusa -i 192.168.191.5 -u alejandr -P claves.txt -i 2222 -H ssh
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooofus Networks <jmk@foofus.net>
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12300 (1 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12301 (2 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12302 (3 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12303 (4 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12304 (5 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12305 (6 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12306 (7 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12307 (8 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12308 (9 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12309 (10 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12310 (11 of 100 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.191.5 (1 of 1, 0 complete) User: alejan
dr (1 of 1, 0 complete) Password: 12311 (12 of 100 complete)

```

Fig. 37. Inicio del ataque de fuerza bruta al honeypot

Para comprobar las estadísticas de intentos de explotación de vulnerabilidades al honeypot se usó kippo-graph, página a la que se puede entrar en la dirección [http://\[direccion io\]/kippo-graph](http://[direccion io]/kippo-graph). La página principal se muestra en la figura 38.

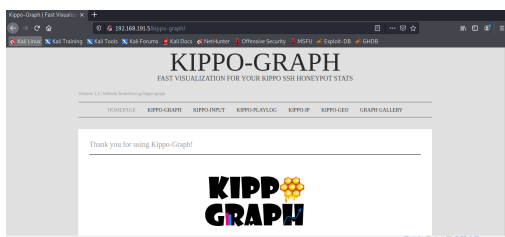


Fig. 38. Pantalla principal de kippo

Como primer resultado se puede visualizar las 10 contraseñas más usadas. Donde la que más veces ha sido usada es 12344 con un total de 7 veces. El gráfico completo puede ser visualizado en la figura 39.

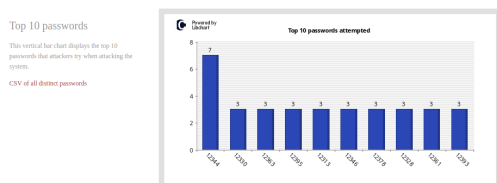


Fig. 39. Las 10 contraseñas más usadas para entrar al honeypot

En la figura 40 se muestran los 10 nombres de usuarios más usados, donde se puede ver que el nombre *alejandr* es el más usado con un total de 300 intentos.

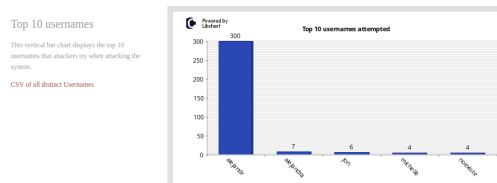


Fig. 40. Gráfica de los usuarios más probados para entrar al honeypot

Como información con un alto nivel de importancia se tienen las 10 combinaciones de usuarios-contraseñas usadas, donde se muestra el usuario con su respectiva contraseña intentada.

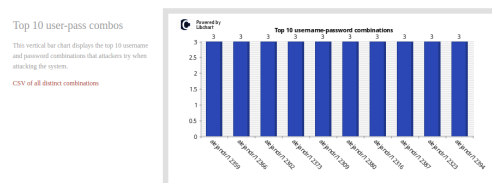


Fig. 41. Gráfica de 10 combinaciones de usuarios-contraseñas usadas

De igual forma, en la figura 42 se muestra el gráfico mencionado anteriormente con una variación en la forma de presentar los datos.

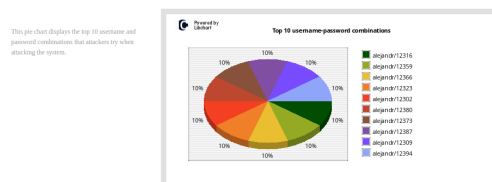


Fig. 42. Diagrama de pastel de las 10 combinaciones de usuarios-contraseñas usadas

Así como las gráficas anteriormente mencionadas, honeypot presenta una gran cantidad de gráficas que proveen información relevante sobre los ataques realizados al mismo y a continuación se muestran algunas de estas:

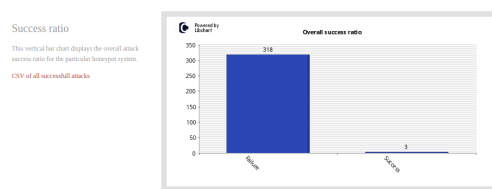


Fig. 43. Razón de éxito en los intentos de ingreso al honeypot

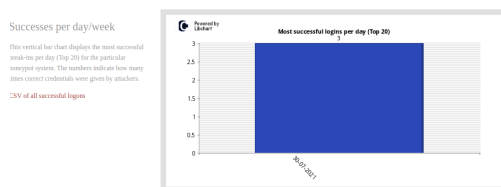


Fig. 44. Los 20 Logins exitosos oor día

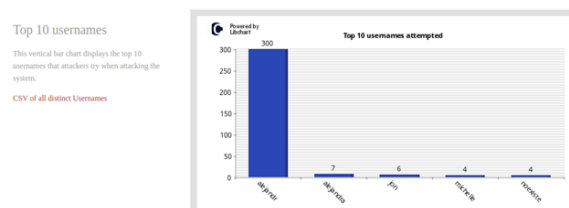


Fig. 48. Usuarios

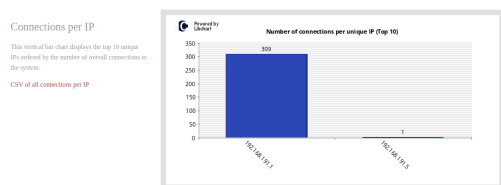


Fig. 45. Las 10 conexiones por dirección IP única

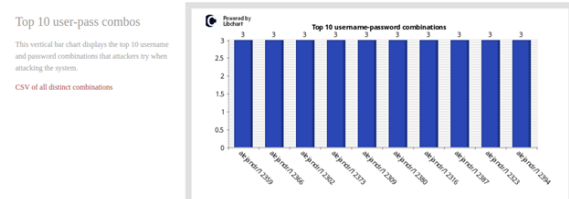


Fig. 49. Combinación de usuario y claves.

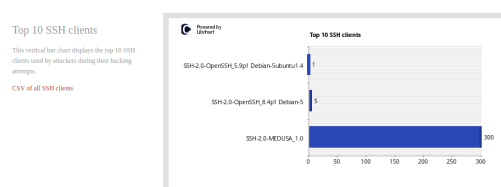


Fig. 46. Los 10 usuarios ssh más usados

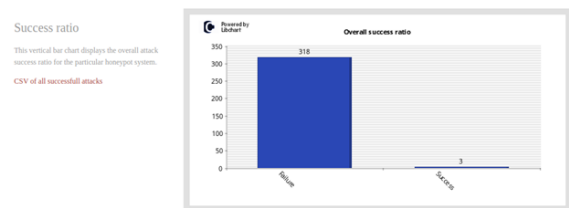


Fig. 50. Ataque exitoso.

## EXTRAS

Se va a colocar 5 gráficas que se obtuvieron en el Kippo-Graph con su respectiva explicación.

En esta figura se puede evidenciar que las información que se posee son las 10 principales contraseñas que los atacantes intentan cuando atacan el sistema.

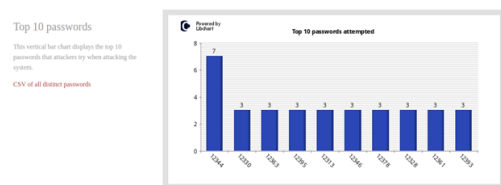


Fig. 47. Contraseñas

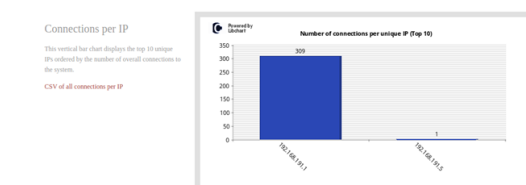


Fig. 51. Conexiones IP.

En la segunda figura se observa que la barra vertical muestra los 10 nombres de usuario principales que los atacantes intentan cuando atacan el sistema. Aquí se identifica que el ussername mas utilizado es Alejandra, lo que es normal ya que es el nombre del estudiante que realizo la practica

En la siguiente figura se tiene que la barra vertical muestra las 10 combinaciones principales de nombres de usuario y contraseñas que los atacantes intentan cuando atacan el sistema

Este gráfico de barras verticales muestra la tasa general de éxito del ataque para el sistema de honeypot particular, con un mensaje de que el ataque es exitoso.

Este gráfico de barras verticales muestra las 10 direcciones IP únicas principales ordenadas por el número de conexiones totales al sistema. Y se verifica que el mayor numero fue desde la maquina atacante que en este caso es el kali con la IP 192.168.191.1.

C. Explique que es una Honeynet e indique las ventajas y desventajas que presenta la implantación de esta en comparación a un Honeypot.

Una Honeynet es una red señuelo que contiene uno o más Honeypots. Parece una red real y contiene varios sistemas, pero está alojado en uno o solo unos pocos servidores, cada uno de los cuales representa un entorno [2]. Las Honeynets se desarrollan para ayudar a los expertos en seguridad informática a mejorar la seguridad de las redes y los sistemas [3]. Aunque puede parecerle a un pirata informático una red legítima, en

realidad está alojada en un único servidor; por diseño, estas redes no están autorizadas para ningún uso auténtico. Si se accede a dicha red trampa, se supone que la persona que accede a ella es un pirata informático [4].

Las principales diferencias entre HoneyNets HoneyPots tradicionales son:

- La seguridad de HoneyPot tiene sus limitaciones ya que el HoneyPot no puede detectar brechas de seguridad en sistemas legítimos y no siempre identifica al atacante. También existe el riesgo de que, habiendo explotado con éxito el HoneyPot, un atacante pueda moverse lateralmente para infiltrarse en la red de producción real. Para evitar esto, debe asegurarse de que el HoneyPot esté adecuadamente aislado [4].
- Todos los sistemas situados dentro de una Honeynet son sistemas comerciales estándar, nada es emulado ni se hace nada para que los sistemas sean menos seguros con lo que los análisis son más realistas.
- Una HoneyNet en lugar de detectar o engañar a los agresores, su uso es recoger información de las amenazas es así como se clasificaría como un HoneyPot para la investigación [5].
- Las HoneyNets pueden utilizar varios sistemas al mismo tiempo, como Solaris, Linux, Windows NT, router Cisco, conmutadores Alteon, etc. Esto crea un entorno de red que refleja de forma más realista una red productiva.
- Una HoneyNet al tener diferentes sistemas con diferentes aplicaciones, como un servidor DNS en Linux, un servidor Web Windows IIS, y un servidor de bases de datos en Solaris, permite aprender sobre diferentes herramientas y tácticas.
- Al tener una variedad de sistemas operativos y aplicaciones, las HoneyNet permiten trazar con más exactitud el perfil de las tendencias y rasgos de blackhat.
- Los riegos y vulnerabilidades encontradas en una Honeynet son las mismas que existen hoy en muchas organizaciones [6].

#### D. Conclusiones

- En un entorno real debe estar bloqueado para el atacante, el atacante debe ver el 5123 como filtrado o no verlo porque esto es para monitorizar el atacante y si ve sin filtro ni protección se verifica que es un HoneyPot.
- Un HoneyPot comprometido que no se aísla de forma eficaz puede utilizarse para lanzar un ataque a la red real. Asimismo, otro gran inconveniente del uso de HoneyPots es que solo puede detectar una intrusión cuando es atacado directamente.
- Un HoneyPot permite analizar a los adversarios y sus ataques de tal forma que se pueda formular estrategias de prevención adecuadas y de esta manera tomar las contramedidas adecuadas para bloquear el acceso del atacante a servidores legítimos.

#### E. Recomendaciones

- Verificar el número de puerto que se esta levantando para no tener problemas de conexión.
- La información recolectada por el honeypot es útil para diagnosticar las debilidades y fortalezas de la red a la que está conectado el honeypot. Por lo que es recomendable prestar especial atención a las gráficas obtenidas por el mismo.
- En el caso de que se visualice que el atacante quiere eliminar o alterar un archivo importante del sistema, es recomendable que se finalice su sesión por medio del modo interactivo.

#### REFERENCES

- [1] "Benefits of Honeypots – There's More to Honeypots Than Wasting Hackers' Time", WebTitan DNS Filter, abr. 29, 2015. <https://www.webtitan.com/blog/honeypots-how-far-can-you-go-in-wasting-a-hackers-time/> (accedido ago. 04, 2021).
- [2] "Honeynet". <https://www.ecured.cu/Honeynet> (accedido ago. 04, 2021).
- [3] "What is a Honeynet? - Definition from Techopedia", Techopedia.com. <http://www.techopedia.com/definition/16103/honeynet> (accedido ago. 04, 2021).
- [4] "What is a Honeypot — Honeynets, Spam Traps & more — Imperva", Learning Center. <https://www.imperva.com/learn/application-security/honeypot-honeynet/> (accedido ago. 04, 2021).
- [5] "What Is a Honeypot in Network Security? Definition, Types & Uses", InfoSec Insights, dic. 30, 2020. <https://sectigostore.com/blog/what-is-a-honeypot-in-network-security-definition-types-uses/> (accedido ago. 04, 2021).
- [6] "What is honeynet? - Definition from WhatIs.com", SearchSecurity. <https://searchsecurity.techtarget.com/definition/honeynet> (accedido ago. 04, 2021).