



HONEYPOTS

Una herramienta para conocer al enemigo

Administración de Sistemas y Seguridad
Universidad de Granada

JOSE ALBERTO GÓMEZ GARCÍA
LUCAS GUTIÉRREZ DURÁN

CURSO 22/23
Máster en Ingeniería Informática





INTRODUCCIÓN

Nuestro activo más valioso: La información

- Necesitamos infraestructuras para asegurarla.
- Existen diferentes métodos y ninguno está exento de riesgo.
- Nosotros vamos a explicaros los Honeypots

A decorative graphic on the left side of the slide, consisting of a cluster of yellow hexagons arranged in a honeycomb pattern. The hexagons are slightly 3D, with a darker yellow outline and a lighter yellow fill. They are positioned on the left side of the slide, partially overlapping the dark blue background.

Breve historia de los honeypots

Historia

- En los 1988, Clifford Stoll desarrolla un honeypot para rastrear un hacker (durante 3 años).
- Simula una máquina militar muy valiosa. Sistema al que llamó The Cuckoo's Egg.
- Usualmente se implementaban en Unix
- Fundamentales para conocer las últimas técnicas de ciberataques.

Historia

- En 1997 → Deception Toolkit (baja interacción)
- En 1998 → Cybercop Sting y NetFacade
- En 1999 → The Honeypot Project (investigación)
- En 1999 → ManTrap
- En 2002 → Tiny Honeypot y Google Hack Honeypot
- En 2004 → Roo (mediante CD-ROM booteable)

A decorative graphic on the left side of the slide, consisting of a cluster of yellow hexagons arranged in a honeycomb pattern. The hexagons are slightly 3D, with a darker yellow outline and a lighter yellow fill. They are positioned on the left side of the slide, with some hexagons overlapping the dark blue background.


**¿QUÉ ES UN
HONEYPOT?**

El honeypot

- Es un recurso de red destinado a ser atacado o comprometido por un tercero externo a la red.
- **¿Qué queremos con esto?**
- Aumentar la seguridad del sistema.

El honeypot

- Desvían la atención de los sistemas reales
- Actúan como sistema de vigilancia.
- Tienen la capacidad de **recopilar información** de manera detallada de los atacantes.

A decorative graphic on the left side of the slide consisting of a grid of yellow hexagons with white outlines, arranged in a pattern that tapers to the right.

**¿QUÉ TIPOS DE
HONEYPOTS
PODEMOS
ENCONTRAR?**

Honeypots de Baja Interacción

- Trabajan únicamente **emulando servicios y sistemas** operativos.
- La actividad del atacante se encuentra limitada al nivel de emulación del Honeypot.

Honeypots de Alta Interacción

- Implican la utilización de sistemas operativos y aplicaciones reales, similares a las de equipos reales.
- Es por esto que exponemos más información al atacante.

Honeynets o honeypots puros

- Tienen las funcionalidades plenas de un sistema normal.
- Es el tipo que más información proporciona.
- Sólo lo utilizan organizaciones de ciberseguridad o investigación.

Honeypots de Producción

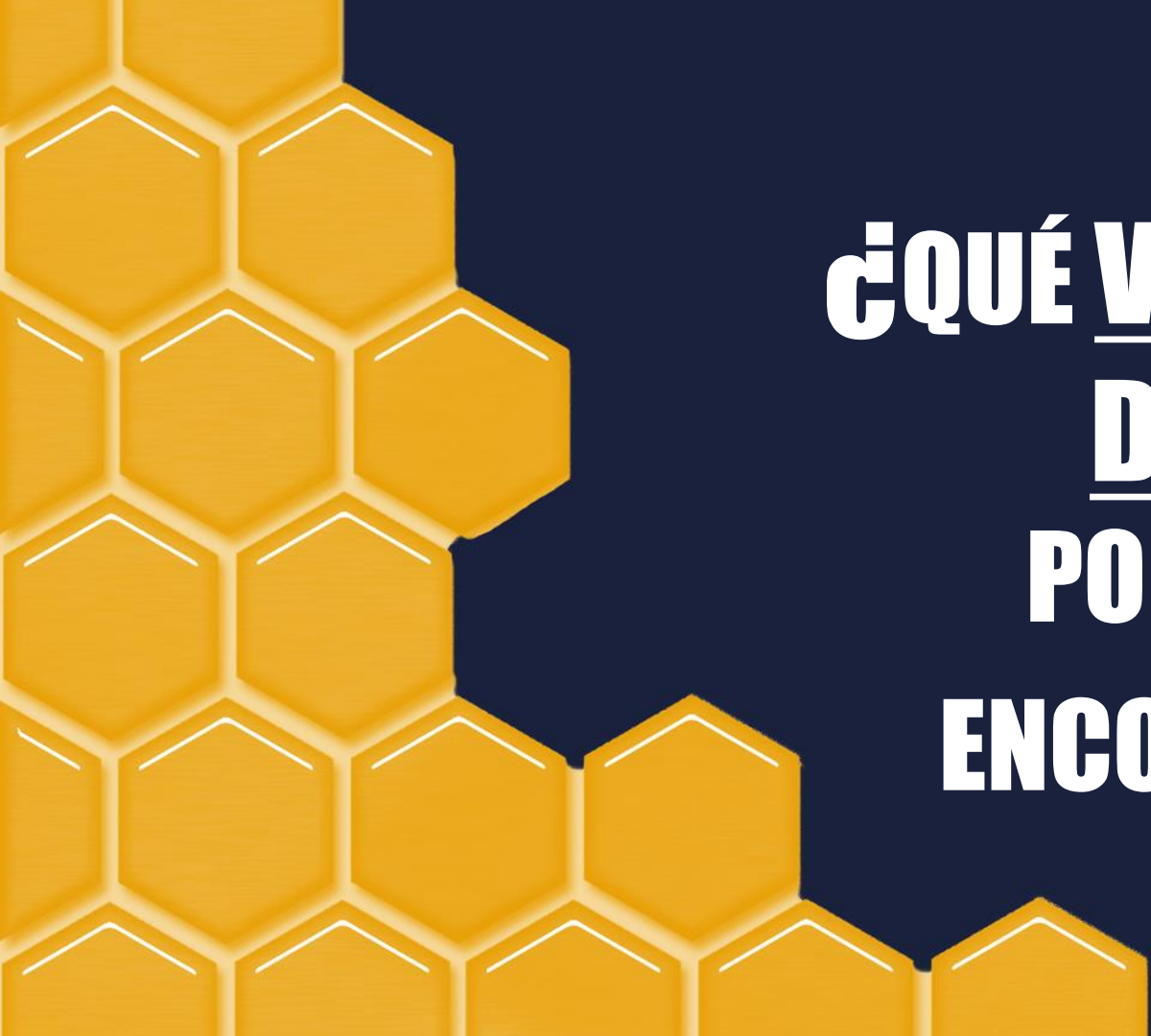
- Para la seguridad y defensa de las redes.
- Está sujeto a ataques constantes.
- Ahora se le da más importancia a las herramientas de detección.

Honeypots de Investigación

- Recolectan información de acciones de intrusos.
- Permiten tener una visión más clara sobre las operaciones, estrategias y motivos de los ataques.
- Difíciles de manejar pero recogen gran cantidad de información.

Honeypots según tipo de amenaza

- Trampas de correo electrónico.
- Bases de datos señuelo.
- Señuelo de malware.
- Señuelo araña.



**¿QUÉ VENTAJAS Y
DESVENTAJAS
PODEMOS
ENCONTRAR?**



1. Reducen las falsas alarmas

Uno de los mayores desafíos de la mayoría de tecnologías de detección es que generan **falsos positivos**.

Cuanto más falsas alarmas sufra un sistema de detección, más se acercará a ser una tecnología inútil.



1. Reducen las falsas alarmas

Los honeypots las reducen drásticamente simplemente porque casi cualquier actividad con honeypots es por definición **no autorizada**.

Esto hace que los honeypots sean extremadamente eficientes en la detección de ataques.



2. Datos muy valiosos

Los honeypots recogen datos cuando alguien o algo está interactuando con ellos.

Como resultado, recogen conjuntos de datos **extremadamente valiosos**.



3. Herramientas de pentesting

Los honeypot de alta interacción nos permiten hacer un examen del sistema, con el que poder descubrir puntos débiles en la seguridad del mismo.

Nos permiten implementar mejoras en el sistema real.



1. Campo de visión muy limitado

Sólo ven lo que interactúa con ellos.


No nos dirán si otra parte del sistema que no interactúa con el honeypot está comprometida o no.



2. El riesgo... ¿necesario?

Un honeypot atrae a atacantes, de eso se trata.

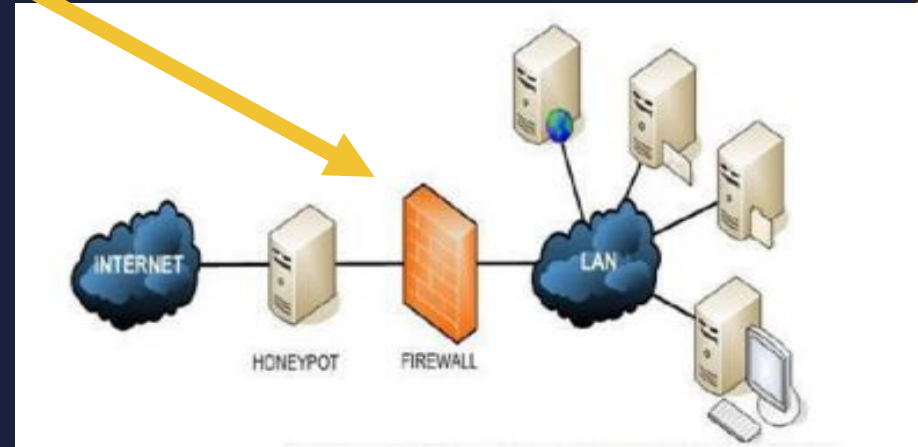
Si no lo configuramos adecuadamente podremos tener problemas.



**¿DÓNDE
PODEMOS
SITUARLO?**

Delante del firewall

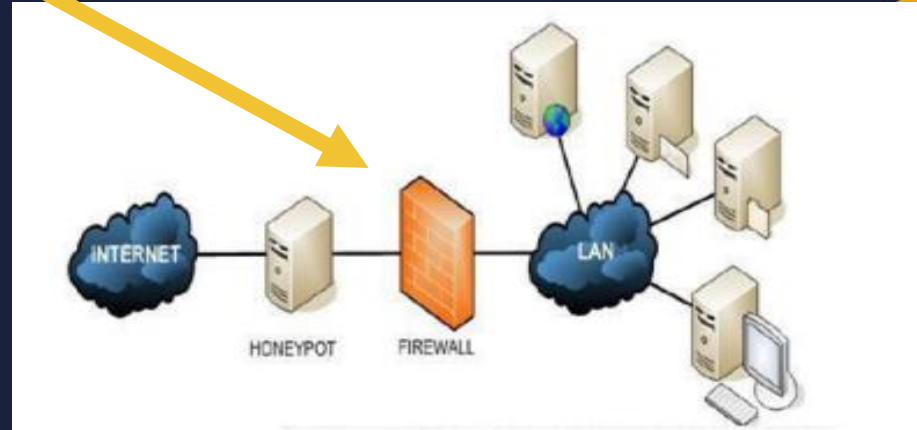
Hace que la seguridad de nuestra red interna no se vea comprometida en ningún momento.



Delante del firewall

Así evitamos ataques que vayan dirigidos a nuestra red interna PERO:

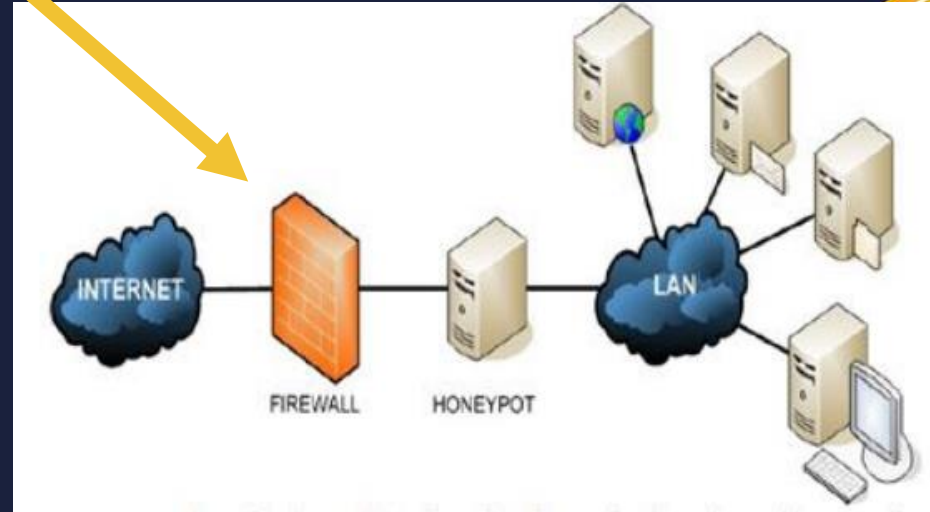
1. Consumimos ancho de banda.
2. No podremos controlar ataques internos.



Detrás del firewall

Nos permite el control de los ataques internos y externos de cualquier tipo PERO:

1. Requiere una configuración específica para dejar acceso al honeypot.
2. Posibles fallos de seguridad en la filtración de tráfico.

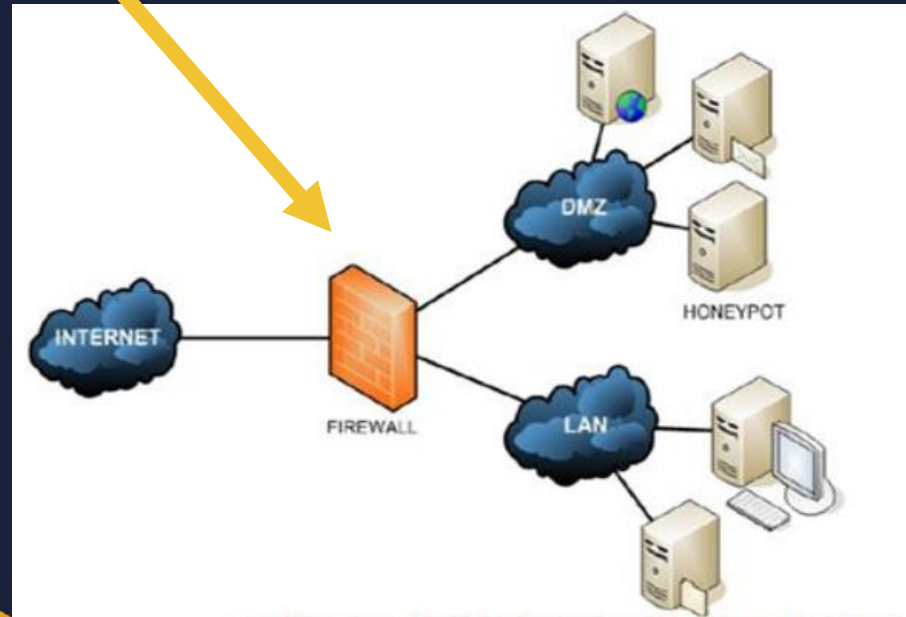


En una zona “desmilitarizada”

Así será posible la separación del honeypot de la red interna y, por tanto, de los servidores.

Nos permite detectar ataques tanto internos como externos PERO:

1. Es necesaria una pequeña modificación del firewall.





**¿DE QUÉ
SOFTWARE
DISPONEMOS?**

Software para honeypots

Creación desde “cero”



Creación a partir de herramientas



Y otras tantas muy curiosas

Demostración con Snort

Fichero de configuración /etc/snort/snort.conf

```
GNU nano 6.2 /etc/snort/snort.conf
ipvar HOME_NET 172.19.58.175/20

# Set up the external network addresses. Leave as "any" in most situations
# ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET
```

```
GNU nano 6.2 /etc/snort/snort.conf

# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET

# List of ports you run web servers on
portvar HTTP_PORTS [80,81,311,383,591,593,901,1220,1414,1741,1830,2301,2381,2809,3037,3128,3702,4343,4848,5250,6988,7

# List of ports you want to look for SHELLCODE on.
portvar SHELLCODE_PORTS !80

# List of ports you might see oracle attacks on
portvar ORACLE_PORTS 1024:

# List of ports you want to look for SSH connections on:
portvar SSH_PORTS 22

# List of ports you run ftp servers on
portvar FTP_PORTS [21,2100,3535]

# List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5600]

# List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
```


Demostración con Snort

Tenemos muchos ficheros con reglas predefinidas.

```
modejota@MSI:~$ ls /etc/snort/rules/
attack-responses.rules  community-nntp.rules      deleted.rules            netbios.rules           sql.rules
backdoor.rules         community-oracle.rules    dns.rules               nntp.rules             telnet.rules
bad-traffic.rules      community-policy.rules    dos.rules               oracle.rules            tftp.rules
chat.rules             community-sip.rules       experimental.rules      other-ids.rules        virus.rules
community-bot.rules    community-smtp.rules      exploit.rules           p2p.rules              web-attacks.rules
community-deleted.rules community-sql-injection.rules finger.rules            policy.rules           web-cgi.rules
community-dos.rules    community-virus.rules     ftp.rules              pop2.rules             web-client.rules
community-exploit.rules community-web-attacks.rules icmp-info.rules        pop3.rules            web-coldfusion.rules
community-ftp.rules    community-web-cgi.rules   imap.rules             porn.rules             web-frontpage.rules
community-game.rules   community-web-client.rules info.rules             rpc.rules             web-iis.rules
community-icmp.rules   community-web-dos.rules   local.rules            rservices.rules       web-misc.rules
community-imap.rules   community-web-iis.rules   misc.rules            scan.rules            web-php.rules
community-inappropriate.rules community-web-misc.rules multimedia.rules       shellcode.rules      x11.rules
community-mail-client.rules community-web-php.rules  mysql.rules           smtp.rules            snmp.rules
community-misc.rules   ddos.rules
```

```
4059 Snort rules read
 3385 detection rules
   0 decoder rules
   0 preprocessor rules
3385 Option Chains linked into 951 Chain Headers
+++++
```

```
+-----[Rule Port Counts]-----+
|      tcp      udp      icmp      ip      |
|  src    151    18       0       0       |
|  dst   3307   126       0       0       |
|  any    383    48       53      22      |
|  nc     27     8       16      20      |
|  s+d    12     5       0       0       |
+-----+-----+-----+-----+-----+
```


Demostración con Snort

Lanzamos con *sudo snort -A console -i eth0 -c /etc/snort/snort.conf*

```
C:\Program Files (x86)\Nmap>nmap 172.19.58.175
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-10 20:27 Hora de verano romance
Nmap scan report for 172.19.58.175
Host is up (0.00033s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:15:5D:FB:1B:41 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

```
modejota@MSI:~$ sudo snort -A console -q -i eth0 -c /etc/snort/snort.conf
06/10-20:27:45.184860  /**] [1:1418:11] SNMP request tcp /**] [Classification: Attempted Informa
tion Leak] [Priority: 2] {TCP} 172.19.48.1:63927 -> 172.19.58.175:161
06/10-20:27:45.194231  /**] [1:1421:11] SNMP AgentX/tcp request /**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 172.19.48.1:63927 -> 172.19.58.175:705
^C*** Caught Int-Signal
```

Demostración con Snort

Definimos reglas personalizadas en *local.rules*

- *alert icmp any any -> \$HOME_NET any (msg:"ICMP TEST"; sid:10000001; rev:001;)*
- *alert tcp any any -> \$HOME_NET 22 (msg:"Possible SSH brute forcing!"; flags: S+; threshold:type threshold, track by_src, count 2,seconds 60; sid:10000002; rev:001;)*

Demostración con Snort

Intentos de conexión SSH desde Windows

```
C:\Program Files (x86)\Nmap>ssh modejota@172.19.58.175
modejota@172.19.58.175's password:
Permission denied, please try again.
modejota@172.19.58.175's password:
Permission denied, please try again.
modejota@172.19.58.175's password:
modejota@172.19.58.175: Permission denied (publickey,password).
```

```
C:\Program Files (x86)\Nmap>ssh modejota@172.19.58.175
modejota@172.19.58.175's password:
Permission denied, please try again.
modejota@172.19.58.175's password:
Permission denied, please try again.
modejota@172.19.58.175's password:
modejota@172.19.58.175: Permission denied (publickey,password).
```

Alerta de posible ataque

```
modejota@MSI:~$ sudo snort -A console -q -i eth0 -c /etc/snort/snort.conf
06/10-20:36:09.741625  [**] [1:1000000002:1] Possible SSH brute forcing! [**] [Priority: 0] {TCP} 172.19.48.1:33524 -> 172.19.58.175:22
```

Demostración con Snort

Pings desde Windows

```
C:\Users\Usuario>ping 172.19.58.175
```

```
Haciendo ping a 172.19.58.175 con 32 bytes de datos:  
Respuesta desde 172.19.58.175: bytes=32 tiempo<1m TTL=64  
Respuesta desde 172.19.58.175: bytes=32 tiempo<1m TTL=64  
Respuesta desde 172.19.58.175: bytes=32 tiempo<1m TTL=64  
Respuesta desde 172.19.58.175: bytes=32 tiempo<1m TTL=64
```

```
Estadísticas de ping para 172.19.58.175:
```

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),
```

```
Tiempos aproximados de ida y vuelta en milisegundos:
```

```
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

```
C:\Users\Usuario>|
```

Avisar por correo

output alert_email:
<SMTP_SERVER_IP>,
<SENDER_EMAIL>,
<RECEIVER_EMAIL>,
<EMAIL_SUBJECT>

```
modejota@MSI:~$ sudo snort -A console -q -i eth0 -c /etc/snort/snort.conf
```

```
06/11-11:26:37.552144  [**] [1:10000001:1] ICMP TEST [**] [Priority: 0] {ICMP} 172.19.48.1 -> 172.19.58.175  
06/11-11:26:37.552170  [**] [1:10000001:1] ICMP TEST [**] [Priority: 0] {ICMP} 172.19.58.175 -> 172.19.48.1  
06/11-11:26:38.640496  [**] [1:10000001:1] ICMP TEST [**] [Priority: 0] {ICMP} 172.19.48.1 -> 172.19.58.175  
06/11-11:26:38.640526  [**] [1:10000001:1] ICMP TEST [**] [Priority: 0] {ICMP} 172.19.58.175 -> 172.19.48.1  
06/11-11:26:39.746596  [**] [1:10000001:1] ICMP TEST [**] [Priority: 0] {ICMP} 172.19.48.1 -> 172.19.58.175  
06/11-11:26:39.746632  [**] [1:10000001:1] ICMP TEST [**] [Priority: 0] {ICMP} 172.19.58.175 -> 172.19.48.1  
06/11-11:26:40.848791  [**] [1:10000001:1] ICMP TEST [**] [Priority: 0] {ICMP} 172.19.48.1 -> 172.19.58.175  
06/11-11:26:40.848824  [**] [1:10000001:1] ICMP TEST [**] [Priority: 0] {ICMP} 172.19.58.175 -> 172.19.48.1
```

Otros logs más detallados

```
WARNING: No preprocessors configured for policy 0.  
06/11-11:42:45.891721 172.19.48.1:32824 -> 172.19.58.175:80  
TCP TTL:128 TOS:0x0 ID:61533 TPlen:20 DgMlen:52 DF  
*****S* Seq: 0x85A8F4A3 Ack: 0x0 Win: 0xFAF0 TcpLen: 32  
TCP Options (6) => MSS: 1460 NOP WS: 8 NOP NOP SackOK  
=====
```

A decorative graphic on the left side of the slide consisting of a grid of yellow hexagons. The hexagons are arranged in a way that they appear to be part of a larger honeycomb structure, with some hexagons missing or cut off at the edges, creating a jagged, organic shape. The hexagons have a slight 3D effect with a darker yellow outline and a lighter yellow fill.

CONCLUSIONES

FINALES