



JAVIER DÍAZ MORENO
17 DE DICIEMBRE DE 2025

DETECCIÓN DE INTRUSIONES EN UN SISTEMA DE INVENTARIO
DE PLANTA

Tutor: Francisco Javier Artés Palacios

CFG ASIR (Administración de Sistemas Informáticos en Red)

DETECCIÓN DE INTRUSIONES EN UN SISTEMA DE INVENTARIO DE PLANTA



ÍNDICE

INTRODUCCIÓN.....	1
CONFIGURACIÓN PRINCIPAL	2
ATAQUE CON KALI LINUX	3
ATAQUE CON ALPINE LINUX.....	4

INTRODUCCIÓN

Este proyecto es un sistema state of the art del montaje del SOC, en los ciclos de SMR2 y ASIR1 y ASIR2. En estos ciclos nombrados, se realizó el montaje de un SOC, con la herramienta de Snort en la versión 2, logstash, elasticsearch y la herramienta Kibana. Con el S.O de KaliLinux de Ubuntu.

Partiendo del SOC inicial, este nuevo escenario es un SOC con bastionado en la que se entra la base de datos de la que podría ser una empresa (el inventario), con los siguientes avances: la actualización de Snort con la versión 3, logstash con correcciones en filtros y entradas, Elasticsearch que tiene una IA integrada y un mejor análisis vectorial y la instalación de la herramienta de visualización de datos gráfica Grafana, la instalación de la base de datos de Mariadb. Así como una nueva máquina de ataques de malware (llamada malísima, con el S.O de Alpine Linux)

¿SOC, Snort, Logstash, Elasticsearch, Grafana, Mariadb?

El SOC “Cerebro” Es el centro de operaciones de seguridad, un equipo especializado y un conjunto de herramientas que monitorizan, detectan, analizan y responden a incidentes de seguridad en tiempo real.

Snort: Inspecciona el tráfico de red en tiempo real y lo compara contra reglas definidas Puede generar alertas o bloquear tráfico sospechoso.

Logstash: Una herramienta de ingestión y procesamiento de datos como por ejemplo los logs de Snort

Elasticsearch: Un motor de búsqueda y análisis de datos distribuido. Almacena grandes volúmenes de datos (logs, métricas, eventos) y permite consultarlos de forma rápida y flexible.

Grafana: Una plataforma de visualización y monitoreo que se conecta a múltiples fuentes de datos (incluido Elasticsearch) y permite crear dashboards interactivos con gráficas, para detectar alertas y paneles.



A parte del SOC, he instalado Mariadb: Una base de datos relacional, que almacena y gestiona datos estructurados en tablas, permitiendo consultas SQL. En esta base de datos se encuentra el inventario de planta de la empresa



EL SOC, se compone de las siguientes máquinas virtuales

- router. (Sandbox) Conexión LAN/WAN. Esta máquina tiene dos adaptadores virtuales de red, el primero en red interna, para que los ataques se queden ahí y no haya entrada ni salida y la segunda en adaptador puente para poder salir al exterior y descargar contenido
- kalisoc. Máquina víctima bastionada con un SOC, conectada a la LAN interna. Kalisoc sólo tiene una red interna, para poder comunicarse con el router y kalitest y sin salida al exterior
- kalitest. Máquina atacante en LAN interna. Kalitest sólo tiene una red interna, para poder comunicarse con el router y kalisoc y sin salida al exterior
- malisima. Máquina adicional de ataque a kalisoc, inyecta malware por los puertos 80,21,22. Tiene diferentes características:
 - Se utiliza para inyectar malware
 - Pesa muy poco (300 Mbs) por lo que se suele utilizar para inyectar por un usb,un mail...

-Ping de la muerte, es un ataque por el comando ping, pero con un tamaño anómalo de datos 6550 Mg

-En esta máquina no hace querys porque con eso se detecta que es un hacker al ejecutar comandos a mano

PUNTO 2

Ficheros de configuración de snort:

```
sudo nano /etc/snort/snort.lua

#####
# En la sección "configure defaults":
#####

HOME_NET = '10.1.1.0/24'

#####
# En la sección "Configure Detection":
#####

ips =
{
    mode = "tap",
    enable_builtin_rules = true,
    rules = [
        include /etc/snort/rules/local.rules
    ],
    variables = default_variables
}

#####
# En la sección "configure outputs":
#####

alert_fast = {                                Crear manualmente el fichero de alertas y darle permisos de lectura y escritura para todos los usuarios:
    file = true,
    format = csv
}
sudo touch /alert_fast.txt
sudo chmod 666 /alert_fast.txt
```

```
sudo nano /etc/systemd/system/snort.service
```

Incluir este contenido en el fichero de servicio en cuestión:

```
#####
[Unit]
Description=snort

[Service]
ExecStart=/usr/sbin/snort -A alert_fast -q -v -i eth0 -c /etc/snort/snort.lua --daq afpacket

[Install]
WantedBy=multi-user.target

#####
```

kali@kalisoc: ~

Archivo Acciones Editar Vista Ayuda

GNU nano 8.4 /etc/snort/rules/local.rules

#BATERIA DE REGLAS DE SNORT

#

```
# Regla para detectar un ping (ICMP)
alert icmp any any → $HOME_NET any (msg:";Trafico ICMP!"; sid:3000001; rev:1;)

# Regla para detectar un SSH y un SFTP (TCP)
alert tcp any any → any 22 (msg:";Acceso SSH/SFTP!"; sid:3000002; rev:1;)

# Regla para detectar un Ping of Death (Ping de la muerte)
alert icmp any any → any any (
    msg:"ICMP Ping of Death (tamaño anómalo)";
    dsize:>1400;
    sid:3000003;
    rev:1;
)

# Regla para detectar un FTP (TCP)
alert tcp any any → any 21 (msg:";Acceso Inseguro FTP"; sid:3000004; rev:1;)

# Regla para detectar el malware ILOVEYOU en un acceso web
alert tcp any any → any 80 (
    msg:"Detectado malware ILOVEYOU en Acceso Web";
    content:"ILOVEYOU";
    sid:3000005;
    rev:1;
)

# Regla para detectar el malware MYDOOM en un acceso web
alert tcp any any → any 80 (
    msg:"Detectado malware MYDOOM en Acceso Web";
    content:"MYDOOM";
    sid:3000006;
    rev:1;
)

# Regla para detectar el malware STUXNET en un acceso web
alert tcp any any → any 80 (
    msg:"Detectado malware STUXNET en Acceso Web";
    content:"STUXNET";
    sid:3000007;
    rev:1;
)

# Regla para detectar el malware WANNACRY en un acceso web
alert tcp any any → any 80 (
    msg:"Detectado malware WANNACRY en Acceso Web";
    content:"WANNACRY";
)
```

Regla para detectar el malware ZEUS en un acceso web

```
alert tcp any any → any 80 (
    msg:"Detectado malware ZEUS en Acceso Web";
    content:"ZEUS";
    sid:3000009;
    rev:1;
)
```

Regla para detectar el acceso remoto a la base de datos

```
alert tcp any any → any 3306 (
    msg:"Detectado Acceso Remoto al inventario";
    sid:3000010;
    rev:1;
)
```

Configuración de elasticsearch: `sudo nano /etc/elasticsearch/elasticsearch.yml`

```
#####
cluster.name: siem.ac.net
node.name: nodo01.siem.ac.net
network.host: 0.0.0.0
http.port: 9200
discovery.type: single-node
xpack.security.enabled: false
xpack.security.enrollment.enabled: false

xpack.security.http.ssl:
    enabled: false

xpack.security.transport.ssl:
    enabled: false

# Asegurarse de que está comentada la siguiente línea rela
más de una vez):
# cluster.initial_master_nodes: ["kalisoc"]

http.host: 0.0.0.0
transport.host: 0.0.0.0

#####
sudo nano /etc/elasticsearch/jvm.options.d/siem_ac_net.opt
-Xms256m
-Xmx256m
```

Configuración de logstash: `sudo nano /etc/logstash/conf.d/logstash.conf` reglas del icmp y ssh

El potente parser Logstash tiene un lenguaje de especificación de reglas de proceso de texto llamado Grok.

Patrón del Grok Debugger para el comando ping

Línea del log a procesar:

```
09/22-18:17:17.785950 [**] [1:1000001:1] ";Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 -> 10.1.1.1
```

Patrón codicioso que almacena toda la línea del log en una variable:

```
%{GREEDYDATA:cadena}
```

Resultado JSON:

```
[  
  {  
    "cadena": "09/22-18:17:17.785950 [**] [1:1000001:1] \\\";Trafico ICMP!\\\" [**] [Priority: 0] {ICMP} 10.1.1.20 -> 10.1.1.1"  
  }  
]
```

Línea de procesamiento de los logs

```
09/22-18:17:17.785950 [**] [1:1000001:1] ";Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 -> 10.1.1.1
```

```
Resultado JSON:  
[  
  {  
    "mes": 9,  
    "dia": 22,  
    "hora": 18,  
    "minutos": 17,  
    "segundos": 17.78595,  
    "cadena": "[**] [1:1000001:1] \";Trafico ICMP!\" [**] [Priority: 0]",  
    "protocolo": "ICMP",  
    "dir_a": "10.1.1.20",  
    "dir_b": "10.1.1.1"  
  },  
  null  
]
```

Pipelines:

Un pipeline o tubería tiene tres partes:

- Entrada de datos.
- Proceso de datos (con sentencias Grok).
- Salida de datos (output)

```
#####
# Pipeline general para pruebas de interconexion de modulos

input {
  file {
    path => ["/alert_fast.txt"]
    start_position => beginning
  }
}

filter {
  grok {
    match => {"message" => "%{GREEDYDATA:cadena}"}
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "logstash"
  }
}

#####
```

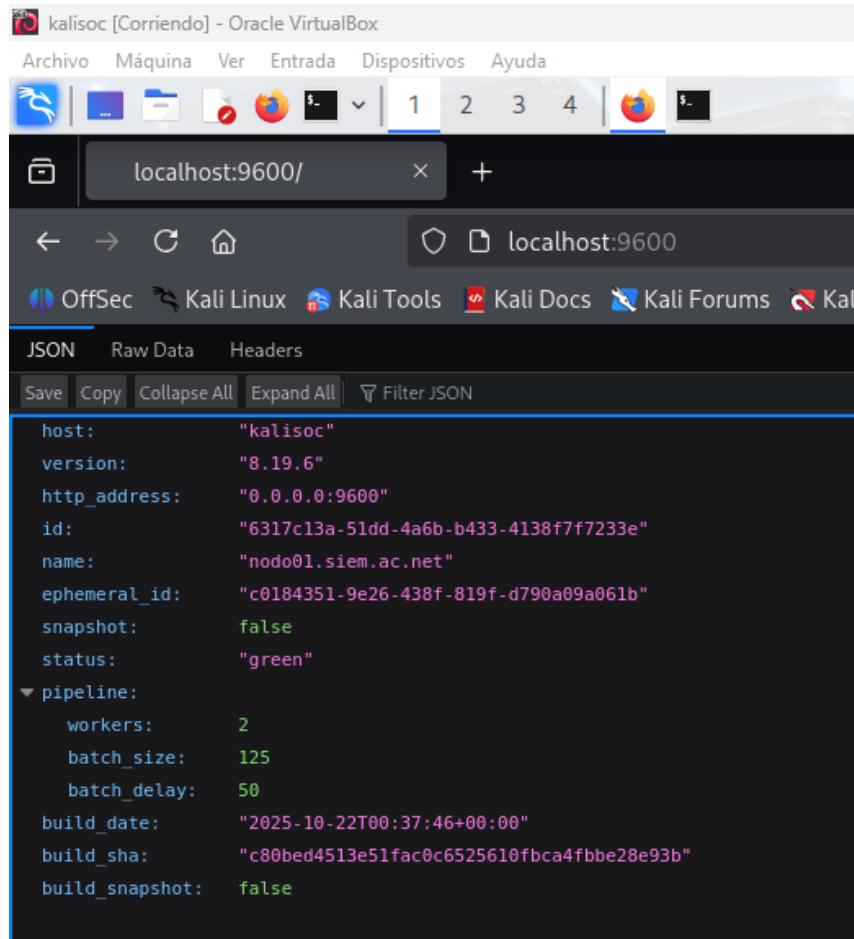
```
# Pipeline para pruebas de ping y ssh

input {
  file {
    path => ["/alert_fast.txt"]
    start_position => beginning
  }
}

filter {
  grok {
    match => {"message" => "%{MONTHNUM:mes}/%{MONTHDAY:dia}-%{HOUR:hora}:%{MINUTE:minutos}:
%{SECOND:segundos}.%{GREEDYDATA:cadena}.%{WORD:protocolo}.%{IP:dir_a}....%{IP:dir_b}"}
    match => {"message" => "%{MONTHNUM:mes}/%{MONTHDAY:dia}-%{HOUR:hora}:%{MINUTE:minutos}:
%{SECOND:segundos}.%{GREEDYDATA:cadena}.%{WORD:protocolo}.%{IP:dir_a}:%{INT:puerto_a}....%{IP:dir_b}:
%{INT:puerto_b}"}
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "logstash"
  }
}
```

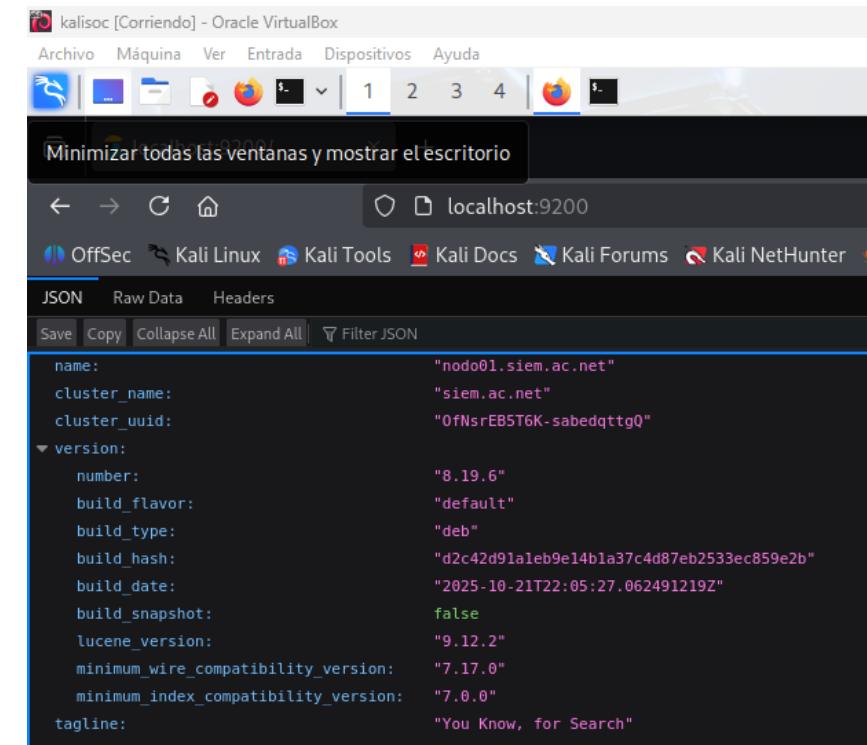
Probar que logstash escucha por el puerto 9600



A screenshot of a Firefox browser window titled "localhost:9600/". The address bar shows "localhost:9600". The page content is a JSON object representing a Logstash configuration:

```
host: "kalisoc"
version: "8.19.6"
http_address: "0.0.0.0:9600"
id: "6317c13a-51dd-4a6b-b433-4138f7f7233e"
name: "nodo01.siem.ac.net"
ephemeral_id: "c0184351-9e26-438f-819f-d790a09a061b"
snapshot: false
status: "green"
pipeline:
  workers: 2
  batch_size: 125
  batch_delay: 50
build_date: "2025-10-22T00:37:46+00:00"
build_sha: "c80bed4513e51fac0c6525610fbca4fbbe28e93b"
build_snapshot: false
```

Comprobar que los servicios de elasticsearch y logstash están activos y respondiendo por el puerto 9200



A screenshot of a Firefox browser window titled "localhost:9200". The address bar shows "localhost:9200". The page content is a JSON object representing an Elasticsearch node information:

```
name: "nodo01.siem.ac.net"
cluster_name: "siem.ac.net"
cluster_uuid: "0fNsrEB5T6K-sabedqttg0"
version:
  number: "8.19.6"
  build_flavor: "default"
  build_type: "deb"
  build_hash: "d2c42d91aleb9e14bla37c4d87eb2533ec859e2b"
  build_date: "2025-10-21T22:05:27.062491219Z"
  build_snapshot: false
  lucene_version: "9.12.2"
  minimum_wire_compatibility_version: "7.17.0"
  minimum_index_compatibility_version: "7.0.0"
tagline: "You Know, for Search"
```

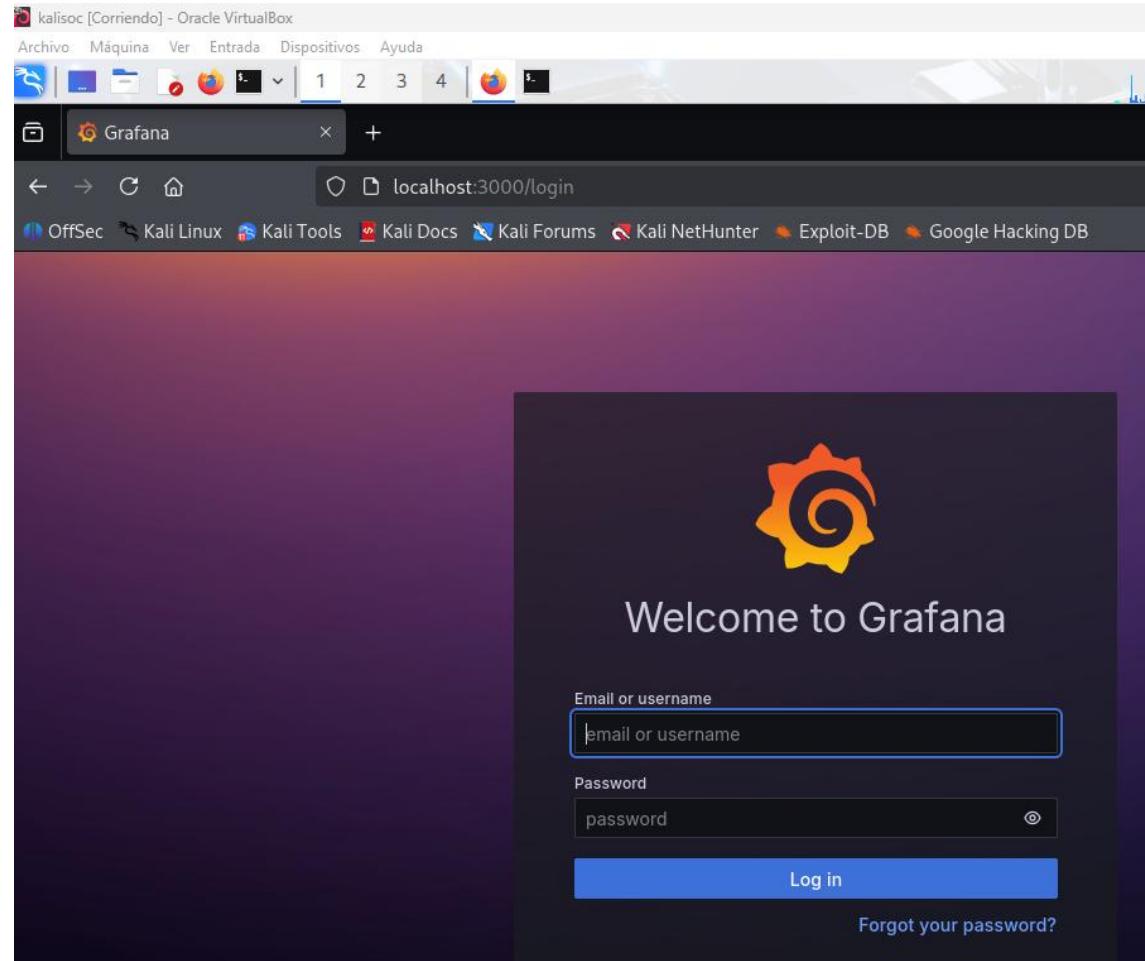
Configuración de Grafana: Descargar las fuentes y ejecutarlo en la web

```
sudo apt install -y software-properties-common  
sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
```

Sino funcionan, ejecutar el comando

```
(kali㉿kalisoc)-[~]  
$ wget -q -O - https://packages.grafana.com/gpg.key | sudo gpg --dearmor -o /usr/share/keyrings/grafana.gpg  
echo "deb [signed-by=/usr/share/keyrings/grafana.gpg] https://packages.grafana.com/oss/deb stable main" | sudo tee /etc/apt/sources.list.d/grafana.list
```

```
sudo systemctl start grafana-server
```



Ficheros de automatización de arranque/parada del SOC

ARRANCAR_SOC (crear con nano y autorizar con chmod +x) :

```
#####
sudo systemctl start snort elasticsearch logstash grafana-server
#####
```

PARAR_SOC (crear con nano y autorizar con chmod +x) :

```
#####
sudo systemctl stop snort elasticsearch logstash grafana-server
#####
```

Mariadb:

Sudo apt-install mariadb-server

Sudo mariadb-secure-installation

Editar el fichero de configuración del servidor (
 sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf

Buscar bind-address y cambiarlo de 127.0.0.1 a 0.0.0.0

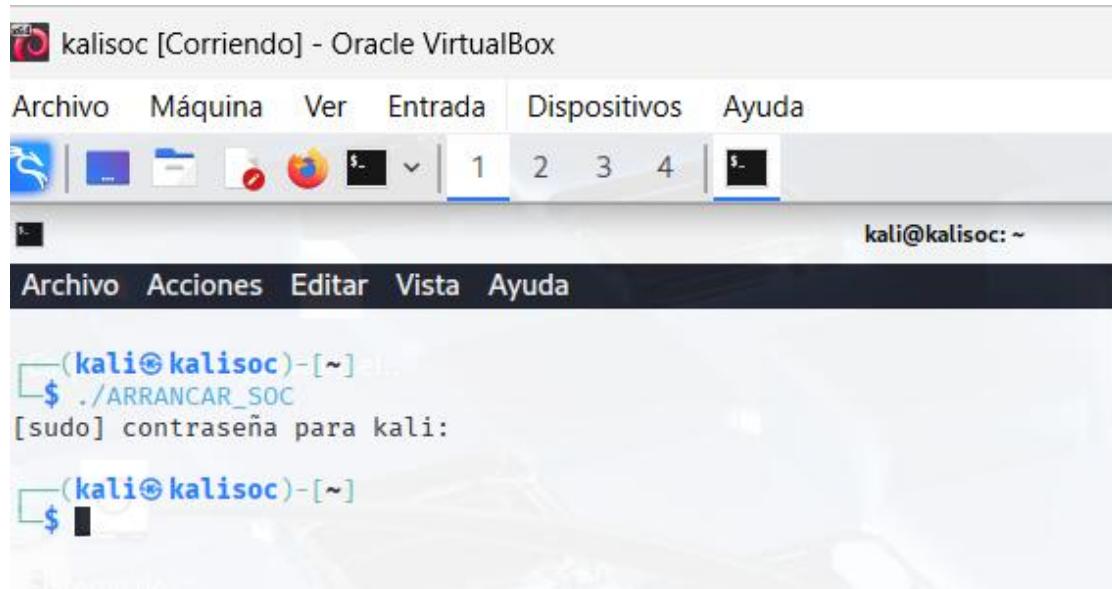
Comprobamos que escucha por el puerto 3396

```
└─(kali㉿kalisoc)─[~]
$ nmap localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 22:07 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

ATAQUE CON KALI

Ataque de comandos Ping, SSH y Acceso Remoto a la base de datos de MariaDb



The screenshot shows a terminal window titled "kalisoc [Corriendo] - Oracle VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu is a toolbar with icons for file operations and browser. A tab bar shows tabs 1 through 5, with tab 5 currently selected. The terminal prompt is "kali@kalisoc: ~". The command history shows:

```
(kali㉿kalisoc)~$ ./ARRANCAR_SOC  
[sudo] contraseña para kali:  
(kali㉿kalisoc)~$
```

(kali㉿kalisoc) [~]

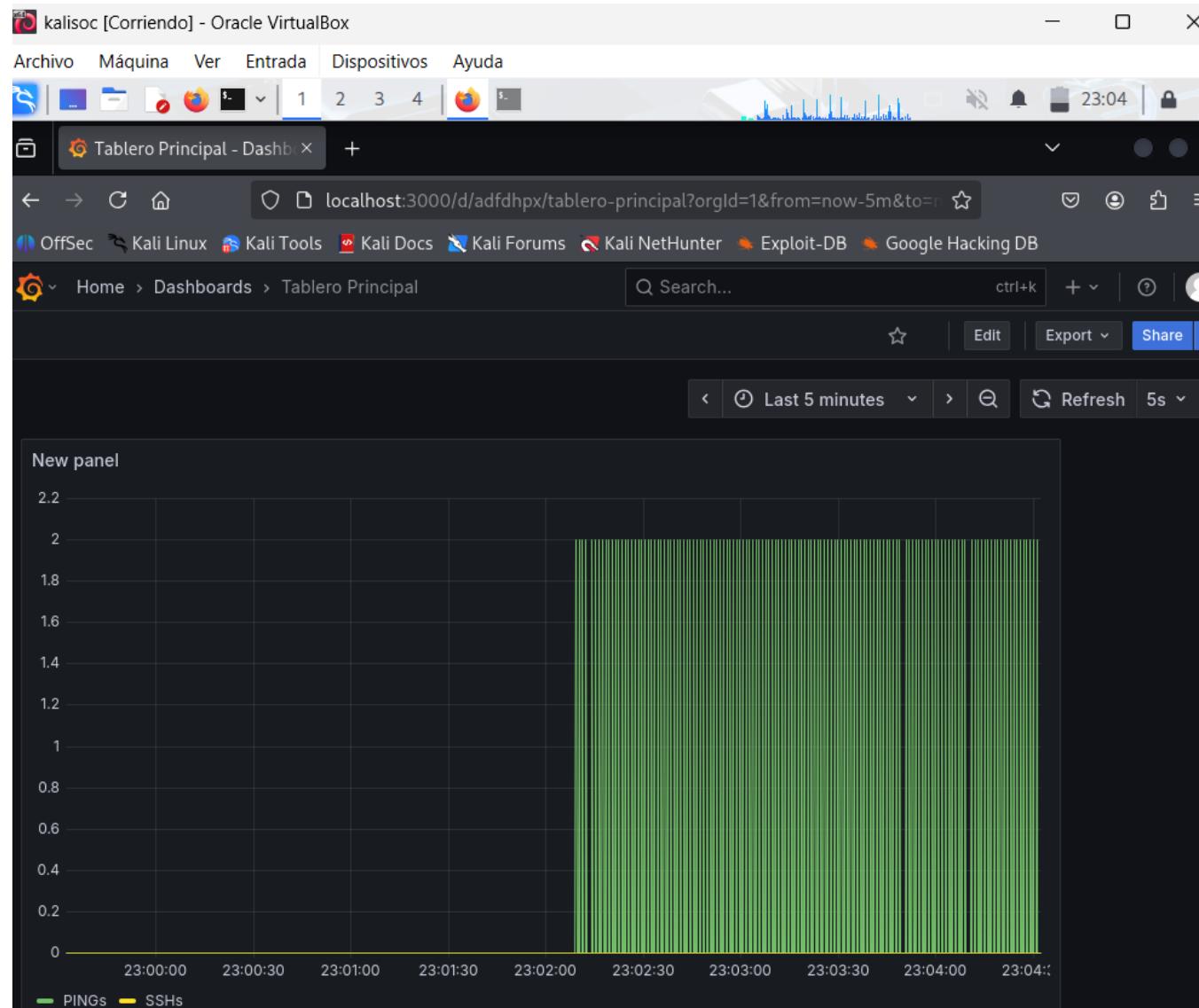
```
$ sudo tail -f /alert_fast.txt
```

12/08-22:57:55.508891 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.532809 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.550151 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.568251 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.570332 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.583576 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.586637 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.586735 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.587129 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-22:57:55.643300 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:37832 → 10.1.1.20:22
12/08-23:02:09.182431 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.10 → 10.1.1.20
12/08-23:02:09.182538 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10
12/08-23:02:10.184171 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.10 → 10.1.1.20
12/08-23:02:10.184243 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10
12/08-23:02:11.201853 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.10 → 10.1.1.20
12/08-23:02:11.201982 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10
12/08-23:02:12.258674 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.10 → 10.1.1.20
12/08-23:02:12.258734 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10

(kali㉿kalitest) [~]

```
$ ping 10.1.1.20
```

PING 10.1.1.20 (10.1.1.20) 56(84) bytes of data.
64 bytes from 10.1.1.20: icmp_seq=1 ttl=64 time=1.65 ms
64 bytes from 10.1.1.20: icmp_seq=2 ttl=64 time=0.848 ms
64 bytes from 10.1.1.20: icmp_seq=3 ttl=64 time=1.40 ms
64 bytes from 10.1.1.20: icmp_seq=4 ttl=64 time=1.15 ms



(kali㉿kalisoc) [~]

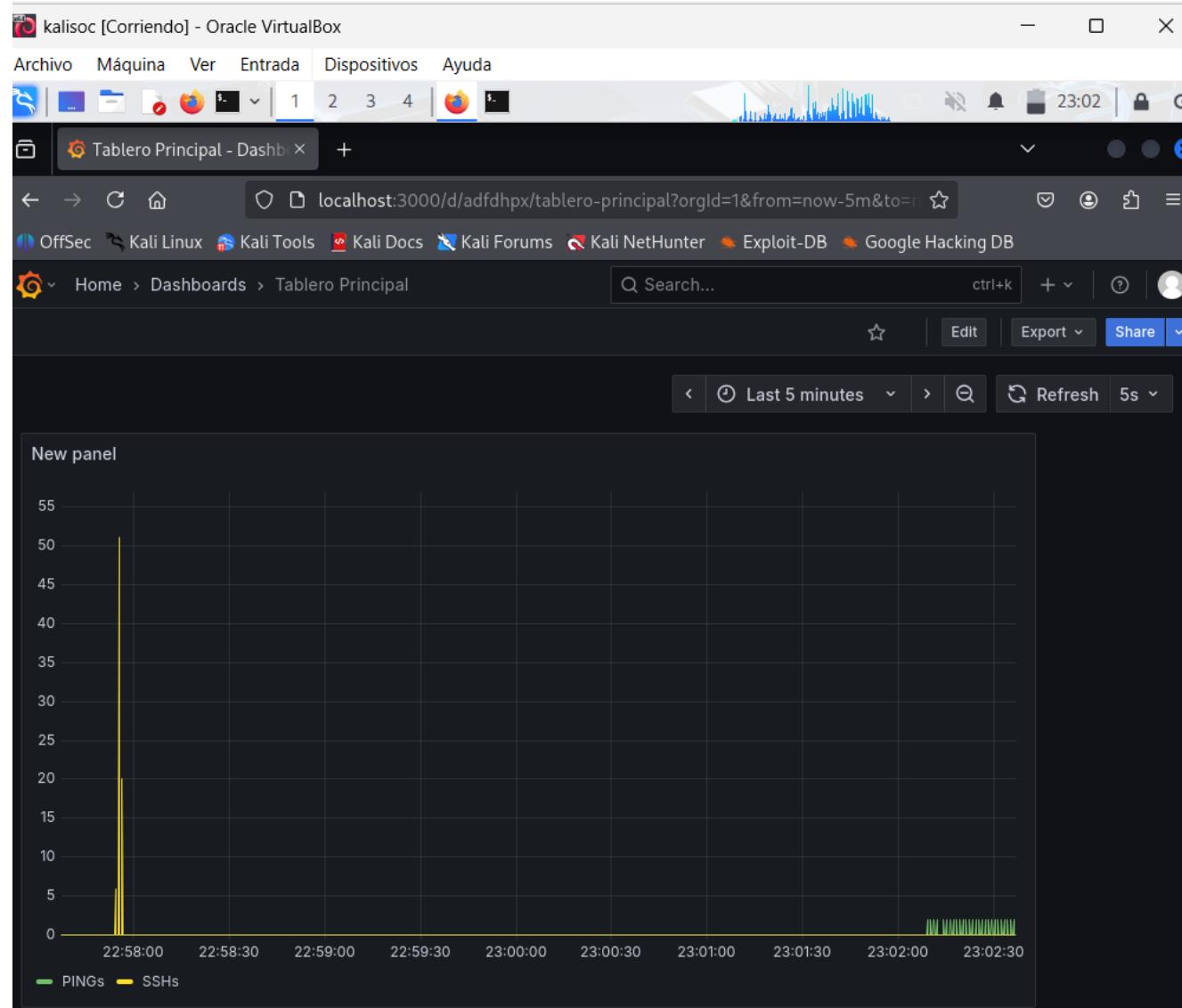
```
$ sudo tail -f /alert_fast.txt
```

12/08-23:04:51.232371 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10
12/08-23:04:52.257692 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.10 → 10.1.1.20
12/08-23:04:52.257732 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10
12/08-23:04:53.401196 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.10 → 10.1.1.20
12/08-23:04:53.401218 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10
12/08-23:04:54.403533 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.10 → 10.1.1.20
12/08-23:04:54.403610 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10
12/08-23:04:54.433090 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/08-23:04:55.404985 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.10 → 10.1.1.20
12/08-23:04:55.405009 [**] [1:3000001:1] "Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.10
12/08-23:05:26.385706 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.386812 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.387478 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.397980 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.398818 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth} →
12/08-23:05:26.410314 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.414865 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.420809 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth} →
12/08-23:05:26.422136 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.426286 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.473826 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.475139 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:05:26.527781 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22

(kali㉿kalitest) [~]

```
$ ssh 10.1.1.20
```

kali@10.1.1.20's password: █



kalisoc [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

kali@kalisoc: ~

Emulador de terminal
Usar la línea de órdenes

```

12/08-23:06:08.271659 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.292622 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.314686 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.338940 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.368621 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.391026 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.411139 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.431605 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.458057 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.478489 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.508920 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.523758 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.544083 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.565588 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.590249 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.609834 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.630628 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.650254 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.674329 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.692445 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.713543 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.734878 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.763077 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.778262 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.802277 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.830973 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.852677 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.877225 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.897322 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.920899 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.941431 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.962570 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:08.984922 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.005707 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.026006 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.046111 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.065286 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.090734 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.108631 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.130196 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.151234 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.173040 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.193224 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.214117 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.240806 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.256099 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.276142 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.297073 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.326216 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.339018 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:09.382544 [**] [1:3000002:1] "Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22

```

(kali@kalitest)-[~]

\$ ssh 10.1.1.20

kali@10.1.1.20's password:

Linux kalisoc 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.1.2.33-1kali1 (2025-06-25) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

Last login: Mon Dec 8 22:55:48 2025 from 10.1.1.10

(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely want to install supplementary tools. Learn how:
→ <https://www.kali.org/docs/troubleshooting/common-minimum-setup/>

(Run: "touch ~/.hushlogin" to hide this message)

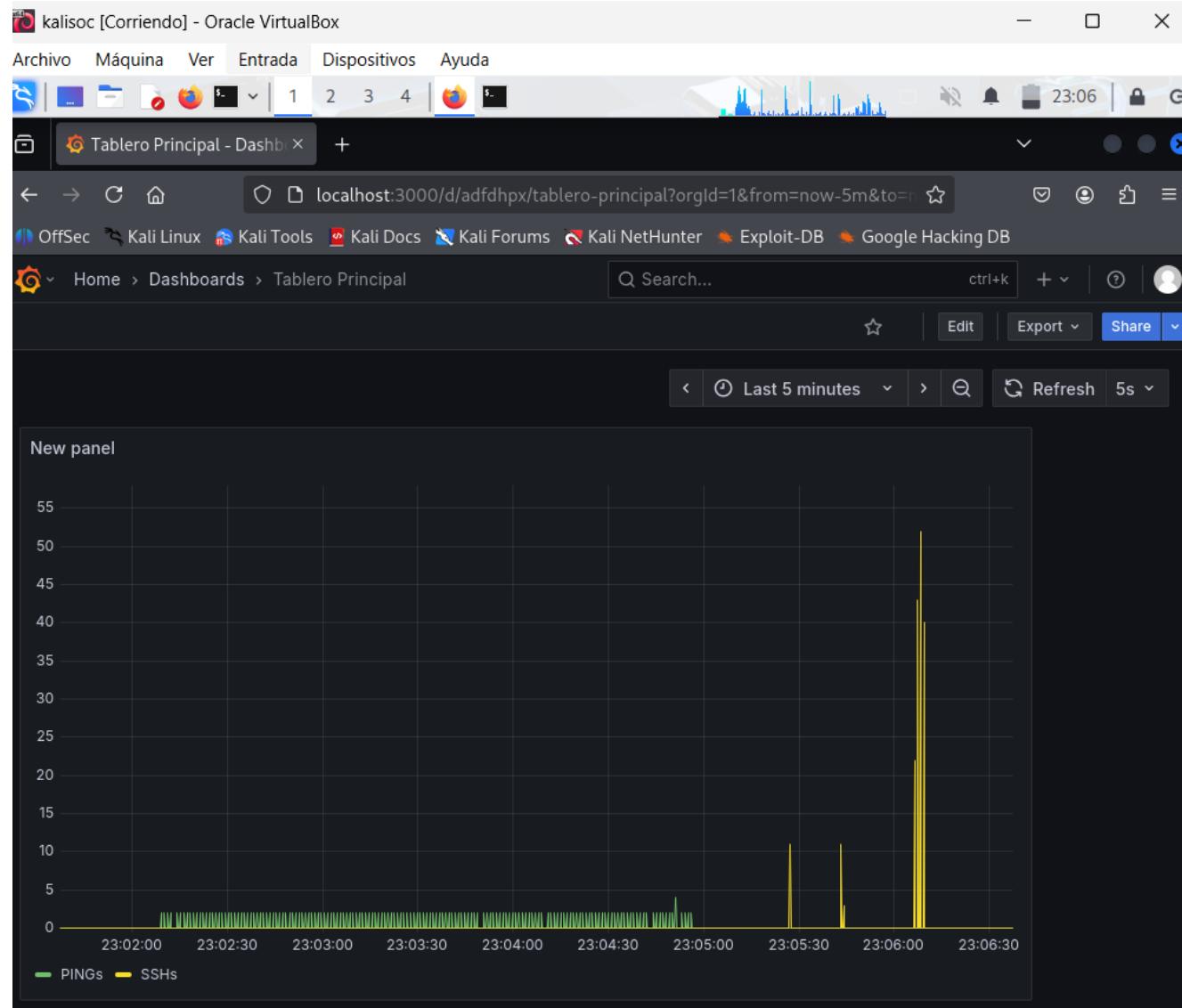
(kali@kalisoc)-[~]

\$ pwd

/home/kali

(kali@kalisoc)-[~]

\$



kalisoc [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

kali@kalisoc: ~

```
(kali㉿kalisoc) [~]
$ sudo tail -f /alert_fast.txt
12/08-23:06:52.072695 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.093606 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.113594 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.137800 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.155975 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.164597 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.168894 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.169347 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.169349 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:06:52.231752 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.10:40716 → 10.1.1.20:22
12/08-23:09:06:817378 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:06:818704 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:11.820828 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/08-23:09:12.042700 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/08-23:09:19.116992 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:19.118387 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:19.169034 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth} →
12/08-23:09:19.185999 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth} →
12/08-23:09:19.186969 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:19.193514 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:19.193975 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:19.196708 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:19.222423 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
12/08-23:09:19.276648 [**] [1:3000010:1] "Detectedo Acceso Remoto al Inventario" [**] [Priority: 0] {TCP} 10.1.1.10:55780
→ 10.1.1.20:3306
```

kalitest [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

kali@kalitest: ~

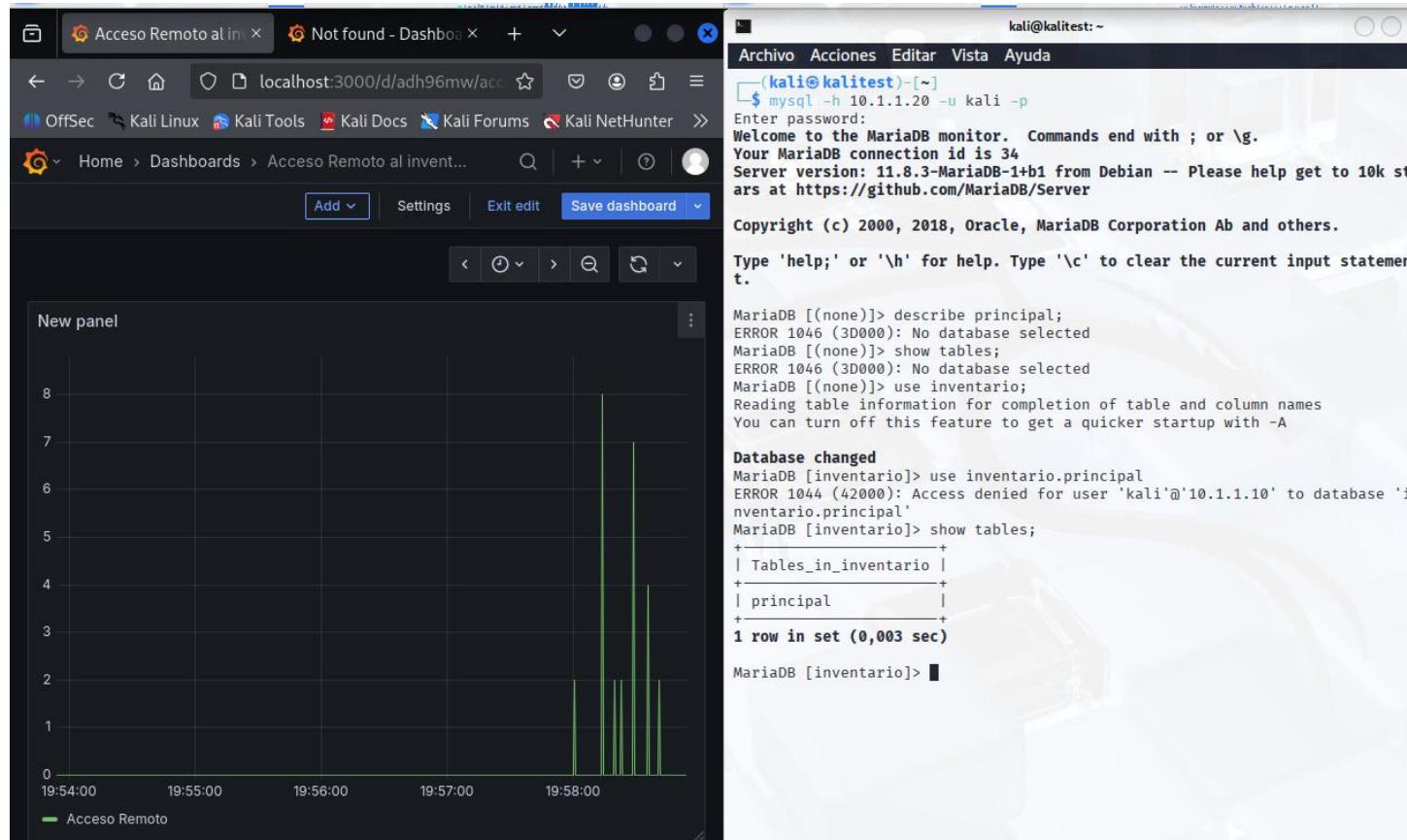
```
(kali㉿kalitest) [~]
$ mysql -h 10.1.1.20 -u kali -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Comprobamos con Grafana, que se detecta el acceso a la base de datos



ATAQUE CON ALPINE LINUX

En esta máquina aparte de atacar por los comandos del ping, ssh a gran escala, tiene añadidos los ataques por ftp, y por apache (puerto 80)

- Regla para detectar un ping (flooding)
- Regla para detectar SSH/SFTP (flooding)
- Regla para detectar un Ping of Death (ping de la muerte)
- Regla para detectar un FTP (flooding)
- Reglas para detectar la inyección de malware en el website de la máquina objetivo en este caso kalisoc

Previamente hemos instalado tanto el Vsftpd como Apache

```
sudo apt update
sudo apt-get install vsftpd
sudo systemctl start vsftpd
```

Sudo apt-get install apache2

Contenido de la máquina Alpine Linux

```
OpenRC 0.62.6 is starting up Linux 6.12.56-0-lts (x86_64)

* /proc is already mounted
* Mounting /run ... [ ok ]
* /run/openrc: creating directory
* /run/lock: creating directory
* /run/lock: correcting owner
* Remounting devtmpfs on /dev ... [ ok ]
* Mounting /dev/mqueue ... [ ok ]
* Mounting security filesystem ... [ ok ]
* Mounting debug filesystem ... [ ok ]
* Mounting persistent storage (pstore) filesystem ... [ ok ]
* Mounting bpf filesystem ... [ ok ]
* Starting busybox mdev ... [ ok ]
* Scanning hardware for mdev ...
* Loading hardware drivers ...
* Loading modules ...
* Setting system clock using the hardware clock [UTC] ...
* Checking local filesystems ...
/dev/sda3: clean, 6580/80320 files, 57532/321033 blocks
/dev/sda1: recovering journal
/dev/sda1: clean, 25/76912 files, 66671/307200 blocks
* Remounting root filesystem read/write ...
* Remounting filesystems ...
* Activating swap devices ...
* Mounting local filesystems ...
* Configuring kernel parameters ...
* Creating user login records ...
* Setting hostname ...
* Setting keymap ...
* Starting networking ...
*   lo ...
*   eth0 ...
* Seeding random number generator ...
* Seeding 256 bits and crediting
* Saving 256 bits of creditable seed for next boot
* Starting busybox syslog ...
* Starting busybox acpid ...
* Starting busybox crond ...
* Starting busybox ntpd ...
* Starting sshd ...
```

```
malisima login: root
Password:
```

```
#####
#
```

```
TFG - JAVIER DIAZ MORENO
```

```
MAQUINA MALISIMA DE ATAQUE CONTINUO
```

```
"The only easy day was yesterday"
```

```
#####
#
```

```
malisima:~# ls
ATAQUE_CONTINUO  lftp_auto.sh      ssh_auto.sh
malisima:~#
```

```
malisima:~# cat lftp_auto.sh
#!/usr/bin/expect -f

set timeout -1

set host "10.1.1.20"
set user "kalo"
set password "kili"

spawn lftp -u $user,$password $host

expect {
    "Password:" {
        send "$password\r"
        exp_continue
    }
    "lftp" {
        # ya estamos dentro de la shell de lftp
        send "dir\r"
        send "exit\r"
    }
}

interact
malisima:~#
```

```
malisima:~# cat ATAQUE_CONTINUO
# SCRIPT DE ATAQUE CONTINUO

while true; do

ping -c1 10.1.1.20

arp -d 10.1.1.10
arp -d 10.1.1.20
arp -a
ip neigh

ping -c3 -s 65500 10.1.1.20
curl "http://10.1.1.20/ILOVEYOU"
ping -c1 10.1.1.20
curl "http://10.1.1.20/MYDOOM"
ping -c1 10.1.1.20
curl "http://10.1.1.20/STUXNET"
ping -c1 10.1.1.20
curl "http://10.1.1.20/WANNACRY"
ping -c1 10.1.1.20
curl "http://10.1.1.20/ZEUS"
ping -c1 10.1.1.20
/root/ssh_auto.sh
ping -c1 10.1.1.20
/root/lftp_auto.sh

done

malisima:~# _
```

```
malisima:~# cat ssh_auto.sh
#!/usr/bin/expect -f

set timeout -1
set user "kalo"
set host "10.1.1.20"
set password "kili"

spawn ssh $user@$host

expect "password:"
send "$password\r"

expect "password:"
send "$password\r"

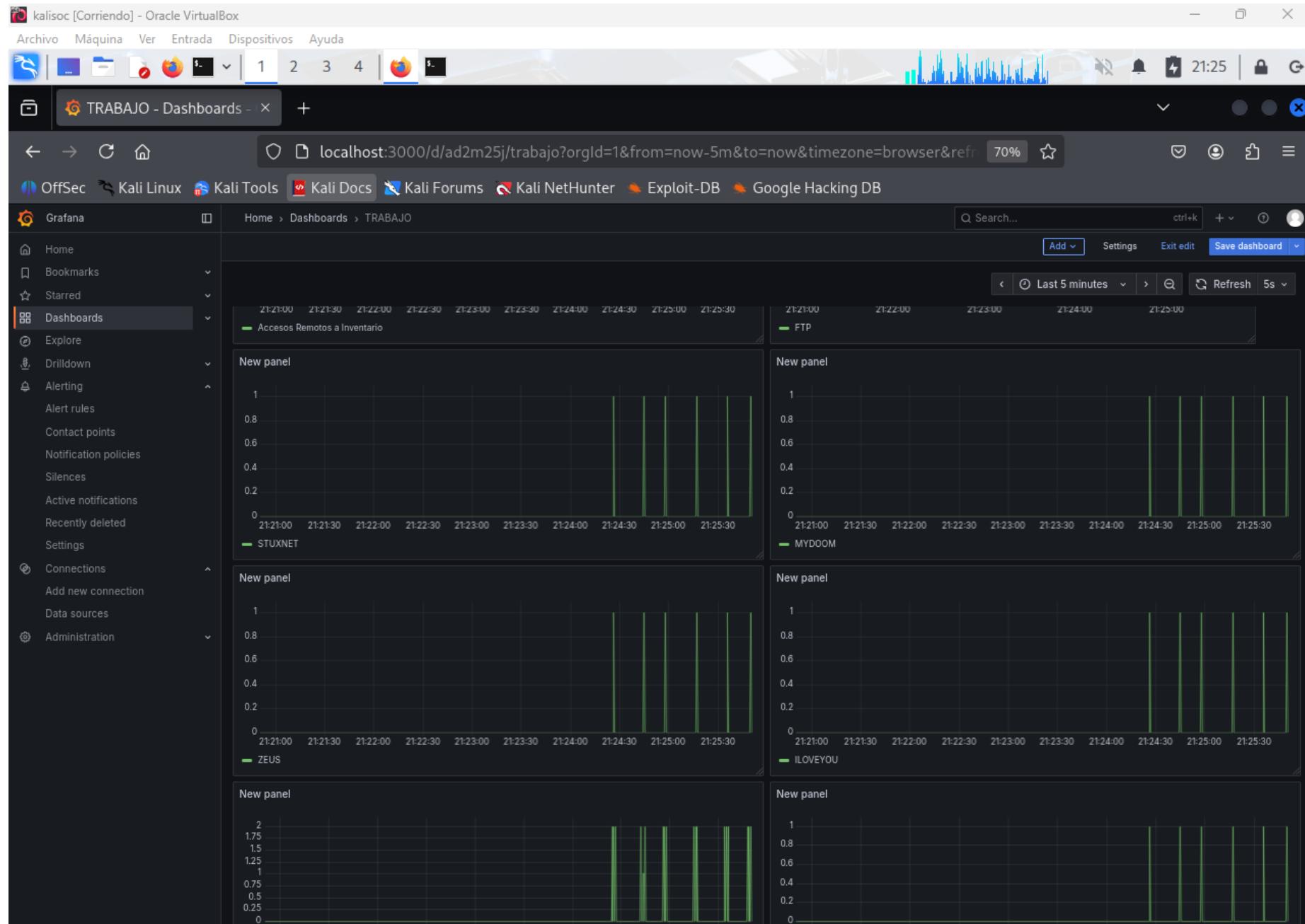
expect "password:"
send "$password\r"

interact
malisima:~#
```

```
(kali㉿kalisoc)-[~]
$ sudo tail -f /alert_fast.txt
```

12/09-19:56:51.471554 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:33446 → 10.1.1.20:22
12/09-19:56:51.474015 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:33446 → 10.1.1.20:22
12/09-19:56:51.482319 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:33446 → 10.1.1.20:22
12/09-19:56:54.924080 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:33446 → 10.1.1.20:22
12/09-19:56:58.367482 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:33446 → 10.1.1.20:22
12/09-19:56:58.368935 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:56:58.368961 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:56:58.373589 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:33446 → 10.1.1.20:22
12/09-19:56:58.391378 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:56:58.391464 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:03.415523 [**] [1:3000003:1] "ICMP Ping of Death (tamaño anómalo)" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:03.415523 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:03.421656 [**] [1:3000003:1] "ICMP Ping of Death (tamaño anómalo)" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:03.421656 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:04.433276 [**] [1:3000003:1] "ICMP Ping of Death (tamaño anómalo)" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:04.433276 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:04.438452 [**] [1:3000003:1] "ICMP Ping of Death (tamaño anómalo)" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:04.438452 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:05.457708 [**] [1:3000003:1] "ICMP Ping of Death (tamaño anómalo)" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:05.457708 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:05.462325 [**] [1:3000003:1] "ICMP Ping of Death (tamaño anómalo)" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:05.462325 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:05.470706 [**] [1:3000005:1] "Detectado malware ILOVEYOU en Acceso Web" [**] [Priority: 0] {TCP} 10.1.1.40:47316 → 10.1.1.20:80
12/09-19:57:05.476093 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:05.476172 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:05.486029 [**] [1:3000006:1] "Detectado malware MYDOOM en Acceso Web" [**] [Priority: 0] {TCP} 10.1.1.40:47320 → 10.1.1.20:80
12/09-19:57:05.494393 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:05.494509 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:05.504970 [**] [1:3000007:1] "Detectado malware STUXNET en Acceso Web" [**] [Priority: 0] {TCP} 10.1.1.40:47332 → 10.1.1.20:80
12/09-19:57:05.515113 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:05.515205 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:05.524857 [**] [1:3000008:1] "Detectado malware WANNACRY en Acceso Web" [**] [Priority: 0] {TCP} 10.1.1.40:47342 → 10.1.1.20:80
12/09-19:57:05.533854 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:05.533953 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:05.545391 [**] [1:3000009:1] "Detectado malware ZEUS en Acceso Web" [**] [Priority: 0] {TCP} 10.1.1.40:47346 → 10.1.1.20:80
12/09-19:57:05.568243 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.40 → 10.1.1.20
12/09-19:57:05.568325 [**] [1:3000001:1] "¡Trafico ICMP!" [**] [Priority: 0] {ICMP} 10.1.1.20 → 10.1.1.40
12/09-19:57:05.583052 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.587546 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.588154 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.631933 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.632571 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth} →
12/09-19:57:05.640143 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.674753 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.684218 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth} →
12/09-19:57:05.686173 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.697147 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.745438 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.757139 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22
12/09-19:57:05.768532 [**] [1:3000002:1] "¡Acceso SSH/SFTP!" [**] [Priority: 0] {TCP} 10.1.1.40:56478 → 10.1.1.20:22

Comprobamos con Grafana que se registran los ataques



Verificamos con la herramienta Wireshark

kalisoc [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Capturing from eth0

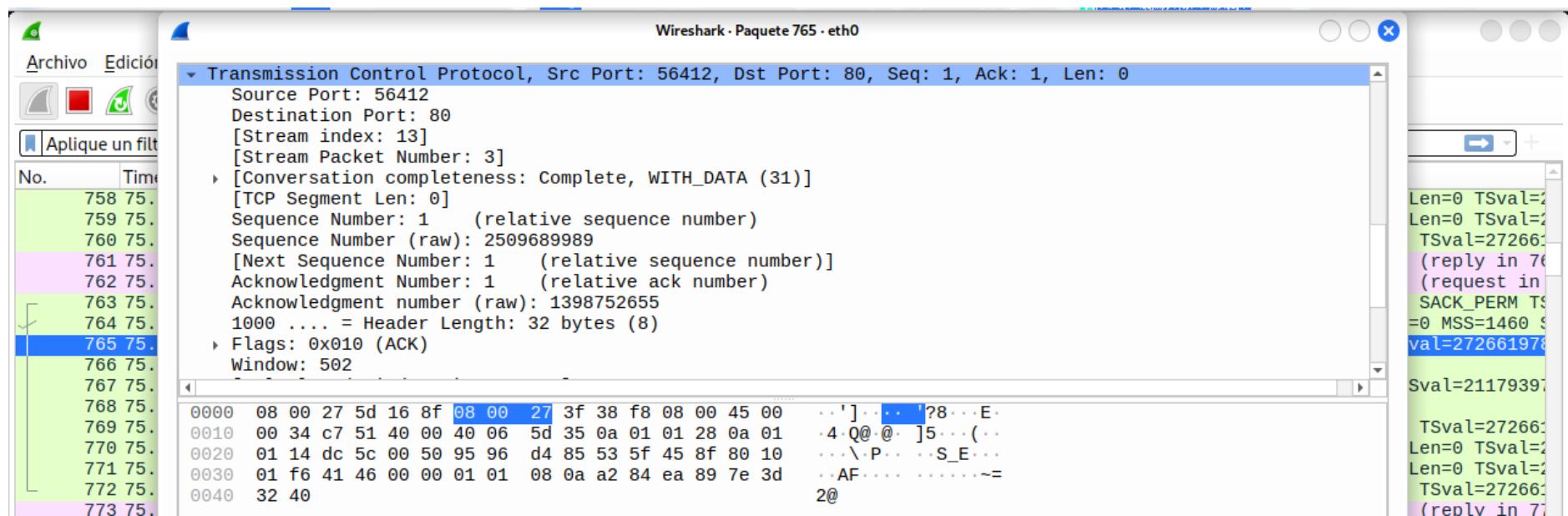
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
758	75.751906353	10.1.1.40	10.1.1.20	TCP	66	56400 → 80 [FIN, ACK] Seq=82 Ack=433 Win=64128 Len=0 TSval=272661978
759	75.752386786	10.1.1.20	10.1.1.40	TCP	66	80 → 56400 [FIN, ACK] Seq=433 Ack=83 Win=65152 Len=0 TSval=272661978
760	75.753200197	10.1.1.40	10.1.1.20	TCP	66	56400 → 80 [ACK] Seq=83 Ack=434 Win=64128 Len=0 TSval=272661978
761	75.753762688	10.1.1.40	10.1.1.20	ICMP	98	Echo (ping) request id=0x0899, seq=0/0, ttl=64 (reply in 76)
762	75.753824458	10.1.1.20	10.1.1.40	ICMP	98	Echo (ping) reply id=0x0899, seq=0/0, ttl=64 (request in 76)
763	75.757637306	10.1.1.40	10.1.1.20	TCP	74	56412 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=272661978
764	75.757842534	10.1.1.20	10.1.1.40	TCP	74	80 → 56412 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 TSval=272661978
765	75.758570475	10.1.1.40	10.1.1.20	TCP	66	56412 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=272661978
766	75.759437263	10.1.1.40	10.1.1.20	HTTP	143	GET /ZEUS HTTP/1.1
767	75.759517824	10.1.1.20	10.1.1.40	TCP	66	80 → 56412 [ACK] Seq=1 Ack=78 Win=65152 Len=0 TSval=211793978
768	75.760658627	10.1.1.20	10.1.1.40	HTTP	498	HTTP/1.1 404 Not Found (text/html)
769	75.761767340	10.1.1.40	10.1.1.20	TCP	66	56412 → 80 [ACK] Seq=78 Ack=433 Win=64128 Len=0 TSval=272661978
770	75.762652291	10.1.1.40	10.1.1.20	TCP	66	56412 → 80 [FIN, ACK] Seq=78 Ack=433 Win=64128 Len=0 TSval=272661978
771	75.763024918	10.1.1.20	10.1.1.40	TCP	66	80 → 56412 [FIN, ACK] Seq=433 Ack=79 Win=65152 Len=0 TSval=272661978
772	75.764008506	10.1.1.40	10.1.1.20	TCP	66	56412 → 80 [ACK] Seq=79 Ack=434 Win=64128 Len=0 TSval=272661978
773	75.765105840	10.1.1.40	10.1.1.20	ICMP	98	Echo (ping) request id=0x089b, seq=0/0, ttl=64 (reply in 774)
774	75.765131642	10.1.1.20	10.1.1.40	ICMP	98	Echo (ping) reply id=0x089b, seq=0/0, ttl=64 (request in 773)
775	75.773421916	10.1.1.40	10.1.1.20	TCP	74	52990 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=272661978
776	75.773542783	10.1.1.20	10.1.1.40	TCP	74	22 → 52990 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 TSval=272661978

Frame 19: Packet, 105 bytes on wire (840 bits), 105 bytes captured (105 bytes) on interface eth0 at 2013-07-10 10:11:20.000000000 UTC
Ethernet II, Src: PCSSystemtec_5d:16:8f (08:00:27:5d:16:8f), Dst: PCSSystemtec_5d:16:8f (08:00:27:5d:16:8f)
Internet Protocol Version 4, Src: 10.1.1.20, Dst: 34.36.137.203
Transmission Control Protocol, Src Port: 51910, Dst Port: 443, Seq: 1, Ack: 1, Len: 105
Transport Layer Security

0000	08 00 27 8f 0d 22 08 00	27 5d 16 8f 08 00 45 00	.. ' . " . '] .
0010	00 5b 24 c1 40 00 40 06	5e d8 0a 01 01 14 22 24	[\$ @ @ . ^ .
0020	89 cb ca c6 01 bb 48 81	d5 c2 62 79 83 88 80 18 H . . b .
0030	02 90 b7 51 00 00 01 01	08 0a 83 4f 96 f7 bb 9d	. . Q
0040	d9 e3 17 03 03 00 22 77	08 d1 dd 48 33 45 f4 5e " w . . .
0050	34 24 c0 87 44 13 0a 6c	0c 48 5b 86 86 78 4a 4b	4\$. D . l . H [
0060	57 a7 c6 a6 e7 09 35 8b	28	W 5 . (



This work is subject to the Creative Commons **Attribution - Non-Commercial - No Derivative Works** license.