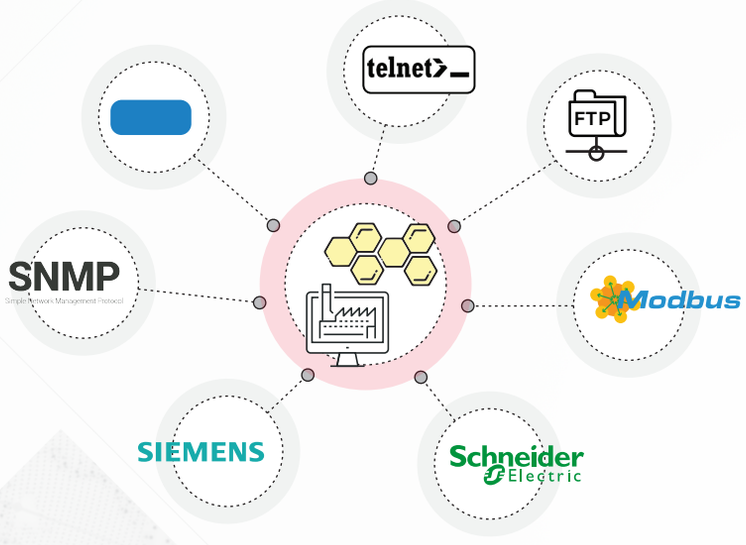
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe-cert_

Despliegue de un honeypot industrial



INSTALACIÓN DE HONEYD

INSTALACIÓN DE GIT

```
sudo apt-get install git
```

DESCARGA DE HONEYD

```
git clone https://github.com/DataSoft/Honeyd
```

INSTALACIÓN DE DEPENDENCIAS

```
sudo apt-get install libevent-dev libdumbnet-dev libpcap-dev libpcre3-dev
libedit-dev bison flex libtool automake zliblg-dev python net-tools
```

COMPILACIÓN E INSTALACIÓN DE HONEYD

```
cd Honeyd/
./autogen.sh
./configure
make
```

CREACIÓN DE DIRECTORIO PARA FICHEROS DE CONFIGURACIÓN

```
cd ..
mkdir <nombre_directorio>
```

CONFIGURACIÓN DEL HONEYPOT

DESCARGA DE SCADA HONEYNET PROJECT

```
http://www.sf.net/projects/scadahoneynet
```

MOVER DIRECTORIO SCRIPTS A LA RUTA DEL HONEYPOT

```
cd <ruta_descarga>
tar -xvzf <archivo_scadahoneynet.tar>
cp -a ./cernsacadahoneynet/files/scripts <nombre_directorio>/scripts
```

Esta última ruta se etiquetará como <ruta_scripts> para los siguientes pasos.

MODIFICACIÓN DEL SCRIPT WEB

Editar <ruta_scripts>/honeyd-http-siemens.py

```
webroot = "/var/cshoneynet/scripts/web-siemens" -> webroot = "<ruta_scripts>/web-siemens"
```

RENOMBRAR Y MODIFICAR ARCHIVO TELNET

Dentro de <ruta_scripts>

```
cp honeyd-telnet-schneider.py honeyd-telnet-siemens.py
```

Modificar fichero honeyd-telnet-siemens.py:

```
logintext = "\n\rVxWorks login: " -> logintext = "\n\rSiemens Login: "
```

MODIFICAR ARCHIVO NMAP.ASSOC

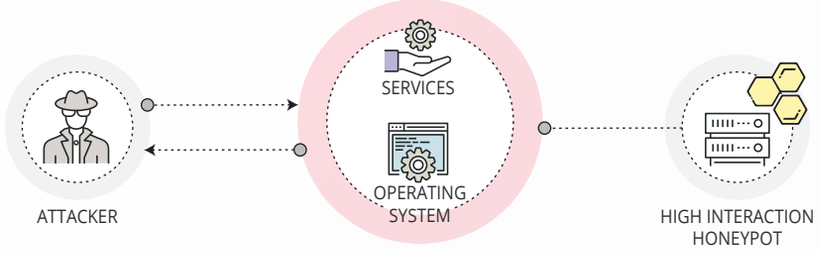
```
cat /usr/share/honeyd/nmap-os-db | grep "Siemens\ Simatic\ 300"
```

Añadir el resultado (sin Fingerprint) al final de la lista de /usr/share/honeyd/nmap.assoc. En caso de que ya esté, asegurarse de que no quede como comentario.

ARCHIVO DE CONFIGURACIÓN

Crear un archivo de configuración (<nombreFichero.conf>) dentro del directorio <nombre_directorio> e incluir las siguientes líneas de configuración:

```
create siemens
set siemens ethernet "00:1f:f8:cc:d0:23"
set siemens default tcp action closed
set siemens default udp action reset
set siemens personality "Siemens Simatic 300 programmable logic controller"
add siemens tcp port 21 "python <ruta_scripts>/honeyd-ftp-siemens.py"
add siemens tcp port 23 "python <ruta_scripts>/honeyd-telnet-siemens.py"
add siemens tcp port 80 "python <ruta_scripts>/honeyd-http-siemens.py"
add siemens tcp port 102 "python <ruta_scripts>/honeyd-s7.py"
add siemens udp port 161 " python <ruta_scripts>/honeyd-snmp-siemens.py"
add siemens tcp port 502 " python <ruta_scripts>/honeyd-modbus.py"
set siemens uptime <timestamp in seconds>
bind <ip_address> siemens
```



EJECUCIÓN DE HONEYD

```
sudo honeyd -d -p nmap-os-db -i <interfaz> -l <nombre_log.log> -f <nombreFichero.conf>
<IP_address_or_subnet > -u 0 -g 0 --disable-webserver
```