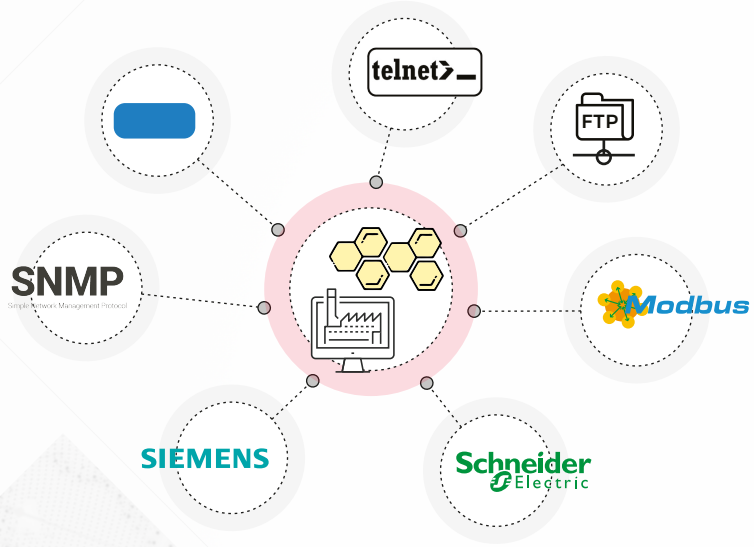
incibe_
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe-cert_

Deployment of an industrial honeypot



HONEY INSTALLATION

GIT INSTALLATION
```
sudo apt-get install git
```

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

DEPENDENCIES INSTALLATION
```
sudo apt-get install libevent-dev libdumbnet-dev libpcap-dev libpcre3-dev
libedit-dev bison flex libtool automake zlib1g-dev python net-tools
```

HONEYD COMPILATION AND INSTALLATION
```
cd Honeyd/
./autogen.sh
./configure
make
```

CREATION OF DIRECTORY FOR CONFIGURATION FILES
```
cd ..
mkdir <path_name>
```

HONEYPOT CONFIGURATION

SCADA HONEYNET PROJECT DOWNLOAD
```
http://www.sf.net/projects/scadahoneynet
```

MOVE SCRIPTS DIRECTORY TO HONEYPOT PATH
```
cd <download_path>
tar -xvzf <scadahoneynet_file.tar>
cp -a ./cernsacadahoneynet/files/scripts <path_name>/scripts
```

This last path will be labeled as <scripts_path> for the following steps.

SCRIPT WEB MODIFICATION

Edit <scripts_path>/honeyd-http-siemens.py

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

RENAME AND MODIFY TELNET FILE

Inside <scripts_path>

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

Modify honeyd-telnet-siemens.py file:

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

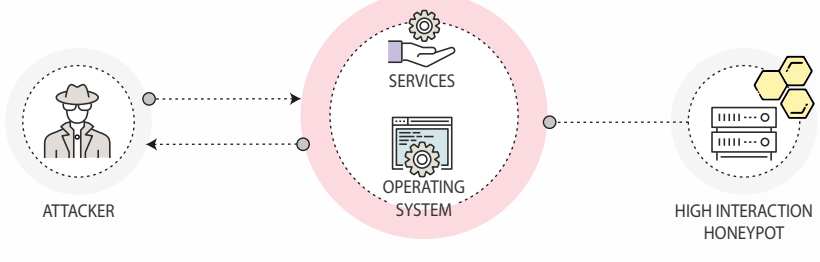
MODIFY NMAP.ASSOC FILE
```
cat /usr/share/honeyd/nmap-os-db | grep "Siemens\ Simatic\ 300"
```

Add the result (without Fingerprint) to the end of the /usr/share/honeyd/nmap.assoc list. In case it is already there, make sure that it does not remain as a comment.

CONFIGURATION FILE

Create a configuration file (<filename.conf>) inside the directory <path_name> and including the following configuration lines:

```
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 <scripts_path>/honeyd-ftp-siemens.py"
add siemens tcp port 23 "python <scripts_path>/honeyd-telnet-siemens.py"
add siemens tcp port 80 "python <scripts_path>/honeyd-http-siemens.py"
add siemens tcp port 102 "python <scripts_path>/honeyd-s7.py"
add siemens udp port 161 " python <scripts_path>/honeyd-snmp-siemens.py"
add siemens tcp port 502 " python <scripts_path>/honeyd-modbus.py"
set siemens uptime <timestamp in seconds>
bind <ip_address> siemens
```



RUNNING HONEYD

```
sudo honeyd -d -p nmap-os-db -i <interface> -l <log_name.log> -f <filename.conf>
<IP_address_or_subnet> -u 0 -g 0 --disable-webserver
```