Documentation
SSH attack on different Honeypots

Erika Kovács
2023.

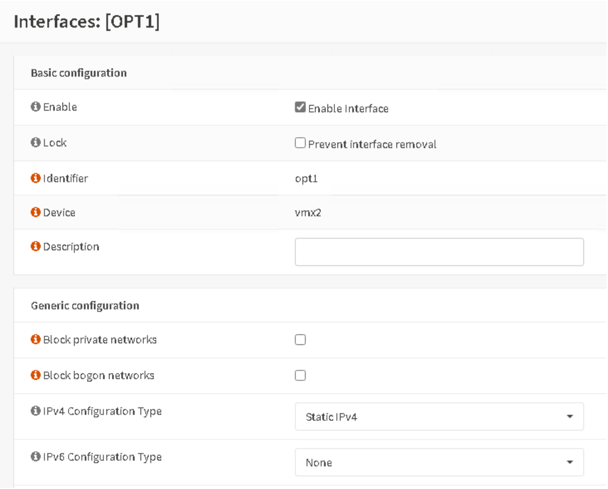
Table of content

Opnsense

1. Open the Opnsense Console in Vcenter and enter the option 1 as “Assign interfaces”.
2. Answer the following questions:

```
Do you want to configure LAGGs now? - NO
Do you want to configure VLANs now? - NO
Enter the WAN interface name: vmx0
Enter the LAN interface name: vmx1
Enter the Optional Interface name: vmx2
Press Enter
Do you want to proceed? - YES
```

3. Browse to 10.10.26.1 from Windows and log in using your account.
4. Configure the OPT1 interface at the *Interfaces / OPT1* and set the IP address for OPT1 interface.
   (You have another option if you enter the option 2 at Web Console)



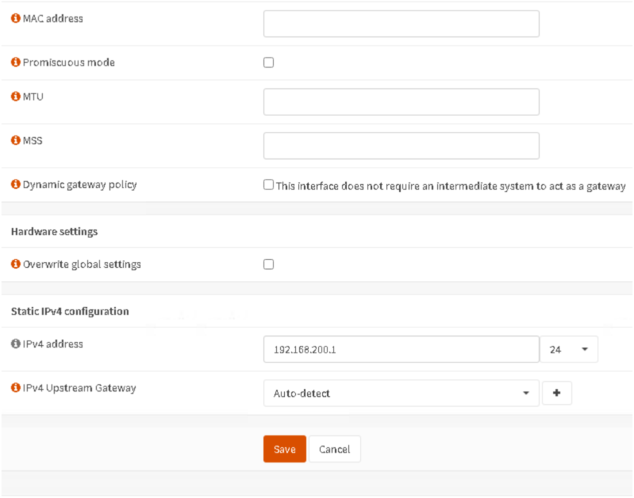
Interfaces: [OPT1]

Basic configuration

Enable	☑ Enable Interface
Lock	□ Prevent interface removal
Identifier	opt1
Device	vmx2
Description	

Generic configuration

Block private networks	□
Block bogon networks	□
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None



MAC address	
Promiscuous mode	□
MTU	
MSS	
Dynamic gateway policy	□ This interface does not require an intermediate system to act as a gateway

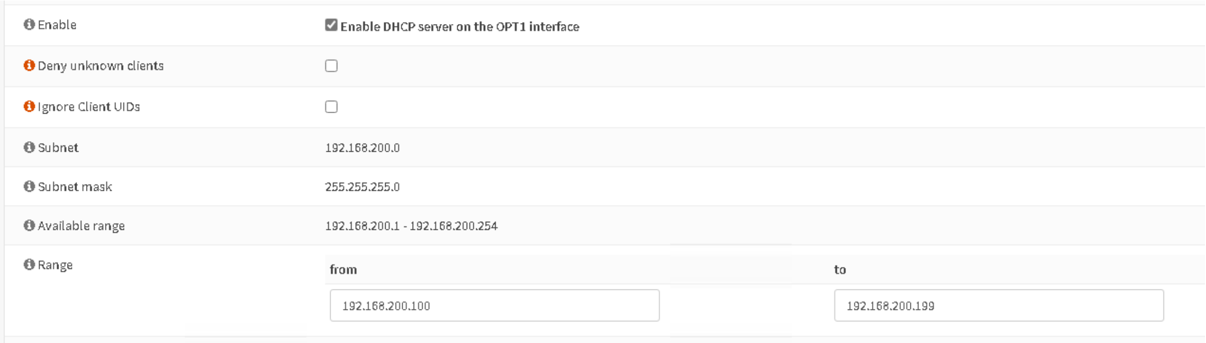
Hardware settings

Overwrite global settings	□

Static IPv4 configuration

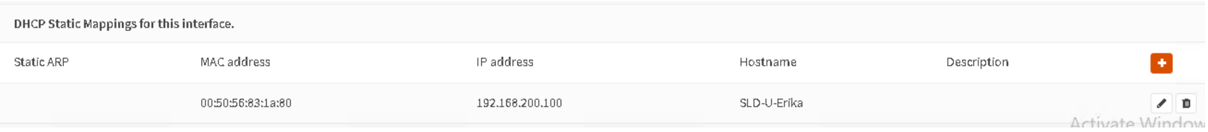
IPv4 address	192.168.200.1 / 24
IPv4 Upstream Gateway	Auto-detect

5. Configure DHCP at *Services / DHCPv4 / [OPT1]*



Enable	☑ Enable DHCP server on the OPT1 interface
Deny unknown clients	☐
Ignore Client UIDs	☐
Subnet	192.168.200.0
Subnet mask	255.255.255.0
Available range	192.168.200.1 - 192.168.200.254
Range	from: 192.168.200.100 to: 192.168.200.199

6. Set fix lease for the 192.168.200.100 IP address



DHCP Static Mappings for this interface.

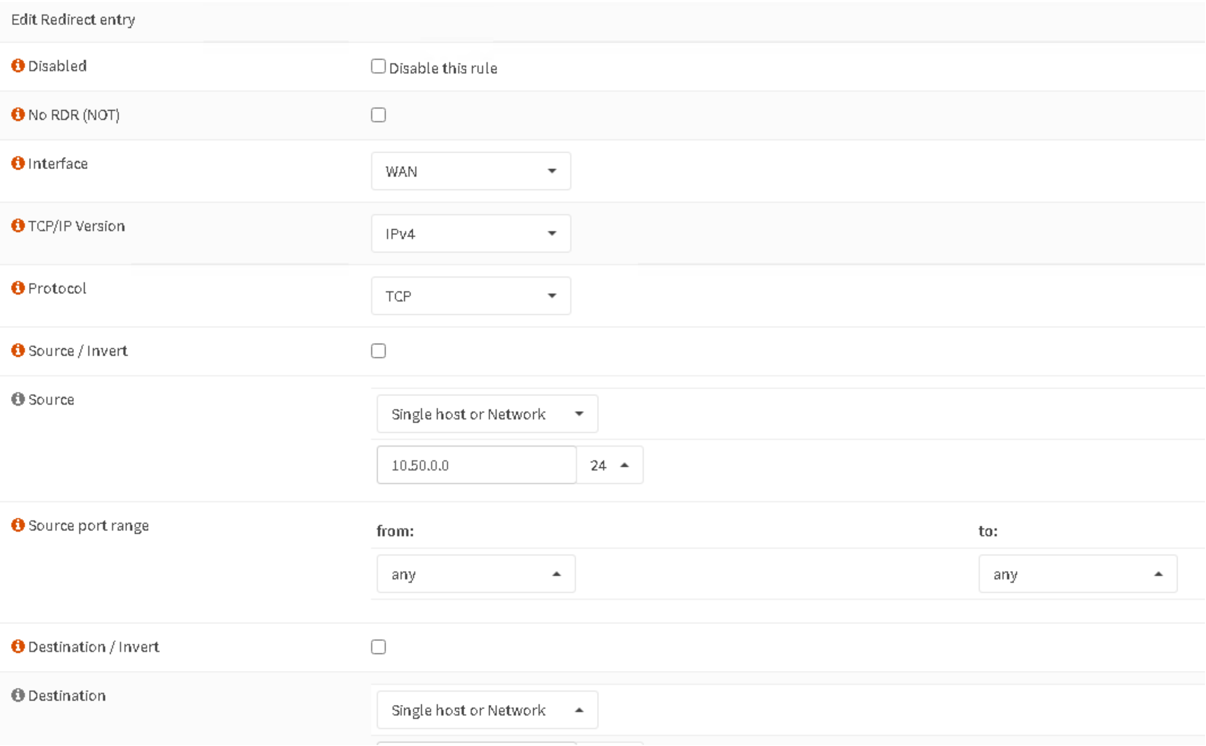
Static ARP	MAC address	IP address	Hostname	Description
	00:50:56:83:1a:80	192.168.200.100	SLD-U-Erika	

Note: MAC Address you can find with the command “*ip a”* located in the line starting with *“link/ether”* on SLD-U-Erika.

7. In the Opnsense Web console enter the number 11 to reload all services.
8. Check the IP address with the command “*ip a”* or *“ifconfig”* on SLD-U-Erika.

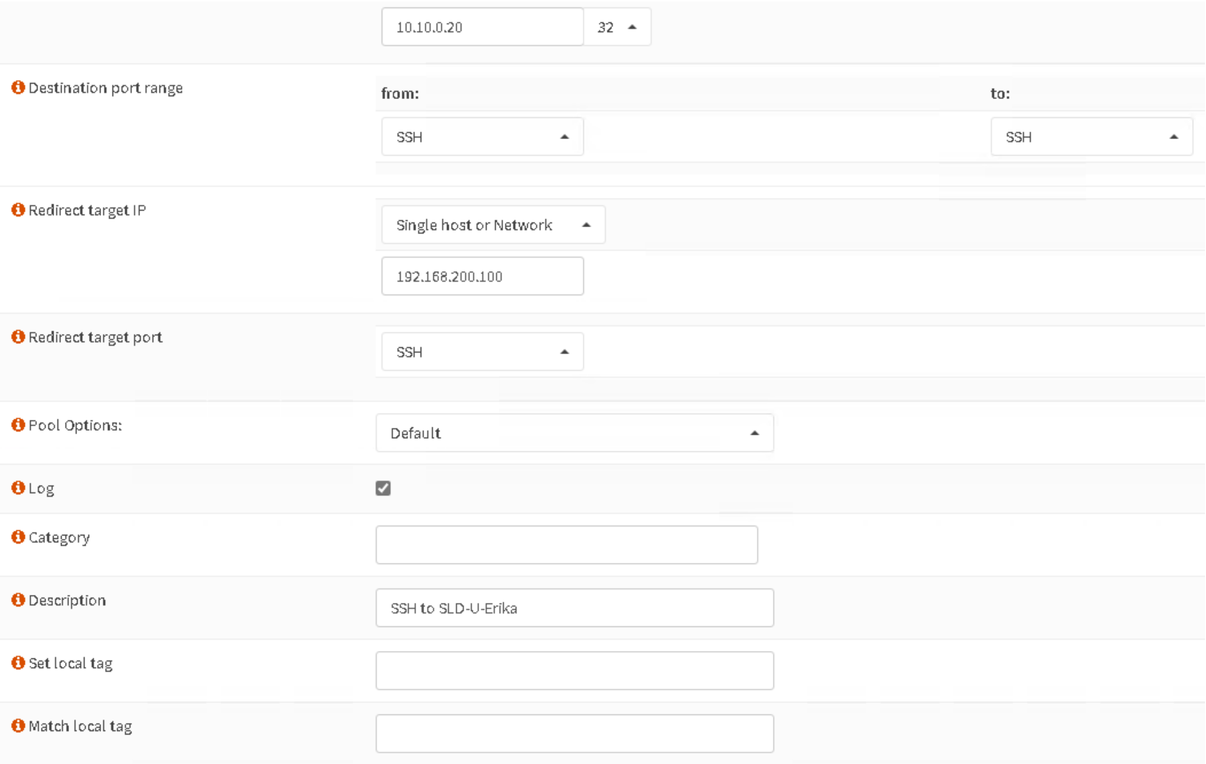
SSH

1. Enable SSH on SLD-U-Erika:
   Follow the steps either:
   - Setting Up and Securing SSH on Ubuntu 22.04: A Comprehensive Guide - Documentation Vault - ServerAstra or
   - How to enable and disable SSH for user on Linux
2. Disable root login for SSH:
   Open the SSH configuration file sshd_config with the text editor vim:
   “sudo vim /etc/ssh/sshd_config”
   In the line PermitRootLogin yes replace the word Yes with the word No
   sudo service ssh restart
3. Set port forward on Opnsense at *Firewall / NAT/ Port Forward* and **Apply changes**:

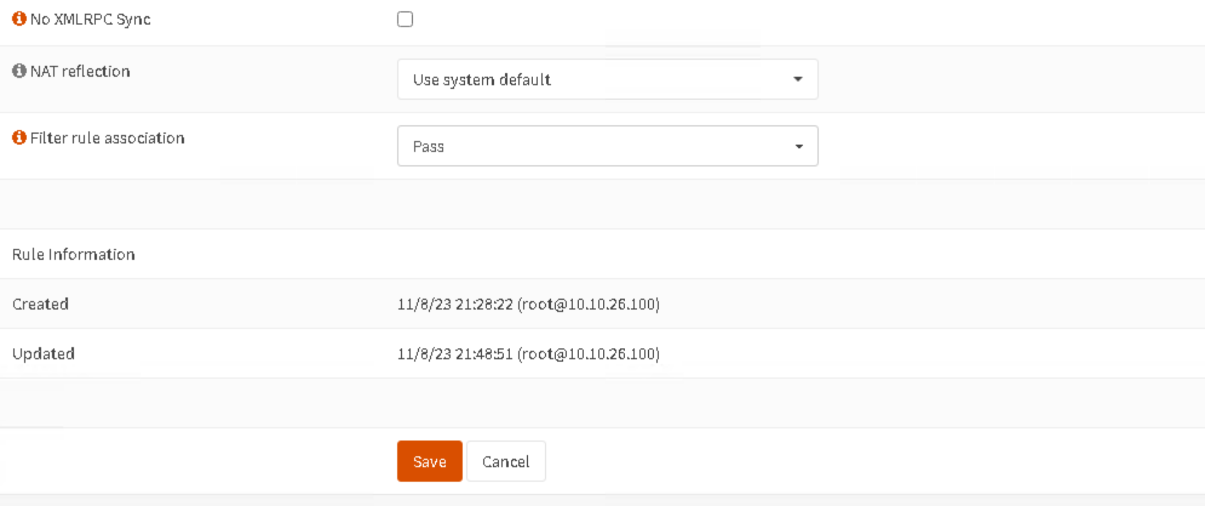


Edit Redirect entry

Disabled	□ Disable this rule
No RDR (NOT)	□
Interface	WAN
TCP/IP Version	IPv4
Protocol	TCP
Source / Invert	□
Source	Single host or Network 10.50.0.0 / 24
Source port range	from: any to: any
Destination / Invert	□
Destination	Single host or Network



	10.10.0.20 / 32
Destination port range	from: SSH to: SSH
Redirect target IP	Single host or Network 192.168.200.100
Redirect target port	SSH
Pool Options:	Default
Log	☑
Category	
Description	SSH to SLD-U-Erika
Set local tag	
Match local tag	



No XMLRPC Sync ☐

NAT reflection: Use system default

Filter rule association: Pass

Rule Information

Created 11/8/23 21:28:22 (root@10.10.26.100)

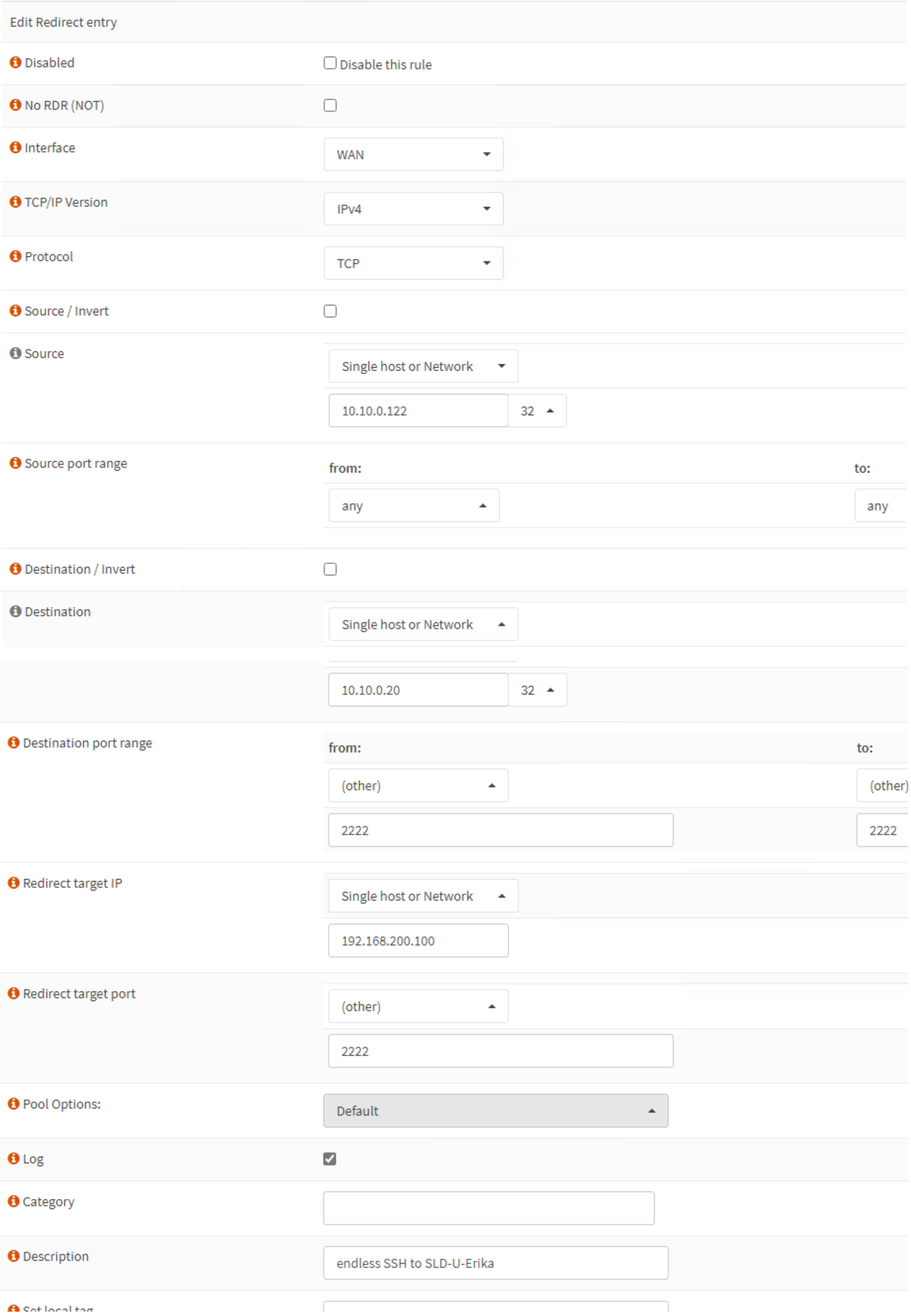
Updated 11/8/23 21:48:51 (root@10.10.26.100)

Honeypots

1. Install Endlessh tarpit

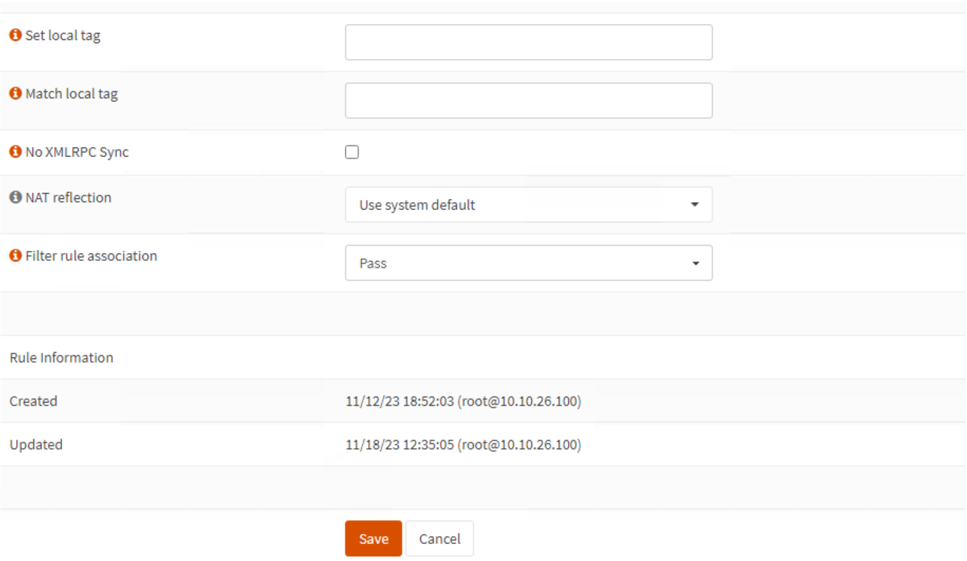
My computer	Honeypot (SLD-U-Erika)
1. ssh erika@10.10.0.20	2. mkdir PA
	3. cd PA
	4. sudo apt install git
	5. mkdir endless
	6. git clone https://github.com/skeeto/endlessh.git
	7. cd endlessh/
	8. sudo apt install build-essential
	9. sudo make install
	10. endlessh -v >endlessh.log 2>endlessh.err
	11. telnet localhost 2222 / ssh localhost -p 2222 -v
	12. cat endlessh.log
	13. sudo ufw allow 2222/tcp
Try it: ssh 10.10.0.20 -p 2222 -v	

2. Set port forward on Opnsense at *Firewall / NAT/ Port Forward* and **Apply changes**:



Edit Redirect entry

Disabled	□ Disable this rule
No RDR (NOT)	□
Interface	WAN
TCP/IP Version	IPv4
Protocol	TCP
Source / Invert	□
Source	Single host or Network 10.10.0.122 32
Source port range	from: any to: any
Destination / Invert	□
Destination	Single host or Network 10.10.0.20 32
Destination port range	from: (other) 2222 to: (other) 2222
Redirect target IP	Single host or Network 192.168.200.100
Redirect target port	(other) 2222
Pool Options:	Default
Log	☑
Category	
Description	endless SSH to SLD-U-Erika
Set local tag	



Set local tag	
Match local tag	
No XMLRPC Sync	□
NAT reflection	Use system default
Filter rule association	Pass

Rule Information

Created	11/12/23 18:52:03 (root@10.10.26.100)
Updated	11/18/23 12:35:05 (root@10.10.26.100)

3. Install SSH- auth -logger (low interaction)

My computer	SLD-U-Erika
	1. sudo apt install golang-go
	2. mkdir low
	3. cd low
	4. go install github.com/JustinAzoff/ssh-auth-logger@latest
	5. sudo ufw allow 2223/tcp
	6. opnsensen 2223 port forward
	7. ~/go/bin/ssh-auth-logger
8. Try it: ssh 10.10.0.20 -p 2223 -v	
9. type a wrong password	

4. Set port forward on Opnsense at *Firewall / NAT/ Port Forward* and **Apply changes**:

- Clone the *“endless SSSh to SLD-U-Erika”* and the “*Destination port range*”set from 2223 to 2223 and the “Redirect target port” set 2223
- Give a new description

5. Cowrie - high interaction

My computer	SLD-U-Erika
	mkdir high
	sudo apt-get install git python3-virtualenv libssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind virtualenv
	sudo adduser --disabled-password cowrie (enter 5x, y)
	sudo su - cowrie
	git clone http://github.com/cowrie/cowrie
	cd cowrie
	pwd
	exit -> sudo apt install python3.10-venv
	sudo su - cowrie
	python3 -m venv cowrie-env
	source cowrie-env/bin/activate
	python -m pip install --upgrade pip
	python -m pip install --upgrade -r requirements.txt
	touch cowrie.cfg nano cowrie.cfg [telnet] enabled = false [ssh] listen_endpoints = tcp:2224:interface=0.0.0.0 OR at the 11.
	bin/cowrie start

Try it: ssh phil@10.10.0.20 -p 2224	

6. Set port forward on Opnsense at *Firewall / NAT/ Port Forward* and **Apply changes**:

- Clone the *“endless SSSh to SLD-U-Erika”* and the “*Destination port range*”set from 2224 to 2224 and the “Redirect target port” set 2224
- Give a new description

7. Change user Phil to Erika:
sudo vim honeyfs/etc/passwd

   erika:x:1000:1000:Erika California,,,:/home/erika:/bin/bash

8. Correct python to python3:
sudo vim fsctl

9. Move the file from Phil to Erika:
bin/fsctl share/cowrie/fs.pickle
mv /home/phil /home/erika

10. Exit from fs.pickle and bin/crowie restart

11. Set the listen endpoint in the cowrie.cfg file:
[ssh]
listen_endpoints = tcp:2224:interface=0.0.0.0

12. Reload sshd with the “*sudo systemctl reload sshd”*

13. Give the “*password*”as a new password in the /home/cowrie/etc/userdb.txt
bin/cowrie restart

Managing with systemd

1. Add new users for services:

   ```
   cd /etc/systemd/system
   sudo useradd endless
   sudo useradd low
   sudo useradd high
   cat /etc/passwd
   ```

2. Create new files in /etc/systemd/system:

   Endlessh

   ```
   sudo touch endlessh.service
   sudo nano endlessh.service
   ```

   ```
   [Unit]
   Description=ENDLESSH demo service
   After=network.target
   StartLimitIntervalSec=0

   [Service]
   Type=simple
   Restart=always
   RestartSec=1
   User=endlessh
   ExecStart=/usr/local/bin/endlessh -v

   [Install]
   WantedBy=multi-user.target
   ```

   SSH-auth-logger

   ```
   sudo touch low.service
   sudo nano low.service
   ```

   ```
   [Unit]
   Description=Low demo service
   After=network.target
   StartLimitIntervalSec=0
   [Service]
   Type=simple
   Restart=always
   RestartSec=1
   User=low
   ExecStart=/usr/local/bin/ssh-auth-logger
   Environment="SSHD_BIND=:2223"

   [Install]
   WantedBy=multi-user.target
   ```

Cowrie

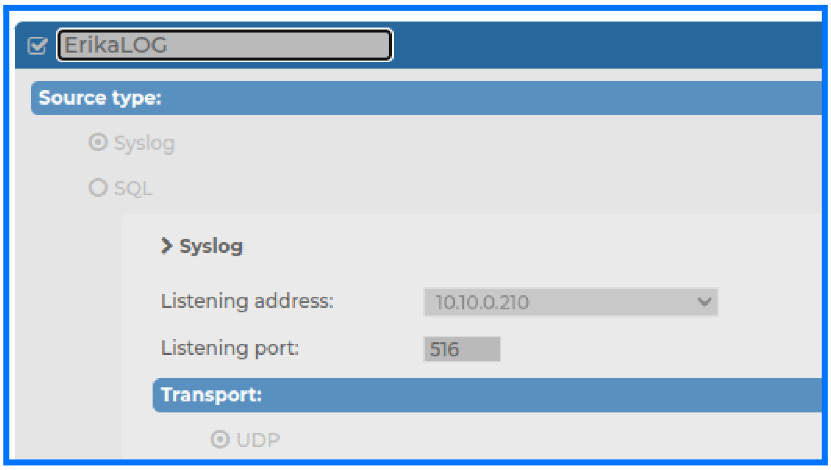
```
sudo su cowrie
cd /home/cowrie/cowrie
```

```
[Unit]
Description=Cowrie demo service
After=network.target
StartLimitIntervalSec=0

[Service]
Type=simple
Restart=always
RestartSec=5
User=cowrie
ExecStart=/home/cowrie/cowrie-env/bin/twistd --umask=0022 --nodaemon -l -- cowr>
WorkingDirectory=/home/cowrie/cowrie
Environment=PYTHONPATH=/home/cowrie/cowrie/src
SyslogIdentifier=cowrie

[Install]
WantedBy=multi-user.target
```

exit from cowrie user

Syslog-ng

1. sudo apt install syslog-ng-core
2. Browse to 10.10.0.210 and log in with your user credentials.
3. In the menu on the left side go to Log / Logspaces / ErikaLOG



☑ ErikaLOG

Source type:

● Syslog

○ SQL

> Syslog

Listening address: 10.10.0.210

Listening port: 516

Transport:

● UDP

4. Configure the syslog-ng:

```
sudo vim /etc/syslog-ng/syslog-ng.conf

@version:3.35
@include "scl.conf"

options {flush_lines (0); keep_hostname (yes);};

source s_sys { system(); internal();};
source s_cowrie { file("/home/cowrie/cowrie/var/log/cowrie/cowrie.log"
program-override("cowrie")); };
destination d_mesg { file("/var/log/messages"); };
destination d_logserver { network("10.10.0.210" transport(udp) port(516)); };
filter f_default { level(info..emerg) and not (facility(mail)); };

log {
        source(s_sys);
        source(s_cowrie);
            destination(d_mesg);
            destination(d_logserver);
 };
```

SLD-Kali-Erika

1. ssh erika@10.10.0.122
2. Create a new file "*passwords.txt*" with the command touch password.txt
3. Copy the last 100 words from fasttrack.txt with the command *"tail -n 100 /usr/share/wordlists/fasttrack.txt > /home/erika/passwords.txt"*
4. Add the "*password*"password to the table at the end of the column with the command "*vi password.txt*"

5. Port scanning: nmap -p 2222-2224 10.10.0.20 - Pn
6. Interact with Endlessh: ssh root@10.10.0.20 -p 2222 -v
7. cat password.txt
8. Hydra brute force ssh-auth-logger: hydra -s 2223 -l root -P passwords.txt 10.10.0.20 ssh -V -t 4 -w 3
9. Hydra brute force cowrie: hydra -s 2223 -l root -P passwords.txt 10.10.0.20 ssh -V -t 4 -w 3
10. Cowrie fake shell: ssh root@10.10.0.20 -p 2224 -v
    passwords: root,123456,honeypot,password
11. ifconfig

Splunk

1. Browse to 10.10.0.166:8000
2. Choose the app called "ErikaLOG"
3. Search for index = erikaindex and endlessh/ssh-auth-logger/cowrie

Links

1. https://github.com/skeeto/endlessh
2. https://github.com/cowrie/cowrie
3. https://github.com/JustinAzoff/ssh-auth-logger
4. https://github.com/paralax/awesome-honeypots
5. https://www.geeksforgeeks.org/how-to-use-hydra-to-brute-force-ssh-connections/
6. https://nmap.org/book/man-port-specification.html
7. https://journey.study/v2/learn/courses/219/modules/472/units/0
8. https://serverastra.com/docs/Tutorials/Setting-Up-and-Securing-SSH-on-Ubuntu-22.04%3A-A-Comprehensive-Guide
9. https://linuxconfig.org/how-to-enable-and-disable-ssh-for-user-on-linux
10. https://www.ibm.com/docs/en/db2/11.1?topic=installation-enable-disable-remote-root-lo

gin

11. https://cowrie.readthedocs.io/en/latest/INSTALL.html
12. https://github.com/cowrie/cowrie/issues/1614
13. https://cowrie.readthedocs.io/en/latest/systemd/README.html