RASPBERRY PI 4 HONEYPOT

BY STOKELY DE FREITAS

WHAT IS A HONEYPOT?

Honeypots are setup on real servers, real OS accompanied by information that looks authentic to cyber criminals.

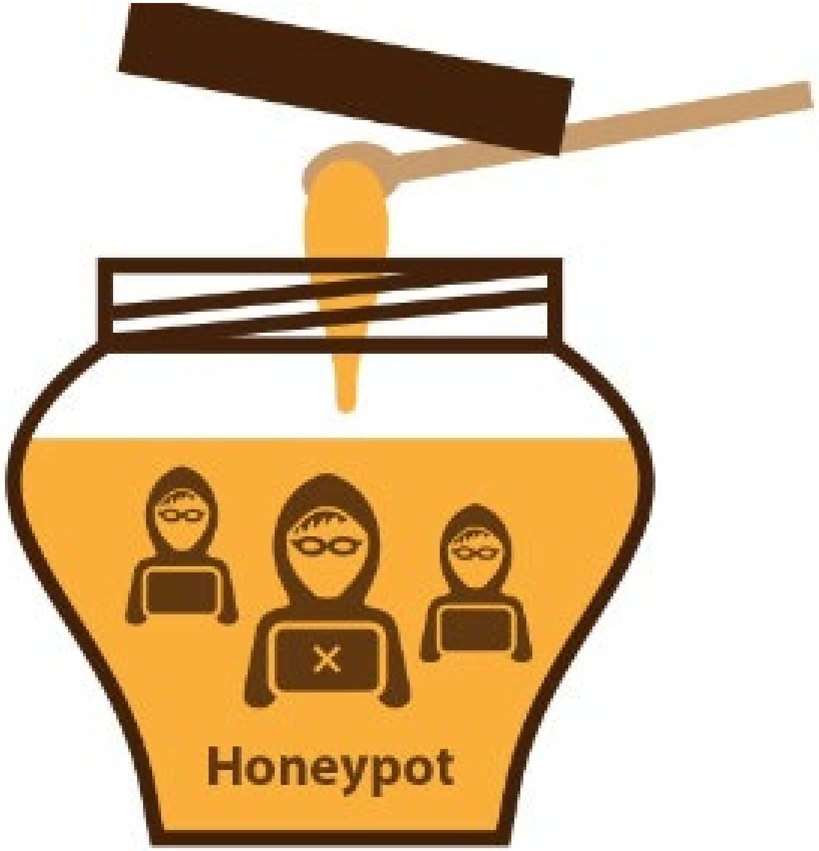
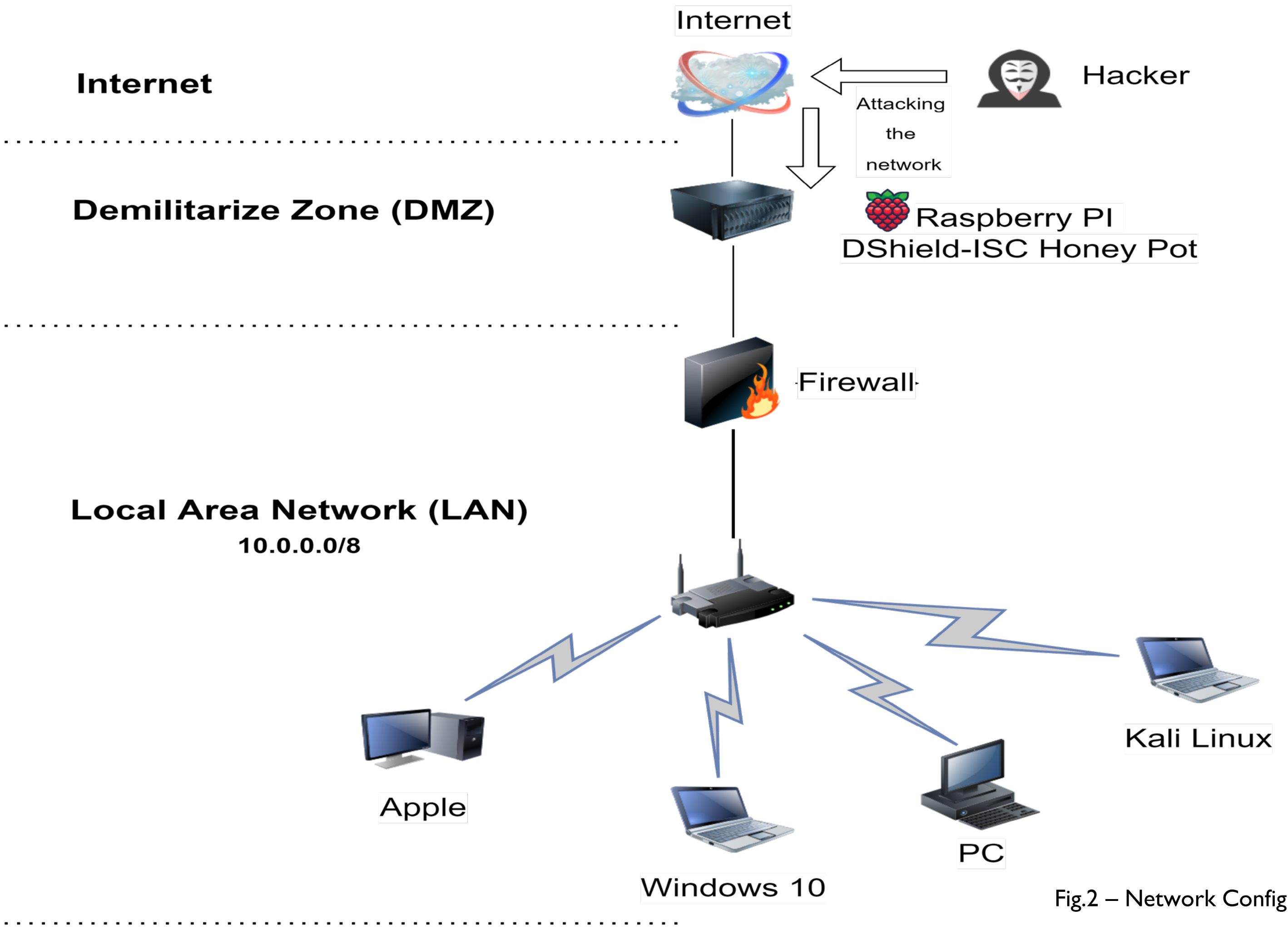


Fig.1 – Honeypot Image

VISUALIZATION OF NETWORK DESIGN



Internet

Internet

Hacker

Attacking the network

Demilitarize Zone (DMZ)

Raspberry PI
DShield-ISC Honey Pot

Firewall

Local Area Network (LAN)
10.0.0.0/8

Kali Linux

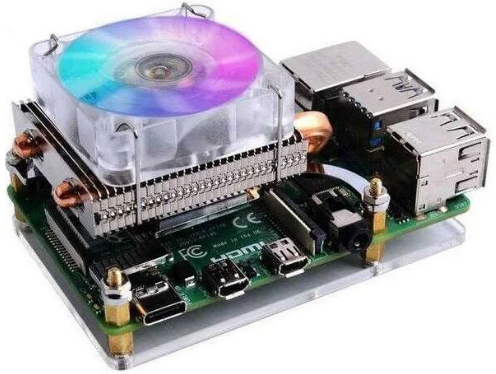
Apple

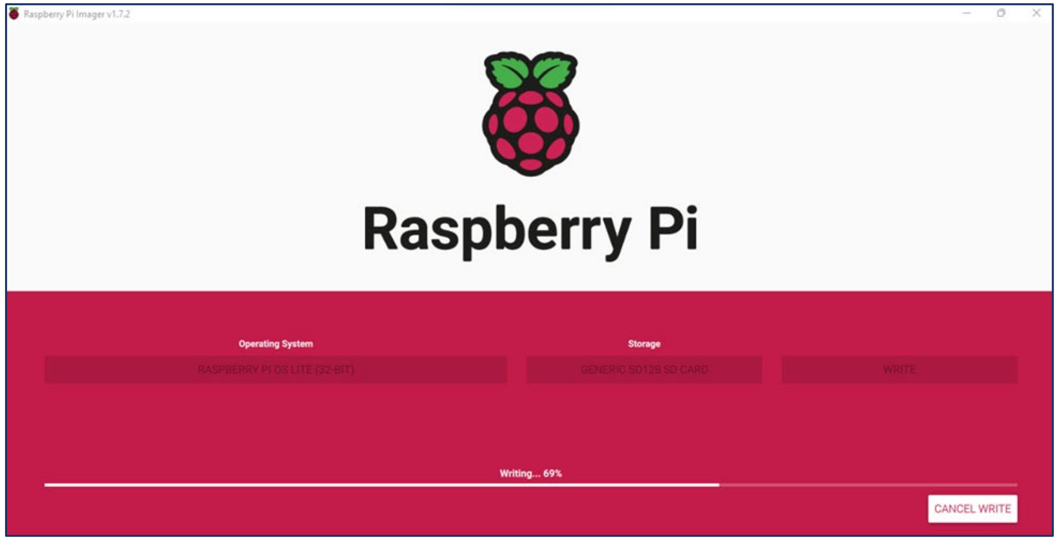
PC

Windows 10

Fig.2 – Network Configuration

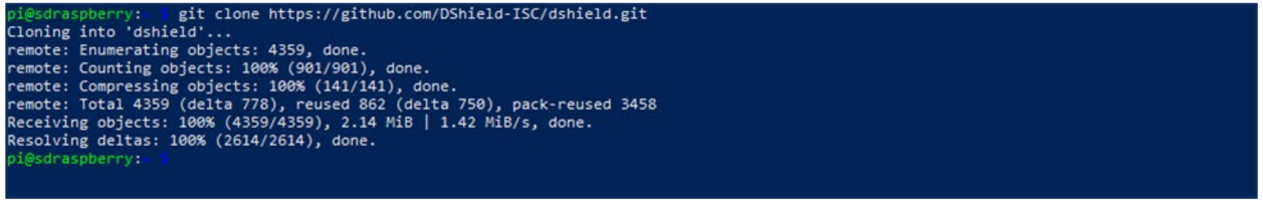
HONEYPOT CONFIGURATION



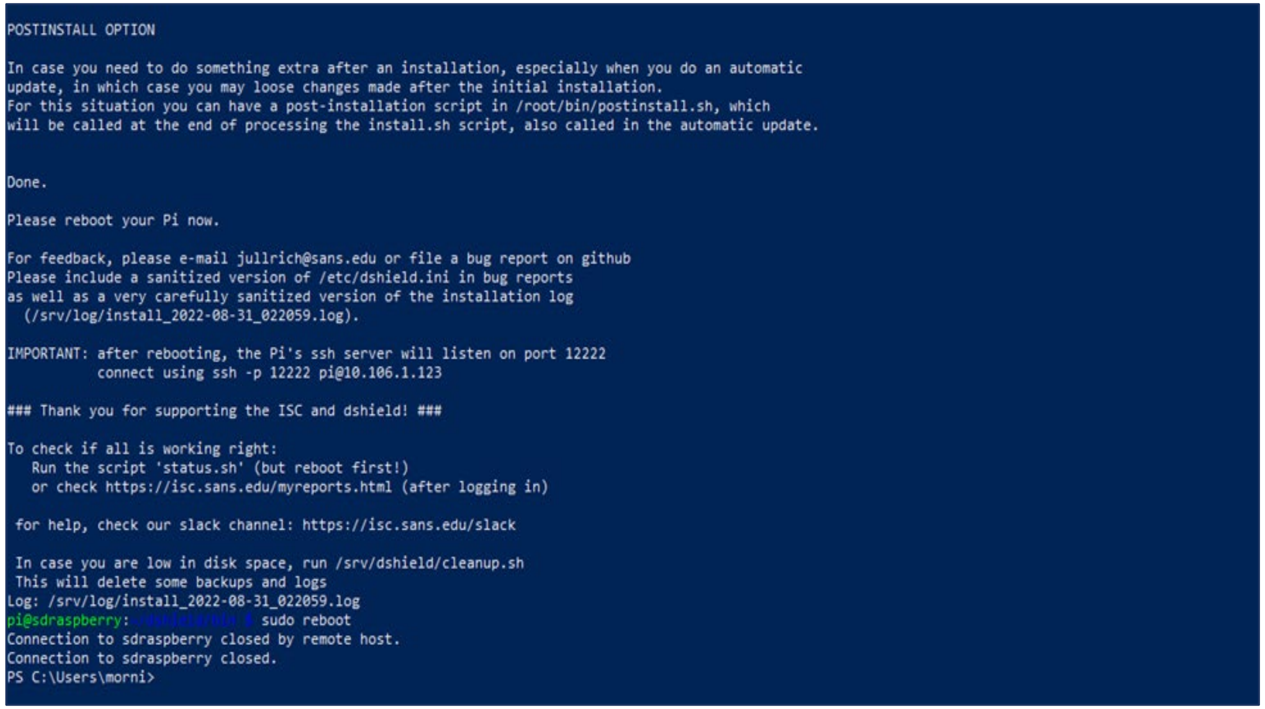


Operating System: RASPBERRY PI OS LITE (32-BIT)

Storage: GENERIC SD128 SD CARD



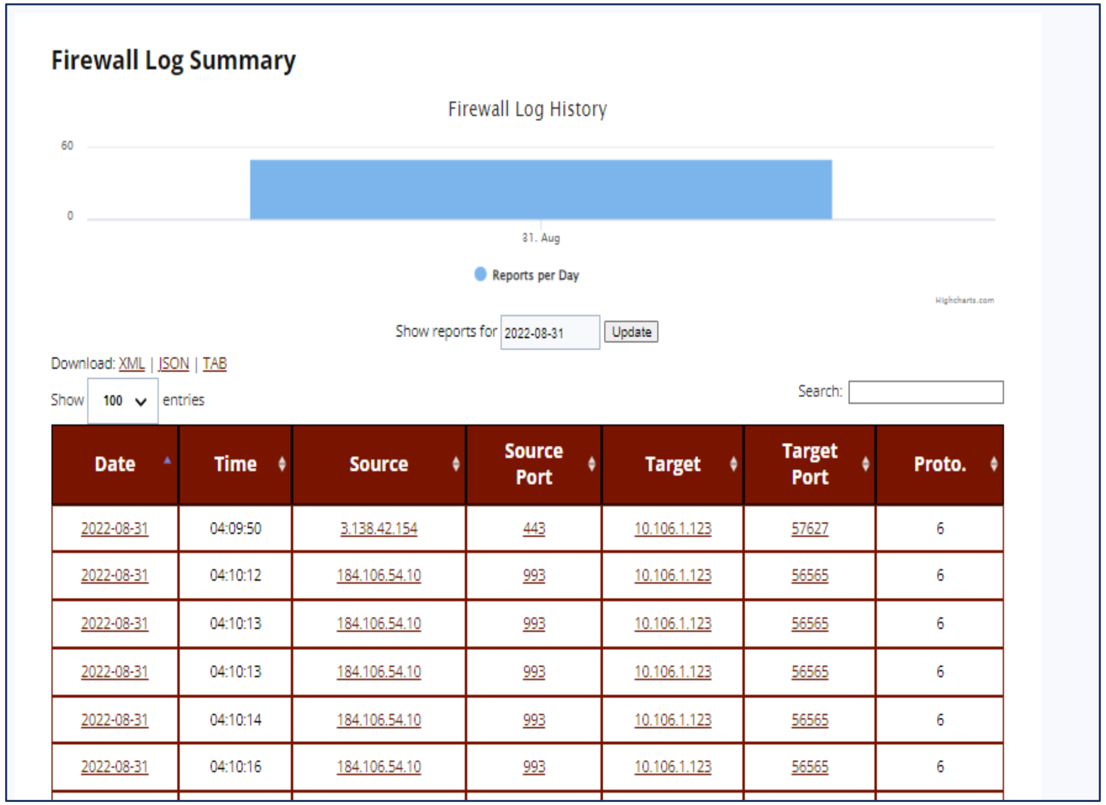
```
pi@sdraspberry:~ $ git clone https://github.com/DShield-ISC/dshield.git
Cloning into 'dshield'...
remote: Enumerating objects: 4359, done.
remote: Counting objects: 100% (901/901), done.
remote: Compressing objects: 100% (141/141), done.
remote: Total 4359 (delta 778), reused 862 (delta 750), pack-reused 3458
Receiving objects: 100% (4359/4359), 2.14 MiB | 1.42 MiB/s, done.
Resolving deltas: 100% (2614/2614), done.
pi@sdraspberry:~ $
```



```
POSTINSTALL OPTION

In case you need to do something extra after an installation, especially when you do an automatic
update, in which case you may loose changes made after the initial installation.
For this situation you can have a post-installation script in /root/bin/postinstall.sh, which
will be called at the end of processing the install.sh script, also called in the automatic update.


Done.

Please reboot your Pi now.

For feedback, please e-mail jullrich@sans.edu or file a bug report on github
Please include a sanitized version of /etc/dshield.ini in bug reports
as well as a very carefully sanitized version of the installation log
  (/srv/log/install_2022-08-31_022059.log).

IMPORTANT: after rebooting, the Pi's ssh server will listen on port 12222
           connect using ssh -p 12222 pi@10.106.1.123

### Thank you for supporting the ISC and dshield! ###

To check if all is working right:
   Run the script 'status.sh' (but reboot first!)
   or check https://isc.sans.edu/myreports.html (after logging in)

 for help, check our slack channel: https://isc.sans.edu/slack

 In case you are low in disk space, run /srv/dshield/cleanup.sh
 This will delete some backups and logs
Log: /srv/log/install_2022-08-31_022059.log
pi@sdraspberry:~/dshield/bin $ sudo reboot
Connection to sdraspberry closed by remote host.
Connection to sdraspberry closed.
PS C:\Users\morni>
```

Fig.3 – Raspberry Pi 4 and Honeypot Configuration

HONEYPOT DASHBOARD



Firewall Log Summary

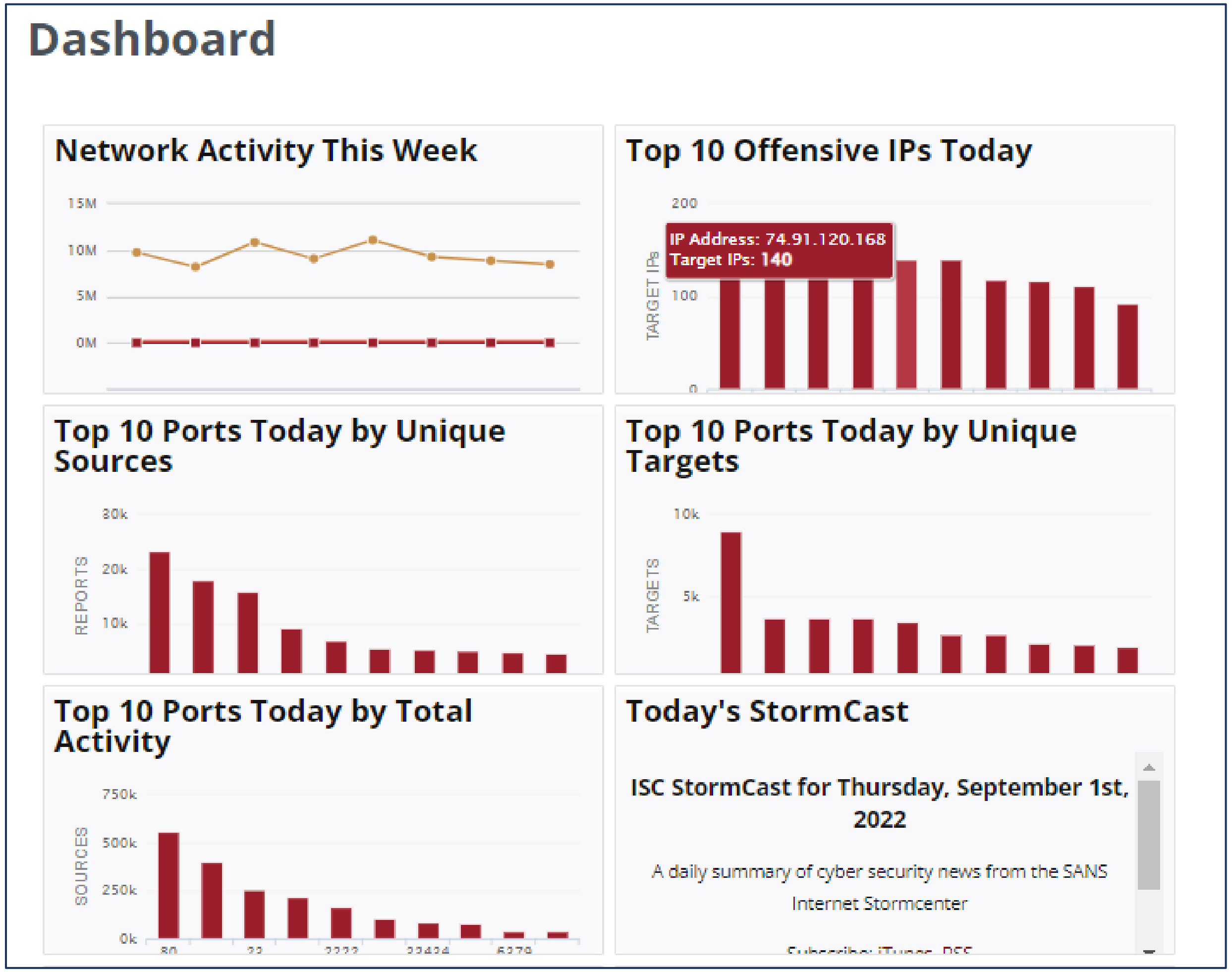
Show reports for 2022-08-31 Update

Download: XML | JSON | TAB

Show 100 entries

Search:

Date	Time	Source	Source Port	Target	Target Port	Proto.
2022-08-31	04:09:50	3.138.42.154	443	10.106.1.123	57627	6
2022-08-31	04:10:12	184.106.54.10	993	10.106.1.123	56565	6
2022-08-31	04:10:13	184.106.54.10	993	10.106.1.123	56565	6
2022-08-31	04:10:13	184.106.54.10	993	10.106.1.123	56565	6
2022-08-31	04:10:14	184.106.54.10	993	10.106.1.123	56565	6
2022-08-31	04:10:16	184.106.54.10	993	10.106.1.123	56565	6



Dashboard

Network Activity This Week
15M
10M
5M
0M
Top 10 Offensive IPs Today
200
100
0
TARGET IPs
IP Address: 74.91.120.168
Target IPs: 140
Top 10 Ports Today by Unique Sources
30k
20k
10k
REPORTS
Top 10 Ports Today by Unique Targets
10k
5k
TARGETS
Top 10 Ports Today by Total Activity
750k
500k
250k
0k
SOURCES
80
22
2222
23424
6379
Today's StormCast

ISC StormCast for Thursday, September 1st, 2022

A daily summary of cyber security news from the SANS Internet Stormcenter

Subscribe: iTunes, RSS

Fig.4 – Web Dashboard

WALKTHROUGH

MAIN GOALS OF A HONEYPOT & RESOURCES

- Divert Malicious traffic away from important systems, get early warning of a current attack before critical systems are hit.

- Gather information about attackers and their attack methods

- Resources
  - Honeypot Dashboard Link - https://www.dshield.org/login.html
  - Login Credentials – email: sdbootcon@gmail.com, password: Boot_Con2022!#

THANK YOU

QUESTIONS?