Playbook for Network Traffic Analysis and Firewall Configuration

Objective

This playbook provides a step-by-step guide to analyzing network traffic using Wireshark logs and configuring a firewall on Parrot Security OS.

Tools Used

- **Parrot Security OS** (Linux-based security-focused distribution)
- **Wireshark** (Network protocol analyzer)
- **UFW (Uncomplicated Firewall)** (Firewall management tool for Linux)

---

1. Firewall Configuration Using UFW

1.1 Install UFW

sudo apt-get install ufw

1.2 Enable UFW

sudo ufw enable

1.3 Default Firewall Rules

Set default rules to block all incoming traffic and allow outgoing traffic.

sudo ufw default deny incoming
sudo ufw default allow outgoing

1.4 Allow Specific Services

For SSH access, allow SSH traffic.

sudo ufw allow ssh

To check the firewall status with verbose output:

sudo ufw status verbose

---

2. Analyzing Wireshark Logs

2.1 Identifying Network Traffic

Captured network traffic logs include MDNS, DHCP, and NBNS queries.

Key Findings:

- **Multicast DNS (mDNS) Queries:** Devices attempting to discover local network services.
- **NetBIOS Name Service (NBNS) Queries:** Windows devices searching for names in the local network.
- **Spotify and AirPlay Traffic:** Devices broadcasting availability over the network.
- **DCHP Requests:** Devices requesting IP configurations.

2.2 Filtering Logs in Wireshark

To focus on specific network protocols, use the following Wireshark filters:

- **For DNS traffic:** `dns`
- **For DHCP traffic:** `bootp`
- **For SSH traffic:** `tcp.port == 22`
- **For Spotify traffic:** `mdns && ip.dst == 224.0.0.251`
- **For NetBIOS traffic:** `nbns`

2.3 Identifying Suspicious Traffic

- Look for repeated mDNS queries to unusual services.
- Detect unexpected NetBIOS name resolution queries.
- Identify DHCP requests from unauthorized sources.
- Unusual outbound traffic patterns may indicate exfiltration attempts.

---

3. Memory Dump Analysis

3.1 Creating a Memory Dump

A memory dump was created using `dd` command:

sudo dd if=/dev/vda2 of=~/Desktop/memory.dump bs=100

- The dump file size is 572 MB, indicating potential system memory analysis.

3.2 Analyzing the Dump

- Use `strings` to extract human-readable data.
- Use `volatility` framework to analyze running processes and open network connections.

strings memory.dump | grep password
volatility -f memory.dump --profile=Linux profile pslist

---

4. Conclusion and Recommendations

4.1 Secure Firewall Configuration

- Ensure all unnecessary ports are closed.
- Enable logging for unauthorized access attempts:

sudo ufw logging on

- Restrict SSH access to specific IP addresses:

sudo ufw allow from <trusted_ip> to any port 22

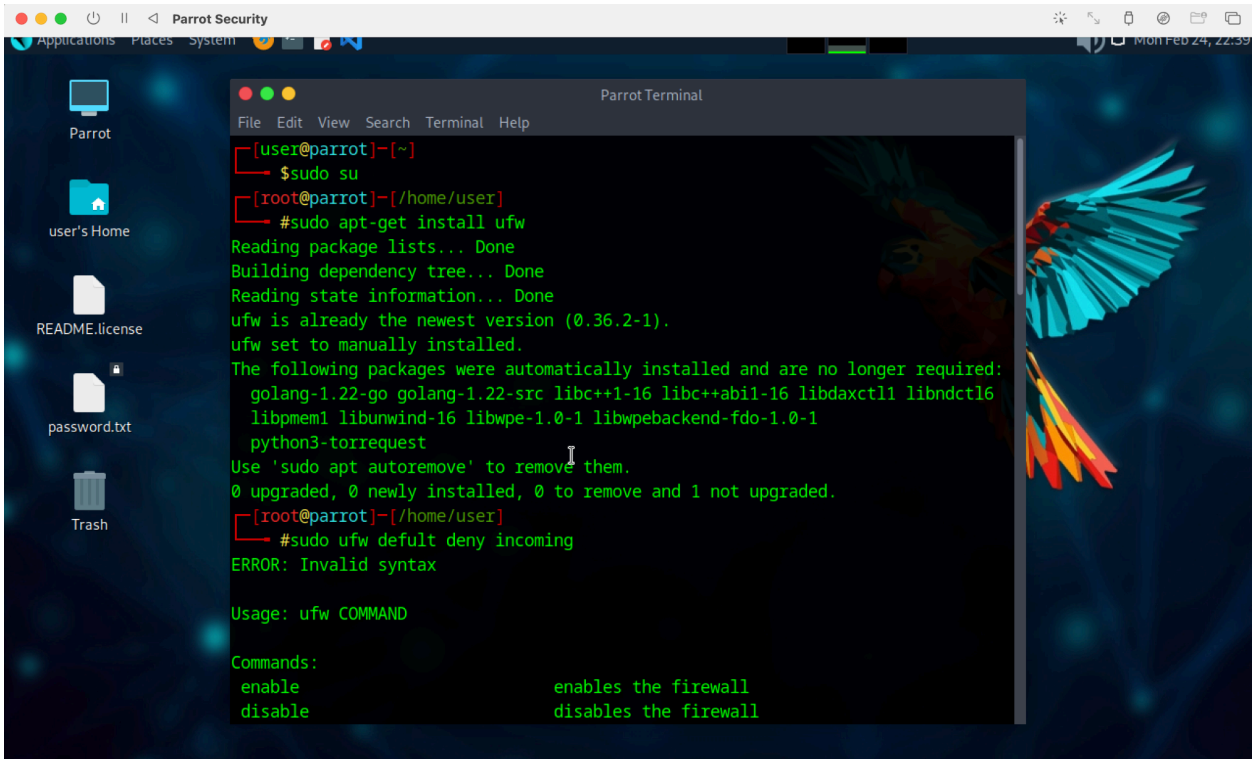
4.2 Monitor Network Activity

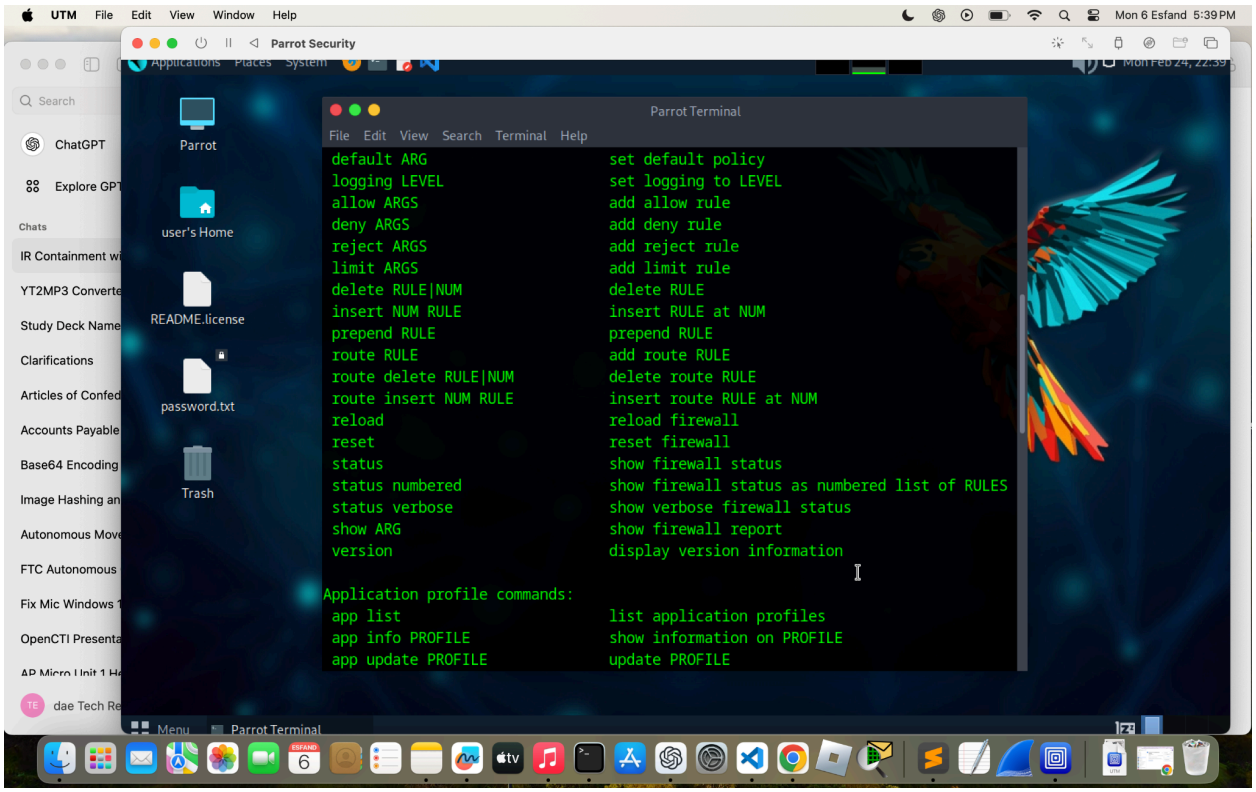
- Regularly capture network logs using Wireshark to identify anomalies.
- Automate alerts for unusual traffic patterns.

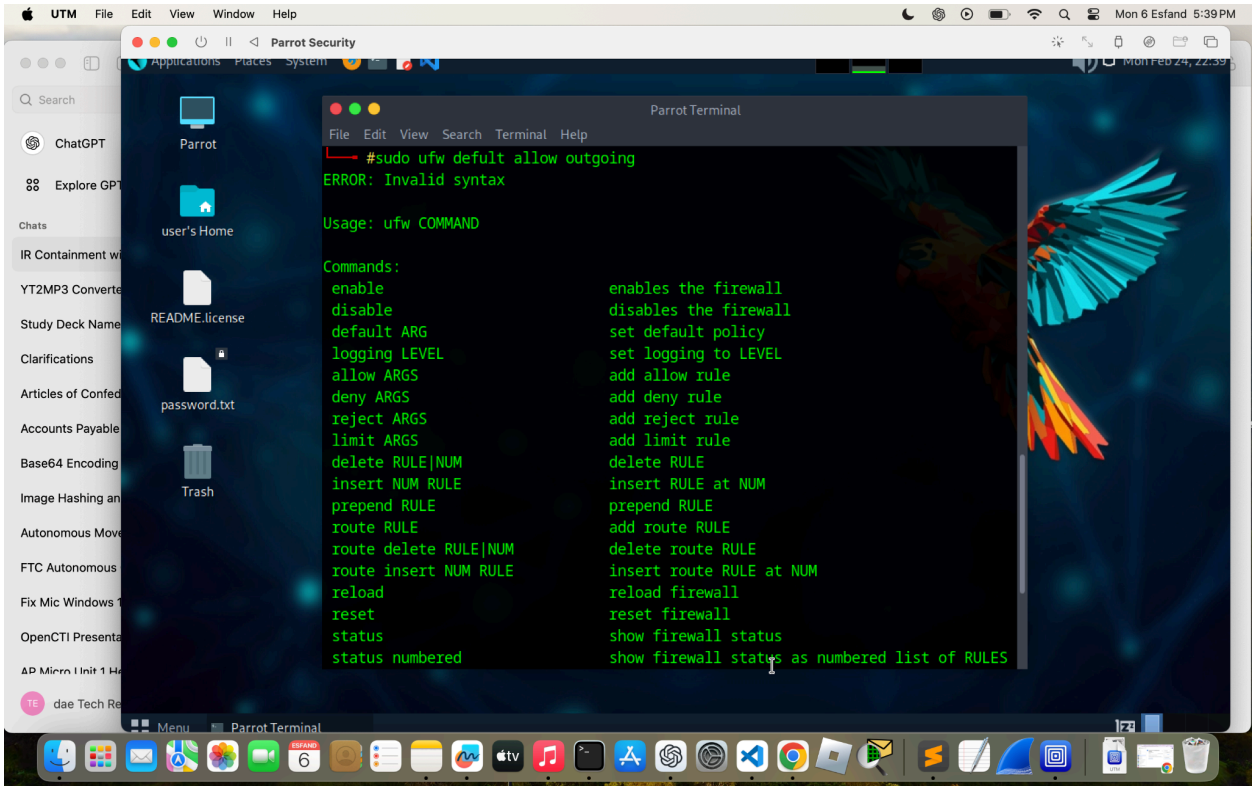
4.3 Secure System Memory

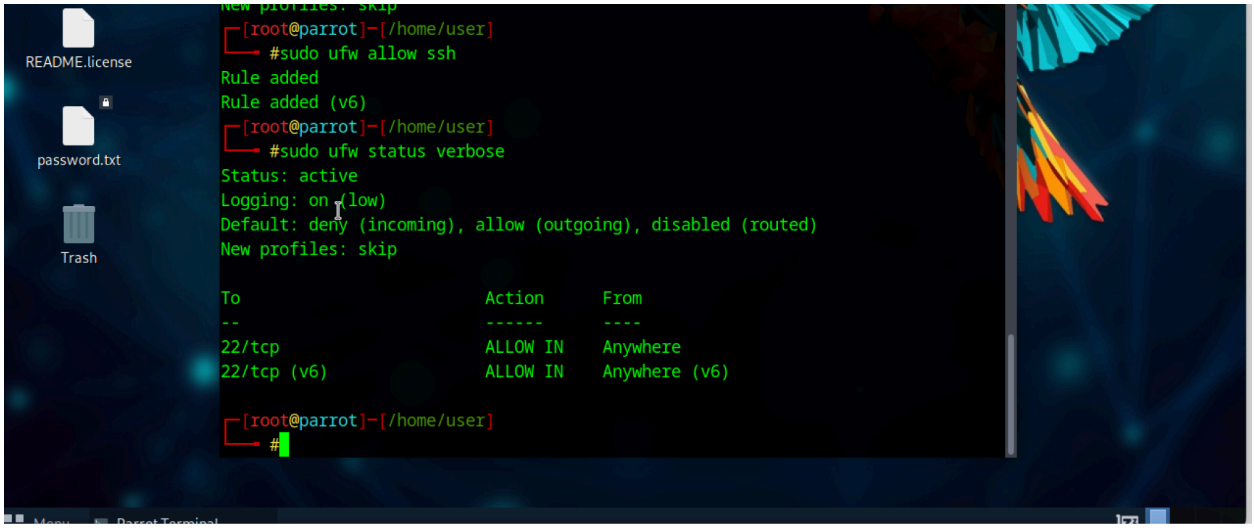
- Regularly audit processes using memory forensics tools.
- Avoid storing sensitive information in memory.

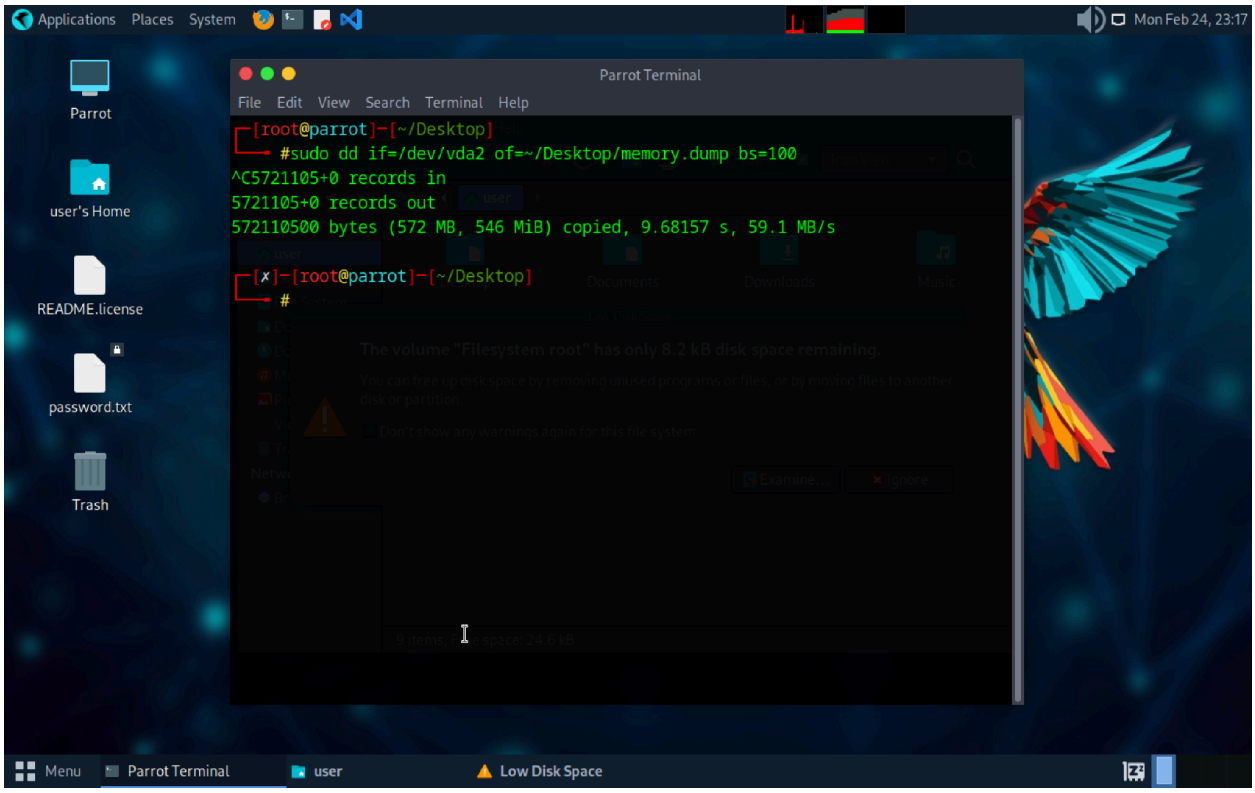
End of Playbook


Parrot Security
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]-[~]
$sudo su
[root@parrot]-[/home/user]
#sudo apt-get install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-1).
ufw set to manually installed.
The following packages were automatically installed and are no longer required:
golang-1.22-go golang-1.22-src libc++1-16 libc++abi1-16 libdaxctl1 libndctl6
libpmem1 libunwind-16 libwpe-1.0-1 libwpebackend-fdo-1.0-1
python3-torrequest
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
[root@parrot]-[/home/user]
#sudo ufw defult deny incoming
ERROR: Invalid syntax
Usage: ufw COMMAND
Commands:
enable enables the firewall
disable disables the firewall
Parrot
user's Home
README.license
password.txt
Trash


UTM File Edit View Window Help
Mon 6 Esfand 5:39 PM
Parrot Security
Parrot Terminal
File Edit View Search Terminal Help
default ARG set default policy
logging LEVEL set logging to LEVEL
allow ARGS add allow rule
deny ARGS add deny rule
reject ARGS add reject rule
limit ARGS add limit rule
delete RULE|NUM delete RULE
insert NUM RULE insert RULE at NUM
prepend RULE prepend RULE
route RULE add route RULE
route delete RULE|NUM delete route RULE
route insert NUM RULE insert route RULE at NUM
reload reload firewall
reset reset firewall
status show firewall status
status numbered show firewall status as numbered list of RULES
status verbose show verbose firewall status
show ARG show firewall report
version display version information
Application profile commands:
app list list application profiles
app info PROFILE show information on PROFILE
app update PROFILE update PROFILE
Parrot
user's Home
README.license
password.txt
Trash
ChatGPT
Explore GPT
Chats
Menu
Parrot Terminal


UTM File Edit View Window Help
Mon 6 Esfand 5:39 PM
Parrot Security
Parrot Terminal
File Edit View Search Terminal Help
#sudo ufw defult allow outgoing
ERROR: Invalid syntax
Usage: ufw COMMAND
Commands:
enable enables the firewall
disable disables the firewall
default ARG set default policy
logging LEVEL set logging to LEVEL
allow ARGS add allow rule
deny ARGS add deny rule
reject ARGS add reject rule
limit ARGS add limit rule
delete RULE|NUM delete RULE
insert NUM RULE insert RULE at NUM
prepend RULE prepend RULE
route RULE add route RULE
route delete RULE|NUM delete route RULE
route insert NUM RULE insert route RULE at NUM
reload reload firewall
reset reset firewall
status show firewall status
status numbered show firewall status as numbered list of RULES
Parrot
user's Home
README.license
password.txt
Trash
Menu
Parrot Terminal


README.license
password.txt
Trash
[root@parrot]-[/home/user]
#sudo ufw allow ssh
Rule added
Rule added (v6)
[root@parrot]-[/home/user]
#sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From
-- ------ ----
22/tcp ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
[root@parrot]-[/home/user]
#


Applications
Places
System
Mon Feb 24, 23:17
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~/Desktop]
#sudo dd if=/dev/vda2 of=~/Desktop/memory.dump bs=100
^C5721105+0 records in
5721105+0 records out
572110500 bytes (572 MB, 546 MiB) copied, 9.68157 s, 59.1 MB/s
[✗]-[root@parrot]-[~/Desktop]
#
Menu
Parrot Terminal
user
Low Disk Space