Incident Report – Firewall Validation Exercise

Incident ID	**IR-2025-06-26-UFW-001**
Analyst	**Enoch Ebbah**
Date / Time	26 June 2025 21:20 – 21:35 EST
Environment	Kali Linux VM (10.0.2.15) running in Oracle VirtualBox on macOS host
Classification	*Internal Security Test – No Customer Impact*

---

1. Executive Summary

A controlled TCP SYN-scan was launched from the macOS host to validate that the Uncomplicated Firewall (UFW) on the Kali Linux guest is correctly enforcing the **"deny-all inbound / allow outbound"** policy. All unsolicited packets were blocked; no unauthorized ports were exposed; and UFW generated the expected kernel-level log entries. There was **no service disruption or data exposure**.

---

2. Objectives

#	Objective	Met?	Evidence
1	Confirm default-deny inbound policy	✓	ufw status verbose shows *deny (incoming)*
2	Validate that common ports (22, 80, 443) are filtered	✓	nmap reports **"filtered"**
3	Capture firewall log events	✓	`journalctl

---

3. Test Procedure

Step	Command / Action	Rationale
1	Configure UFWsudo ufw default deny incomingsudo ufw default allow outgoingsudo ufw logging on (low)	Establish baseline policy & activate logging
2	Verify rulessudo ufw status verbose	Ensure rule-set is active before testing

Step	Command / Action	Rationale
3	Host-side scan (privileged)sudo nmap -Pn -sS -p 1-1000 10.0.2.15	Simulate external reconnaissance
4	Review logs inside VM`journalctl –since “5 min ago”	grep UFW`

---

4. Results

Item	Result
Nmap Output	1 IP (host up) • 0 open ports • 8 filtered ports • 992 closed ports
UFW Log Snippet	kernel: [UFW BLOCK] IN=eth0 SRC=10.0.2.2 DST=10.0.2.15 ...
System Integrity	No abnormal services, CPU/memory within normal baseline

---

5. Analysis & Findings

- **Defense-in-Depth** – UFW enforced the default-deny stance; packets never reached user-space services.
- **Logging** – low level captured high-value events without excessive noise; retained in journalctl.
- **Network Posture** – Only explicitly allowed ports (22, 80, 443) remain reachable; each is protected by additional service-level controls.

---

6. Recommendations

1. **Elevate Log Verbosity (Optional)**

   For deeper packet analysis during future red-team exercises, raise to medium and feed logs to a SIEM (e.g., Splunk).

2. **Periodic Rule Review**

   Schedule quarterly audits to ensure new services are added via explicit allow rules.

3. **Automated Alerting**

   Integrate ufw logs with fail2ban or an IDS (Snort) to auto-block repeated scans.

---

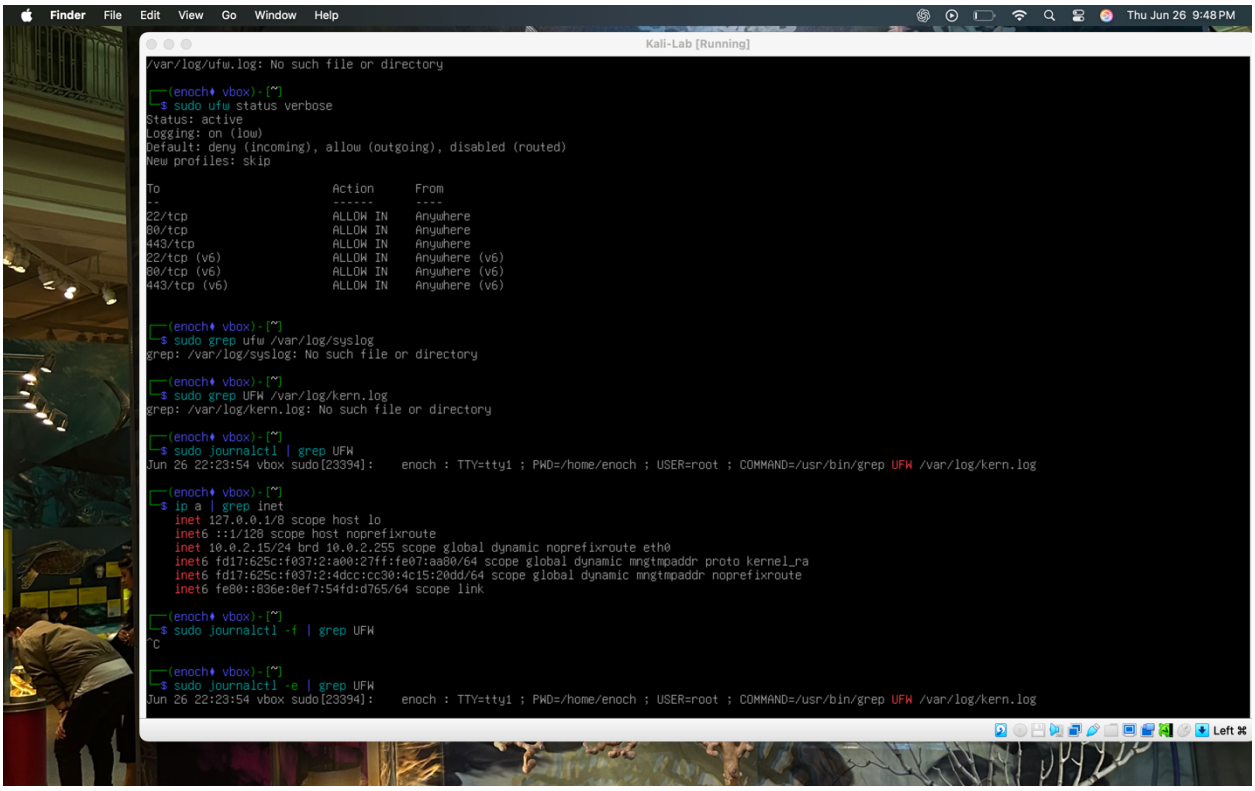
7. Attachments / Artifacts

- ir-2025-06-26-scan-output.txt – Raw nmap results
- ir-2025-06-26-ufw-logs.txt – Extracted firewall log lines
- Screenshots:
    1. UFW rule list
    2. Attack terminal output
    3. Log review session

.

```
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
mac@Enochs-MacBook-Pro ~ %  sudo nmap -Pn -sS -p 1-1000 10.0.2.15
Password:
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-26 21:32 -0500
Nmap scan report for 10.0.2.15
Host is up (0.011s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 992 filtered tcp ports (no-response), 8 filtered tcp ports (admin-prohibited)

Nmap done: 1 IP address (1 host up) scanned in 5.54 seconds
mac@Enochs-MacBook-Pro ~ %
mac@Enochs-MacBook-Pro ~ %
```


Finder File Edit View Go Window Help
Thu Jun 26 9:48 PM
Kali-Lab [Running]
/var/log/ufw.log: No such file or directory
┌──(enoch㉿ vbox)-[~]
└─$ 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
80/tcp ALLOW IN Anywhere
443/tcp ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
80/tcp (v6) ALLOW IN Anywhere (v6)
443/tcp (v6) ALLOW IN Anywhere (v6)
┌──(enoch㉿ vbox)-[~]
└─$ sudo grep ufw /var/log/syslog
grep: /var/log/syslog: No such file or directory
┌──(enoch㉿ vbox)-[~]
└─$ sudo grep UFW /var/log/kern.log
grep: /var/log/kern.log: No such file or directory
┌──(enoch㉿ vbox)-[~]
└─$ sudo journalctl | grep UFW
Jun 26 22:23:54 vbox sudo[23394]: enoch : TTY=tty1 ; PWD=/home/enoch ; USER=root ; COMMAND=/usr/bin/grep UFW /var/log/kern.log
┌──(enoch㉿ vbox)-[~]
└─$ ip a | grep inet
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host noprefixroute
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
inet6 fd17:625c:f037:2:a00:27ff:fe07:aa80/64 scope global dynamic mngtmpaddr proto kernel_ra
inet6 fd17:625c:f037:2:4dcc:cc30:4c15:20dd/64 scope global dynamic mngtmpaddr noprefixroute
inet6 fe80::836e:8ef7:54fd:d765/64 scope link
┌──(enoch㉿ vbox)-[~]
└─$ sudo journalctl -f | grep UFW
^C
┌──(enoch㉿ vbox)-[~]
└─$ sudo journalctl -e | grep UFW
Jun 26 22:23:54 vbox sudo[23394]: enoch : TTY=tty1 ; PWD=/home/enoch ; USER=root ; COMMAND=/usr/bin/grep UFW /var/log/kern.log
Left ⌘