Task 16: Incident Response & Security Breach Simulation

Target System: Kali Linux (SSH Enabled)
Log Monitoring Tool: journalctl
Service Monitored: SSH

1️⃣ Objective

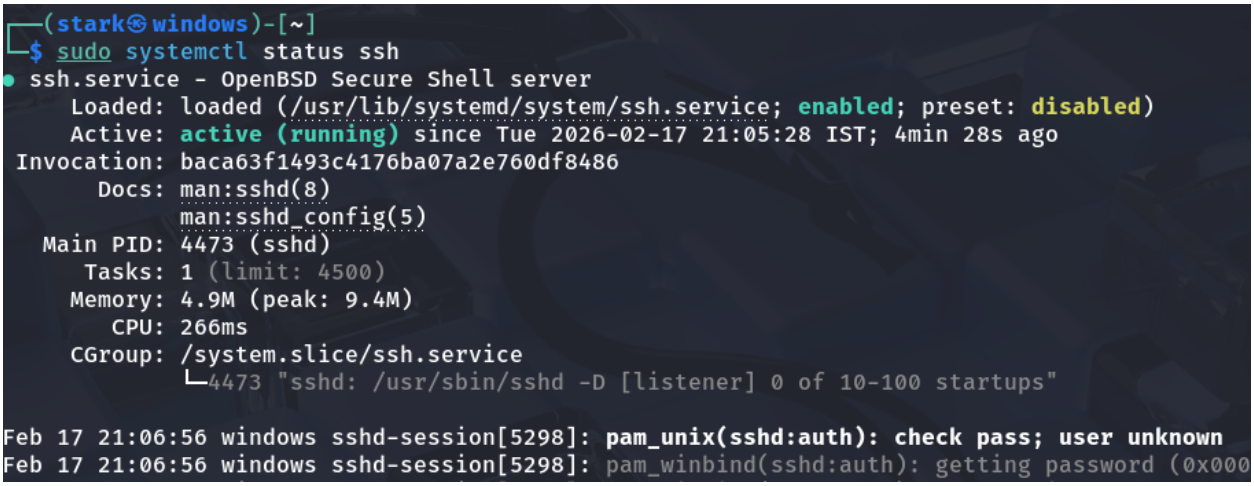
To detect and respond to a simulated brute-force SSH login attack by analyzing authentication logs, identifying the attacker IP, performing containment, and securing the system.

2️⃣ Start & Verify SSH Service

Command:

sudo systemctl status ssh

Result:
SSH service is active and running.



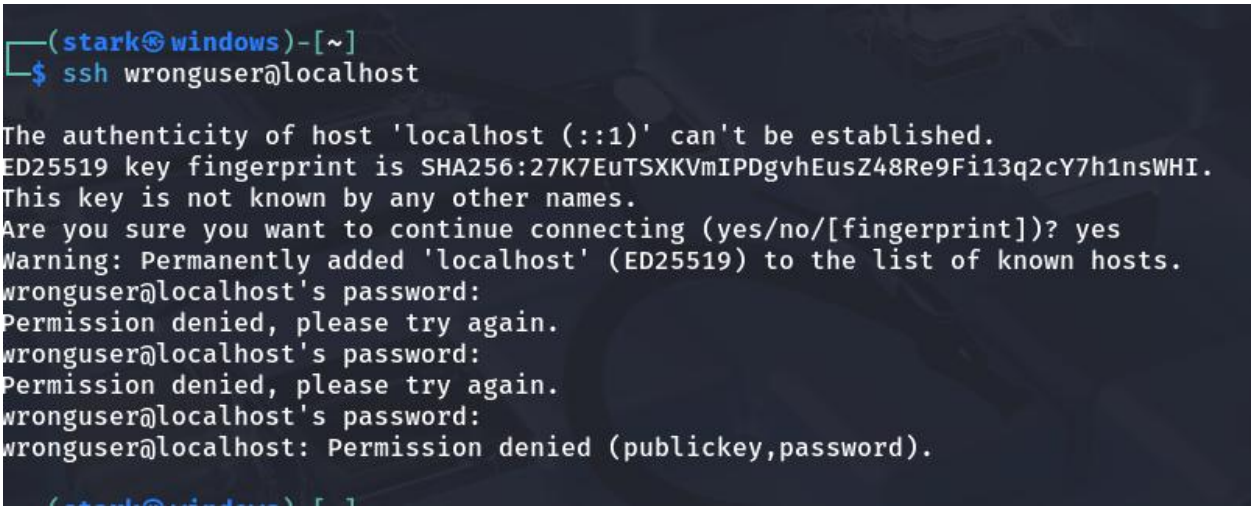
3️⃣ Simulate Failed Login Attempts

Command:

ssh wronguser@localhost

Enter incorrect password multiple times.

Result:
Permission denied messages displayed.

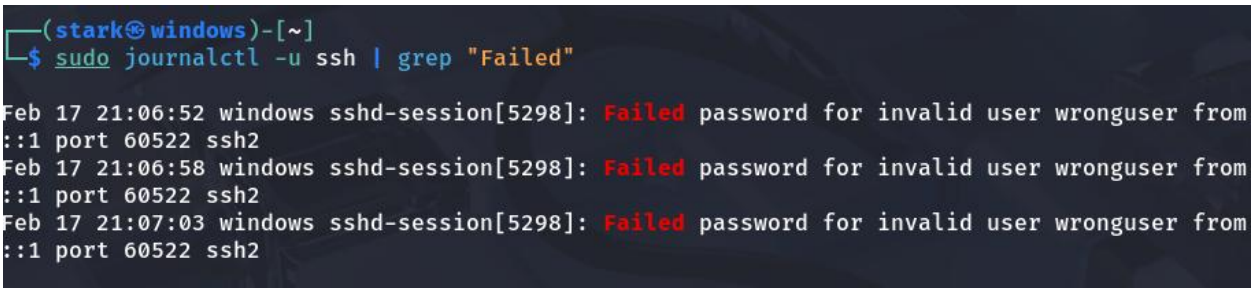


4️⃣ Analyze Failed Login Logs

Command:

sudo journalctl -u ssh | grep "Failed"

Result:



5️⃣ Identify Attacker IP

Command:

sudo journalctl -u ssh | grep "Failed password"

Attacker IP Identified:

::1

6️⃣ Containment – Lock Suspicious Account

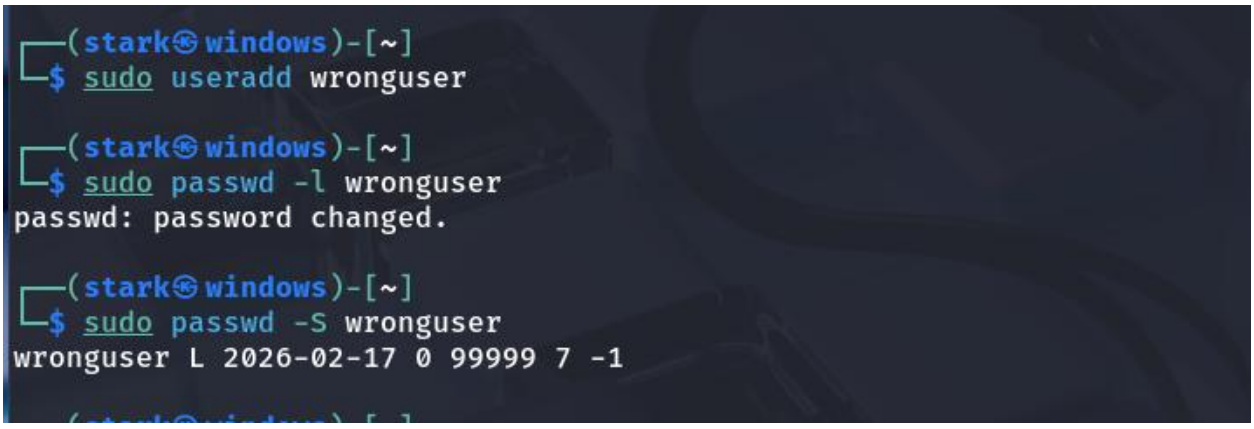
Command:

sudo passwd -l wronguser

Verify:

sudo passwd -S wronguser

Result:
Account locked successfully.



7️⃣ Containment – Block Attacker IP

Command:

sudo ufw deny from ::1

Verify:

sudo ufw status

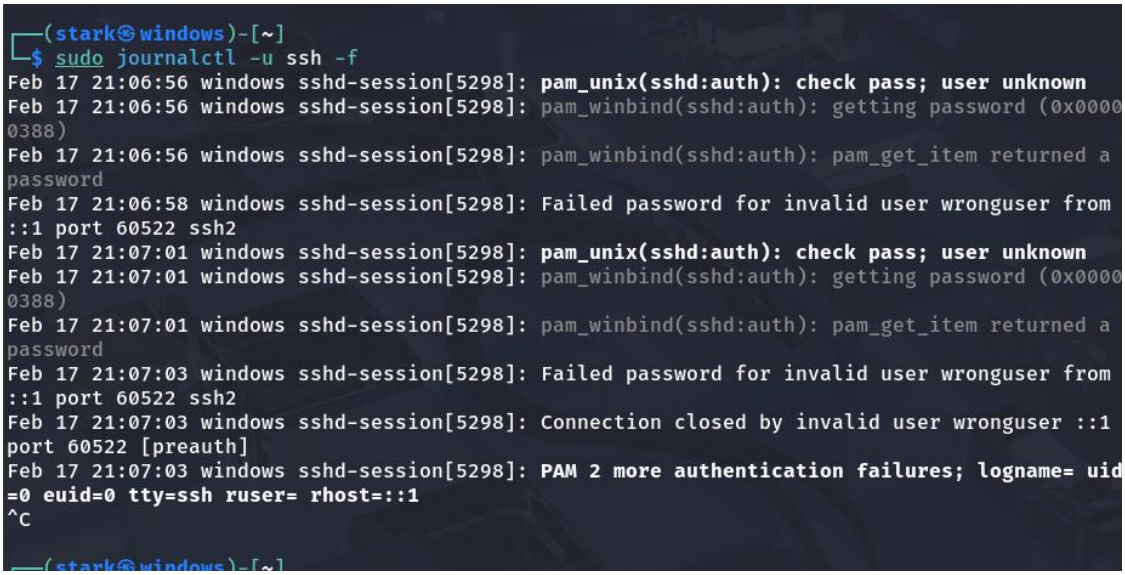
Result:
Firewall rule added.

8️⃣ Monitor Logs After Containment

Command:

sudo journalctl -u ssh -f

Result:
No further failed login attempts detected.



9️⃣ Incident Timeline

Time Event

21:06 Failed login attempts detected

21:07 Log analysis performed

21:08 Attacker IP identified

21:09 Account locked

21:10 IP blocked

21:12 System secured

🔟 Final Outcome

- Brute-force SSH attack simulated
- Failed login attempts detected
- Attacker IP identified
- Account locked

- Firewall rule implemented
- System secured successfully