🛡️ Thiết lập hệ thống va

và phòng thủ mạng tại nhà

(Dễ hiểu, dễ làm)

🎯 Mục tiêu:

- **Phát hiện và chặn tấn công SSH từ bên ngoài**
- **Ghi lại thông tin kẻ tấn công (IP, quốc gia, tổ chức, cổng mở)**
- **Tự động phản ứng, không cần can thiệp sau khi cài**

🧰 1. Cài công cụ cần thiết

Trên Arch/Manjaro:

bash

```
sudo pacman -S whois geoip nmap iptables
```

2. Trên Debian/Ubuntu:

3. bash

```
sudo apt install whois geoip-bin nmap iptables
```

📁 2. Tạo thư mục và file cơ bản

bash

- `sudo mkdir -p ~/attackers`
- `sudo touch ~/network_bans.txt`

🧠 3. Script thu thập thông tin kẻ tấn công: `intel_report.sh`

bash

- `sudo nano ~/intel_report.sh`

Dán vào:

bash

```
#!/bin/bash
   METADATA_DIR="$HOME/attackers"
   echo "=== Báo cáo tình báo kẻ tấn công ==="
   echo "Ngày: $(date)"
   echo ""

for ip in $(ls "$METADATA_DIR"); do
  echo "🕵️ IP: $ip"
  grep -E 'OrgName|Organization|NetRange|
Country' "$METADATA_DIR/$ip/whois.txt"
  grep 'GeoIP Country Edition'
"$METADATA_DIR/$ip/geoip.txt"
  echo -n "Cổng mở: "
  grep -E '^[0-9]+/tcp'
"$METADATA_DIR/$ip/nmap.txt" | awk '{print
$1}' | paste -sd ", " -
  echo ""
done
```

Làm cho script có thể chạy:

bash

```
 chmod +x ~/intel_report.sh
```

🛡️ 4. Script giám sát và chặn tấn công: `hybrid_guard.sh`

bash

```
sudo nano ~/hybrid_guard.sh
```

Dán vào:

bash

```
#!/bin/bash
BAN_LIST="$HOME/network_bans.txt"
METADATA_DIR="$HOME/attackers"

collect_metadata() {
  local ip="$1"
  local dir="$METADATA_DIR/$ip"
  mkdir -p "$dir"
  whois "$ip" > "$dir/whois.txt"
  geoiplookup "$ip" > "$dir/geoip.txt"
  nmap -Pn "$ip" -oN "$dir/nmap.txt"
}

ban_ip_locally() {
  local ip="$1"
  iptables -A INPUT -s "$ip" -j DROP
  echo "$ip" >> "$BAN_LIST"
  collect_metadata "$ip"
}

monitor_ssh() {
  tail -Fn0 /var/log/auth.log | \
  grep --line-buffered "Failed password" | \
  awk '{print $(NF-3)}' | \
  sort | uniq -c | \
```

```
  awk '$1 > 5 {print $2}' | while read ip; do
    grep -q "$ip" "$BAN_LIST" ||
ban_ip_locally "$ip"
  done
}

monitor_ssh
```

Làm cho script có thể chạy:

bash

```
 chmod +x ~/hybrid_guard.sh
```

🔁 5. Tạo dịch vụ tự động chạy khi khởi động

bash

```
 sudo nano
/etc/systemd/system/hybrid_guard.service
```

Dán vào:

ini

```
[Unit]
Description=Hybrid Guard Surveillance Monitor
After=network.target

[Service]
ExecStart=/home/your-username/hybrid_guard.sh
Restart=always
User=your-username

[Install]
WantedBy=multi-user.target
```

Kích hoạt dịch vụ:

bash

```
sudo systemctl daemon-reexec
sudo systemctl enable hybrid_guard.service
sudo systemctl start hybrid_guard.service
```

✅ **Sau khi cài xong:**

- **Hệ thống sẽ tự giám sát và chặn IP nguy hiểm**
- **Ghi lại thông tin để bạn phân tích sau**
- **Không cần mở máy kiểm tra mỗi ngày**