🛡️ Network Surveillance Monitor Setup Guide

Author: Zsan Nguyen

Purpose: Forensic-grade logging, attacker profiling, and automated defense across local and network-wide threats.

🧠 Overview

Layer	Function	Tools
1️⃣ Surveillance	Detect intrusions	`auth.log`, `iptables`, `tcpdump`, watchdog script
2️⃣ Memory	Log and profile attackers	`whois`, `geoiplookup`, `nmap`, bash
3️⃣ Defense	Ban and document	`iptables`, `systemd`, CLI scripts

🔧

Installation Steps

1. Create Core Directories & Files

bash

```
mkdir -p ~/attackers
```

```
touch ~/network_bans.txt
```

2. Install Required Tools

On Arch/Manjaro:

bash

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

On Debian/Ubuntu:

bash

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

3. Create `intel_report.sh`

bash

```
nano ~/intel_report.sh
```

Paste:

```
#!/bin/bash
METADATA_DIR="$HOME/attackers"
echo "=== Attacker Intelligence Report ==="
echo "Date: $(date)"
echo ""

for ip in $(ls "$METADATA_DIR"); do
    echo "🔹 IP: $ip"
    grep -E 'OrgName|Organization|NetRange|Country' "$METADATA_DIR/$ip/whois.txt" 2>/dev/null
    grep 'GeoIP Country Edition' "$METADATA_DIR/$ip/geoip.txt" 2>/dev/null
    echo -n "Open Ports: "
    grep -E '^[0-9]+/tcp' "$METADATA_DIR/$ip/nmap.txt" 2>/dev/null | awk '{print $1}' | paste -sd "," -
    echo ""
done
```

Make it executable:

bash

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

4. Create `hybrid_guard.sh`

bash

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

Paste:

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
```

Make it executable:

bash

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

5. Create systemd Service

bash

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

Paste:

ini

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

[Service]
ExecStart=/home/you-usr-name/hybrid_guard.sh
Restart=always
User=your-usr-name

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

Enable and start:

bash

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

6. Test the Pipeline

bash

```
echo "192.0.2.123" >> ~/network_bans.txt
mkdir -p ~/attackers/192.0.2.123
whois 192.0.2.123 > ~/attackers/192.0.2.123/whois.txt
geoiplookup 192.0.2.123 > ~/attackers/192.0.2.123/geoip.txt
```

```
nmap -Pn 192.0.2.123 -oN ~/attackers/192.0.2.123/nmap.txt
~/intel_report.sh
```

🧩 Optional Enhancements

- Export to CSV/JSON
- Cross-reference threat feeds (AbuseIPDB, Spamhaus)
- Visual dashboard (Grafana, CLI overlays)
- Remote sync or encrypted push
- Honeypot redirection (`cowrie`, `dionaea`)

🌐 Network-Wide Monitoring (Advanced)

To monitor all devices:

- Use `tcpdump` on a SPAN port or network tap
- Collect logs via `rsyslog` or `syslog-ng`
- Deploy agents or honeypots on other nodes
- Centralize metadata and alerts