bumblebee_monitor.sh – TCPDump-Hintergrundüberwachung

Stand: 07.07.2025
Autor: Lars @ Kali
Ziel: Hintergrund-Mitschnitt von Verbindungen zur C2-IP 79.254.205.77

Skript

```
#!/bin/bash

INTERFACE="eth0"
C2_IP="79.254.205.77"
DUMP_DIR="/var/tmp/bumblebee_logs"
DUMP_BASENAME="bumblebee-c2"
ROTATE_SIZE_MB=10
ROTATE_COUNT=10
PID_FILE="$DUMP_DIR/tcpdump.pid"

sudo mkdir -p "$DUMP_DIR"
sudo chmod 777 "$DUMP_DIR"

start_capture() {
  echo "[*] Starte tcpdump..."
  sudo tcpdump -i "$INTERFACE" host "$C2_IP" -nn -tttt \
    -C "$ROTATE_SIZE_MB" -W "$ROTATE_COUNT" \
    -w "$DUMP_DIR/$DUMP_BASENAME.pcap" \
    > "$DUMP_DIR/tcpdump.log" 2>&1 &
  echo $! | sudo tee "$PID_FILE" > /dev/null
  echo "[✔] tcpdump läuft im Hintergrund. PID unter $PID_FILE"
}

stop_capture() {
  if [ -f "$PID_FILE" ]; then
    PID=$(cat "$PID_FILE")
    echo "[*] Beende tcpdump mit PID $PID..."
    sudo kill "$PID"
    sudo rm -f "$PID_FILE"
    echo "[✔] Mitschnitt gestoppt."
  else
    echo "[!] Kein laufender Mitschnitt gefunden."
  fi
}

status() {
```

```
  if [ -f "$PID_FILE" ]; then
    PID=$(cat "$PID_FILE")
    if ps -p "$PID" > /dev/null; then
      echo "[] tcpdump läuft mit PID $PID."
    else
      echo "[✖] PID-Datei vorhanden, aber Prozess läuft nicht."
    fi
  else
    echo "[] Kein Mitschnitt aktiv."
  fi
}

help() {
  echo "Verwendung: $0 {start|stop|status}"
}

case "$1" in
  start) start_capture ;;
  stop) stop_capture ;;
  status) status ;;
  *) help ;;
esac
```

Verwendung

- Skript ausführbar machen: chmod +x ~/bumblebee_monitor.sh
- Start: ~/bumblebee_monitor.sh start
- Status prüfen: ~/bumblebee_monitor.sh status
- Beenden: ~/bumblebee_monitor.sh stop
- Log prüfen: sudo tail -f /var/tmp/bumblebee_logs/tcpdump.log
- .pcap-Dateien analysieren: sudo tshark -r /var/tmp/bumblebee_logs/bumblebee-c2.pcap0

Dateistruktur

```
/var/tmp/bumblebee_logs/
  ├── bumblebee-c2.pcap0 … .pcap9
  ├── tcpdump.log
  └── tcpdump.pid
```

Status

- Läuft im Hintergrund
- Terminal kann geschlossen werden
- Stoppen jederzeit möglich
- Erweiterbar (CSV, Systemd, Mail, etc.)

Hinweis

- Nur root darf schreiben – Mitschnitt läuft mit sudo
- Verzeichnis: /var/tmp/bumblebee_logs (nicht im Home-Verzeichnis!)