

Forum:[Hack Forums](#)

Thread: [\[Release\] Operational Security & Hardening Toolkit](#)

CyberXero - August 22, 2026, 2:27 am

About the Release:

Recently had to spin up a fresh device and configure a host OS, which naturally led to setting up a VM and a VPS. Since I had to implement my own opsec from scratch, I figured I'd share it with the community here.

I wanted to throw together some visuals to keep it clean, so the toolkit is split into three options: Host, VM, and VPS. Each one handles opsec differently tailored to its environment—specifically tuned so you can lock things down without bricking your setup. If you've got questions about how any of the three types work, feel free to ask.

Supported Systems:

Ubuntu / Debian / Linux Mint (and derivatives)
Requires Root/Sudo privileges

Usage Instructions:

1) makes the script executable
Code `chmod +x opsec.sh` 2) executes the script
Code `sudo ./opsec.sh`

Visual Demonstration::

Spinning Up Script.

Finished Result & Deployment.

Official Script Code:

Spoiler [\(Click to View\)](#) Code `#!/usr/bin/env bash`

```
set -e
```

```
RED='\033[1;31m'  
GREEN='\033[1;32m'  
YELLOW='\033[1;33m'  
BLUE='\033[1;34m'  
NC='\033[0m'
```

```
if [ "$EUID" -ne 0 ]; then  
    echo -e "${RED}[!] Please run as root (sudo ./core_opsec.sh)${NC}"
```

```
exit 1
fi
```

```
echo -e "${BLUE}===== ${NC}"
echo -e "${GREEN}          OPSEC & HARDENING TOOLKIT          ${NC}"
echo -e "${BLUE}===== ${NC}"
echo "Select your deployment environment:"
echo -e "${YELLOW}1)${NC} Bare-Metal Host (Linux Mint - Wi-Fi Stealth)"
echo -e "${YELLOW}2)${NC} USB VM Sandbox (Anti-Forensics & Isolation)"
echo -e "${YELLOW}3)${NC} Remote VPS (Cloud Scraping & Brute-Force Defense)"
echo -e "${BLUE}===== ${NC}"
read -p "Choice (1, 2, or 3): " env_choice
```

```
echo -e "\n${BLUE}[*] PHASE 0: Prepping the Base OS...${NC}"
echo -e "${BLUE}[!] WARNING: Linux may be processing background updates.${NC}"
echo -e "${BLUE}[!] Please wait wait patiently...${NC}"
export DEBIAN_FRONTEND=noninteractive
apt-get update -qq && apt-get full-upgrade -y -qq
```

```
apt-get purge -y timeshift > /dev/null 2>&1 || true
apt-get autoremove -y --purge > /dev/null
```

```
echo -e "${BLUE}[*] PHASE 1: Universal Network Stealth...${NC}"
apt-get install -y ufw > /dev/null
ufw --force reset > /dev/null
ufw default deny incoming
ufw default allow outgoing
```

```
cat <<EOF > /etc/sysctl.d/99-opsec.conf
net.ipv4.icmp_echo_ignore_all = 1
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_timestamps = 0
net.ipv4.conf.all.accept_redirects = 0
EOF
sysctl --system > /dev/null 2>&1
```

```
if [ "$env_choice" == "1" ]; then
    echo -e "${GREEN}[+] PHASE 2: Hardening Bare-Metal Host...${NC}"
```

```
    echo -e "[-] Setting up Automatic MAC Address Spoofing..."
    apt-get install -y macchanger > /dev/null
```

```
    cat <<EOF > /etc/NetworkManager/conf.d/00-macrandomize.conf
[device]
wifi.scan-rand-mac-address=yes
```

```
[connection]
wifi.cloned-mac-address=random
ethernet.cloned-mac-address=random
EOF
```

```

systemctl restart NetworkManager
echo -e "${GREEN}[+] Host locked down. Hardware MAC hidden.${NC}"

elif [ "$env_choice" == "2" ]; then
    echo -e "${GREEN}[+] PHASE 2: Hardening USB VM Sandbox...${NC}"

    echo -e "[-] Nuking Bash History (Amnesic Terminal)..."
    ln -sf /dev/null ~/.bash_history

    echo -e "[-] Disabling Swap Memory..."
    swapoff -a
    sed -i 's/^(\.*)$/#\1/g' /etc/fstab

    echo -e "[-] Disabling Core Dumps..."
    echo "* hard core 0" >> /etc/security/limits.conf

    echo -e "[-] Removing VM Guest Additions (Clipboard Isolation)..."
    apt-get remove -y open-vm-tools virtualbox-guest-utils > /dev/null 2>&1 || true

    echo -e "${GREEN}[+] VM Sandboxed. Anti-forensics active.${NC}"

elif [ "$env_choice" == "3" ]; then
    echo -e "${GREEN}[+] PHASE 2: Hardening Remote VPS...${NC}"

    read -p "Enter your SSH Port (Default 22): " ssh_port
    ssh_port=${ssh_port:-22}

    echo -e "[-] Configuring strict UFW rules..."
    ufw limit "$ssh_port"/tcp comment 'SSH Rate-Limited'
    ufw allow 80/tcp comment 'HTTP'
    ufw allow 443/tcp comment 'HTTPS'

    echo -e "[-] Installing and configuring Fail2Ban..."
    apt-get install -y fail2ban > /dev/null
    systemctl enable fail2ban > /dev/null
    systemctl start fail2ban > /dev/null

    echo -e "[-] Moving /var/log to RAM (tmpfs)..."
    if ! grep -q "/var/log tmpfs" /etc/fstab; then
        echo "tmpfs /var/log tmpfs defaults,noatime,nosuid,mode=0755,size=100m 0 0" >> /etc/fstab
        mount -a
    fi

    echo -e "${GREEN}[+] VPS Secured. Volatile logs and Brute-force defense active.${NC}"

else
    echo -e "${RED}[!] Invalid choice. Exiting safely.${NC}"
    exit 1
fi

echo -e "${BLUE}[*] Enabling UFW...${NC}"
ufw --force enable > /dev/null

```

```
echo -e "${GREEN}===== ${NC}"
echo -e "${GREEN} SYSTEM SECURED & DEPLOYMENT COMPLETE      ${NC}"
echo -e "${GREEN}===== ${NC}"
ufw status numbered
```

Environment Hardening Overview

Feature / Environment Bare-Metal (Host) VM Sandbox Remote VPS Network Stealth
(ICMP/IPv6/TCP) ? Enabled ? Enabled ? Enabled Identity Masking (MAC Spoofing) ? Active ? N/A
? N/A Anti-Forensics (No History/Swap) ? Disabled ? Active ? Disabled Guest Isolation (No
Clipboard/Tools) ? N/A ? Active ? N/A Brute-Force Defense (Fail2Ban) ? Disabled ? Disabled ?
Active Volatile Logging (RAM-only) ? Disabled ? Disabled ? Active

Bare-Metal (Host): Focuses on Hardware Anonymity. It randomizes MAC addresses to prevent physical tracking via Wi-Fi/Ethernet.

VM Sandbox: Focuses on Anti-Forensics. It disables swap, wipes bash history, and removes guest tools to prevent data leaks from the VM to the host.

Remote VPS: Focuses on Persistence & Defense. It uses Fail2Ban to stop brute-force attacks, stores logs in RAM so they vanish instantly if the server is rebooted or seized.

Universal: All environments benefit from Network Hardening, which includes disabling IPv6 (to prevent leaks), ignoring Pings (stealth mode), and strict Firewall rules.

G33K - September 8, 2026, 9:10 am

Looking good you planning on expanding the project? Keep up the good work!

CyberXero - September 9, 2026, 12:04 pm

(Sep 8, 2026 09:10 AM)G33K Wrote: [\[CITE\]](#) Looking good you planning on expanding the project? Keep up the good work!
Certainly!

But... I have started with updating the thread adding the overview that i missed out, now people will know the purpose of each, great for those that can read the code, i personally assumed that most would know how to read the source,

more features are to be added ?

HeySister - September 20, 2026, 12:15 am

Amazing! Love ur proyects