

NetHunter Unleashed

O Guia Definitivo para Pentesters e Operadores



Davi "dmx" Trindade
Pentester and everything else in free time





\$ Whoami



xdavimob [Seguir](#) ...

6 publicações 807 seguidores 708 seguindo

DMX

hacking to breathe

- Pentester e nas horas vagas pesquisador
- Formado em Cybersecurity na FIAP
- Speaker: H2HC 2024 e BSides SP 2025
- Aulas de Tips & Tricks do Hacking Club
- Proplayer quando dá no CS e Valorant (Ex-plat)



Tópicos

- Introdução: Contexto e motivação da pesquisa
- A origem do NetHunter
- Impacto real na segurança ofensiva
- Instalação e compatibilidade
- Funcionalidades e Ferramentas
- Provas de Conceito reais
- Limitações e como contornar
- NetHunter em **RedOps**
- Considerações finais e próximos passos

Introdução





Motivação da Pesquisa

- Estudo contínuo sobre Mobile Security
- Publicação técnica no blog da Hakai
- Necessidade de uma fonte clara, técnica e realista sobre o uso do NetHunter em campo

“Não existia um guia moderno e completo em português focado em RedOps com NetHunter.”



Objetivos da Palestra

O que o público vai levar?

- Ter um overview da instalação e uso prático do NetHunter
- Entender seu potencial como ferramenta ofensiva
- Ver ataques reais simulados via celular
- Saber quando, onde e como usar no Red Team físico

Origem do NetHunter





Origem do NetHunter

- Iniciativa da Offensive Security
- Levar o Kali para Android com mobilidade e eficácia
- Crescimento com apoio da comunidade

“Pentest não precisa mais de mochila com notebook – só de criatividade.”

Kali NetHunter Kernels

- Kali NetHunter has a total of [243 kernels](#)
 - These kernels can be used on [104 device models](#)
- [Kali NetHunter Statistics Overview](#)

Display Name	Kernel-ID	Android Version	Linux Version	Kernel Version	Description	Features	Author
Asus Zenfone 2 Laser (720p)	zooe-l0s	marshmallow	3.1		LineageOS 13.0	HID, Injection	adrenogamer
Google Nexus 10	manta	lollipop	3.04		Android 5	BT_RFCOMM, CDROM, HID, Injection	jmmmbnnn
Google Nexus 4	mako	kitkat	3.04		Android 4	HID, Injection	Binkybear
Google Nexus 4	mako	lollipop	3.04		Android 5	HID, Injection	Binkybear
Google Nexus 4	mako-cm	marshmallow	3.04		CyanogenMod 13	HID, Injection	jeadduono
Google Nexus 5	hammerhead	kitkat	3.04		Android 4.4	CDROM, HID, Injection	Binkybear
Google Nexus 5	hammerhead	lollipop	3.04		Android 5	CDROM, HID, Injection	Binkybear
Google Nexus 5	hammerhead	marshmallow	3.04		Android 6	BT_RFCOMM, HID, Injection, NEXMON	Re4son
Google Nexus 5	hammerhead-caf-l0s	nougat	3.04		CAF LineageOS 14.1	HID, Injection	chrisk44

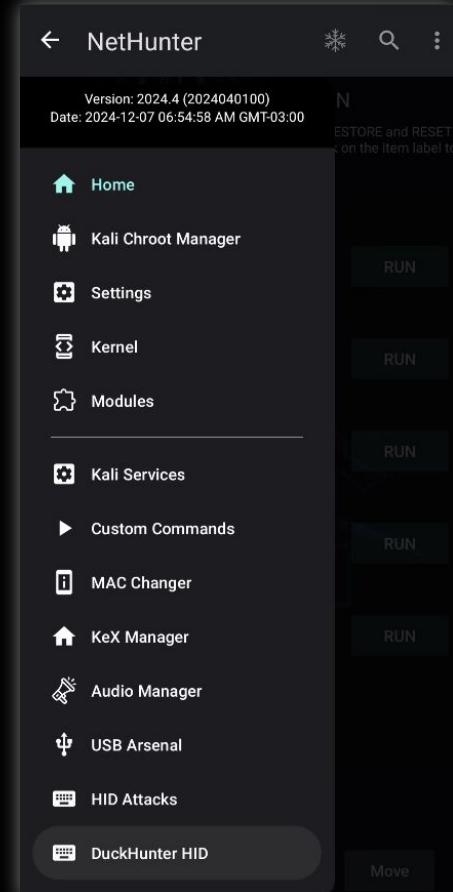
Impacto do NetHunter





Impacto do NetHunter

- Portabilidade real: tudo no bolso
- Interface Kali nativa (Nmap, MITM, HID, DeAuth, etc)
- Agilidade em ambientes com pouco tempo ou alto risco





Impacto do NetHunter

- Terminal Kali Linux
 - Acesso ao Bash
 - Suporte a ferramentas
 - Scripts e Exploits
 - Integração com OTG
 - É um Kali Linux real, não um simulador
 - Ecossistema Kali Toolkit
 - Todos os pacotes do Kali
 - Chroot ou proot dinâmico - separa o Android sem perder recursos
 - Ataques Wi-Fi em campo com mobilidade total
 - Monitor mode + Packet Injection
 - DeAuth, captura de handshake, fake AP's
 - **Aircrack-ng, wifite, hcxdumptool**
 - Wifipumpkin e EvilTwin

"Mesmo sem atualização específica do NetHunter, o Kali está sempre na minha mão – literalmente."



Impacto do NetHunter

Ano	Evento/Versão	Tipo	Descrição	Fonte
2014	NetHunter Launch	NetHunter Core	Lançado com suporte a HID, USB attacks e ambiente Kali via chroot.	https://www.kali.org/blog/kali-nethunter/
2015	NetHunter v1.1	NetHunter Core	Suporte aprimorado para OnePlus One e Nexus 4.	OffSec
2015	NetHunter v1.2	NetHunter Core	Suporte a Android Lollipop, Nexus 6 e Nexus 9.	OffSec
2016	NetHunter 3.0	NetHunter Core	Reescrita completa do app Android com nova interface.	OffSec
2019	NetHunter Store Launch	NetHunter Core	Lançamento da NetHunter Store para distribuição de apps ofensivos.	Kali Docs Kali Linux Documentation
2019	Rootless Mode via Proot	NetHunter Core	Execução de ambiente Kali no Android sem root.	Kali Linux Blog
2020	NetHunter KeX	NetHunter Core	GUI completa via VNC com ambiente Kali full.	https://www.kali.org/blog/nethunter-kex-update-2020/
2020	Kali Linux 2020.3	Kali Linux Base	Introdução do Bluetooth Arsenal e suporte expandido a dispositivos.	Kali Linux Blog
2022	NetHunter Pro (PinePhone)	NetHunter Core	Primeira versão do Kali Linux completo em smartphone (PinePhone/Pro).	Kali Linux Blog
2022	Kali Linux 2022.4	Kali Linux Base	Anúncio do NetHunter Pro e melhorias no ecossistema móvel.	Kali Linux Blog
2023	Kali Linux 2023.1	Kali Linux Base	Lançamento comemorativo de 10 anos do Kali Linux.	Kali Linux Blog
2023	Kali Linux 2023.2	Kali Linux Base	Correções para UEFI, Hyper-V e refinamentos de kernel.	Kali Linux Blog
2023	Kali Linux 2023.3	Kali Linux Base	Atualizações e melhorias contínuas.	Kali Linux Blog
2023	Kali Linux 2023.4	Kali Linux Base	Melhorias incrementais de ferramentas.	Kali Linux Blog
2024	Kali Linux 2024.x	Kali Linux Base	Atualizações regulares de toolset, kernel e compatibilidade.	Kali Linux Blog

Casos Reais + Cenários Possíveis





Caso Real

Em janeiro de 2022, o **Condado de Bernalillo** (Novo México, EUA) foi alvo de um **ataque de ransomware**.

Resultados

immediatos:

- Portas automáticas da prisão desligadas
- Monitoramento remoto de celas e movimentações desativado
- Sistema judiciário interrompido por dias

Ataque teve **impacto físico direto** e representou um risco real à segurança pública.





Cenários Possíveis

Como o NetHunter poderia ter sido usado nesse cenário?

Não foi um ataque via celular... mas poderia ter começado com um!

1. Recon físico e digital

- a. Identificar SSIDs locais (Wi-Fi interno, visitantes, IoT)
- b. Mapear dispositivos visíveis na rede com `netdiscover`, `nmap`, `arp-scan`
- c. Fingerprint de sistemas por banners, headers e portas

2. Delivery físico de payloads (BadUSB / HID)

- a. NetHunter configurado com **DuckHunter HID**
- b. Execução automática de script via USB em estação vulnerável de um funcionário
- c. Download e execução de um dropper inicial (ponto de persistência)

3. Engenharia Social + Rogue AP

- a. Criação de rede Wi-Fi maliciosa próxima ao perímetro da prisão ou prefeitura
- b. Redirecionamento via captive portal falso (Wi-Fi Pumpkin)

"Se você tivesse que entregar um artefato de acesso inicial sem levantar suspeitas..."

"Usaria um notebook ou um celular carregando o NetHunter no bolso?"

Dispositivos e Instalação





Dispositivos

XIAOMI:

- Mi 9T (davinci) - altamente recomendado
- Mi 9T Pro (raphael) - um grande desafio
- ...

SAMSUNG (o maior desafio é o bypass da Samsung):

- S10
- S-Vários
- J-Tudo
- A-Fodase

MOTOROLA:

- G5
- X4

Samsung

Samsung Galaxy A7 (2016) (LineageOS 18.1)	↓ 120M	torrent	sum
Samsung Galaxy S10 (A15)	↓ 2.2G	torrent	sum
Samsung Galaxy Tab S4 LTE (Oreo)	↓ 2.2G	torrent	sum
Samsung Galaxy Tab S4 WiFi (Oreo)	↓ 2.2G	torrent	sum
Samsung Galaxy S7 Edge (Pie)	↓ 2.2G	torrent	sum
Samsung Galaxy S7 Edge (LineageOS 16.0)	↓ 120M	torrent	sum
Samsung Galaxy S7 (Pie)	↓ 2.2G	torrent	sum
Samsung Galaxy S7 (LineageOS 16.0)	↓ 2.2G	torrent	sum
Samsung Galaxy J7 Pro (Pie)	↓ 2.2G	torrent	sum
Samsung Galaxy S5 Mini (LineageOS 16.0)	↓ 120M	torrent	sum
Samsung Galaxy J7 Prime (Pie)	↓ 2.2G	torrent	sum
Samsung Galaxy S20 FE 5G (Thirteen)	↓ 2.2G	torrent	sum
Samsung Galaxy S9 (LineageOS 20)	↓ 2.2G	torrent	sum
Samsung Galaxy S9+ (LineageOS 20)	↓ 2.2G	torrent	sum
Samsung Galaxy S6 Edge (LineageOS 14.1)	↓ 2.2G	torrent	sum



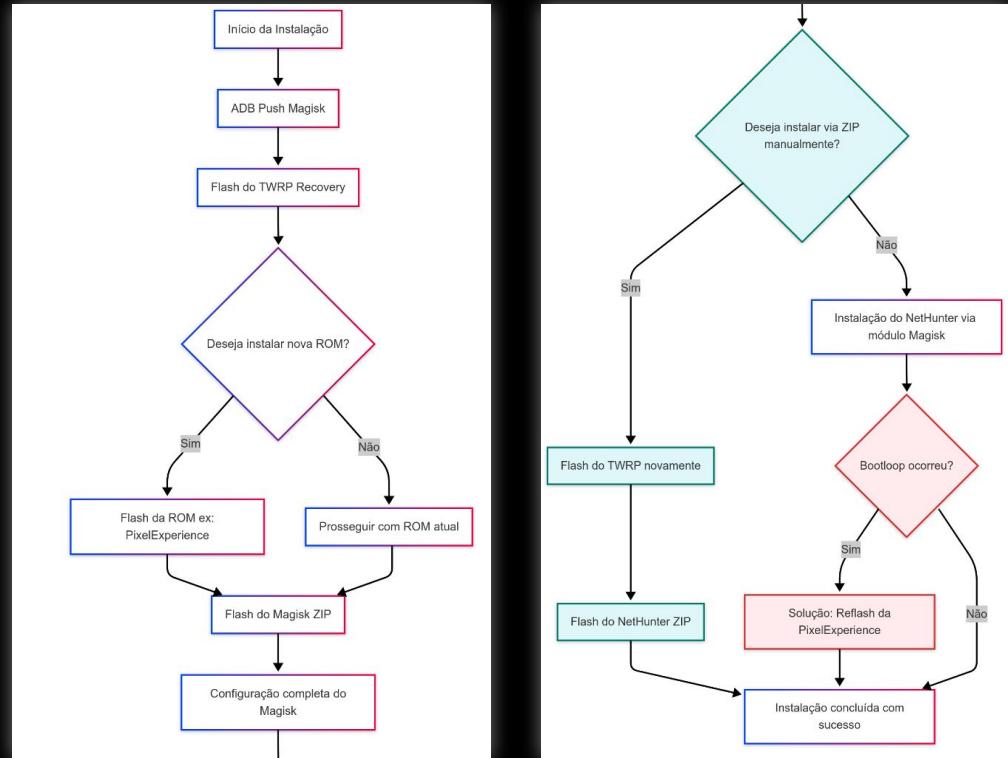
Dispositivos

Versão	Versão Requisitos	Acesso Root	Recursos Habilitados	Vantagens	Desvantagens
NetHunter Rootless	Dispositivo sem root; instalação via APK; builds oficiais ou customizadas	Não requer	Ambiente chroot com diversas ferramentas do Kali (com algumas limitações)	Não exige root, facilitando a instalação em dispositivos restritos	Acesso limitado a módulos avançados; menos controle total
NetHunter Lite	Dispositivo com root; bootloader desbloqueado; pode usar builds customizadas	Requer	Funcionalidades intermediárias; maior compatibilidade com módulos essenciais	Equilíbrio entre funcionalidade e facilidade de instalação	Pode não oferecer todos os recursos disponíveis na versão Full
NetHunter Full	Dispositivo com root; bootloader desbloqueado; preferencialmente builds oficiais (ex.: Mi 9T, OnePlus, Pixel)	Requer	Acesso completo a todos os módulos e recursos do Kali Linux, suporte avançado (Wi-Fi, USB, etc.)	Experiência robusta e completa, ideal para testes avançados	Instalação mais complexa; maior consumo de recursos e bateria



Instalação

- Imagem do TWRP compatível
- Fastboot e ADB
- Arquivo do Magisk
- Imagem do NetHunter Full



Funcionalidades- Chave





Funcionalidades-Chave

- HID
- BadUSB
- MITM
- Wi-Fi (handshake, deauth, rogue)
- Bluetooth/NFC
- NetHunter Store + Kali Chroot

Attack

Attacks

*Transforma o celular em um
Rubber Ducky + Rogue AP + MITM
Proxy + Kali.*

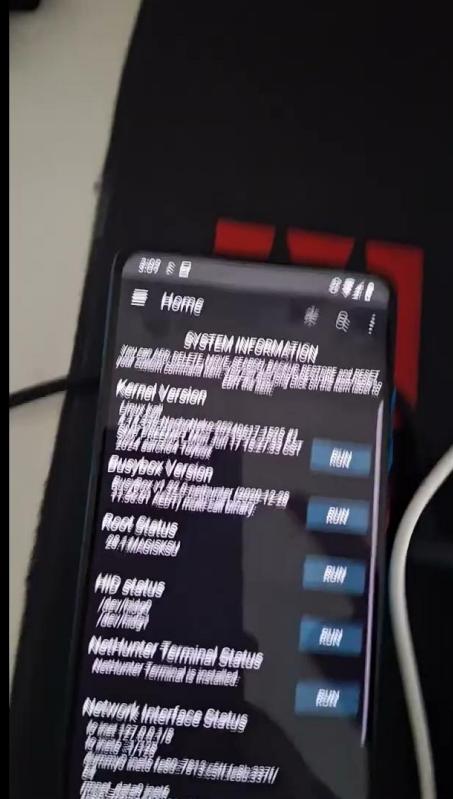
The screenshot shows the NetHunter Store application interface. It features a navigation bar at the bottom with icons for Latest, Categories, Nearby, Updates, and Settings. Above the navigation bar are four main sections: 'Development' (with three items: Termux, Termux:API, and Termux:Float), 'Exploitation' (with three items: Rucky, cSploit, and Router Keygen), 'Forensics' (with two items: SysLog and Hash Droid), and 'Information Gathering' (with one item: a magnifying glass icon). Each section has a 'VIEW ALL' button to its right.

PoCs com
NetHunter



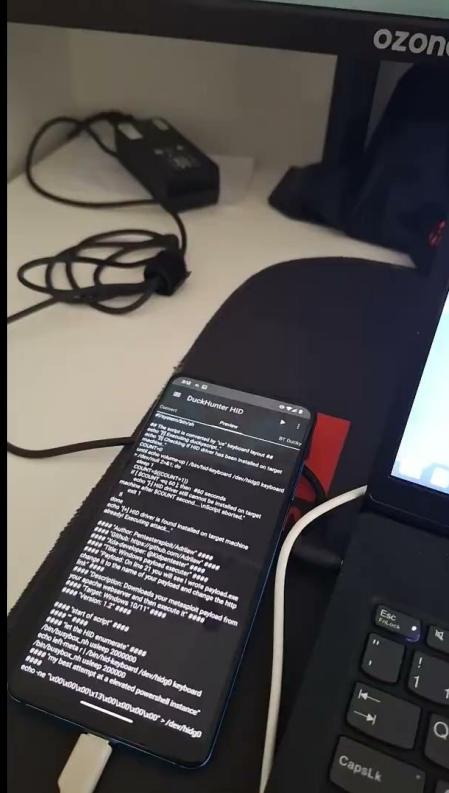


PoC 1 - HID Attack (DuckHunter)





PoC 1 - HID Attack (DuckHunter)





PoC 2 - Rogue AP com Wifipumpkin

Start an Evil-Twin Access Point and intercept HTTP traffic. Custom captive portals, featuring mobile network upstream (rmnet_data2), internal wlan0 upstream, internal wlan0/wlan1 AP mode, and external adapters. Custom portals are also supported. Testing version. Preview will be added soon.

Internal Wifi AP mode: Supported

Virtual wlan1 interface

Access Point wlan1

Upstream wlan0

SSID Wi-Fi a bordo

BSSID 00:11:22:33:44:55

Channel 1

Captive Portal

↻

None

[Install from zip](#)

Start





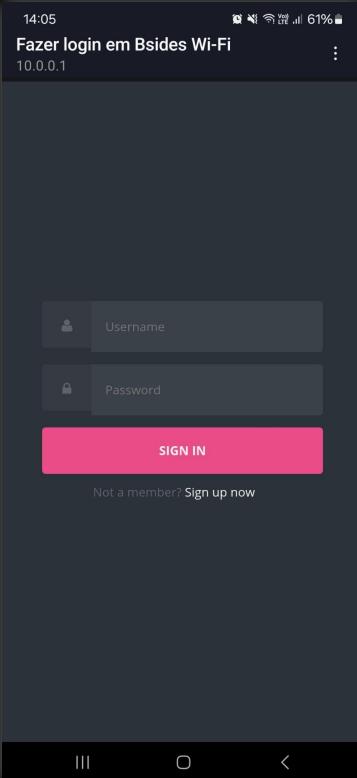
PoC 2 - Rogue AP com Wifipumpkin

```
Wifipumpkin3
[  ]012] hostname: 'A54-de-Davi'
[  ]050] requested_ip_address: IPv4Address('10.0.0.21')
[  ]053] dhcp_message_type: DHCP.REQUEST
[X]054] server_identifier: IPv4Address('10.0.0.1')
[  ]055] parameter_request_list: 053:dhcp_message_type,
054:server_identifier
[  ]057] maximum_dhcp_message_size: 1500
[  ]060] vendor_class_identifier: 'android-dhcp-14'
[  ]061] client_identifier: [398, 17879, 24811]

(16:54:07) [*] 10.0.0.21: proxying the response of type 'A' for
dns.adguard.com
[  ]pydhcp_server] 16:54:07 - REQUEST: packet from 10.0.0.21
to 10.0.0.1
[*] 08:45:d7:60:eb:5c client join the AP
[  ]pydhcp_server] 16:54:07 - SEND TO ('0.0.0.0', 68):
:header:
    op: BOOTREPLY
    hmac: MAC('8e:45:d7:60:eb:5c')
    flags:
    hops: 0
    secs: 0
    xid: 3785248275
    siaddr: IPv4Address('0.0.0.0')
    giaddr: IPv4Address('0.0.0.0')
    ciaddr: IPv4Address('0.0.0.0')
    yiaddr: IPv4Address('10.0.0.21')
    name: ''
    file: ''

:Body:
    [x][001] subnet_mask: IPv4Address('255.0.0.0')
    [x][003] router: [IPv4Address('10.0.0.1'), IPv4Address(
'8.8.8.8')]
    [x][006] domain_name_servers: [IPv4Address('10.0.0.1')]
    [  ]012] hostname: 'A54-de-Davi'
    [X]051] ip_address.lease_time: 7200
    [-]053] dhcp_message_type: DHCP.ACK
    [X]054] server_identifier: IPv4Address('10.0.0.1')

[  ]sniffkin3] 16:54:07 - [ 10.0.0.21 > 172.217.30.131 ] SET
connectivitycheck.gstatic.com/generate_204
(16:54:07) [*] 10.0.0.21: proxying the response of type 'A' for
www.google.com
[  ]sniffkin3] 16:54:08 - [ 10.0.0.21 > 77.74.177.233 ] SET
touch.kaspersky.com?os=Android&appID=2280&reason=wifi
```



```
Wifipumpkin3
1.1* 302 -
[  ]sniffkin3] 17:05:47 - [ 10.0.0.21 > 10.0.0.1 ] SET
0.0.1/assets/images/icons.svg
[  ]sniffkin3] 17:05:48 - [ 10.0.0.21 > 10.0.0.1 ] SET
0.0.1/favicon.ico
[  ]sniffkin3] 17:05:48 - [ 10.0.0.21 > 172.217.172.131 ] GET
connectivitycheck.gstatic.com/generate_204
17:06:25 [*] 10.0.0.21: proxying the response of type 'A' for
connectivitycheck.gstatic.com
[  ]captiveflask] 17:06:25 - { '10.0.0.21': { 'login': 'dmx',
'password': "bsides<'_>" } }

(*) CaptiveFlask credentials:
IP      | Login   | Password
+-----+-----+
10.0.0.21 | dmx     | bsides<'_>

[  ]sniffkin3] 17:06:25 - [ 10.0.0.21 > 10.0.0.1 ] POST
10.0.0.1/login?orig_url=http%3A%2F%2Fconnectivitycheck.gstatic.com%2Fgenerate_204
payload: login=dmx&password=bsides%3C%27%3E
_X27%3E
Username: dmx
Password: bsides%3C%27%3E

17:06:25 [*] 10.0.0.21: proxying the response of type 'AA' for
dns.adguard.com
17:06:25 [*] 10.0.0.21: proxying the response of type 'A' for
dns.adguard.com
[  ]sniffkin3] 17:06:25 - [ 10.0.0.21 > 10.0.0.1 ] POST
10.0.0.1/Login?orig_url=http%3A%2F%2Fconnectivitycheck.gstatic.com%2Fgenerate_204
[  ]captiveflask] 17:06:25 - 10.0.0.21 -- [07/Apr/2025:17:06:25]
POST /login?orig_url=http://connectivitycheck.gstatic.com/generate_204 HTTP/1.1" 200
[0.0.0.21 -- [07/Apr/2025 17:06:25] "GET /static/css/bootstrap.min.css HTTP/1.1" 304
[0.0.0.21 -- [07/Apr/2025 17:06:25] "GET /static/fonts/google_fonts.css HTTP/1.1" 304
[0.0.0.21 -- [07/Apr/2025 17:06:25] "GET /static/js/jquery-1.11.1.min.js HTTP/1.1" 304
[0.0.0.21 -- [07/Apr/2025 17:06:25] "GET /static/js/bootstrap.min.js HTTP/1.1" 304
[0.0.0.21 -- [07/Apr/2025 17:06:25] "GET /assets/images/icon.svg HTTP/1.1" 302 -
```

Limitações e Soluções





Limitações

Limitações Técnicas Adicionais

- Instabilidade em ROMs customizadas
 - Builds sem suporte adequado ao SELinux, módulos do kernel ou serviços necessários
 - Pode causar falhas em ferramentas críticas como aircrack-ng, HID gadget etc
- Problemas com permissões Android modernas
 - Android +11 implementa restrições de acesso ao filesystem, dificultando execuções direta de scripts, uso de payloads locais e acesso a partições como /data
- Falta de suporte a adaptadores modernos (Wi-Fi/Bluetooth)
 - Muitos adaptadores incompatíveis com as builds do kernel do NetHunter

Limitações Operacionais

- Detecção fácil por antivírus e MDMs corporativos
 - Dispositivos com NetHunter Full são identificáveis em soluções de Mobile Threat Defense ou controle de endpoints (Jamf, Microsoft Intune)
- Não é stealth por padrão
 - É literalmente um Kali conectado na rede (?)
- Ausência de atualizações frequentes em algumas versões



Soluções

- Comunidade ativa no XDA e outros fóruns, sempre desenvolvendo algo novo, arrumando bugs, manuais de uso etc
- PowerBank
- Updates atuais dos resources do Kali
- Problemas operacionais:
 - Muito troubleshooting
 - MUITO
 - ...

NetHunter em RedOps

Onde entra o NetHunter dentro de uma operação real ofensiva?





NetHunter em RedOps

Fase	Descrição da Fase	Como o NetHunter ajuda
1. Reconhecimento	Coleta de informações do alvo	Wi-Fi scan, SSID spoofing, nmap, fingerprint física
2. Armamento	Preparação de malware, scripts ou payloads	Fora do escopo direto do NH, mas pode testar payloads
3. Entrega	Transmissão do artefato para o alvo	HID Attack via DuckHunter, BadUSB, Rogue AP com trap
4. Exploração	Execução do payload e abuso da falha	Execução automática via teclado simulado ou WiFi MITM
5. Instalação	Persistência, scripts adicionais, backdoors	Criação de usuários, backdoors via teclado (PoC 1)
6. C2	Comunicação com host comprometido	NetHunter pode iniciar listeners ou tunelamentos
7. Ações nos Objetivos	Extração de dados, sabotagem, etc.	Possível integração com ferramentas para exfiltração



Casos de uso por fase

- **Reconhecimento físico**
- Escaneamento de redes internas e dispositivos próximos
- Uso em eventos, áreas públicas, recepções
 - ◆ **Entrega (Delivery)**
- HID Attack conectado por poucos segundos
- BadUSB com scripts silenciosos
- Rogue AP em campo com captive portal clonado



◆ Exploração

- Execução de scripts como PoC #1
- Início de shells reversas discretas

◆ Instalação e Persistência

- Criação de contas locais, backdoor em startup
- Shells automatizadas com delays

Considerações Finais





Considerações Finais

- Revolução prática no pentest/RedOps com mobile
- Portátil, poderoso, funcional
- Uso aplicável em campo
- Engajado com a comunidade

Call to Action





Call to Action

- Instale o NetHunter, comece a testar
- Pratique com HID, WiFi, MITM
- Contribua com tutoriais, PoCs, scripts.
- Blog Post em breve com passos da instalação



<Thank you!>

davitrindadesec@gmail.com

@dmxhck - @xdavimob

