

Kali in Your Pocket – NetHunters i Raspberries

Wprowadzenie

W niektórych przypadkach podczas przeprowadzania pentestu klient może poprosić nas o przeprowadzenie właściwego ataku red team. W takich przypadkach wejście do biura z laptopem w rękę może wyglądać podejrzanie. Możemy przeprowadzić red teaming przy użyciu małego urządzenia, takiego jak telefon komórkowy lub Raspberry Pi, i skutecznie przeprowadzić pentest przy ich użyciu. W tym rozdziale omówimy konfigurację Kali Linux na Raspberry Pi i kompatybilnych telefonach komórkowych oraz wykorzystanie go do przeprowadzenia kilku fajnych ataków na sieć.

Instalowanie Kali na Raspberry Pi

Raspberry Pi to niedrogi komputer ARM. Jest niezwykle mały, co czyni go przenośnym, a dzięki temu najlepiej nadaje się do systemów podobnych do Kali Linux do przeprowadzania pentestów na urządzeniach przenośnych. W tym przepisie dowiesz się, jak zainstalować obraz Kali Linux na Raspberry Pi.

Przygotowania

Raspberry Pi obsługuje karty SD. Najlepszym sposobem na skonfigurowanie Kali na Raspberry Pi jest utworzenie rozruchowej karty SD i włożenie jej do Pi. Jak to zrobić...

Aby zainstalować Kali na Raspberry Pi, wykonaj następujące kroki:

1. Najpierw pobierzemy obraz ze strony Offensive Security pod adresem <https://www.offensive-security.com/kali-linux-arm-images/> :

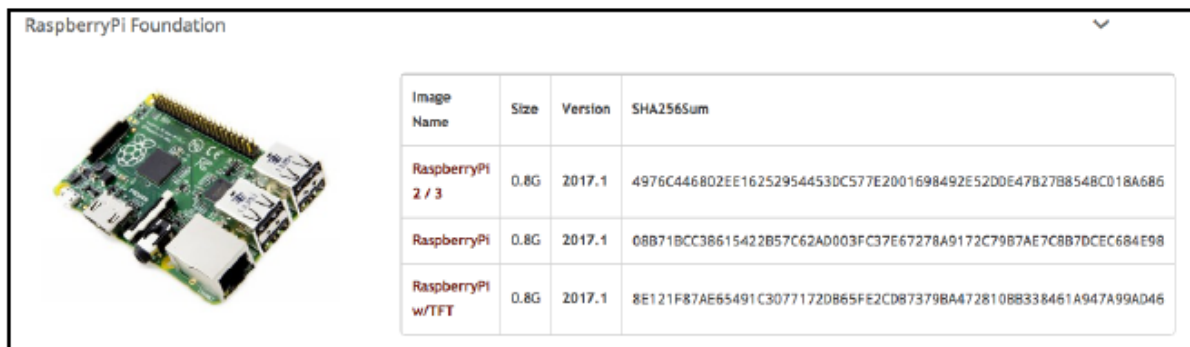


Image Name	Size	Version	SHA256Sum
RaspberryPi 2 / 3	0.8G	2017.1	4976C446802EE16252954453DC577E2D01698492E52D0E47B27B854BC018A686
RaspberryPi	0.8G	2017.1	08B71BCC38615422B57C62AD003FC37E67278A9172C79B7AE7C8B7DCEC684E98
RaspberryPi w/TFT	0.8G	2017.1	8E121F87AE65491C3077172DB65FE2CD87379BA472810BB338461A947A99AD46

2. Po pobraniu obrazu możemy użyć różnych sposobów, aby zapisać go na karcie pamięci.

3. W systemie Linux/macOS można to zrobić za pomocą narzędzia dd. Narzędzie dd można użyć za pomocą następującego polecenia:

```
dd if=/path/to/kali-2.1.2-rpi.img of=/dev/sdcard/path bs=512k
```

4. Po zakończeniu tego procesu możemy podłączyć kartę SD do Pi i włączyć ją.

5. Zobaczmy, jak uruchamia się Kali:



Instalowanie NetHunter

Jak opisano na oficjalnej wiki Offensive Security:

„Kali NetHunter to nakładka ROM Androida, która zawiera solidną platformę Mobile Penetration Testing Platform. Nakładka zawiera niestandardowe jądro, chroot Kali Linux i towarzyszącą aplikację Androida, która umożliwi łatwiejszą interakcję z różnymi narzędziami bezpieczeństwa i atakami. Oprócz arsenału narzędzi do testowania penetracji w Kali Linux, NetHunter obsługuje również kilka dodatkowych klas, takich jak ataki klawiatury HID, ataki BadUSB, ataki Evil AP MANA i wiele innych. Aby uzyskać więcej informacji o ruchomych częściach, z których składa się NetHunter, sprawdź naszą stronę NetHunter Components. NetHunter to projekt typu open source opracowany przez Offensive Security i społeczność”.

W tym przepisie dowiesz się, jak zainstalować i skonfigurować NetHunter na urządzeniu z Androidem oraz przeprowadzać ataki przy jego użyciu. Listę obsługiwanych sprzętu można znaleźć na stronie <https://github.com/offensive-security/kali-NetHunter/wiki>.

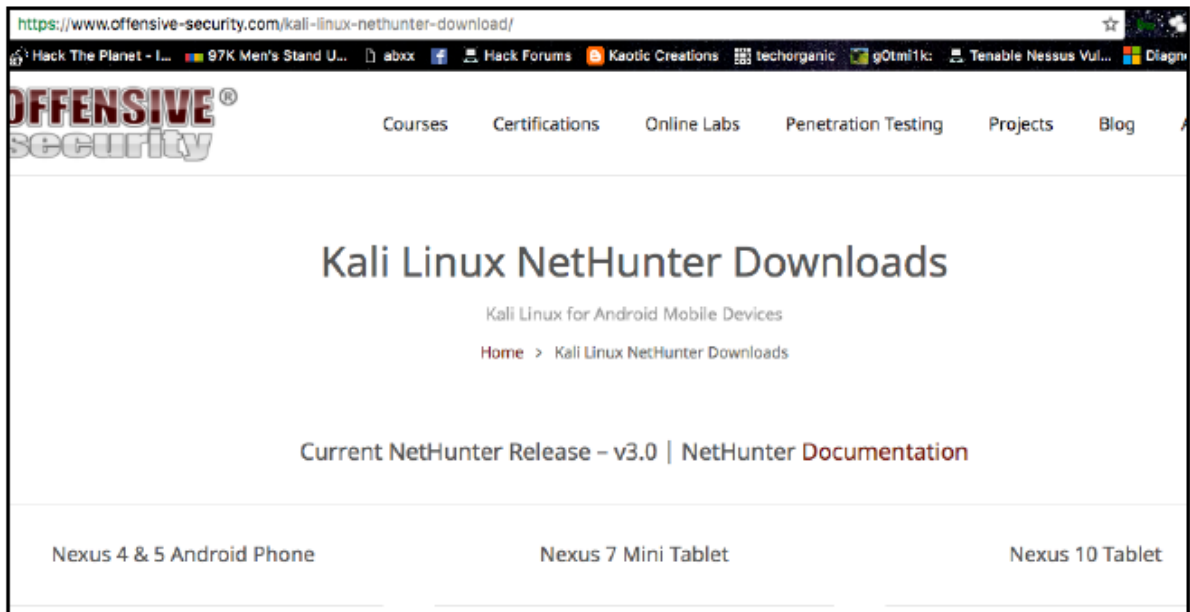
Przygotowanie

Zanim zaczniemy, musimy zrootować urządzenie z zainstalowanym Team Win Recovery Project jako niestandardowym recovery.

Jak to zrobić...

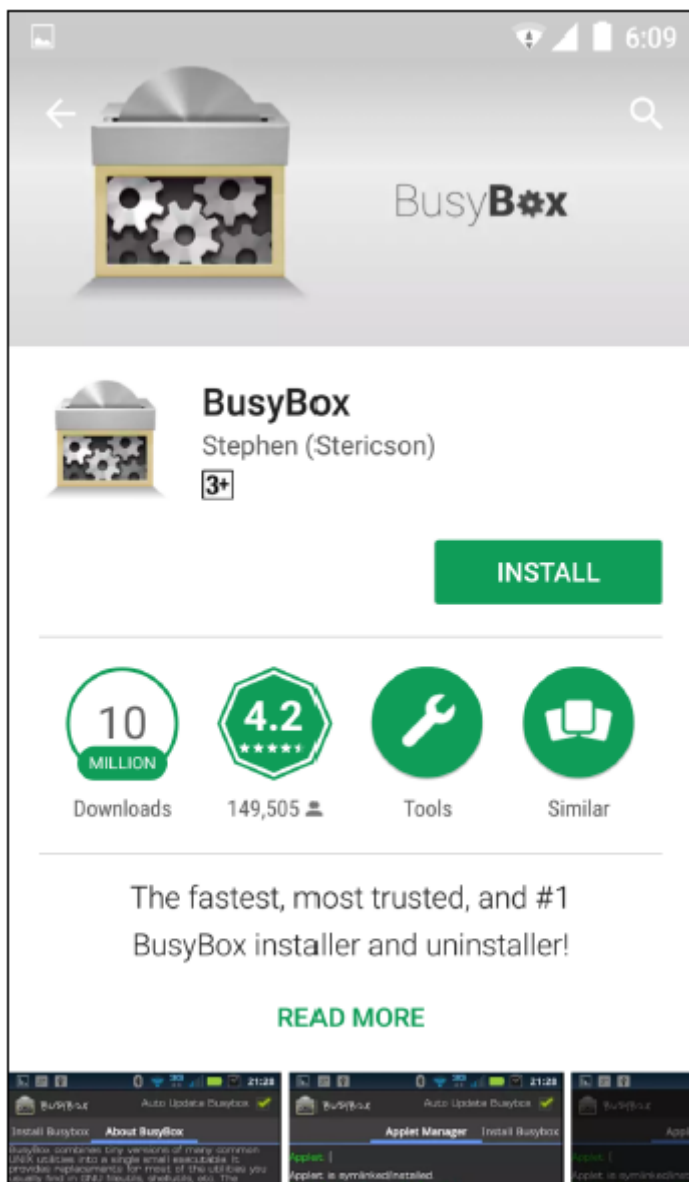
Aby zainstalować NetHunter, wykonaj następujące kroki:

1. Pobieramy plik ZIP NetHunter i kopiujemy go na kartę SD, a następnie restartujemy telefon w trybie recovery. Używamy OnePlus One z Cyanogenmod 12.1. Tryb recovery można uruchomić, naciskając jednocześnie przycisk zasilania i przycisk zmniejszania głośności.
2. Po przejściu w tryb recovery wybieramy instalację na ekranie i wybieramy plik ZIP. Możemy pobrać plik ZIP z <https://www.offensive-security.com/kali-linux-NetHunter-download/>:

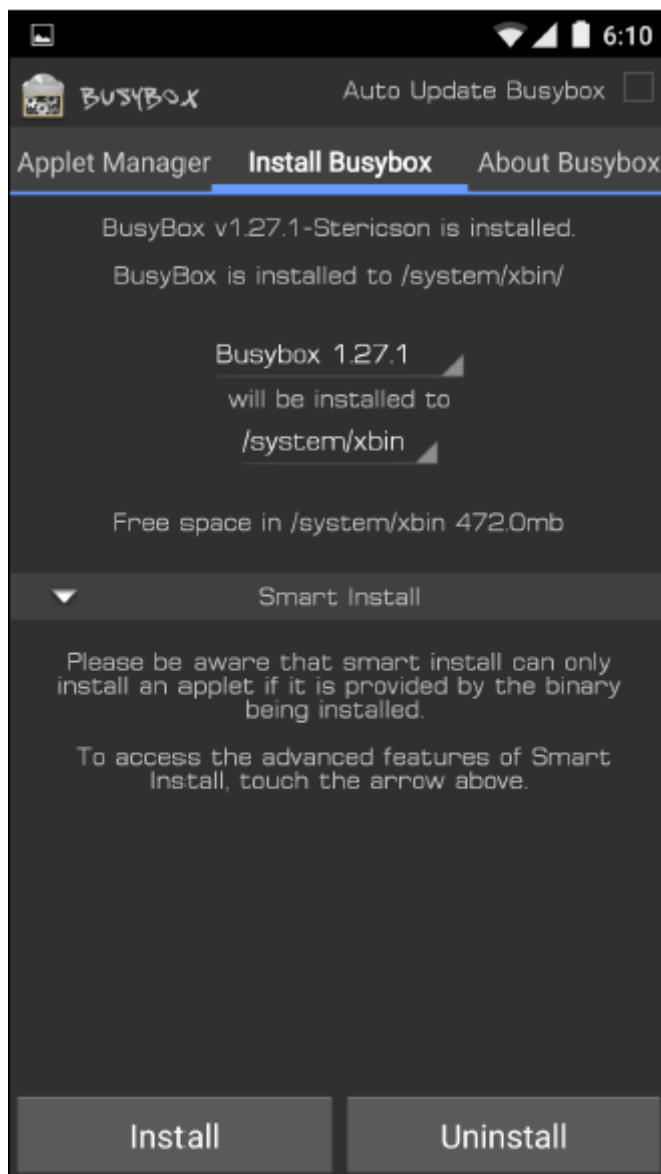


3. Po zakończeniu operacji należy ponownie uruchomić telefon. W menu aplikacji powinniśmy zobaczyć aplikację NetHunter.

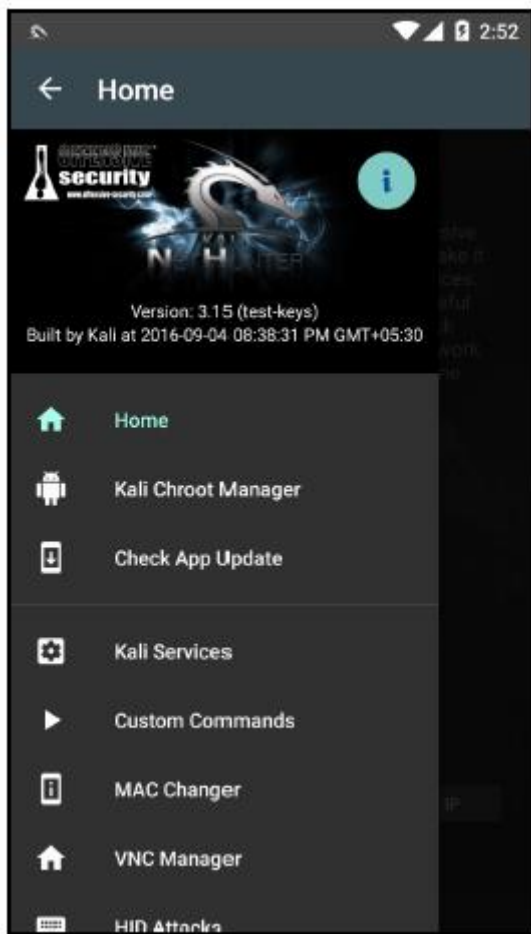
4. Ale zanim zaczniemy, musimy zainstalować BusyBox na telefonie ze sklepu Play:



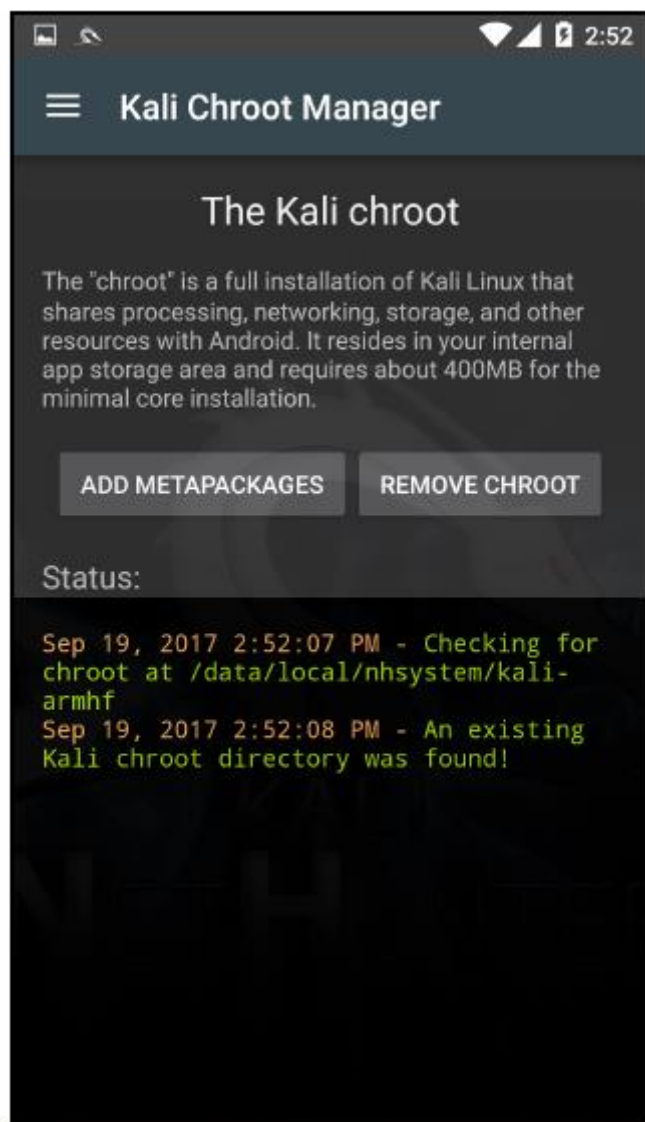
5. Po wykonaniu tej czynności uruchamiamy aplikację i klikamy Zainstaluj:



6. Następnie otwieramy NetHunter i z menu wybieramy Kali Chroot Manager:



7. Klikamy DODAJ METAPAKOWANIA i będziemy gotowi na kolejny przepis:



Pisanie Supermana – ataki HID

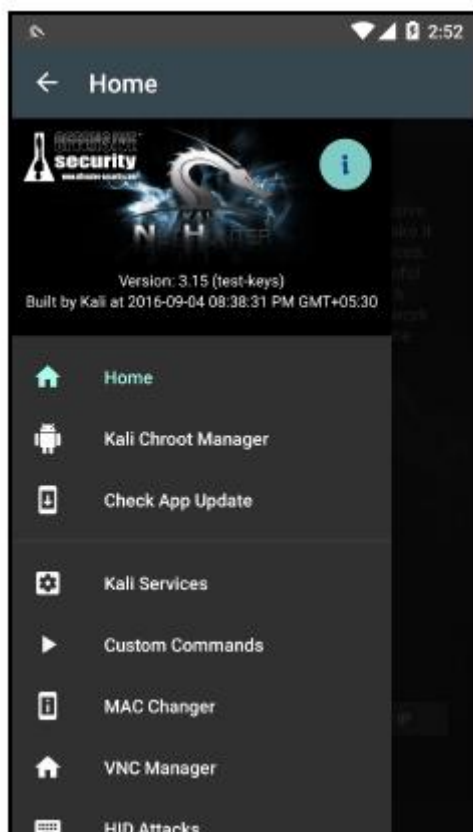
NetHunter ma funkcję, która pozwala nam zmienić nasze urządzenie i kabel OTG tak, aby zachowywały się jak klawiatura, a zatem wpisywać dowolne polecenia na dowolnym podłączonym komputerze. Pozwala nam to przeprowadzać ataki HID. „Wektor ataku HID (urządzenie interfejsu człowieka) to niezwykła kombinacja dostosowanego sprzętu i obejścia ograniczeń poprzez emulację klawiatury. Tak więc, gdy włożymy urządzenie, zostanie ono wykryte jako klawiatura, a używając mikroprocesora i wbudowanej pamięci flash, możesz wysłać bardzo szybki zestaw naciśnień klawiszy do maszyny docelowej i całkowicie ją skompromitować”. –

<https://www.safaribooksonline.com/library/view/metasploit/9781593272883/>

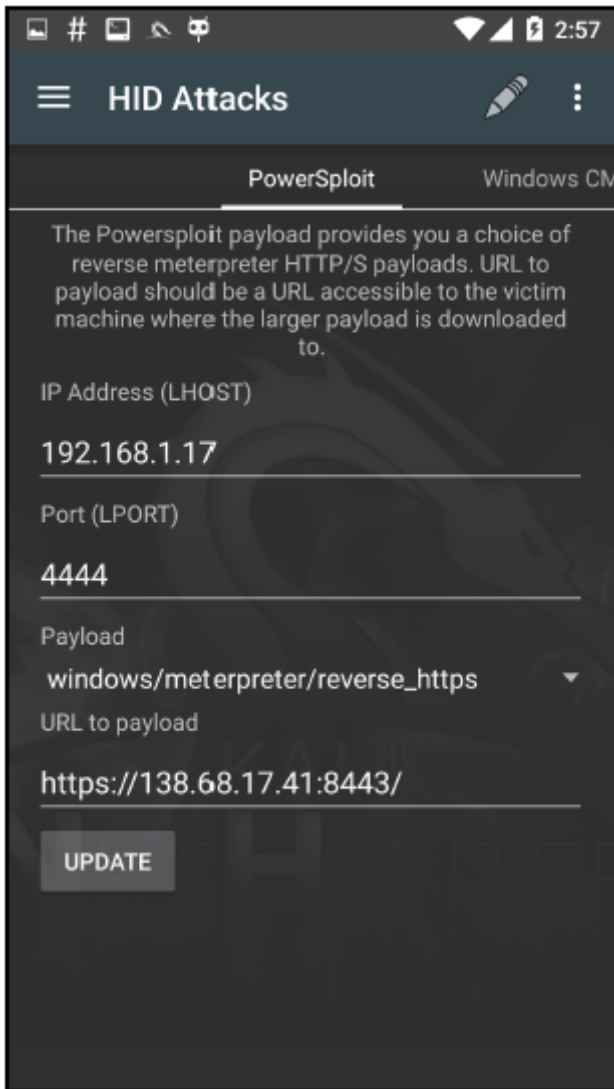
Jak to zrobić...

Aby przeprowadzić ataki HID, wykonaj następujące kroki:

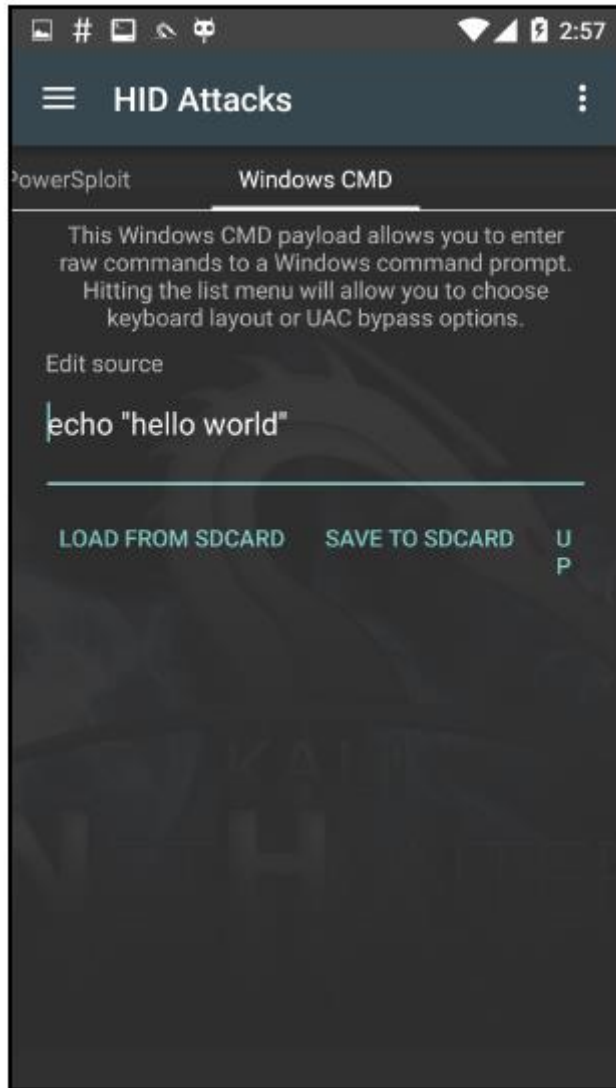
1. Możemy je przeprowadzić, otwierając aplikację NetHunter.
2. W menu wybieramy ataki HID:



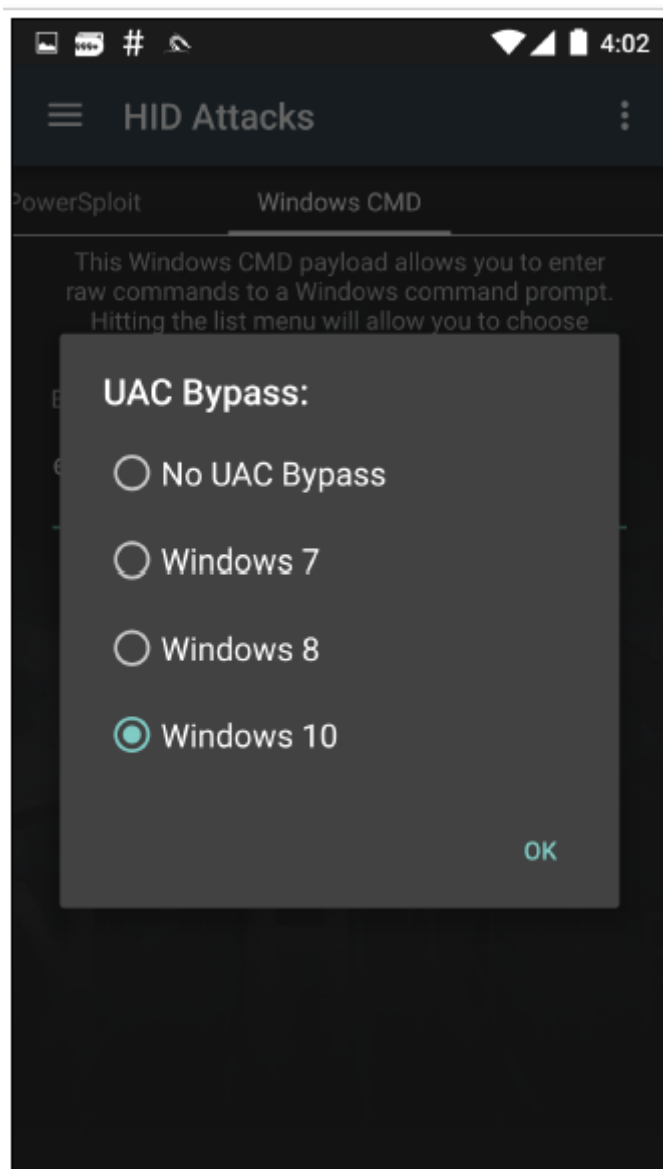
3. Zobaczymy dwie zakładki: PowerSploit i Windows CMD:



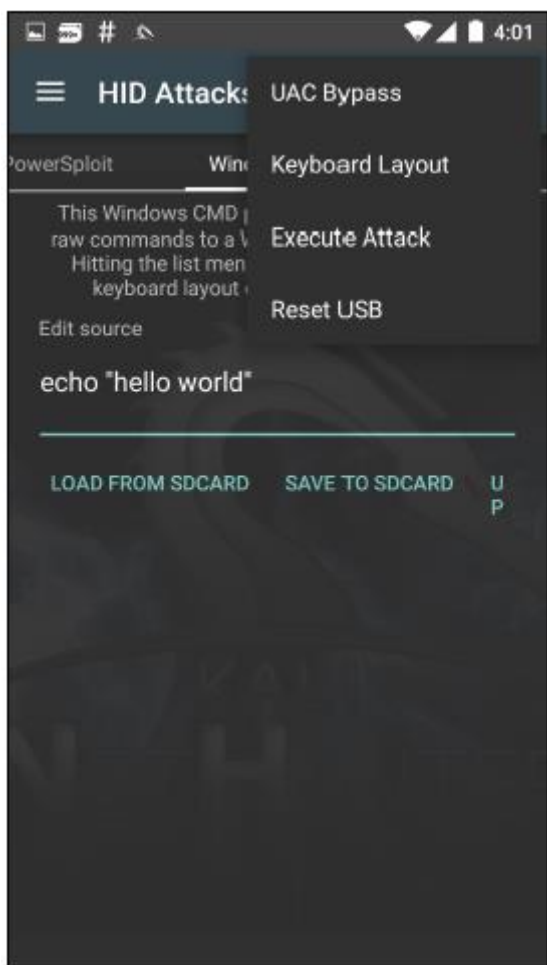
4. Wypróbujmy Windows CMD; w polu Edytuj źródło możemy wpisać polecenie, które chcemy wykonać. Możemy nawet wybrać UAC Bypass z opcji, aby polecenie działało jako admin w różnych wersjach Windows:



5. Wybieramy Windows 10 z menu UAC Bypass, a następnie wpisujemy proste polecenie:
echo "hello world"



6. Następnie podłączamy telefon do urządzenia z systemem Windows 10 i z menu wybieramy opcję Wykonaj atak:



7. Zobaczmy wykonywane polecenie:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\bugsbounty>echo "hello world"
"hello world"

C:\Users\bugsbounty>
```

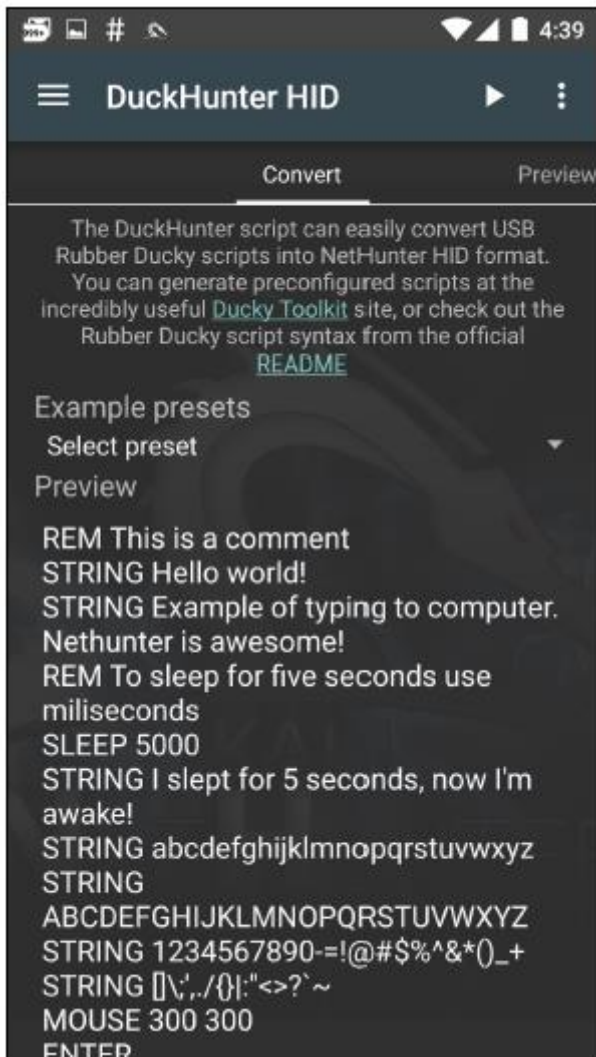
Czy mogę naładować telefon?

W tym przepisie przyjrzymy się innemu typowi ataku HID, znanemu jako DuckHunter HID. Pozwala nam to na konwersję niesławnych skryptów USB Rubber Ducky na ataki NetHunter HID.

Jak to zrobić...

Aby przeprowadzić ataki DuckHunter HID, wykonaj następujące kroki:

1. Możemy je przeprowadzić, otwierając aplikację NetHunter.
2. W menu wybieramy ataki DuckHunter HID.
3. Karta Konwertuj to miejsce, w którym możemy wpisać lub załadować nasze skrypty do wykonania:



4. Zaczniemy od użycia prostego skryptu Hello world!
5. Otwieramy edytor tekstu na dowolnym urządzeniu, a następnie podłączamy nasze urządzenie i klikamy przycisk odtwarzania.
6. Zobaczymy, że jest to automatycznie wpisywane w edytorze:

```
Hello world!
Example of typing to computer. Nethunter is awesome!
I slept for 5 seconds, now I'm awake!
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
1234567890-!@#$%^&*()_+
[]
```

7. W Internecie dostępnych jest wiele skryptów, które można wykorzystać do przeprowadzenia wielu ataków za pomocą NetHunter:

```
Payload – Hello World
Payload – WiFi password grabber
Payload – Basic Terminal Commands Ubuntu
Payload – Information Gathering Ubuntu
Payload – Hide CMD Window
Payload – Netcat-FTP-download-and-reverse-shell
Payload – Wallpaper Prank
Payload – YOU GOT QUACKED!
Payload – Reverse Shell
Payload – Fork Bomb
Payload – Utilman Exploit
Payload – WiFi Backdoor
Payload – Non-Malicious Auto Defacer
Payload – Lock Your Computer Message
Payload – Ducky Downloader
Payload – Ducky Phisher
Payload – FTP Download / Upload
Payload – Restart Prank
Payload – Silly Mouse, Windows is for Kids
Payload – Windows Screen rotation hack
Payload – Powershell Wget + Execute
```

8. Można je pobrać i załadować do NetHunter, a następnie wykorzystać do ataku na komputer ofiary.

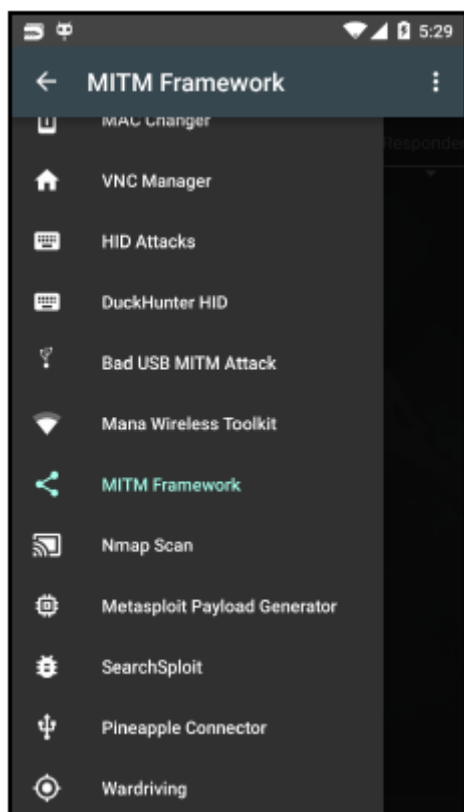
Konfigurowanie złego punktu dostępu

Zestaw narzędzi MANA to zestaw narzędzi do implementacji złego punktu dostępu stworzony przez SensePost, który może być używany do przeprowadzania ataków Wi-Fi, AP i MITM. Gdy ofiara połączy się z naszym punktem dostępu, będziemy mogli wykonać wiele czynności, o których dowiesz się w tym przepisie.

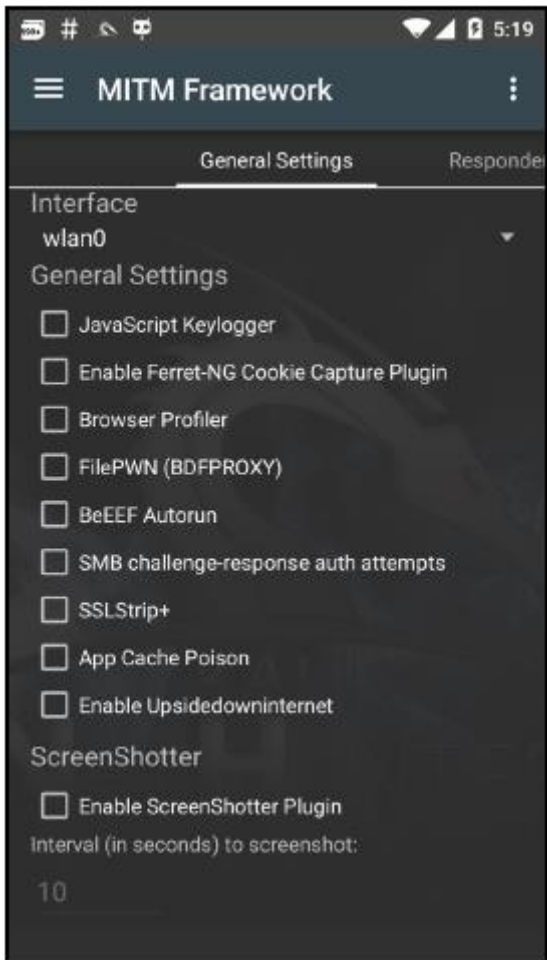
Jak to zrobić...

Aby skonfigurować zły punkt dostępu, wykonaj następujące kroki:

1. Jest łatwy w użyciu. W menu NetHunter wybieramy Mana Wireless Toolkit:



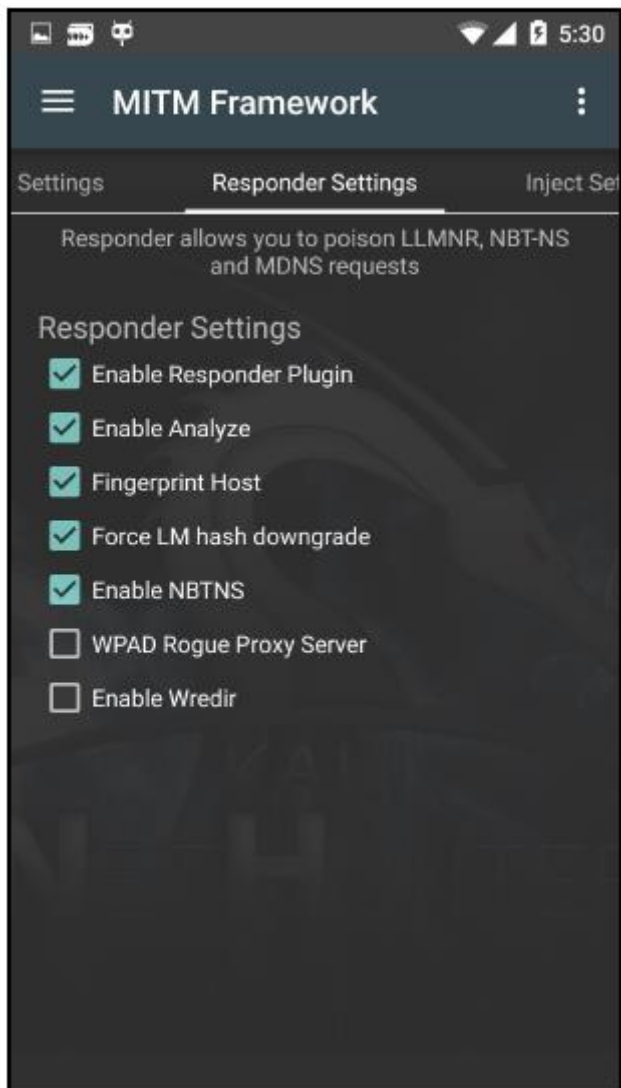
2. Otwiera się w zakładce Ustawienia ogólne. Tutaj możemy wybrać interfejs i inne opcje, takie jak przechwytywanie plików cookie. Można tego użyć do przeprowadzenia ataku bezprzewodowego, wykonując atak evil twin przy użyciu zewnętrznej karty bezprzewodowej obsługiwanej przez NetHunter:



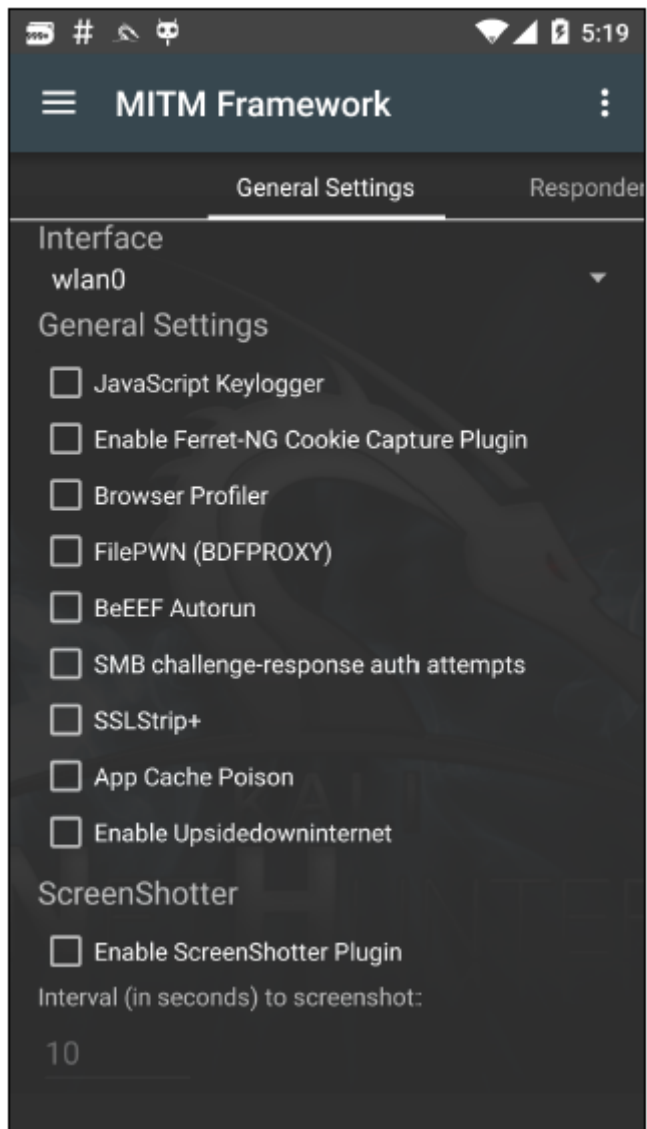
3. Poznałeś responder w poprzednich rozdziałach. Możemy użyć responder za pomocą tego zestawu narzędzi, aby przechwycić hasze sieciowe.

4. Najpierw łączymy się z siecią, na którą chcemy przeprowadzić atak.

5. Następnie przechodzimy do zakładki Responder Settings i sprawdzamy ataki, które chcemy wykonać. Wybieramy wlan0 jako nasz interfejs:



6. Aby zmienić interfejs, którego chcemy słuchać, przechodzimy do zakładki Ustawienia ogólne i wybieramy z listy rozwijanej interfejs:



7. Teraz klikamy na Start mitm attack z menu opcji po prawej stronie.

8. Zobaczymy otwarte okno Terminala i nasz atak zostanie wykonany. Zobaczymy informacje o hoście, a także hasła przechwycone przez atak:

```
1) No title
[*] MITMf v0.9.7 online... initializing plugins
  _ Responder v0.2
  | _ NBT-NS, LLMNR & MDNS Responder v2.1.2 by Laurent Gaffi
  e online
  | _ You can ICMP Redirect on this network. This workstation (192.168.110.19) is not on the same subnet than the DNS server (208.67.220.220)
  | _ You can ICMP Redirect on this network. This workstation (192.168.110.19) is not on the same subnet than the DNS server (208.67.222.222)
  | _ Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned
  | _ Sergio-Proxy v0.2.1 online
  | _ SSLstrip v0.9 by Moxie Marlinspike online
  | _ Net-Creds v1.0 online
  | _ DNSChuf v0.4 online
  | _ SMBserver online (Impacket 9.13)
2017-09-19 12:53:13 [SMBserver] Config file parsed
2017-09-19 12:53:13 [SMBserver] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3_0
2017-09-19 12:53:13 [SMBserver] Config file parsed
2017-09-19 12:53:28 [LLMNRPoisoner] 192.168.110.26 is looking for: printer
2017-09-19 12:53:28 [LLMNRPoisoner] 192.168.110.26 is looking for: printer
2017-09-19 12:53:29 [NBTNSPoisoner] 192.168.110.26 is looking for: PRINTER | Service requested: File Server Service | OS: Windows 10 Home 15063 | Client Version: Windows 10 Home 6.3
2017-09-19 12:53:29 [NBTNSPoisoner] 192.168.110.26 is looking for: PRINTER | Service requested is: File Server Service
2017-09-19 12:53:29 [NBTNSPoisoner] 192.168.110.26 is looking for: PRINTER | Service requested is: File Server Service
```

9. Podobnie, istnieją inne ataki, takie jak skanowanie Nmap, generowanie ładunków Metasploit i tak dalej.