The Hash Slinging Passers
Jared Jones, Randy Thai,
Christopher Gutierrez, Connor Burkman

> Overview

1. Discovery
    a. Use Nmap to scan the network space for Windows machines with port 445 open to create a list of possibly vulnerable machines
2. Intrusion - Metasploit (Eternal Blue)
    a. Gather initial hashes by running the Eternal Blue exploit on a vulnerable machine
3. Collection - Metasploit (Psexec)
    a. Using the initial hashes gathered attempt to access other machines on the network, adding additional hashes gained to the running list
    b. Attack is less likely to get noticed because it uses legitimate access methods

> What is a Pass the Hash attack?

Pass the hash is a technique that allows us to authenticate with an NTLM hash instead of a plaintext password.

The attack exploits an implementation weakness in the authentication protocol, where password hashes remain static from session to session until the password is next changed.

> Assumptions

- Network is outward facing
- All machines on network share the first 24 bits
- A machine on the network is vulnerable to eternal blue
- Other machines are vulnerable to psexec pass the hash

> Tools

- Python-nmap
- Msfrpc
- Pymetasploit
  - Eternal Blue
  - PSExec

> Possible Use Cases

- Collecting as many hashes as possible to crack offline
- Infecting many machines on a network at once

> Problems Encountered

- Fixing & interacting with pymetasploit
- Crackmapexec not working against our Windows VMs
- Exploits can be unreliable / time consuming using MSFRPC
- Windows patches preventing Psexec on some machines

> What we could improve upon

- Supplementing the reliability of pymetasploit
- Adding multithreading support for faster exploitation
- Do better network mapping to find machines on different domains
- Show progress on nmap scan
- Adding more options to the script
  - More nmap target range options
  - Timeout options