Mason Competitive Cyber

Windows Privilege Escalation

Upcoming Competitions & Events

- UVA MetaCTF
  - Sat 9am-5:30pm
  - In-person @ UVA

Overview- Priv Esc

- You have access to a machine
  - Not enough privs to do something

- Where will I use this?
  - CTF challenge category
  - Pen testing

Commands to Gather Info

- Get OS Name and Version
  - `systeminfo`
  - `type C:/Windows/system32/eula.txt`
- Hostname
  - `hostname`
- Current user
  - `echo %username%`
- List all users
  - `net user`
- Network info
  - `ipconfig /all`
  - `arp -A`
- Network connections
  - `netstat`

Commands to Gather Info

- Firewall Info
  - `netsh firewall show state`
  - `netsh firewall show config`
- Scheduled Tasks
  - `schtasks /query /fo LIST /v`
- Services
  - `tasklist /SVC`

Cleartext Passwords

- The “Hail Mary”
  - `findstr /si password *.txt`
- The “Hope They Suck at Config Files”
  - `dir /s *pass* == *cred* == *vnc* == *.config*`
- PSReadline
  - `%APPDATA%\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt`
  - Persists across PS sessions, unlike `Get-History`
  - Not always present. Default in Win10

Service Enumeration

- Replace binary of services running as admin or SYSTEM
  - Need to have file permissions to do it
    - `cacls <servicebin.exe>`
  - Take ownership of file
    - `icacls <servicebin.exe> /setowner <user>`
- Unquoted paths and spaces in service path
  - C:\Program Files\stuff\service.exe
    - `C:\Program.exe`

AlwaysInstallElevated

- Registry key that allows all MSI files to run as SYSTEM
  - `reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated`
    - check if 1

DLL Hijacking

- Bad permissions, missing DLLs
  - Make own malicious DLL that will be run with SYSTEM privileges when loaded
  - https://github.com/itm4n/Ikeext-Privesc

Password Cracking

- Windows passwords stored as LM(super old) or NTLM hash
  - LM hashes aren't case sensitive
- Hashes for local users in SAM registry hive

```
mimikatz # lsadump::sam
Domain : WIN-541GSLG5KBP
SysKey : 50181446e87c44d84d9f8debcc4704a9
ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx KO
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accoun
ts (0x00000005)
```

```
C:\Users\test>reg save HKLM\SYSTEM SystemBkup.hiv
ERROR: A required privilege is not held by the client.
```

- John the Ripper
- Crackstation.net

Better than Password Cracking

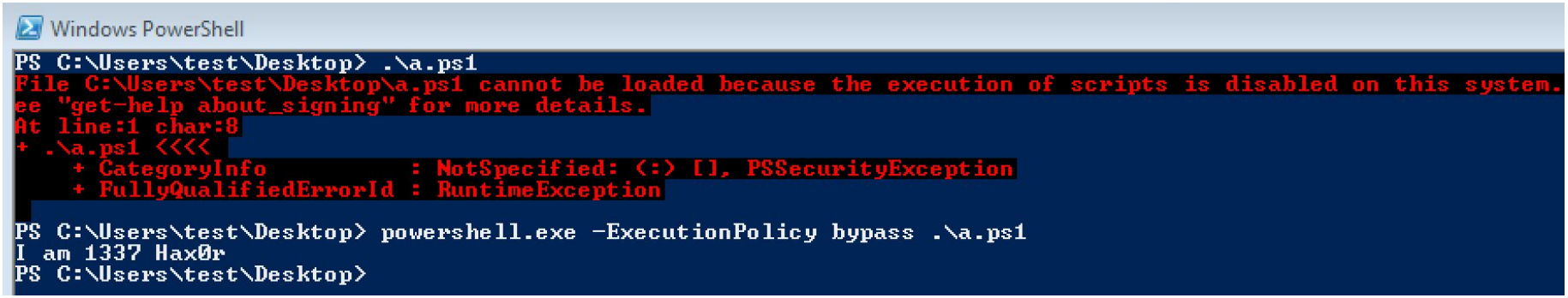
- Rainbow Tables
- Mimikatz search for plaintext passwords in memory
- Pass the Hash

Other

- Windows Kernel Exploit
  - https://github.com/GDSSecurity/Windows-Exploit-Suggester/blob/master/windows-exploit-suggester.py
    - run against output of systeminfo
- Admin to SYSTEM
  - `psexec.exe -i -s %SystemRoot%\system32\cmd.exe`

PowerShell

- Running .ps1 scripts when not admin



lol

https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/

https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc

Practical Exercises

- TCTF Hash Cracking Challenges
  - Man Lan
  - Not Too Little Mayonnaise

- Vulnerable VM
  - Join the wifi “CCMembersOnly”
    - password: hackallthethings
  - ONLY this IP

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™