Adversaries Have it Easy: Having a Peek Behind the Curtain. Build Your Own Lab At Home

# Andy Gill & Neil Lines

Lares Labs



https://labs.lares.com

### Contents

Adversaries Have it Easy: Having a Peek Behind the Curtain	1
Lab Resources	3
Server 2022 setup guide	4
How to convert your server into a domain controller	28
Creating a vulnerable windows domain	39
Windows 11 setup guide	54
Cloning a Windows 11 VM	73
Adding a Windows 11 VM to the hacklab domain	76
Slinky Cat	84

#### Overview

This document will walk you through how to setup a lab environment, step by step regardless of your skill level. It doesn't have all the different vulnerabilities but for a quick win on setup VulnerableAD(<u>https://github.com/WazeHell/vulnerable-AD</u>) will give and pre-configure some known attacks for easy attack paths.

#### Lab Resources

- Server 2022 ISO: <u>https://info.microsoft.com/ww-landing-windows-server-2022.html</u>
- Windows 11 ISO: <u>https://www.microsoft.com/en-us/evalcenter/evaluate-windows-11-enterprise</u>
- Virtual Box (Needed if you don't have VM): <u>https://www.virtualbox.org/</u>
- Hack Lab Domain Controller
   <u>https://github.com/myexploit/LAB/blob/master/Hack\_Lab\_Domain</u>

#### Server 2022 setup guide

#### Using VM Workstation

- 1. Click on create a New Virtual Machine.
- 2. Select the server 2022 ISO.
- 3. Click Next.



VM 16 didn't have a server 2022 predefined setup so opted for Windows 10 Pro.

- 4. Add an account name.
- 5. Add a password.

W	ORKSTATION 1	<b>6</b> PRO <sup>™</sup>
Create a New Virtu Machine	al Open a Virtual Machine	Connect to a Remote Server
New Virtual Machine V	/izard	×
Easy Install Inform	ation	
This is used to in Windows product key		
This is used to in Windows product key - Version of Windows to in Windows	stall vindows 10 and later x04.	
This is used to in Windows product key Version of Windows to in Windows Personalize Windows	stall 10 Pro	~
This is used to in Windows product key Version of Windows to in Windows Personalize Windows Full name: admin	stall vindows 10 and later x04.	✓
This is used to in Windows product key Version of Windows Personalize Windows Full name: admin Password:	stall vindows 10 and later x04.	(optional)
This is used to in Windows product key Version of Windows to in Windows Personalize Windows Full name: admin Password: Confirm:	stall vindows 10 and later x04.	<pre>v (optional)</pre>
This is used to in Windows product key Version of Windows to in Windows Personalize Windows Full name: admin Password:	y (requires a password)	(optional)

- 6. Rename the virtual machine.
- 7. Rename the location name to match (not required but for logical reason it makes sense.)
- 8. Click Next.

Name the Virtual Machin What name would you	<b>ne</b> like to use for this virtual machine?	
/irtual machine name:		
Steelcon-Server-2022		
ocation:		
	Steelcon-Server-2022	Browse
he default location can be ch	anged at Edit > Preferences.	
The default location can be ch	anged at Edit > Preferences.	

- 9. VM defaults to 60 GB of storage, but you should be able to get by with 30-40 GB if you're short on space?
- 10. Click Next.

How large do you	ı want this disk to be?
The virtual machine's hard physical disk. These file(s) files, and data to your virt	d disk is stored as one or more files on the host computer's ) start small and become larger as you add applications, ual machine.
Maximum disk size (GB):	60.0
Recommended size for Wi	indows 10 and later x64: 60 GB
but may reduce perfor	mance with very large disks.

- 11. Untick' Power on this virtual machine after creation'.
- 12. Click Finish.

and later x64	and then VMware Tools.	) windows 10
The virtual machine	will be created with the following settings:	
Name:	Steelcon-Server-2022	
Location:	C:\Users	Steelcon-Serv.
Version:	Workstation 16.2.x	
Operating System:	Windows 10 and later x64	
Hard Disk:	60 GB, Split	
Memory:	2048 MB	
Network Adapter:	NAT	
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Prin	iter, Sound Card
Customize Hardv	vare	
Devver on this vid	hul machine often mention	
_ Power on this vir		

13. Click on 'Edit virtual machine settings.'

Steelcon-Server-2022 - VMw	are Workstation
File Edit View VM Tabs H	lelp 🕨 🗸 🛱 🖗 🕰 💭 🗖 🖓 🖄
ि Home × □ 📊 Windows_Serve	er_2022 × Windows_11_1 × Windows_11_2 ×
Steelcon-Server-2	022
Power on this virtual machine Edit virtual machine settings	s
▼ Devices	
📟 Memory	2 GB
Processors	2
🕞 Hard Disk (NVMe)	60 GB
💿 CD/DVD (SATA)	Using file C:\Use
💾 Floppy	Using file autoin
🛱 Network Adapter	NAT
🚭 USB Controller	Present
🕸 Sound Card	Auto detect
🛱 Printer	Present
Display	Auto detect
<ul> <li>Description</li> </ul>	
Type here to enter a description machine.	n of this virtual

14. Click on Floppy and Remove.

Hardware Options		
Device	Summary	
E Memory	2 GB	
Processors	2	
Hard Disk (NVMe)	60 GB	
💿 CD/DVD (SATA)	Using file C:\User	<u>s\nlines</u> \Doc
Floppy	Using file autoins	t.flp
Network Adapter	NAT	
🚭 USB Controller	Present	
🕼 Sound Card	Auto detect	
🖶 Printer	Present	
Display	Auto detect	
	Add	Remove

15. Click on Network Adapter and change from NAT to Bridged: Connected directly to the physical network' (This is dependent of location and if there is a DHCP server, if not pick Custom: Specific virtual network and select whichever one you have configured VM to offer a DHCP IP address on, then make sure all your other LAB VM's are on the same network so they can communicate with each other.

Device Memory Processors Hard Disk (NVMe) CD/DVD (SATA) Network Adapter USB Controller Osound Card Printer Display	Summary 2 GB 2 60 GB Using file C:\Users\nlines\Doc NAT Present Auto detect Present Auto detect Present Auto detect	Device status Connected Connected Connect at power on Network connection Bridged: Connected directly to Replicate physical network NAT: Used to share the host's Host-only: A private network Custom: Specific virtual networ VMnet0 LAN segment:	b the physical net c connection state ; IP address shared with the h prk LAN	work	<ul> <li>Advanced</li> </ul>
			-		

17. First boot you see the VM BIOS splash followed by Press any key to boot from CD or DVD, you must click in the screen and press enter fast!!

If you miss it don't worry just restart the VM and repeat until you get it!

ð

s_11_2	× 🕞 Steelo	on-Server-2022 ×			
	Press any	key to boot f	rom CD or	DVD.	
. You sh	ould see a Winc	lows splash screer	press enter.		
. Change	e options to Eng	lish.			
Click N	ext.				

Microsoft Server Operating System Setup	
Microsoft	
Language to install: Foolish (United States)	-
Time and currency format: English (United Kingdom)	
Keyboard or input method: United Kingdom	•
Enter your language and other preferences and click "Next" to continue.	
D Microsoft Corporation. All rights reserved.	<u>N</u> ext

21. Click Install now.



You should see Setup is starting.



- 22. Make sure you pick an option with Desktop Experience, or you will install server core. (Pick the second option in the list).
- 23. Click Next

Select the operating system you want to install		
Operating system	Architecture	Date modified
Windows Server 2022 Standard Evaluation	х64	3/3/2022
Windows Server 2022 Standard Evaluation (Desktop Experien	. хб4	3/3/2022
Windows Server 2022 Datacenter Evaluation	хб4	3/3/2022
Description: This option installs the full Windows graphical environment, cc useful if you want to use the Windows desktop or have an app	onsuming extra dı that requires it.	ive space. It can b



- 24. Tick the Terms.
- 25. Click Next.
- 26. The next option offers you Upgrade or Custom Installation, Select Custom Installation.
- 27. Click Next.

Wher	e do you w	ant to install the	operating system?		
	Name		Total size	Free space	Туре
	Drive 0 Unal	located Space	60.0 GB	60.0 GB	
<b>∳</b> ∱ <u>R</u> ef	resh	Delete	€ormat	* N <u>e</u> w	

It should redirect to the installing page.



During the install it should auto reboot.



### Getting ready

28. Add a password for the Administrator account (Select a password you can 100% remember).29. Click Finish.

Customize	settings
Type a password for the	built-in administrator account that you can use to sign in to this computer.
User name	Administrator
Password	
Reenter password	········ ~
<i>d</i> .	
<b>O</b>	Finish

30. Login using the password you just set.



31. Click Yes on the Networks option.

e Serve	er Manager					
	Server Manager			×		Networks
-	Try managing servers with Wi	indows Admin Center				
	Windows Admin Center brings to app. It runs on a server or a PC, a licenses.	gether new and familiar featu and there's no additional cost	res in one browser- beyond your Wind	based ows		╏ <mark>규</mark> Network
	Get more info at aka.ms///indows	sAdminCenter			this local serve	Do you want to allow your PC to be discoverable by other PCs and devices
	Don't show this message agai	in			10.1	on this network:
			2	AUCTOR	es and features	We recommend allowing this on your
			3	Add oth	er servers to manag	public ones.
		WHAT'S NEW	4	Create a	a server group	
			5	Connec	t this server to cloud	Yes No
		LD MIT MORE				
		ROLES AND SERVE	R GROUPS			
		Roles: 0   Server grou	ps: 1   Servers t	otal: 1		
		Local Serve	r ·	1	All Servers	
		<ul> <li>Manageabili</li> </ul>	ty	- 6	Manageability	
		Events			Events	
		Services			Services	
		Performance			Performance	
		BPA results			BPA results	
	0			_		

32. Click file explorer which is on the bottom toolbar.



33. Right click on the DVD Drive and select Eject (so you can mount and install VM tools).



34. Click on VM tool bar, select VM then click Install VMware Tools...



- 35. The VM tools Disk should mount the DVD Drive.
- 36. Double click to open.



37. Double click 'setup64' to start installing VM Tools.

✓ Files Currently on the Disc (7)				
📙 Program Files	31/08/2021 03:14			
vm autorun	31/08/2021 03:14			
🔊 autorun	31/08/2021 03:14			
i manifest	31/08/2021 03:14			
🔄 setup	31/08/2021 03:14			
🛃 setup64	31/08/2021 03:14			
VMwareToolsUpgrader	31/08/2021 03:14			

38. The VM tools installer will flash on the bottom taskbar, click it.39. Click Next.



- 40. Select Typical
- 41. Click Next.



42. Click Install.



Once it finishes installing you will see the screen resolution improve, and the VM should the fill your monitor, if not reboot it.

눰 Server	Manager				
¢	Server Manager Try managing servers w	ith Windows Admin Center	×		
<b>iii</b> L	Windows Admin Center brin app. It runs on a server or a licenses.	ngs together new and familiar features in PC, and there's no additional cost beyon	one browser-based Id your Windows		
ii A	Get more info at aka.ms/Wi	ndowsAdminCenter	WMware Tools Setup		– 🗆 X
	Don't show this messag	e again			
			-	Completed the VMv	ware Tools Setup Wizard
			3		
		WHAT'S NEW	4	Click the Finish button to e	exit the Setup Wizard.
			5		
		LEARN MORE			
		ROLES AND SERVER GROU	PS		
		Roles: 1   Server groups: 1   S	Serv		
		File and Storage	<b>vm</b> ware <sup>.</sup>		
		Services		< Back	Finish Cancel
		<ul> <li>Manageability</li> </ul>		C DUCK	· · · · · · · · · · · · · · · · · · ·
		Events	Events	5	Events

43. VM Tools Setup Asks you to restart.

	🛃 VMwar	e Tools Setup		$\times$
JC	i	You must restart your changes made to VMw to restart now or No if later.	system for the configuration are Tools to take effect. Click t f you plan to manually restart	Yes
		Yes	No	

It is strongly recommended that you assign a static IP address to any server, this demo includes a walkthrough on how to assign an IP address using the network configuration we set for this demo.

lardware Options			
Device Memory Processors Hard Disk (NVMe) CD/DVD (SATA) Network Adapter CUSB Controller Sound Card Printer Display	Summary 2 GB 2 60 GB Using file C:\Users\ Bridged (Automatic) Present Auto detect Present Auto detect	Doc	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet0 LAN segment:

If you don't set a static IP address, there is a high chance that DNS will fail to resolve the domain name for any joining host machines.

This demo should also work for those who during the initial network settings opted for Custom, just make sure the VM custom network provides DHCP, you can do this by looking under VM tool bar \ Edit \ Virtual Network Editor.

44. Login to the Server 2022 VM and on the Windows bottom tool bar towards the clock right click on Network Internet Access option.



45. Select Open Network & Internet settings.



46. Click on Change adaptor options.

# Status

### Network status



Private network

#### You're connected to the Internet

You're on a metered network. Some apps might work differently to help you save data while on this network.



귯

Show available networks View the connection options around you.

### Advanced network settings

Change adapter options View network adapters and change connection settings.

#### Which should allow you access to your network card.



47. Before we change that, open CMD (type cmd into search bar, which is next to the windows button, bottom tool bar, to the left).

Best match
Command Prompt App
$\mathcal{P}$ cmd

- 48. Type in ipconfig /all
- 49. Press enter and make a note of your original IP address.



In this demo our IP address is 192.168.68.125 our subnet is 255.255.255.0 (/24), default gateway and DNS IP addresses are 192.168.68.1 make a note of your addresses.

#### Administrator: Command Prompt

Host NameHost NamePrimary Dns SuffixHybridIP Routing EnabledNoWINS Proxy EnabledNoWINS Proxy EnabledNoEthernet adapter Ethernet0:Connection-specific DNS SuffixIntel(R) 82574L Gigabit Network ConnectioPhysical AddressIntel(R) 82574L Gigabit Network ConnectioPhysical AddressYesAutoconfiguration EnabledYesLink-local IPv6 Address192.168.68.125(Preferred)Subnet Mask09 June 2023 03:41:53Lease Obtained99 June 2023 05:41:52Default Gateway192.168.68.1DHCP Server192.168.68.1DHCPv6 IAID192.168.68.1DHCPv6 Client DUID192.168.68.1		
Node Type	Host Name	
IP Routing Enabled.	Node Type Hybrid	
WINS Proxy Enabled : No Ethernet adapter Ethernet0: Connection-specific DNS Suffix . : Description Intel(R) 82574L Gigabit Network Connectio Physical Address	IP Routing Enabled No	
Ethernet adapter Ethernet0:         Connection-specific DNS Suffix . :         Description : Intel(R) 82574L Gigabit Network Connectio         Physical Address : Physical Address : Physical Address : Yes         Autoconfiguration Enabled : Yes         Link-local IPv6 Address : Physical Address : Physical Address : Physical	WINS Proxy Enabled No	
Connection-specific DNS Suffix . :         Description : Intel(R) 82574L Gigabit Network Connectio         Physical Address : Yes         DHCP Enabled : Yes         Autoconfiguration Enabled : Yes         Link-local IPv6 Address : 192.168.68.125(Preferred)         Subnet Mask : 255.255.25.0         Lease Obtained : 09 June 2023 03:41:53         Lease Expires : 09 June 2023 05:41:52         Default Gateway : 192.168.68.1         DHCP Server : 192.168.68.1         DHCPv6 Client DUID : : 192.168.68.1	Ethernet adapter Ethernet0:	
Description	Connection-specific DNS Suffix . :	
Physical Address.	Description Intel(R) 82574L Gigabit Netwo	ork Connectio
DHCP Enabled	Physical Address	
Autoconfiguration Enabled :       Ves         Link-local IPv6 Address :       IPv4 Address :         IPv4 Address : :       192.168.68.125(Preferred)         Subnet Mask : :       255.255.255.0         Lease Obtained : :       09 June 2023 03:41:53         Lease Expires : :       09 June 2023 05:41:52         Default Gateway : :       192.168.68.1         DHCP Server : :       192.168.68.1         DHCPv6 IAID : :       192.168.68.1         DNS Servers : : : :       192.168.68.1	DHCP Enabled Yes	
Link-local IPv6 Address : IPv4 Address : 192.168.68.125(Preferred) Subnet Mask : 255.255.255.0 Lease Obtained : 09 June 2023 03:41:53 Lease Expires : 09 June 2023 05:41:52 Default Gateway : 192.168.68.1 DHCP Server : 192.168.68.1 DHCPv6 IAID : 192.168.68.1 DHCPv6 Client DUID : 192.168.68.1	Autoconfiguration Enabled : Yes	
IPv4 Address.	Link-local IPv6 Address :	
Subnet Mask	IPv4 Address	
Lease Obtained.	Subnet Mask	
Lease Expires	Lease Obtained	
Default Gateway	Lease Expires	
192.168.68.1         DHCP Server       192.168.68.1         DHCPv6 IAID       192.168.68.1         DHCPv6 Client DUID       192.168.68.1         DNS Servers       192.168.68.1	Default Gateway :	
DHCP Server	192.168.68.1	
DHCPv6 IAID	DHCP Server	
DHCPv6 Client DUID : DNS Servers : 192.168.68.1	DHCPv6 IAID	
DNS Servers	DHCPv6 Client DUID :	
	DNS Servers	

50. Go back to the Network card and right click and select Properties.

Vetwork Connection	ons		
$\leftarrow \rightarrow \cdot \cdot \uparrow $	Control Panel > Netw	ork and Internet > Netwo	rk Connections
Organize 🔹 Dis	able this network device	Diagnose this connection	on Rename
Ethernet0			
Intel(R) 82	5 👎 Disable		
	Status		
	Diagnose		
	Bridge Connection	S	
	Create Shortcut		
	👎 Delete		
	👎 Rename		
	Properties		

- 51. Click on Internet Protocol Version 4 (TCP/IPv4) so it is selected.
- 52. Then click on Properties.



This will open the Network card IP4 configuration options which by default, are as such.

	Protocol Version 4 (TCP/	irv4) rioperties	X
General	Alternate Configuration		
You ca this ca for the	an get IP settings assigned a pability. Otherwise, you nee appropriate IP settings.	automatically if your network supports ed to ask your network administrator	
	)btain an IP address automa	atically	
- <b>(</b>	lse the following IP address	:	
IP a	address:		
Sub	net mask:		
Def	ault gateway:		
	)btain DNS server address a	utomatically	
-Õl	lse the following DNS serve	r addresses:	
-Ou Pre	Ise the following DNS server Ferred DNS server:	r addresses:	
Pre	Ise the following DNS server ferred DNS server: ernate DNS server:	r addresses:	
Pre	Jse the following DNS server ferred DNS server: ernate DNS server: Validate settings upon exit	r addresses:	

53. Select Use the following IP address.

Now look back at your CMD open session as you need to set an IP address from within that IP range.

Below is the IP address that we were allocated during this demo.

IPv4 Address	: 192.168.68.125(Preferred)
Subnet Mask	. : 255.255.255.0
Default Gateway	192.168.68.1
DNS Servers	: 192.168.68.1

As an example, under our circumstances we would set the servers static IP address configuration as such.

IP address: 192.168.68.200

Subnet mask: 255.255.255.0

Default gateway: 192.168.68.1

Preferred DNS Server: 192.168.68.1

54. Add your configuration, then click OK.

nternet Protocol Version 4 (TCP/IPv4)	nternet Protocol Version 4 (TCP/IPv4) Properties					
General						
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.						
$\bigcirc$ Obtain an IP address automatically	,					
• Use the following IP address:						
IP address:	192 . 168 . 68 . 200					
Subnet mask:	255 . 255 . 255 . 0					
Default gateway:	192 . 168 . 68 . 1					
Obtain DNS server address automa	atically					
$- \odot$ Use the following DNS server addr	esses:					
Preferred DNS server:	192 . 168 . 68 . 1					
Alternate DNS server:						
Validate settings upon exit Advanced						
	OK Cance	el				

- 55. Close network settings, and go back to CMD.
- 56. Verify the settings changed by typing in ipconfig /all.
- 57. Check you can access the default gateway via pinging it's IP address.

```
Connection-specific DNS Suffix . :
  Description . . . . . . . . . . . . . Intel(R) 82574L Gigabit Network Connection
  Physical Address. . . . . . . . . .
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . :
  IPv4 Address. . . . . . . . . . . . . . . . . 192.168.68.200(Preferred)
  Default Gateway . . . . . . . . .
                                 192.168.68.1
  DHCPv6 Client DUID. . . . . . . . .
  NetBIOS over Tcpip. . . . . . . : Enabled
C:\Users\Administrator>ping 192.168.68.1
Pinging 192.168.68.1 with 32 bytes of data:
Reply from 192.168.68.1: bytes=32 time=5ms TTL=64
Reply from 192.168.68.1: bytes=32 time=3ms TTL=64
Reply from 192.168.68.1: bytes=32 time=5ms TTL=64
Reply from 192.168.68.1: bytes=32 time=7ms TTL=64
Ping statistics for 192.168.68.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 3ms, Maximum = 7ms, Average = 5ms
```

Depending on how you configured your VM network setting, you may also wish to test access to the internet from the VM server. Internet access is not required for lab testing but is always nice to have.

```
Pinging new-fp-shed.wg1.b.yahoo.com [87.248.100.215] with 32 bytes of data:
Reply from 87.248.100.215: bytes=32 time=40ms TTL=52
Reply from 87.248.100.215: bytes=32 time=31ms TTL=52
Ping statistics for 87.248.100.215:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 40ms, Average = 35ms
Control-C
^C
C:\Users\Administrator>
```

And with that your Server 2022 should be built and be ready to convert into a domain controller.

## How to convert your server into a domain controller

Easy use a PowerShell script that does it all for you.

1. Search for PowerShell, right click on it and select Run as administrator.

Σ	Windows PowerShell	5	Run as administrator
Apps	5	⊑à	Run as different user
2	Windows <b>PowerShell</b> ISE	$\square$	Open file location
	Windows <b>PowerShell</b> (v86	58	Unpin from Start
		다	Pin to taskbar
2	Windows PowerShell ISE	,,	

#### 2. Copy and paste the following into the PowerShell session:

Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force ; Install-WindowsFeature AD-Domain-Services ; Import-Module ADDSDeployment ; Install-ADDSForest -DatabasePath "C:\Windows\NTDS" -DomainMode "Win2008R2" -DomainName "hacklab.local" -DomainNetbiosName "HACKLAB" -ForestMode "Win2008R2" -InstallDns:\$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:\$true -SysvolPath "C:\Windows\SYSVOL" -Force:\$true ; Add-WindowsFeature RSAT-AD-Tools ; Restart-Computer

The above script was taken from https://github.com/myexploit/LAB/blob/master/Hack\_Lab\_Domain

For those who like to know what the one-liner is doing read below.

Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force: This command installs the NuGet package provider on your system. NuGet is a package manager for .NET, allowing you to install and manage software libraries and packages easily.

Install-WindowsFeature AD-Domain-Services: This command installs the Active Directory Domain Services role on your Windows server. Active Directory is a directory service provided by Microsoft that enables centralized management of users, groups, and computers in a network environment.

Import-Module ADDSDeployment: This command imports the ADDSDeployment module, which provides additional cmdlets for deploying Active Directory.

Install-ADDSForest: This command installs and configures a new Active Directory forest with the specified settings on your server. The provided parameters define various configuration options, such as the database and log file paths, Domain and forest modes, DNS installation, and more.

Add-WindowsFeature RSAT-AD-Tools: This command installs the Remote Server Administration Tools for Active Directory (RSAT-AD-Tools). These tools allow you to manage Active Directory from a different computer remotely.

Restart-Computer: This command restarts the computer to apply any changes made during installation.

These commands are used to automate the installation and configuration of Active Directory Domain Services on a Windows server, creating a new domain with the specified settings.

After pasting the one-liner in you will see each stage been configured.



🔀 Administrator: Windows PowerShell			
Windows PowerShell Copyright (C) Microsoft Corpora	ation. All rights	reserved.	
Start Installation 46% [cccccccccccccccccccccccccccccccccccc	000000000000000000000000000000000000000	000000000000000000000000000000000000000	
Add-WindowsFeature RSAT-AD-Tool	ls ; Restart-Compu	uter	
Name	Version	Source	Summary
nuget	2.8.5.208	https://onege	NuGet provider for the OneGet meta-package manager

3. During which you will be asked to add a password, it is important you remember this password.

```
PS C:\Users\Administrator> Install-PackageProvider -Name NuGet -
mainMode "Win2008R2" -DomainName "hacklab.local" -DomainNetbio
Add-WindowsFeature RSAT-AD-Tools ; Restart-Computer
Name
                                    Version
                                                        Source
                                     _____
                                                         _____
____
                                     2.8.5.208
                                                       https://onege...
nuget
                : True
Success
RestartNeeded : No
FeatureResult : {Active Directory Domain Services, Remote Server
ExitCode
                : Success
```

SafeModeAdministratorPassword: \*\*\*\*\*\*\*\*

Message		You must restart this computer to complete the operation.
Context Report Required	:	DCPromo.General.4
Repoolkequired		i ride
Status		Success

If you see the above message, just ignore it do not reboot, once all is complete it will reboot itself.

After the reboot you should be able to login as a domain member for the first time.

You can click the Ctrl+Alt+Delete key on the top VM tool bar in a VM.





You should see the domain hacklab\ with the Administrator account set up during the conversion to a domain controller.



4. Type in Active into the search bar and this should bring up Active Directory Users and Computers, right click it and select pin to toolbar as you will be using it quite often.

	Best match
	Active Directory Administrative Center
	Apps
	Active Directory Domains and Trusts
	Active Directory Sites and Services
	Active Directory Users and Computers
	Active Directory Module for Windows PowerShell
	Settings
	<ul> <li>Activation settings</li> </ul>
	C Change active hours
	🔂 Manage browser add-ons
	i Disconnect your device from your work or school
	(i) Connect your device to your work or school domain
	🔎 active Directory Administrative Center 🛛 🛱 💽 🔚
5.	Open Active Directory Users and Computers by clicking on it.
	Active Directory Users and Computers

Z

r <del>d</del>ar

Welcome to Active Directory.



6. Click on the domain hacklab.local / Users and double click on your Administrator account.

Active Directory Users and Computers -				
File Action View Help				
🗧 🔶 📶 🔏 🖽 🗶 🖾 🖉 🛤				
Active Directory Users and Computers [WIN-MS87LHLC91U.hacklab.local]				
> 🧾 Saved Queries	nistrator			
Y 🗐 hacklab.local	ed RODC Password Replication Group			
> 📔 Builtin	Publishers			
> 📫 Computers				
> 📓 Domain Controllers	able Domain Controllers			
> 📔 ForeignSecurityPrincipals	ed RODC Password Replication Group			
Managed Service Accounts	dmins			
	pdateProxy			
La Do	ain Admins			
A Do	ain Computers			
A Do	ain Controllers			

7. Click on Member Of to see the domain groups the account belongs to, in a real domain any account with these privileges should be considered as a break glass emergency account and should only be used in the initial creation of the Domain.

Ac	Administrator Properties ?						
	Remote control	Remote	Desktop Se	ervices Profile	COM	+	
(	General Addre	ss Account	Profile	Telephones	Organiza	tion	
	Member Of	Dial-in	Env	ironment	Sessions	5	
	Name Administrators		Active Dir	ectory Domain Se ocal/Builtin	ervices Fold	le	
	Domain Admins		hacklab.local/Users				
	Domain Users		hacklab.k	ocal/Users			
	Enterprise Admin	Imins hacklab.local/Users					
	Group Policy Cre	ator Owners	hacklab.local/Users				
	Schema Admins		hacklab.k	ocal/Users			

8. Create a new account for routine admin lab work (This is a lab for testing hacking tools and process in, it will never be secure and any recommendations here are for those proposes only.)



9. Add first name, last name, and user login name, then click Next.

lew Object - User				
Create in:	hacklab.local/Users			
First name:	da1	Initials:		
Last name:				
Full name:	da1			
User logon name:				
da1 @hacklab.local ~			~	
User logon name (pre-Windows 2000):				
HACKLAB\	da1			
	< Back	Next >	Cancel	

10. Add a password, and for lab use only you can tick Password never expiries if you wish. (In a production environment you would not typically tick Password never expiries because it is bad practice to do so.)

New Object - User ×						
Create in: hacklab.local/Users						
Password:	Password:					
Confirm	••••					
User must change password at n	ext logon					
User cannot change password						
Password never expires						
Account is disabled						
	< Back	Next >	Cancel			

11. Click Finish.



12. You should then see your created account, double click it.

Name
Administrator
Allowed RODC Password Replication Group
A Cert Publishers
🧟 Cloneable Domain Controllers
🛃 da1

13. Click on the Member Of tab.

da	da1 Properties ? >						
	Remote	control	Remote D	Remote Desktop Services Profile			M+
(	General	Address	Account	Profile Telephones Orga		Organi	zation
	Member Of Dial-in Environment				Sessio	ons	
	Member o	of:					
	Name		Active Directory Domain Services Folder				
	Domain Users hacklab.local/Users						

14. To add the account as a member to the Domain Admins group, click on Add then type in domain admins and click Check Names.

d	la1 Properties		? $ imes$ ication Group	
	Remote control	Remote	Desktop Services Profile COM+	
	General Addres	ss Account	Select Groups	$\times$
zi	Member Of	Dial-in		
c			Select this object type:	
	Member of:		Groups or Built-in security principals Ob	ject Types
	Name	Active Direct	From this location:	
	Domain Users	hacklab.loca	hacklab.local	ocations
			Enter the object names to select (examples):	ieck Names
			Advanced OK	Cancel
	Add	Remove		

If located, you should see the name domain admins change.
Select Groups	×
Select this object type:	
Groups or Built-in security principals	Object Types
From this location:	
hacklab.local	Locations
Enter the object names to select ( <u>examples</u> ):	
Domain Admins	Check Names

15. Then click OK.

				:	
Remote control	Remote	Desktop Se	ervices Profile	CO	+M
General Addre	ss Account	Profile	Telephones	Organiz	zatior
Member Of	Dial-in	Envi	ironment	Sessio	ns
Member of:					
Name	Active Direct	ory Domain	Services Folder	4	
Domain Admins	hacklab.loca	/Users			
Domain Users	hacklab.local	/Users			
Add Primary group:	Remove Domain Users				
Add Primary group: Set Primary Gro	Remove Domain Users There is r you have applicatio	no need to o Macintosh ins.	change Primary clients or POSIX	group unle (-complian	ess t

16. Logout and then on the login page select Other user and login using the account you just created.



Other user	
da1	
•••••••	
Sign in to: HACKLAB How do I sign in to another domain?	

# Creating a vulnerable Windows domain

Feel free to explore and build your simulation of a vulnerable Windows domain, over the years we have seen many misconfigurations and some of these we have built into a configuration script that you can just copy and paste into your lab domain controller to help speed up the process.

Word of caution this will add purposely created vulnerable accounts and settings for the ease of testing hacking tools and processes.

https://raw.githubusercontent.com/myexploit/LAB/master/Hack Lab Domain

1. The section you need to copy and paste initiates from the # Add Departments comment and concludes right down to the last word on the web page, exit.

But for ease of use below is the complete section you require.

```
\# Add Departments organizational unit (OU) Add Head_Office OU with nested department OU and IT OU.
```

```
dsadd ou ou=Departments,dc=hacklab,dc=local
dsadd ou "ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Admins,ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Service_Accounts,ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Help_Desk,ou=IT,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Sales,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Accounts,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Research,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
dsadd ou "ou=Reception,ou=Head_Office,ou=Departments,dc=hacklab,dc=local"
```

"ou=Senior Management,ou=Head Office,ou=Departments,dc=hacklab,dc=local"

# Create a user groups OU

dsadd ou ou=Groups,ou=Departments,dc=hacklab,dc=local

# Create the following user groups to the group OU

dsadd group cn=sales,ou=Groups,ou=Departments,dc=hacklab,dc=local dsadd group cn=administration,ou=Groups,ou=Departments,dc=hacklab,dc=local dsadd group cn=accounts,ou=Groups,ou=Departments,dc=hacklab,dc=local dsadd group cn=help\_desk,ou=Groups,ou=Departments,dc=hacklab,dc=local dsadd group cn=support,ou=Groups,ou=Departments,dc=hacklab,dc=local dsadd group cn=RDP,ou=Groups,ou=Departments,dc=hacklab,dc=local

# Create Lab Test accounts

# Head Office / Accounts

dsadd user "cn=n.collins, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=o.davidson, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=p.davies, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

dsadd user "cn=q.dawson, ou=Accounts, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=u.dixon, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=r.edwards, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd\_user "cn=s.elliot, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=t.evans, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=u.fisher, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=v.fletcher, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=w.ford, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=x.foster, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=y.fox, ou=Accounts, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=z.gibson, ou=Accounts, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=a.graham, ou=Accounts, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=b.grant, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=c.gray, ou=Accounts, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=d.green, ou=Accounts, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

#### # Head Office / Administration

dsadd user "cn=m.jenkins, ou=Administration, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=n.johnson, ou=Administration, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=o.jones, ou=Administration, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=g.white, ou=Administration, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=h.yalden, ou=Administration, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=i.yarbury, ou=Administration, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=j.yardley, ou=Administration, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no

## # Head\_Office / HR

dsadd user "cn=z.mcdonald, ou=HR, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=a.murphy, ou=HR, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=b.natt, ou=HR, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=c.nelson, ou=HR, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=d.nightingale, ou=HR, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=e.nixon, ou=HR, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=f.nutter, ou=HR, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=f.nutter, ou=HR, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

## # Head Office / Reception

dsadd user "cn=p.kelly, ou=Reception, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=q.kennedy, ou=Reception, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=u.king, ou=Reception, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=r.knight, ou=Reception, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=r.knight, ou=Reception, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=s.lawrence, ou=Reception, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=t.lee, ou=Reception, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

#### # Head Office / Research

dsadd user "cn=u.lewis, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=v.lloyd, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=w.marshall, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=x.martin, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=y.mason, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=g.dell, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=h.osborne, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=i.owen, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=j.oxley, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=k.page, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=l.painter, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=m.palmer, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=n.pastor, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=o.peterson, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=p.quill, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=q.quimby, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=u.quintrell, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

dsadd user "cn=r.ramsey, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=s.ratliff, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=t.richards, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=u.roberts, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=v.robinson, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=w.scott, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=x.simpson, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=y.smith, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=z.stewart, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=a.taylor, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=b.turner, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=c.walsh, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=d.ward, ou=Research, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=e.webb, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=f.west, ou=Research, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

#### # Head Office / Sales

dsadd user "cn=d.atkinson, ou=Sales, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Summer123 -mustchpwd no dsadd user "cn=e.bailey, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=f.baker, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=g.ball, ou=Sales, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=h.bell, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=i.brown, ou=Sales, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=j.burton, ou=Sales, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=k.carter, ou=Sales, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=l.clarke, ou=Sales, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=m.cole, ou=Sales, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=e.griffiths, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=f.hall, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=g.hamilton, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=h.harris, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

dsadd user "cn=i.harvey, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=j.hill, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=k.jackson, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=l.james, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=l.james, ou=Sales, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

## # Head Office / Senior Management

dsadd user "cn=k.yarrow, ou=Senior\_Management, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=l.yates, ou=Senior\_Management, ou=Head\_Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=m.young, ou=Senior Management, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=n.zachary, ou=Senior Management, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=o.zelly, ou=Senior Management, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=p.zinc, ou=Senior Management, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no dsadd user "cn=q.zouch, ou=Senior Management, ou=Head Office, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! mustchpwd no

## # Head Office / Help Desk

dsadd user "cn=a.adams, ou=Help\_Desk, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=b.allen, ou=Help\_Desk, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no dsadd user "cn=c.armstrong, ou=Help\_Desk, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no

#### # Admins / IT / DA

dsadd user "cn=adm.adams, ou=Admins, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof "CN=Domain Admins, CN=Users, dc=hacklab, dc=local" dsadd user "cn=adm.smith, ou=Admins, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof "CN=Domain Admins, CN=Users, dc=hacklab, dc=local" dsadd user "cn=adm.stewart, ou=Admins, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof "CN=Domain Admins, CN=Users, dc=hacklab, dc=local" dsadd user "cn=adm.stewart, ou=Admins, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof "CN=Domain Admins, CN=Users, dc=hacklab, dc=local" dsadd user "cn=adm.natt, ou=Admins, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof "CN=Domain Admins, CN=Users, dc=hacklab, dc=local" dsadd user "cn=adm.nelson, ou=Admins, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof "CN=Domain Admins, CN=Users, dc=hacklab, dc=local" dsadd user "cn=adm.nelson, ou=Admins, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no -memberof "CN=Domain Admins, CN=Users, dc=hacklab, dc=local"

# Service Accounts / IT

dsadd user "cn=svc afds, ou=Service Accounts, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local" dsadd user "cn=svc\_test, ou=Service\_Accounts, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local" dsadd user "cn=svc\_mssql1, ou=Service\_Accounts, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local" dsadd user "cn=svc\_mssql2, ou=Service\_Accounts, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local" dsadd user "cn=svc\_lab, ou=Service\_Accounts, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local" dsadd user "cn=svc\_admin, ou=Service\_Accounts, ou=IT, ou=Departments, dc=hacklab, dc=local" -fn User -ln test -pwd Passw0rd! -mustchpwd no memberof "CN=Domain Admins,CN=Users,dc=hacklab, dc=local"

# Set up Service Principal Name (SPN) for the following accounts so you can kerberoast them.

setspn -s http/server1.hacklab.local:8082 svc\_afds setspn -s http/server1.hacklab.local:8083 svc\_test setspn -s http/server1.hacklab.local:8084 svc\_mssql1 setspn -s http/server1.hacklab.local:8085 svc\_mssql2 setspn -s http/server1.hacklab.local:8086 svc\_lab setspn -s http/server1.hacklab.local:8087 svc\_admin

# Make the following accounts vulnerable to asreproast.

Set-ADAccountControl -Identity m.jenkins -DoesNotRequirePreAuth 1 Set-ADAccountControl -Identity z.mcdonald -DoesNotRequirePreAuth 1 Set-ADAccountControl -Identity u.lewis -DoesNotRequirePreAuth 1

# Create a description filed with a password in it.

Set-ADUser d.atkinson -Description "User Password Summer123"

# Disable SMB Signing on the DC.

Set-SmbClientConfiguration -RequireSecuritySignature 0 EnableSecuritySignature 0 -Confirm -Force

# Add Domain Machines

New-ADComputer -Name "SR2000-1" -SamAccountName "SR2000-1" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-2" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-3" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-4" -SamAccountName "SR2000-4" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-5" -SamAccountName "SR2000-5" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-5" -SamAccountName "SR2000-5" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-6" -SamAccountName "SR2000-6" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-6" -SamAccountName "SR2000-6" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-6" -SamAccountName "SR2000-6" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2000-6" -SamAccountName "SR2000-6" -Enabled \$True -OperatingSystem "Windows Server 2000 Service Pack 4" New-ADComputer -Name "SR2003-1" -SamAccountName "SR2003-1" -Enabled \$True -OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"

Presented by Andy Gill & Neil Lines at Steelcon 2023

```
New-ADComputer -Name "SR2003-2" -SamAccountName "SR2003-2" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-3" -SamAccountName "SR2003-3" -Enabled $True -
New-ADComputer -Name "SR2003-3" -SamAccountName "SR2003-3" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-4" -SamAccountName "SR2003-4" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-5" -SamAccountName "SR2003-5" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-6" -SamAccountName "SR2003-6" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2003-6" -SamAccountName "SR2003-6" -Enabled $True -
OperatingSystem "Windows Server 2003 Datacenter Service Pack 2"
New-ADComputer -Name "SR2008-1" -SamAccountName "SR208-1" -Enabled $True -
OperatingSystem "Windows Server 2008 B2 Standard Service Pack 1"
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-2" -SamAccountName "SR208-2" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-3" -SamAccountName "SR208-3" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-4" -SamAccountName "SR208-4" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-5" -SamAccountName "SR208-5" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2008-6" -SamAccountName "SR208-6" -Enabled $True -
OperatingSystem "Windows Server 2008 R2 Standard Service Pack 1"
New-ADComputer -Name "SR2012-1" -SamAccountName "SR2012-1" -Enabled $True -
OperatingSystem "Windows Server 2012 Standard"
New-ADComputer -Name "SR2012-2" -SamAccountName "SR2012-2" -Enabled $True -
OperatingSystem "Windows Server 2012 Standard"
New-ADComputer -Name "SR2012-3" -SamAccountName "SR2012-3" -Enabled $True -
OperatingSystem "Windows Server 2012 Standard"
New-ADComputer -Name "SR2012-4" -SamAccountName "SR2012-4" -Enabled $True -
OperatingSystem "Windows Server 2012 Standard"
New-ADComputer -Name "SR2019-1" -SamAccountName "SR2019-1" -Enabled $True -
OperatingSystem "Windows Server 2019 Standard"
New-ADComputer -Name "SR2019-2" -SamAccountName "SR2019-2" -Enabled $True -
OperatingSystem "Windows Server 2019 Standard"
New-ADComputer -Name "SR2019-3" -SamAccountName "SR2019-3" -Enabled $True -
OperatingSystem "Windows Server 2019 Standard"
New-ADComputer -Name "SR2019-4" -SamAccountName "SR2019-4" -Enabled $True -
OperatingSystem "Windows Server 2019 Standard"
New-ADComputer -Name "W7-1" -SamAccountName "W7-1" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-2" -SamAccountName "W7-2" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-3" -SamAccountName "W7-3" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-4" -SamAccountName "W7-4" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-5" -SamAccountName "W7-5" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "W7-6" -SamAccountName "W7-6" -Enabled $True -
OperatingSystem "Windows 7 Professional Service Pack 1"
New-ADComputer -Name "XP-1" -SamAccountName "XP-1" -Enabled $True -
OperatingSystem "Windows XP Service Pack 1"
# Set UP ACL's
Import-Module ActiveDirectory
Set-Location AD:
Function SetAcl($for, $to, $right, $inheritance)
```

```
$forSID = New-Object System.Security.Principal.SecurityIdentifier (Get-
ADUser $for).SID
    $objOU = ($to).DistinguishedName
    $objAcl = get-acl $objOU
    # https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectoryrights?view=dotnet-
plat-ext-5.0
    $adRight = [System.DirectoryServices.ActiveDirectoryRights] $right #
https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectoryrights?view=dotnet-
plat-ext-5.0
    $type = [System.Security.AccessControl.AccessControlType] "Allow" #
https://docs.microsoft.com/fr-
fr/dotnet/api/system.security.accesscontrol.accesscontroltype?view=dotnet-
plat-ext-5.0
    $inheritanceType =
[System.DirectoryServices.ActiveDirectorySecurityInheritance] $inheritance
# https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectorysecurityinheritance?v
iew=dotnet-plat-ext-5.0
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule
$forSID,$adRight,$type,$inheritanceType
    $objAcl.AddAccessRule($ace)
    Set-Acl -AclObject $objAcl -path $objOU
Function SetAclExtended($for, $to, $right, $extendedRightGUID,
$inheritance)
    $forSID = New-Object System.Security.Principal.SecurityIdentifier (Get-
ADUser $for).SID
    $objOU = ($to).DistinguishedName
    $objAcl = get-acl $objOU
    # https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectoryrights?view=dotnet-
plat-ext-5.0
    $adRight = [System.DirectoryServices.ActiveDirectoryRights] $right #
https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectoryrights?view=dotnet-
plat-ext-5.0
    $type = [System.Security.AccessControl.AccessControlType] "Allow" #
https://docs.microsoft.com/fr-
fr/dotnet/api/system.security.accesscontrol.accesscontroltype?view=dotnet-
plat-ext-5.0
    $inheritanceType =
[System.DirectoryServices.ActiveDirectorySecurityInheritance] $inheritance
# https://docs.microsoft.com/fr-
fr/dotnet/api/system.directoryservices.activedirectorysecurityinheritance?v
iew=dotnet-plat-ext-5.0
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule
$forSID,$adRight,$type,$extendedRightGUID,$inheritanceType
    $objAcl.AddAccessRule($ace)
    Set-Acl -AclObject $objAcl -path $objOU
## acl values :
# AccessSystemSecurity
# CreateChild
# Delete
```

```
# DeleteChild
# DeleteTree
# ExtendedRight
# GenericAll
# GenericExecute
# GenericRead
# GenericWrite
# ListChildren
# ListObject
# ReadControl
# ReadProperty
# Self
# Synchronize
# WriteDacl
# WriteOwner
# WriteProperty
## extend rights
# "00299570-246d-11d0-a768-00aa006e0529" {$right = "User-Force-Change-
Password"}
# "45ec5156-db7e-47bb-b53f-dbeb2d03c40" {$right = "Reanimate-Tombstones"}
# "bf9679c0-0de6-11d0-a285-00aa003049e2" {$right = "Self-Membership"}
# "ba33815a-4f93-4c76-87f3-57574bff8109" {$right = "Manage-SID-History"}
# "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2" {$right = "DS-Replication-Get-
Changes-All"}
# ACL abuse scenarios
# https://sensepost.com/blog/2020/ace-to-rce/
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces
# https://adsecurity.org/?p=3658
# genericall-on-user1
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#genericall-on-user
SetAcl (Get-ADUser "n.collins") (Get-ADUser "a.adams") "GenericAll" "None"
# genericall-on-group
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#genericall-on-group
SetAcl (Get-ADUser "o.davidson") (Get-ADGroup "Domain Admins") "GenericAll"
"None"
# genericall-genericwrite-write-on-computer
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#genericall-genericwrite-
write-on-computer
SetAcl (Get-ADUser "g.white") (Get-ADComputer "W7-4$") "WriteProperty"
"A]]"
# writeproperty-on-group
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#writeproperty-on-group
SetAcl (Get-ADUser "q.kennedy") (Get-ADGroup "Domain Admins")
"WriteProperty" "All"
```

```
# self-self-membership-on-group
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#self-self-membership-on-
group
SetAclExtended (Get-ADUser "u.roberts") (Get-ADGroup "Domain Admins")
"Self" "bf9679c0-0de6-11d0-a285-00aa003049e2" "None"
# writeproperty-self-membership
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#writeproperty-self-
membership
SetAclExtended (Get-ADUser "f.west") (Get-ADGroup "Domain Admins")
"WriteProperty" "bf9679c0-0de6-11d0-a285-00aa003049e2" "All"
# forcechangepassword
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#forcechangepassword
# https://docs.microsoft.com/fr-fr/windows/win32/adschema/r-user-change-
password
SetAclExtended (Get-ADUser "l.james") (Get-ADUser "y.fox") "ExtendedRight"
"00299570-246d-11<u>d0-a768-00aa006e0529" "None"</u>
# write owner on group
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#writeowner-on-group
SetAcl (Get-ADUser "a.graham") (Get-ADGroup "Domain Admins") "WriteOwner"
"None"
# genericwrite-on-user
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#genericwrite-on-user
SetAcl (Get-ADUser "c.nelson") (Get-ADUser "w.marshall") "GenericWrite"
"None"
# writedacl-writeowner
# https://www.ired.team/offensive-security-experiments/active-directory-
kerberos-abuse/abusing-active-directory-acls-aces#writedacl-writeowner
SetAcl (Get-ADUser "p.kelly") (Get-ADGroup "RDP") "WriteDacl" "None"
```

exit

2. Open PowerShell with an administrative session (Search for PowerShell, right click and select run as administrator.)

≥ Administrato	r: Windows	PowerShell
----------------	------------	------------



Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

3. Highlight, copy and paste the complete PowerShell script into the Administrator session.

≥ Administrator: Windows PowerShell –
<pre>isadd succeeded:ou=Service_Accounts,ou=IT,ou=Departments,dc=hacklab,dc=local 'S C:\Windows\system32&gt; dsadd ou "ou=Help_Desk,ou=IT,ou=Departments,dc=hacklab,dc=local" isadd succeeded:ou=Help_Desk,ou=IT,ou=Departments,dc=hacklab,dc=local 'S C:\Windows\system32&gt; dsadd ou "ou=Head_Office,ou=Departments,dc=hacklab,dc=local" 'S C:\Windows\system32&gt; dsadd ou "ou=HR,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" 'S C:\Windows\system32&gt; dsadd ou "ou=Sales,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" 'S C:\Windows\system32&gt; dsadd ou "ou=Sales,ou=Head_Office,ou=Departments,dc=hacklab,dc=local</pre>
<pre>PS C:\Windows\system32&gt; dsadd ou "ou=Accounts,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Accounts,ou=Head_Office,ou=Departments,dc=hacklab,dc=local PS C:\Windows\system32&gt; dsadd ou "ou=Research,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Research,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" PS C:\Windows\system32&gt; dsadd ou "ou=Reception,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Reception,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Reception,ou=Head_Office,ou=Departments,dc=hacklab,dc=local PS C:\Windows\system32&gt; dsadd ou "ou=Administration,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Administration,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Administration,ou=Head_Office,ou=Departments,dc=hacklab,dc=local PS C:\Windows\system32&gt; dsadd ou "ou=Senior_Management,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Senior_Management,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Senior_Management,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Senior_Management,ou=Head_Office,ou=Departments,dc=hacklab,dc=local" dsadd succeeded:ou=Senior_Management,ou=Head_Office,ou=Departments,dc=hacklab,dc=local</pre>
<pre>&gt;S C:\Windows\system32&gt; # Create a user groups OU &gt;S C:\Windows\system32&gt; &gt;S C:\Windows\system32&gt; dsadd ou ou=Groups,ou=Departments,dc=hacklab,dc=local dsadd succeeded:ou=Groups,ou=Departments,dc=hacklab,dc=local &gt;S C:\Windows\system32&gt; &gt;S C:\Windows\system32&gt; # Create the following user groups to the group OU &gt;S C:\Windows\system32&gt; &gt;S C:\Windows\system32&gt; &gt;S C:\Windows\system32&gt; dsadd group cn=sales,ou=Groups,ou=Departments,dc=hacklab,dc=local dsadd succeeded:cn=sales,ou=Groups,ou=Departments,dc=hacklab,dc=local</pre>

This will add all the OU's, Groups, highly vulnerable User Accounts, Service Accounts, and general bad misconfigurations. All accounts have a password of Passw0rd! for ease of use, and yes this is dreadful and should never be used in production.

4. Once complete, reopen Active Directory Users and Computers. You should see the OU's and accounts, which gives the appearance of a more realistic environment.

Active Directory Users and Computers			_
File Action View Help			
🔶 📦 📶 📋 🗒 🖓 🦛	2 🛅 🍸 🗾 2		
Active Directory Users and Computers [WIN-MSE Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Departments Groups Head_Office Administration HR Reception Research Sales Sales Senior_Management Help_Desk Service Accounts Service Accounts Service Accounts Saved Queries NIN-MSE NIN-M	Name adm.adams adm.natt adm.nelson adm.smith adm.stewart	Type User User User User	Description

Members of the Admins group found under the IT OU are all members of the domain admin group.

Active Directory Users and Computers				
File Action View Help				
	1 🕺 🐮 🛅 🍸 💆 🕯	5		
Active Directory Users and Computers [WIN-MSE ^	Name	Туре	e	Descriptio
> Saved Queries	👗 adm.adams	Use	r	
✓ Image hacklab.local	adm.natt	Use	r	
> 🧾 Builtin	adm.nelson	Use	r	
> Computers	adm.smith	Use	r	
✓ ■ Departments	adm stewart	Lise	r	
Groups	admistewart	030		
✓ I Head_Office				
> 🖬 Accounts	adm.natt Properties			
Administration	finger woodere i			
> 🖬 HR	Remote control	Remote L	Jesktop Se	ervices Profile
> 🗾 Reception	General Address	Account	Profile	Telephones
> 🖻 Research	Member Of	Dial-in	Env	ironment
> 🛱 Sales	Member of:			
> Senior Management				
✓ ☐ IT	Name	Active Directo	ory Domain	Services Folder
Admins	Domain Admins	hacklab.local/	Users	
	Domain Users	hacklab.local/	Users	
> Service_Accounts				

The service accounts are also members of the domain admin group and have been configured so they are ready for you to kerberoast.

Name			Туре		Descript	ion	
svc_admin			User				
svc_afds		I	User				
svc_lab		I	User				
svc_mssql1		I	User				
svc_mssql2		I	User				
svc_test		I	User				
svc_lab Propertie	es					?	×
Remote contr	rol	Remote	Desktop Se	rvices F	Profile	CO	<b>۱</b> +
General Ad	dress	Account	Profile	Tele	ephones	Delega	ation
Organization	Me	mber Of	Dial-in	Envi	ronment	Sess	ions
Member of:							_
Name		Active Direc	tory Domain	Service	es Folder		
Domain Admi	ins	hacklab.loca	al/Users				
Domain User	S	hacklab.loca	al/Users				

Have fun!

In addition to spinning up users, often it is useful to have all the logging enabled too, so the following can be pasted into PowerShell or CMD.exe as administrator to enable on the various machines you have in your domain:

:: Audit Policy Settings

:: Hat tip to <u>https://twitter.com/Antonlovesdnb</u> for the tips on things to enable.

:: Audit Policy: Account Logon

Auditpol /set /category:"Account Logon" /success:enable /failure:enable

:: Audit Policy: Account Management

Auditpol /set /category:"Account Management" /subcategory:"Computer Account Management" /success:enable /failure:enable

Auditpol /set /category:"Account Management" /subcategory:"Other Account Management Events" /success:enable /failure:enable

Auditpol /set /category:"Account Management" /subcategory:"Security Group Management" /success:enable /failure:enable

Auditpol /set /category:"Account Management" /subcategory:"User Account Management" /success:enable /failure:enable

## :: Audit Policy: Detailed Tracking

Auditpol /set /category:"Detailed Tracking" /subcategory:"DPAPI Activity" /success:enable /failure:enable

Auditpol /set /category:"Detailed Tracking" /subcategory:"Process Creation" /success:enable /failure:enable

:: Audit Policy: DS Access

Auditpol /set /category:"DS Access" /success:enable /failure:enable

:: Audit Policy: Logon/Logoff

Auditpol /set /category:"Logon/Logoff" /subcategory:"Account Lockout" /success:enable /failure:enable

Auditpol /set /category:"Logon/Logoff" /subcategory:"Logon" /success:enable /failure:enable

Auditpol /set /category:"Logon/Logoff" /subcategory:"Other Logon/Logoff Events" /success:enable /failure:enable

Auditpol /set /category:"Logon/Logoff" /subcategory:"Special Logon" /success:enable /failure:enable

:: Audit Policy: Object Access

Auditpol /set /category:"Object Access" /subcategory:"Other Object Access Events" /success:enable /failure:enable

Auditpol /set /category:"Object Access" /subcategory:"Registry" /success:enable /failure:enable

:: Audit Policy: Policy Change

Auditpol /set /category:"Policy Change" /subcategory:"Audit Policy Change" /success:enable /failure:enable

:: Audit Policy: Privilege Use

Auditpol /set /category:"Privilege Use" /subcategory:"Sensitive Privilege Use" /success:enable /failure:disable

:: Audit Policy: System

Auditpol /set /category:"System" /subcategory:"Other System Events" /success:enable /failure:enable

Auditpol /set /category:"System" /subcategory:"System Integrity" /success:enable /failure:enable

# Windows 11 setup guide

The process to create a Windows 11 VM is slightly more complex than Server 2022 as it requires you to enable the encrypted Trusted Platform Module and set a boot encryption password, this guide will walk you through that process.

1. Home create a New Virtual Machine.

WORKSTATION 16 PRO™				
Create a New Virtual Machine	Open a Virtual Machine	Connect to a Remote Server		

2. Select the Windows 11 ISO, then click Next.

(+)	Z	$\stackrel{\longrightarrow}{\leftarrow}$
reate a New Virtual Machine New Virtual Machine Wi	Open a Virtual Machine zard	Connect to a Remote Server X
Guest Operating Syst A virtual machine i system. How will y	tem Installation is like a physical computer; it nee you install the guest operating sys	ds an operating tem?
Install from:		
O Installer disc:		
No drives availab	le	$\sim$
<ul> <li>Installer disc image f</li> <li>ILENTENTERPRISE</li> <li>Could not detect You will need to</li> <li>I will install the opera The virtual machine</li> </ul>	ile (iso): <u>EVAL_OEMRET_x64FRE_en-gb.is</u> which operating system is in this specify which operating system v ating system later. will be created with a blank hard	Browse disc image. vill be installed. disk.

3. Select Microsoft Windows 10 and later x64, then click Next.

New Virtual Machine Wizard			$\times$
Select a Guest Operating Syst Which operating system will	<b>tem</b> be installed on th	nis virtual machin	e?
Guest operating system			
<ul> <li>Microsoft Windows</li> <li>Linux</li> <li>VMware ESX</li> <li>Other</li> </ul>			
Version			
Windows 10 and later x64			~
Help	< Back	Next >	Cancel

4. Name the machine, then click Next.

- William -	1	TVIEICI III IC		- Nemore 5	EIVEL
New Virtual Ma	ichine Wizard				×
Name the V What na	<b>irtual Machine</b> me would you like to	o use for this vi	irtual machine?		
Virtual machine	name:				
Windows 11					
Location:					
C:\	Virtual	Machines\Wind	dows 11	Browse	
		< Back	Next >	Cance	

5. Allocate what storage you can, Windows 11 can run on 40GB.

New Virtual Machine Wizard	×
<b>Specify Disk Capacity</b> How large do you want this o	disk to be?
The virtual machine's hard disk is sto physical disk. These file(s) start small files, and data to your virtual machine	ored as one or more files on the host computer's I and become larger as you add applications, e.
Maximum disk size (GB): 60.	.0 🖕
Recommended size for Windows 10 a	and later x64: 60 GB
<ul> <li>Store virtual disk as a single file</li> <li>Split virtual disk into multiple files Splitting the disk makes it easier t but may reduce performance with</li> </ul>	s to move the virtual machine to another computer h very large disks.
Help	< Back Next > Cancel

6. Click on Finish.

and later x64.	create the virtual machine.	. Then you can install Windows 10
The virtual machine	will be created with the fol	lowing settings:
Name:	Windows 11	
Location:	C:\	Virtual Machines\Windows 11
Version:	Workstation 16.2.x	
Operating System:	Windows 10 and later x6	4
Hard Disk:	40 GB, Split	
Memory:	2048 MB	
Network Adapter:	NAT	
Other Devices:	2 CPU cores, CD/DVD, U	SB Controller, Printer, Sound Card
Customize Hardv	vare	

7. Click on Edit virtual machine settings.

Windows 11		
Power on this virtual machine set	achine	
<ul> <li>Devices</li> </ul>		
📟 Memory	2 GB	
Processors	2	
🖂 Hard Disk (NVMe)	40 GB	
💿 CD/DVD (SATA)	Using file C:\Use	
🖵 Network Adapter	NAT	
😌 USB Controller	Present	
্বি» Sound Card	Auto detect	
🛱 Printer	Present	
Display	Auto detect	
<ul> <li>Description</li> </ul>		
Type here to enter a descri machine.	ption of this virtual	

# 8. Click on Options then highlight Access Control and Select Encrypt.

/irtual Machine Settings				
Hardware Options				
Settings General Power Shared Folders Shapshots AutoProtect Guest Isolation Access Control W VMware Tools VNC Connections Unity Autologin Advanced	Summary Windows 11 Disabled Disabled Not encrypted Time sync off Disabled Not available Default/Default		Encryption This virtual machine is not encrypted. You can protect this virtual machine's dat a password.	a and configuration with Encrypt

9. Add a Password then click Encrypt.

Control	Not encrypted
VMware Tools	Time sync off
VNC Connections	Disabled Encrypt Virtual Machine X
Appliance view A Autologin Advanced	Not availal Default/De Set the password for this virtual machine.
	Password:
	Confirm:
	$  \  \  \  \  \  \  \  \  \  \  \  \  \$
	Depending on the size of this virtual machine, the encryption process could take from a few minutes to a few hours.
	Encrypt Cancel

Access Control should now say Encrypted.

Н	ardware Options	
	Settings	Summary
	🖵 General	Windows 11
	Power	
	Shared Folders	Disabled
	C Snapshots	
	AutoProtect	Disabled
	🛆 Guest Isolation	
	Carl Access Control	Encrypted

10. Click back on the Hardware tab, select Add then highlight Trusted Platform Module and click on Finish.

Device	Summary		Memory		
Memory	2 GB		Specify the a	mount of memory allo	cated to th
Processors	2		size must be	a multiple of 4 MB.	
Hard Disk (NVMe)	40 GB		Memory for t	his virtual machine:	2048
CD/DVD (SATA)	Using file C:\			_	2010
Network Adapter	NAT		128 GB -		
Sound Card	Auto detoct		64 GB		
Printer	Present		32 GB	•	
Display	Auto detect		16 GB		<b>N</b>
	riate activit		8 GB ·		(
(			4 GB		0
Add Hardware W	/izard			×	2
Hardware Ty	pe				
What type	of hardware do you wa	ant to install?			2
					_
Hardware types:		Explanation			- 0
Hard Disk		Add a Tru	Add a Trusted Platform Module.		1
CD/DVD Drive	2				
Floppy Drive	ter				
Network Adap	ner				
Controlle	1				
Parallel Port					
Serial Port					
🛱 Printer					
Generic SCSI	Device				
Contracted Platfo	rm Module				
_					
			Finish	Cancel	
			Finish	Cancel	
				-	OK
					UN

11. Give it slightly over 4GB of RAM, if you don't you will not be able to install Windows 11.

12. Finally check there is no Floppy Disk enabled as that will also stop the installation.

- 13. Click OK and then Start up the VM.
- 14. During the initial boot click in the screen and then press any key when prompted.

Press any key to boot from CD or DVD.

15. Select language then click Next.

Langua <u>ge</u> to install:	English (United Kingdom)	T
Time and currency format:	English (United Kingdom)	<b>_</b>
<u>K</u> eyboard or input method:	United Kingdom	•
Enter your language :	and other preferences and click "Next" to continue.	
Microsoft Corporation. All rights reserved.		<u>N</u> ext

16. Click Install Now.

🖆 Windows Setup		
	Install now	
<u>R</u> epair your computer		
Microsoft Corporation. All rights res	erved.	

If you see this error during the initial install.

🕞 💰 Windows Setup	×
This PC can't run Windows 11	
This PC doesn't meet the minimum system requirements to install this version of Windows. Fo more information, visit https://aka.ms/WindowsSysReq	r
	<u>N</u> ext

Check that you have set up Access Control by adding an encrypted password.

Hardware Options				
	Settings	Summary		
	🖵 General	SteelCon_Windows11		
	Power			
	Shared Folders	Disabled		
	🕒 Snapshots			
	AutoProtect	Disabled		
	🔒 Guest Isolation			
	Control	Encrypted		

Check the Trusted Platform Module set to Present.

Н	ardware Options	
	Device	Summary
	Memory	4.3 GB
	Processors	2
	Hard Disk (NVMe)	60 GB
	OCD/DVD (SATA)	Using file C:\Users\nlines\Doc
	Network Adapter	NAT
	🚭 USB Controller	Present
	く Sound Card	Auto detect
	🖶 Printer	Present
	Display	Auto detect
	Trusted Platform Mod	Present

And make sure your VM has slightly over 4GB of RAM and does not have a Floppy Disk installed.

17. Accept the Licence and Click on Next.

🕼 Windows Setup	
Applicable notices and licence terms	
Last updated June 2021	
MICROSOFT SOFTWARE LICENSE TERMS	
WINDOWS OPERATING SYSTEM	
IF YOU LIVE IN (OR IF YOUR PRINCIPAL PLACE OF BUSINESS UNITED STATES, PLEASE READ THE BINDING ARBITRATION AND CLASS ACTION WAIVER IN SECTION 11. IT AFFECTS HO DISPUTES ARE RESOLVED.	IS IN) THE CLAUSE W
Thank you for choosing Microsoft!	
I accept the Microsoft Software Licence Terms. If an organisation is licensing it, to bind the organisation.	I am authorised
	<u>N</u> e

18. Select Customised: Install Windows only (advanced).

Customised: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to
make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue

19. Click Next.

		nuows:		
Name		Total size	Free space	Туре
Drive 0 Uni	allocated Space	60.0 GB	60.0 GB	1
Refresh	Delete	<b>€</b> ormat	* New	

Windows 11 should then start to install and reboot when completed.



🔏 Windows Setup
Installing Windows
Status
Copying Windows files
Getting files ready for installation
✓ Installing features
✓ Installing updates
Finishing up
rinishing up

20. After the reboot select your country.

	Is this the right country or region?
	United Kingdom
1	Afghanistan
	Åland Islands
	Albania
	Algeria
	American Samoa
	Andorra
	Yes

21. Select Sign-In options.



22. Select Domain join instead.

Let's set things up for your work or school You'll use this info to sign in to your devices.
Sign in with a security key   Choose this only if you have enabled a security key for  your account.
○ Domain join instead
~
Back

23. Add a username which will be used as the local admin account.



24. Add a password for the account then click on Next.

Create a really memorable password
Make sure that you pick something you'll absolutely remember.
Enter a password
•••••
Even better, use an online account

25. Confirm the Password then click on Next.

26. Set up your three security questions and answers.

Now add security que	estions
Just in case you forget your password questions. Make sure your answers ar	d, choose 3 security re unforgettable.
Security question (1 of 3)	
Security question (1 of 3)	$\sim$
Your answer	
Even better, use an online account	

27. Configure location settings.



28. Configure Find my device settings.

# Find my device

Choose your settings, then select **Accept** to save them. Check the **Learn more** link for info on these settings, how to change them, how Windows helps protect you from unsafe apps and web content, and the related data transfers and uses.



## 29. Configure Send diagnostic data settings.



## 30. Configure the Improve inking settings.

# Improve inking & typing

Choose your settings, then select **Accept** to save them. Check the **Learn more** link for info on these settings, how to change them, how Windows helps protect you from unsafe apps and web content, and the related data transfers and uses.



## 🖉 Yes

Send optional inking and typing diagnostic data to Microsoft to improve the language recognition and suggestion capabilities of Microsoft apps and services.

## 🔀 №

Don't use my diagnostic data to help improve the language recognition and suggestion capabilities of Microsoft apps and services.

Learn more

Accept

## 31. Configure the advertising settings.



# Get tailored experiences with diagnostic data

Choose your settings, then select **Accept** to save them. Check the **Learn more** link for info on these settings, how to change them, how Windows helps protect you from unsafe apps and web content, and the related data transfers and uses.

Let Microsoft offer you tailored experiences based on the diagnostic data you have chosen (either Basic or Full). Tailored experiences mean personalised tips, ads and recommendations to enhance Microsoft products and services for your needs.

The tips, ads and recommendations you see will be more generic and may be less relevant to you.

Learn more

Accept

32. Configure more advertising settings.

# Let apps use advertising ID

Choose your settings, then select **Accept** to save them. Check the **Learn more** link for info on these settings, how to change them, how Windows helps protect you from unsafe apps and web content, and the related data transfers and uses.



#### Apps can use advertising ID to provide more personalised advertising in accordance with the privacy policy of the app provider.

🕑 Yes



The number of ads you see won't change, but they may be less relevant to you.

Learn more

Accept

## Then host should check for updates.



And finally, you should be close to it completing.



Don't waste time on customising your experience as you will not be using this initial account for long.



33. Firstly, you need to add VM Tools, which uses the same process as with Server 2022.

- Open File Explorer.
- Right Click on the DVD Drive and select Eject.
- Click on the VM tool bar which is outside of your Windows VM.
- Select Install VM Tools.
- Double click the mounted Disk in your VM.
- Double click on setup64.
- Select yes when prompted by UAC.



34. Select Next, Typical Installation followed by Next.

35. Restart the machine.

Windows 11 feels slower than Windows 10 VM's this could improve over time, but it could also be something we just have to get used to.
## Cloning a Windows 11 VM

It is worth cloning the Windows 11 machine so you will have two domain machines to play around with.

- 1. Make sure the VM you wish to clone is powered off.
- 2. Select VM from the tool bar / Manage / Clone.



4. Select The current state in the virtual machine.

Clone Virtual Machine Wizard			$\times$
Clone Source Which state do you want to create	a clone from?		
Clone from			
• The current state in the virtual m	achine		
Creating a linked clone from the	current state wi	ll create a new sn	apshot.
An existing snapshot (powered o	ff only):		~
This virtual machine has no exist	ing cloneable sr	napshots.	
	< Back	Next >	Cancel

5. Click Next.

Clone Virtual Machine Wizard			$\times$				
Clone Type How do you want to clone this vir	tual machine?						
<ul> <li>Clone method</li> <li>Create a linked clone</li> <li>A linked clone is a reference to the disk space to store. However, it disk space to store. However, it disk space to store. However, it disk space a full clone</li> <li>Create a full clone</li> <li>A full clone is a complete copy of state. This virtual machine is full store.</li> </ul>	he original virtu cannot run with of the original vir y independent, l	al machine and r out access to the rtual machine at but requires mor	requires less original its current re disk space to				
You cannot make a linked clone of an encrypted virtual machine.							
	< Back	Next >	Cancel				

6. Rename it then select Finish.

Clone Virtual Machine Wizard		×
Name of the New Virtual Machi What name would you like to use	<b>ne</b> e for this virtual machine?	
Virtual machine name Clone of SteelCon_Windows11		
Location		
C:\	\Clone of SteelCon_V	Browse
process should initiate.	< Back Finish	Cancel
Clone Virtual Machine Wizard		×
Cloning Virtual Machine		
✓ Preparing clone operation	on	
VMware Workstation		
Cloning		
		Canaal
		Cancel

And once its completed you should see your three machines on the top VM tool bar.



## Adding a Windows 11 VM to the hacklab domain

1. Select the VM you want to add to the Domain, and under the setting make sure its Network connection is set to the same network as your domain controller.



2. Open CMD and confirm you can ping the domain controllers IP address.



You can ping a DC even if it has its windows firewall enabled, If you don't get a reply from the DC's IP address you will not be able to add the machine to the Domain, check the DC's IP address is correct, then if that's ok double check the VM networking settings.

If you did get a reply from your DC continue onto step 3.

3. On your Windows 11 VM you need to open Network and Internet settings so you can add the domain controllers IP address for DNS services.



4. Click on Ethernet.

Ne	twork & in twork & in Ethern	ternet	Properties     Public network	● Data usage > 140 MB, last 30 days
<u> </u>	Ethernet Authentication, IP an	d DNS settings, metered network	¢	>
5. U	nder DNS serve	r assignment, click I	Edit.	
Ne	twork & in	ternet > Ethei	rnet	
	<ul> <li>Public netwo Your device is r place.</li> <li>Private netwo Your device is o should know an</li> <li>Configure firewall</li> </ul>	rk (Recommended) ot discoverable on the network. ork liscoverable on the network. Sele Id trust the people and devices o and security settings	Use this in most cases—when connected to a net ct this if you need file sharing or use apps that co n the network.	work at home, work, or in a public ommunicate over this network. You
	Authentication se	ttings		Edit
	Metered connecti Some apps might w Set a data limit to	on ork differently to reduce data usa help control data usage on t	ge when you're connected to this network : <mark>his network</mark>	Off
	IP assignment:	Automatic ([	DHCP)	Edit
	DNS server assign	ment: Automatic (I	DHCP)	Edit

6. Change the default from Automatic (DHCP) to manual.

Edit DNS setting	gs
Automatic (DHCP)	~
Save	Cancel

7. Tick on IPv4, then add the IP address of your domain controller followed by Save.

O Publ		
place	Edit DNS settings	
Priva     Your     shoul	Manual	~
Configur	IPv4	
	On On	
Authentic	Preferred DNS	
Metered	192.168.68.200	×
Some app	DNS over HTTPS	
Set a dat	Off	~
IP assigni	Alternative DNS	
DNS serv	DNS over HTTPS	
Link spee	Off	~
Link-loca IPv4 addı IPv4 DNS	IPv6	
Manufact		
Descripti Driver ve	Save Canc	el

8. Try and ping hacklab.local from your windows 11 host, it should now resolve.

```
C:\Users\ieuser>ping hacklab.local
Pinging hacklab.local [192.168.68.200] with 32 bytes of data:
Reply from 192.168.68.200: bytes=32 time=1ms TTL=128
```

9. If you can ping the Domain, you are ready to add the machine to the Domain, Open File explorer.

🔁 File Explorer						
+ New -	0 [	) () 6	∭ 1↓ Sort × 8= Vi	ew 🗸 🛛 🖓 Filter 🗸		
$\leftarrow \rightarrow \checkmark \uparrow$	↑ Home	>			~ C	Q Search Home
✓ 🏫 Home	✓ Quick a	access				
E Desktop	*	Desktop This PC	Downloads This PC		Documents This PC	Pictures This PC
🛓 Downloads	*	··· ·			*	π
Documents	*	Music This PC	Videos This PC			
Pictures	*	-				
🕖 Music	~ Favour	rites				
🔛 Videos			After	you've pinned some files, v	we'll show them here	
> 🌰 OneDrive	✓ Recent	t				
🔉 💻 This PC			After you've o	pened some files, we'll sho	ow the most recent o	nes here.
> 📫 DVD Drive (D:) C	CEN/					
> 🛬 Network						
6 items						
			📕 Q 🖬 🔎	<b>e e</b>	<b>•</b>	

Right click on This PC and select Show More Options followed by Properties.
 Select the Domain or workgroup settings.

DESK VMwa	TOP-RICLTNO are7,1		Rename this PC
()	Device specificat	tions	Сору
	Device name	DESKTOP-RICLTNO	
	Processor	13th Gen Intel(R) Core(TM) i7-13700HX 2.30 GHz (2 processors)	
	Installed RAM	4.29 GB	
	Device ID	C10C3B86-D97C-48B0-B8D8-E825C19A8D79	
	Product ID	00329-20000-00001-AA177	
	System type	64-bit operating system, x64-based processor	
	Pen and touch	No pen or touch input is available for this display	

12. Click on Change.



13. This is also your chance to rename the machine to something more logical.

C			)
D	System Properties	×	
Pr	Computer Name/Domain Changes X	mote	(2)
In	You can change the name and the membership of this	computer	(
D	computer. Changes might alrect access to network resources.		
P۱	Computer name:	lan/a	
Sy	DESKTOP-RICLTNO	lary s	
Pe	Full computer name:		
	DESKTOP-RICLTNO		
d	More	ork ID	syste
	Member of		-
w	O Domain:	nge	
1	• Workgroup:		
Ec	WORKGROUP		
Ve			
In	OK Cancel		
0	OK Carad	Analy	
Ex	OK Cancer	Арріу	b.0

14. Select Domain then type in the full domain name hacklab.local followed by clicking on OK.

DESKTC VMware7	IP-RICLTNO 7,1		
() (	Device specifications		
	System Properties	×	
E	Computer Name/Domain Changes X	mote	(2 p
11 C	You can change the name and the membership of this computer. Changes might affect access to network resources.	computer	(r h
P	Computer name:	larv's	
S	SteelconWin11-1	aly c	
P	Full computer name: SteelconWin11-1		
Related	More	vrk ID	syste
	Member of		
	Domain:     hacklab.local	nge	
	Watersini		
F	WORKGROUP		
	OK Cancel		

You should then be prompted to enter a domain account, by default any member of the domain users' group can add up to 10 machines to a domain. Yep any standard user!

• ······	
Computer Name	e/Domain Changes
inter the name and pass oin the domain.	sword of an account with permission to
g.white	
g.white	\$

Name	1	Гуре		Descrip	otion	
s.white	ι	Jser				
g.white Properties					?	×
Remote control	Remote Desktop Services Profile			ofile	COM+	
General Address	al Address Account Profile Telephones			Organization		
Member Of	Dial-in	Environment			Sessions	
Member of:						
Name	Active Director	ry Domain	Services	Folder		
Domain Users	hacklab.local/	Users				

And if all is going to plan you should see Welcome to the Domain!



15. Reboot your Windows 11 machine.

If you jump over to the domain controller and look under Computers you will see the machine that you have just added to the Domain.

Active Directory Users and Computers			
File Action View Help			
	8	8 🗑 🍸 🗾 🕱	
> 🚆 Saved Queries	^	Name	Туре
✓ jii hacklab.local		🔙 SR2008-4	Computer
> 🧮 Builtin		i SR2008-5	Computer
Computers		I SR2008-6	Computer
✓ ■ Departments		i SR2012-1	Computer
Groups		i SR2012-2	Computer
		i SR2012-3	Computer
> Accounts		₩ SR2012-4	Computer
		I SR2019-1	Computer
> B Pocontion		₩ SR2019-2	Computer
		₩ SR2019-3	Computer
		NR2019-4	Computer
> Senior Management		STEELCONWIN11-1	Computer
<ul> <li>✓ IT</li> </ul>		₩7-1	Computer

16. After the restart click on Other user.



17. Then use any of the domain user accounts to login.

Other user		
Other user		
Other user g.white	→	

Repeat this process to add any other machines.

## SlinkyCat

Download SlinkyCat: https://github.com/LaresLLC/SlinkyCat

Slinky Cat has been developed to automate some of the methods introduced in living off the land and to supplement ScrapingKit. To help security and IT teams reduce their AD exposures and uncover quick wins and fixes designed for pen-testers and defenders alike.

Slinky Cat attempts to give users an easy-to-navigate menu offering predefined Active Directory Service Interfaces (ADSI) and .NET System.DirectoryServices.AccountManagement namespace queries can be used to enumerate a Windows domain.

1. Download SlinkyCat.ps1 and attempt to import it, if you see the error below you need to bypass the default PowerShell execution policy.



Method 1 to bypass PowerShell execution policy, copy and paste the line below and press enter.

## powershell.exe -nop -exec bypass

	Windows PowerShell	× ≥	Windows PowerShell	×	+					×
PS ipm beca about At + i	C:\Users\g.white\De b : File C:\Users\g ause running script ut_Execution_Polic: line:1 char:1 pmo .\SlinkyCat.ps	esktop J.white is is d ies at	\Steelcon\SlinkyCat> e\Desktop\Steelcon\S disabled on this sys https:/go.microsoft	> ipr Slink stem t.cor	mo . kyCa . Fo m/fw	\SlinkyCat t\SlinkyCa r more inf link/?Link	ps1 t.ps1 cannot ormation, see ID=135170.	be lo	aded	
PS ( Win	+ CategoryInfo + FullyQualifiedEp oduleCommand C:\Users\g.white\De dows PowerShell	rorId	: SecurityError: (: : UnauthorizedAcces \Steelcon\SlinkyCat>	:) [] ss,M: > pow	Impo icro wers	rt-Module] soft.Power hell.exe -	, PSSecurityE Shell.Commands nop -exec bypa	xcept s.Imp ass	ion ortM	
Cop	yright (C) Microso	t Cor	poration. All rights	s reg	serv	ed.				
Ins <sup>.</sup> s	tall the latest Pow	verShe]	ll for new features	and	imp	rovements!	https://aka.u	ms/PS	Windo	w
PS (	C:\Users\g.white\De	esktop	\Steelcon\SlinkyCat>	>						

You should be able to import the script and then execute it.

```
PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat> ipmo .\SlinkyCat.ps1
PS C:\Users\g.white\Desktop\Steelcon\SlinkyCat> Invoke-SlinkyCat
```

Method 2 which is a sneaky method, simply open the complete script in notepad, highlight it all, copy and paste it into a PowerShell session, it should load bypassing the restriction.

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\g.white> # SlinkyCat v1.0
PS C:\Users\g.white> # Lares Labs - https://labs.lares.com/
PS C:\Users\g.white> # Neil Lines & Andy Gill, 2023
PS C:\Users\g.white>
PS C:\Users\g.white> <#
>> .SYNOPSI
>>
>>
>> .DESCRIPTION
>>
ScrapingKit. To help security and IT teams reduce their AD exposures and uncover quick wir
>>
>> .PARAMETER domain
>>
>>
>> .EXAMPLE
>>
```

2. The Menu allows you to select which method you want to use to enumerate the Domain.

```
Windows PowerShell × + ~
```

All sub options from within the ADSI enumeration selection.

X Windows Powershell X + ×
=== Menu ===
1. ADSI Enumeration
2. Dot NET System.DirectoryServices.AccountManagement Namespace Enumeration
3. List Available Individual Functions
Q. Quit
Enter your choice: : 1
ADSI Optinos Menu Please select an option:
1. Enumerate all domain hosts
2. Enumerate all domain controllers
3. Enumerate all domain users
4. List all users in the domain admins group
5. List all accounts with an SPN
6. List all domain groups
7. List all password set to never expire
8. List all users which do not require a password
9. List all users with password must change at next logon
10. List all computers that are not Domain Controllers and are Windows 7
11. List all computers that are not Domain Controllers and are Windows 10
12. List all computers that are not Domain Controllers and are Windows 11
13. List all servers
14. List all Server 2008
15. List all Server 2012
16. List all Server 2016
17. List all Server 2019
18. List all Server 2022
19. List domain groups which are a member of the local admin group
20. List all trusts established with a domain
21. List all Exchange servers
22. List all accounts that have never logged in
23. List all domain user accounts which have a completed AD description field
24. List all accounts that reference 'pass' in their AD description field
25. List all users who have not changed their password in over I year
26. List all users' last password change date and time
27. List all systems with WinKM Open (Not OPSEC SAFE!)
28. List all systems with RDP Open (NOT OPSEC SAFE!)
29. Find all machines where the current user has local admin acess (Not OPSEC Safe, will list all computers then allempt to mount (s)
A. Run all functions and export to an output folder full of txt files

3. Selecting an option such as 22' List all accounts that have never logged in' reveals the response to the ADSI request.

```
Enter your choice: 22
Option: ADSI List all accounts that have never logged in
Guest
krbtgt
NULL
david
robert
chris
mike
dave
richard
thomas
steve
mark
daniel
george
paul
charlie
```

4. Option 29 'Find all machines where the current user has local admin access'.

For more information on how SlinkyCat works check out the blog post <u>https://labs.lares.com/introducing-slinkycat/</u>

Thank You For Reading; go forth and build, break, defend, and fix!