



Announcements

- CTF teams have been announced
- FDM "She Lives Tech" bootcamp
- Hoodies coming... eventually



Exciting news at the end of the session...



But first...



Bring all yer
mates!

Bring your
brothers and
sisters!

Bring your
housemates!



Bring your
aunts and
uncles!

Bring your
second cousin
twice removed!

Bring your
partners!



 @hackers.dmu

 @dmuhackers



Windows Infrastructure + Corporate Security



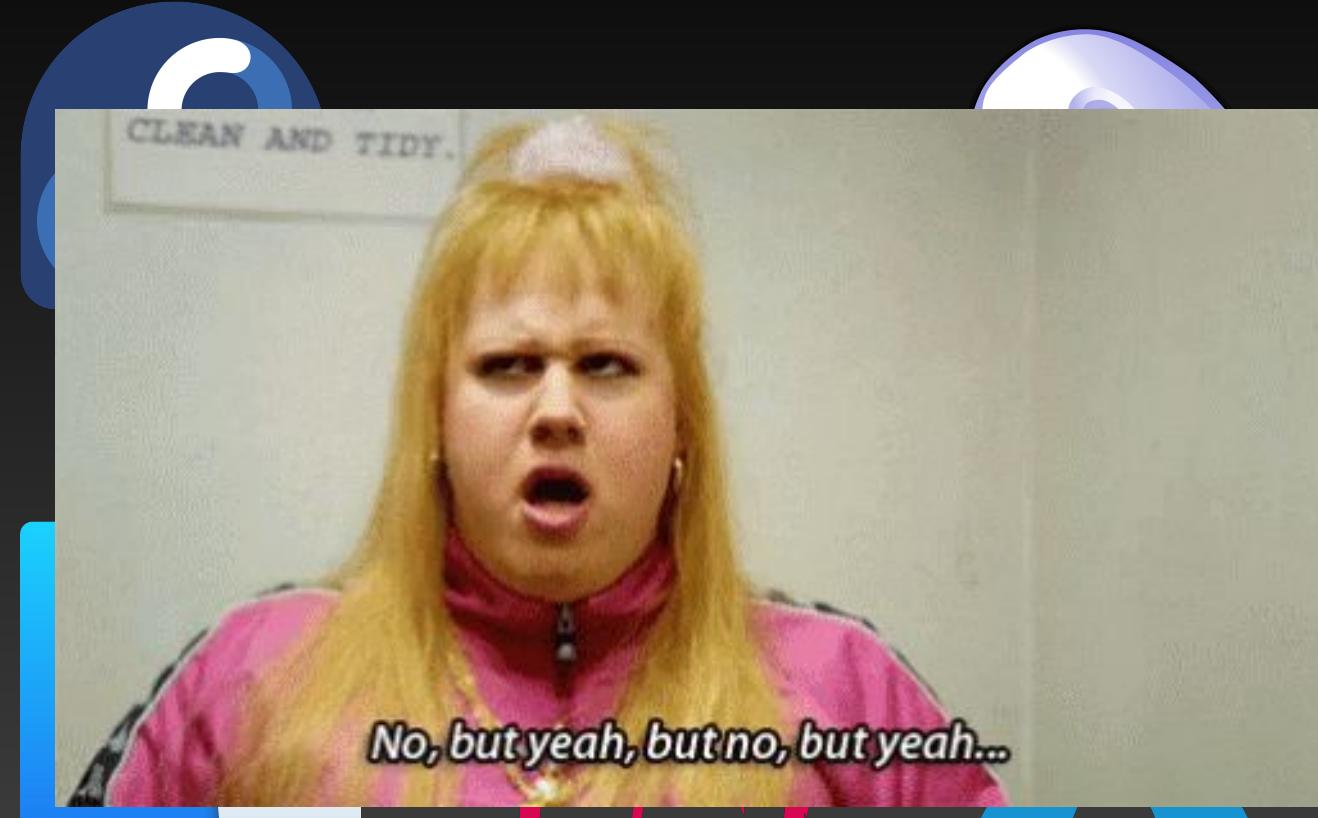
Don't do illegal shit



What OSes will I use as an IT professional?



What OSes will I use as an IT professional?



Mac OS





Mac OS

~16%

~73% Market share



3.83%





Mac OS

~16%



3.83%





Why Windows?



Dealer: J21 DEALER BUSINESS SYSTEM DS300041
 Store: 02 Release ID: 2.3.004

(Enter S to select function; CF12 to Return; CF24 to SIGNOFF with joblog)		Function Name: <input type="text"/>	
FUNCTION	DESCRIPTION	FUNCTION	DESCRIPTION
_ OPMENU	Order Processing	_ CMENU	Customer Information
_ IPMENU	Parts Invntry Processing	_ MRMENU	Merchandising
_ WHMENU	Warehouse Operations	_ GQMENU	Global Product Quoter
_ WOMENU	Service Work Order	_ MOMENU	Mobile Office
_ SJMENU	Standard Jobs	_ FNMENU	Finance
_ OCMENU	Operator's DBS Menu	_ NRMENU	Notes Receivable
_ GAMENU	General Applications	_ EPMENU	Extended Pricing Params
_ EMMENU	Equipment Management	_ CPMENU	Customer Purchases
_ WPMENU	Warranty	_ ARMENU	Alternate Applications
_ PMENU	Planned Maintenance	_ CTMENU	Contract Tracking
_ RNMENU	Rental Menu	_ INMENU	Invoicing
_ FPMENU	CAT Financial Products	_ EDMENU	Project Menu
		_ ADMENU	Administrator Menu

--- USER FUNCTIONS ---

_ UPMENU	Parts (USR)	_ UMMENU	Merchandising (USR)
_ USMENU	Service (USR)	_ UJMENU	Project Mngt (USR)

CF7: Change Break Mode More...

UDS1104: No function specified; Please enter function



Honourable mentions



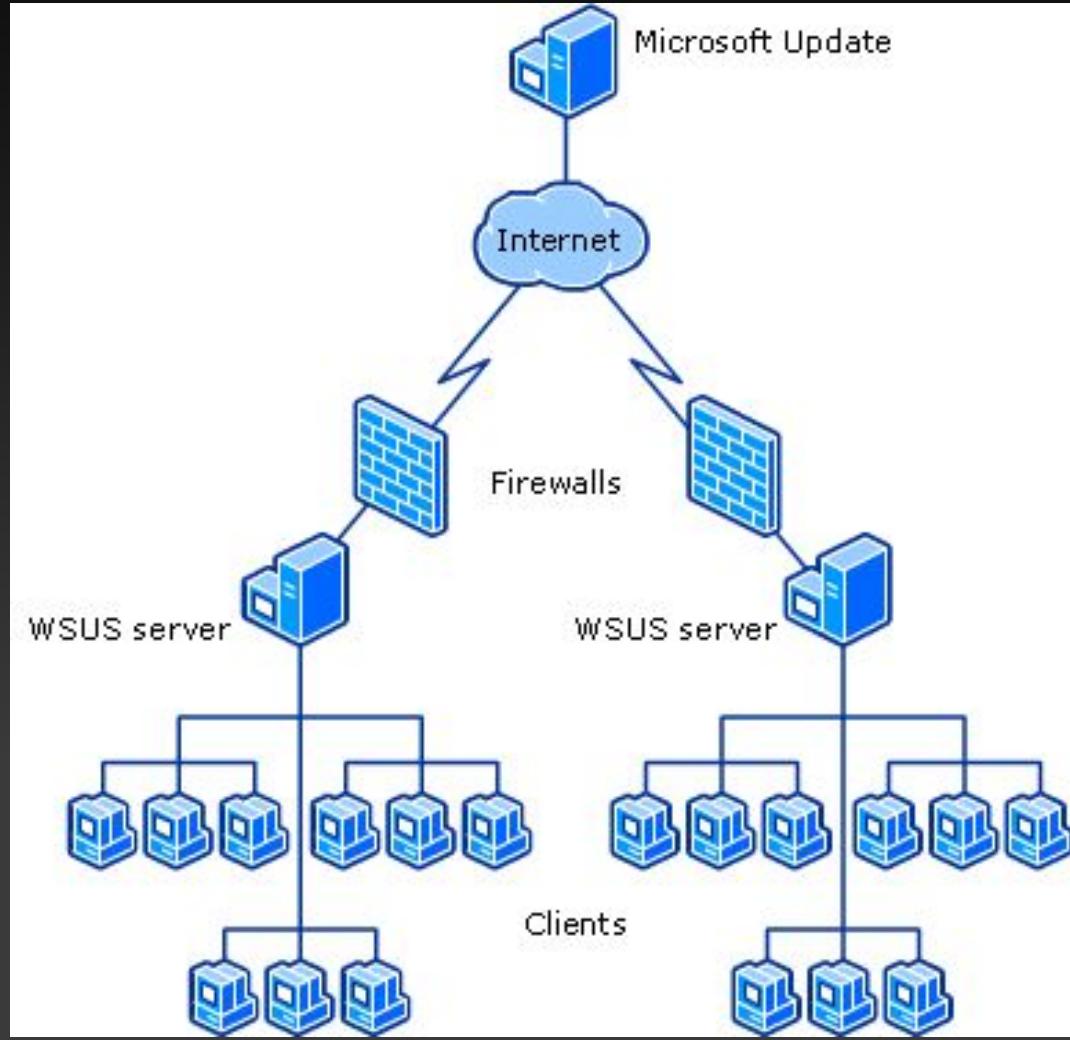
SharePoint vs OneDrive



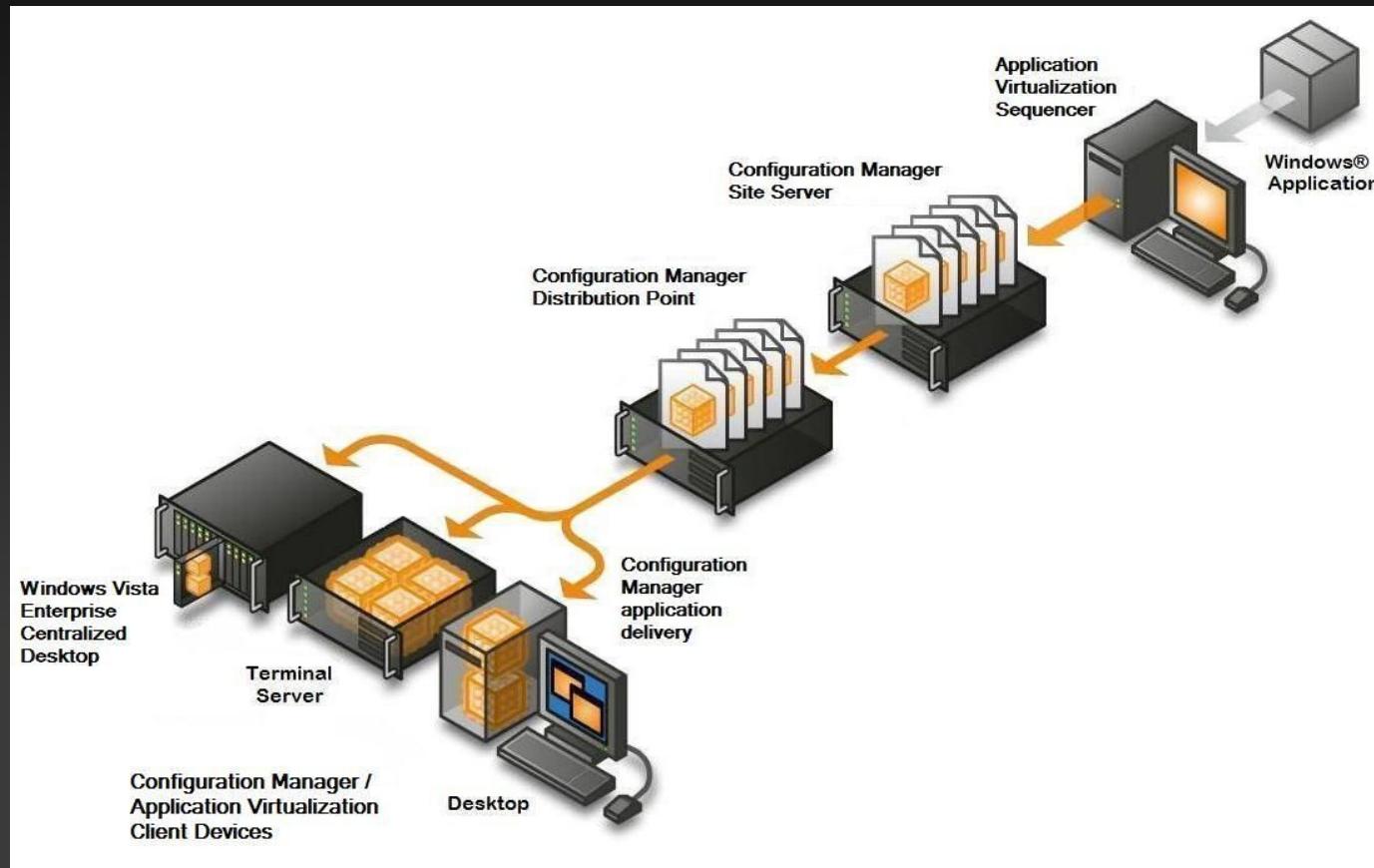
SharePoint vs OneDrive



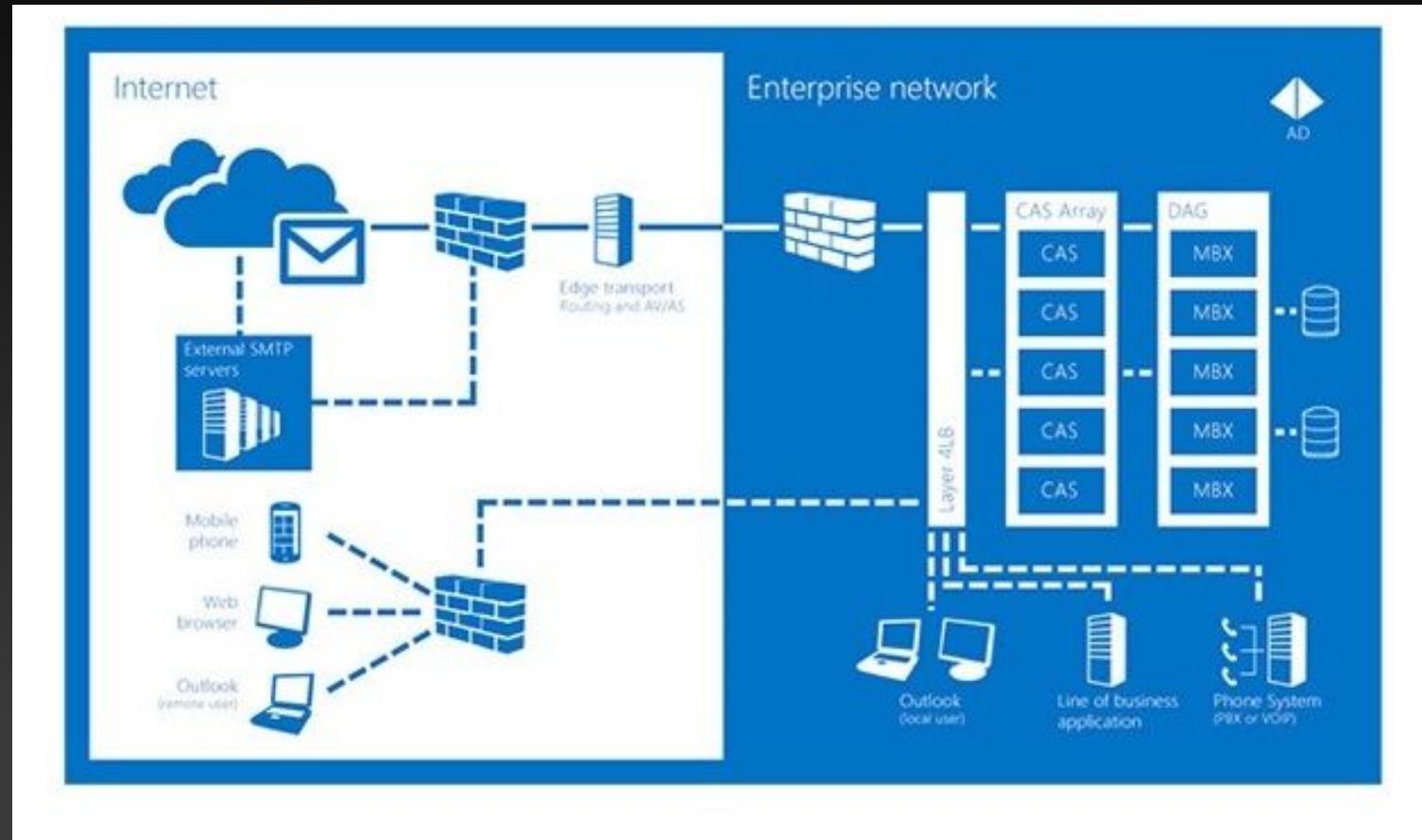
WSUS (Windows Server Update Services)



SCCM (Secure Center Configuration Manager) Aka MECM (Microsoft Endpoint Configuration Manager)



Microsoft Exchange



Heavily integrates with our good friend...



Active Directory (the proper cool stuff)

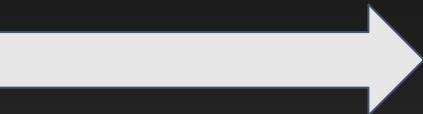
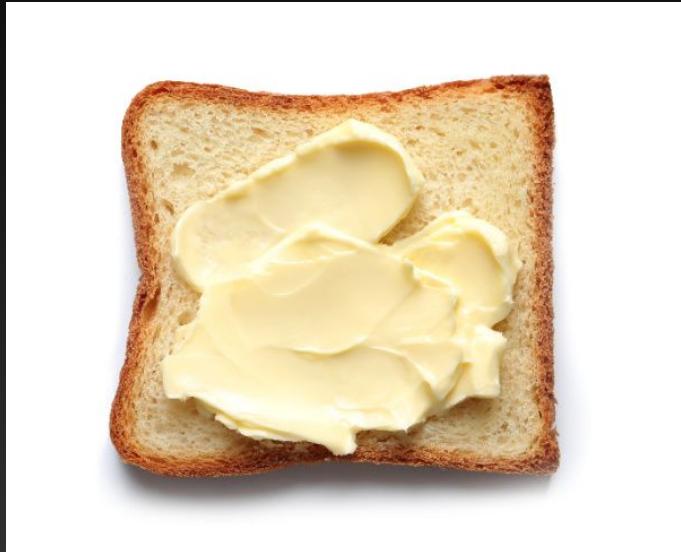


Active Directory

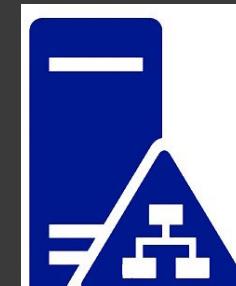
- Microsoft's proprietary directory services
- Connects everything in a corporate network



Active Directory



Domain Controller



But why?



Domain Controllers

Authentication +
Authorisation

Single Sign On

Manage resource
access

Redundancy

Read-only

Global Catalog

Also...

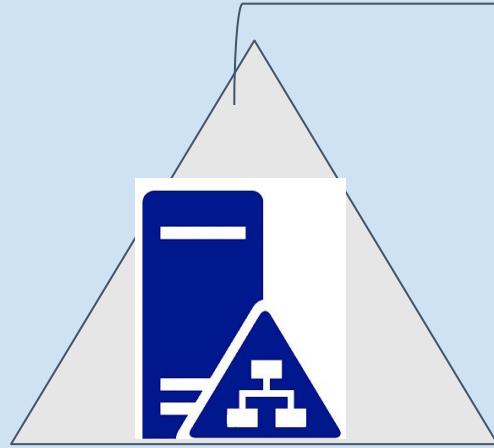


All objects, only some attributes

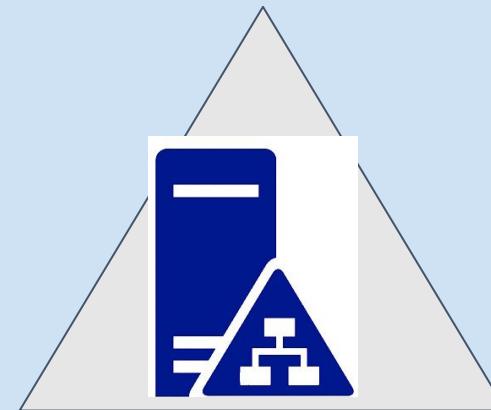


Forest

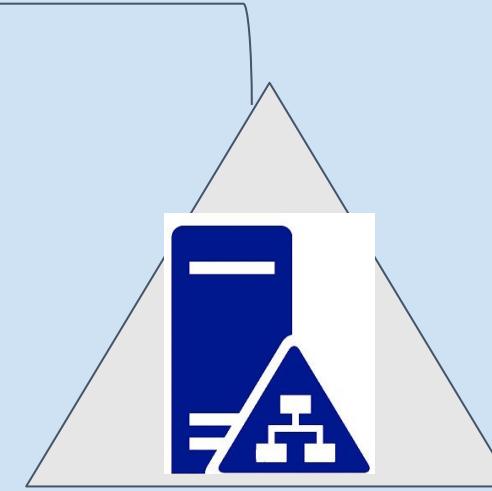
DMU



Domain 1:
DMU UK



Domain 2:
DMU Kazakhstan

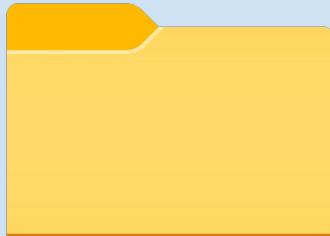


Domain 3:
DMU Dubai

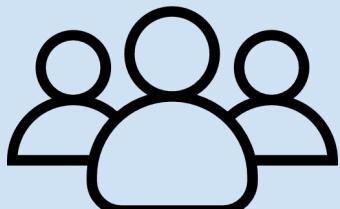


Container Objects

Organizational Units
(OUs)



Groups



Leaf Objects



Security Groups



Security Groups

HR



Managers



Leicester



Legal



GDPR Group



Dubai



"Group Policy"



Group Policy Objects



IT
Administrator

Group Policies



Active Directory

Users



Computers

Container Objects

Organizational Units
(OUs)



Groups



Leaf Objects





PCs

- 'Join the domain'
- Can be placed in OUs
- Either add beforehand or move from default container

domain\Computers





Users

- Authentication/Authorisation
- Manage security groups
- User management facilities
- Roaming/Local Profiles

User profile

Profile path: \\dmuhackers-dc01\Profiles\tumerj\

Logon script:

Joey Turner Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile
		Telephones	Organization

User logon name: tumerj @corp.dmuhackers.com

User logon name (pre-Windows 2000): DMUHACKERS\tumerj

Log On To... Logon Hours...

Unlock account

Account options:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption

Account expires

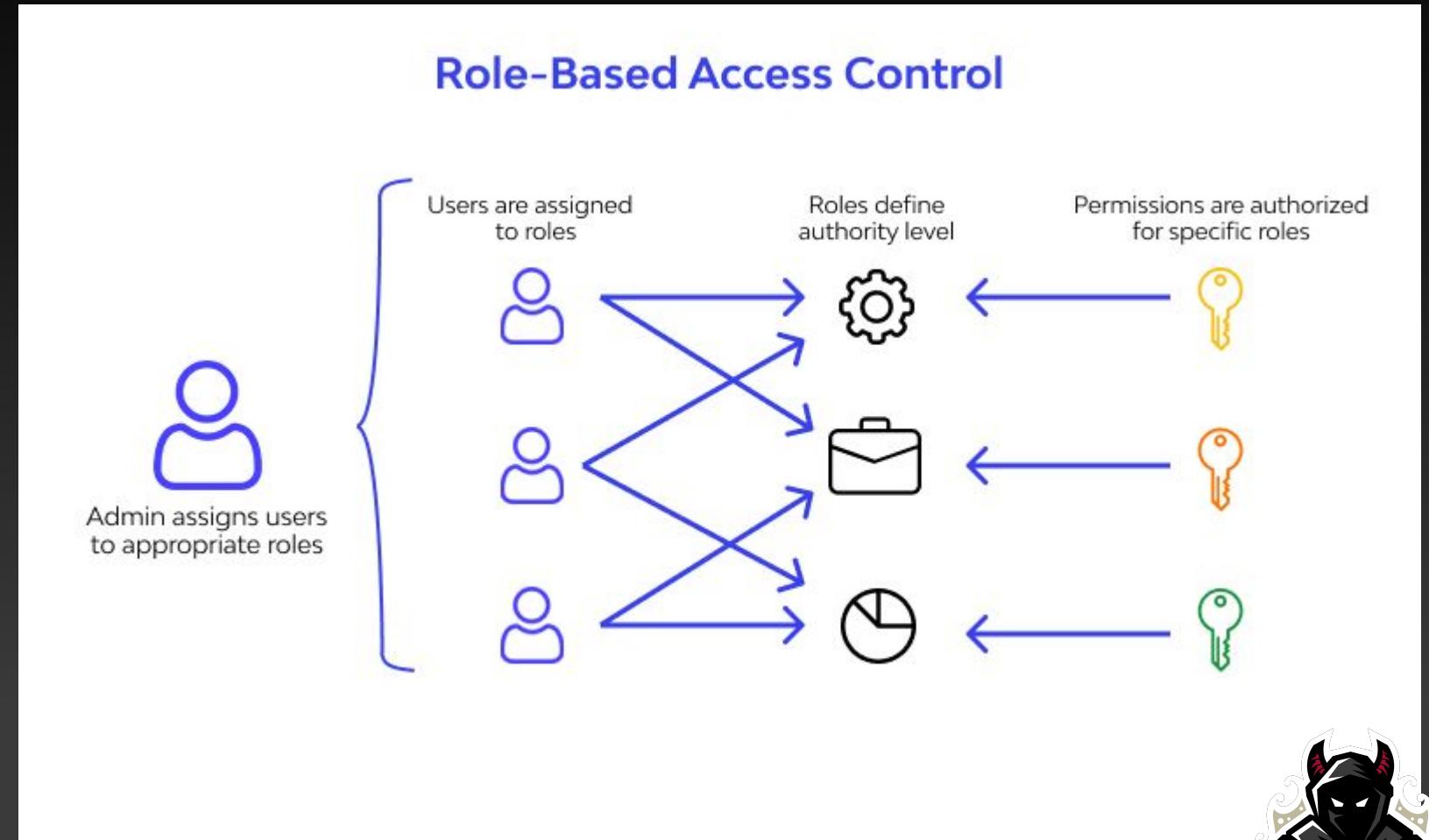
Never

End of: 02 March 2024

OK Cancel Apply

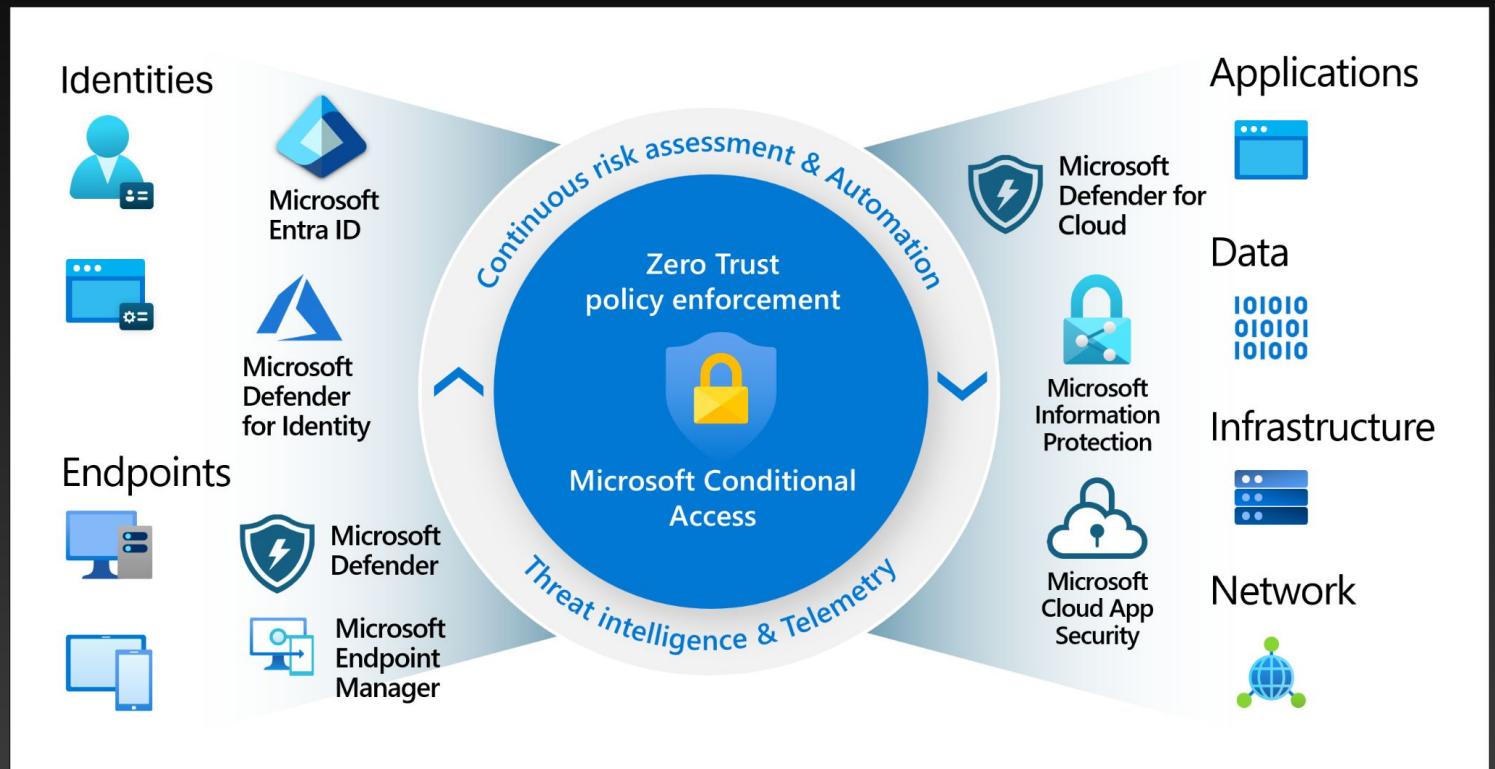


- A “best” secure practice (or one of)
- Follows the principle of least privilege
- Simplified auditing, reduction of likelihood of things spiralling out of control!



Conditional Access

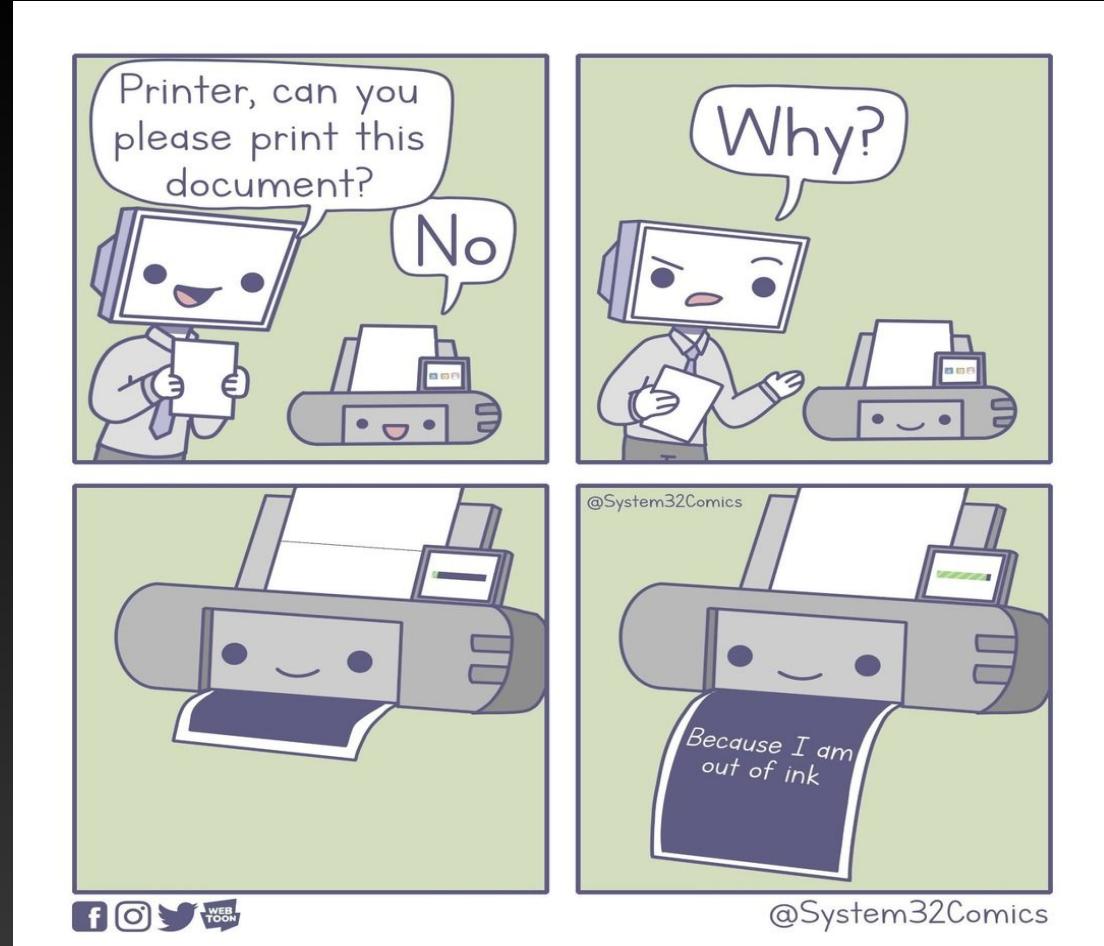
- An emerging security practice
- Utilises MFA (lots of factors!)
- Often described as “context aware”
- Complements Zero-Trust





Printers (when they're working)

- Accessibility across the network
- Can be mapped to security groups



Legal
Legal
Printer General
Printer



PowerShell

- Microsoft's scripting language
- Integrations with many MS products (through modules)
- Many uses within AD in particular:

Queries/reporting

Automate
repetitive tasks

Bulk modification/
deletion

It can also integrate with 3rd party services

```
Windows PowerShell
Property      long workingSet64 {get;}
PropertySet   PSConfiguration
PropertySet   PSResources
PropertySet   PSResources {Name, Id, PriorityClass}
Company      ScriptProperty System.Object Company {get=$this.MainModule}
CPU          ScriptProperty System.Object CPU {get=$this.TotalProcessorTime}
Description   ScriptProperty System.Object Description {get=$this.MainModule}
FileVersion  ScriptProperty System.Object FileVersion {get=$this.MainModule}
Path         ScriptProperty System.Object Path {get=$this.MainModule}
Product      ScriptProperty System.Object Product {get=$this.MainModule}
ProductVersion ScriptProperty System.Object ProductVersion {get=$this.MainModule}

PS C:\Users\wikiHow>
PS C:\Users\wikiHow> .Get-Process | Where-Object { $_.Name -eq "notepad" }
.Get-Process : The term '.Get-Process' is not recognized as the name of a cmdlet,
operable program. Check the spelling of the name, or if a path was included, veri-
and try again.
At line:1 char:1
+ .Get-Process | Where-Object { $_.Name -eq "notepad" }
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (.Get-Process:String) [], CommandNo-
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\wikiHow> Get-Process | where-object { $_.name -eq "notepad" }
Handles  NPM(K)    PM(K)    WS(K)    CPU(s)   Id SI ProcessName
----  --  --  --  --  --  --
240       14     3084    14764    0.23  6208  1 notepad

PS C:\Users\wikiHow>
```



Security Considerations of Active Directory



AD Security

- Adversary has Domain Admin? You're fucked.
- Be weary of permissions creep



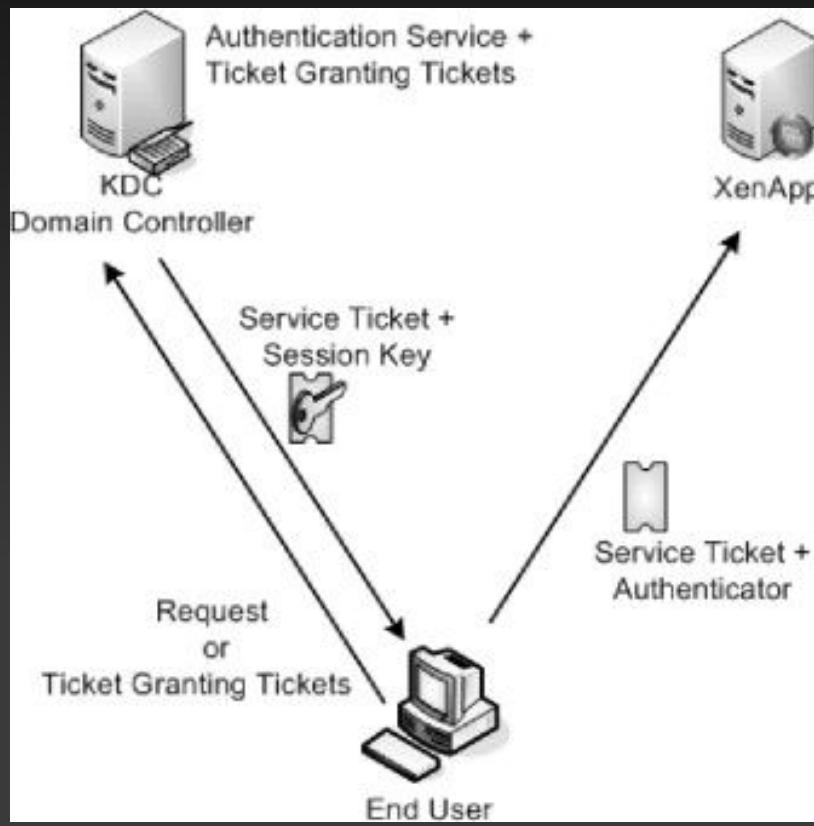
- Secure your backups - or everything else is pointless



Kerberoasting



- Exploits Kerberos (funny that)



Kerberoasting



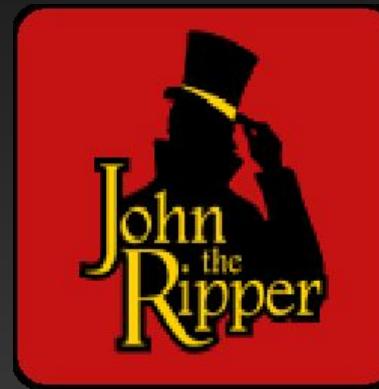
- Find service accounts
- (Legitimately) request a ticket
- Key Distribution Center sends it back, and it's encrypted using the NTLM hash of service account's password

Whatever gives access
to the ticket is the
password



Kerberoasting

- Crack using whatever you like



And then...

```
[root@kali] ~
└─# john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt ./winpasswords.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (User)
qwerty        (testuser)
sanmy         (Guest)
bigdog        (Administrator)
                (DefaultAccount)
5g 0:00:00:00 DONE (2022-11-11 11:26) 6.329g/s 18156Kp/s 18156Kc/s 18166KC/s      markinho..*7;Vamos!
Use the '--show --format=NT' options to display all of the cracked passwords reliably
Session completed.
```



Kerberoasting



- Why is it so dangerous?
 - Service accounts often highly privileged but seldom audited
 - Highly lucrative PrivEsc methodology
 - Can be done offline, so doesn't create much noise



Kerberoasting

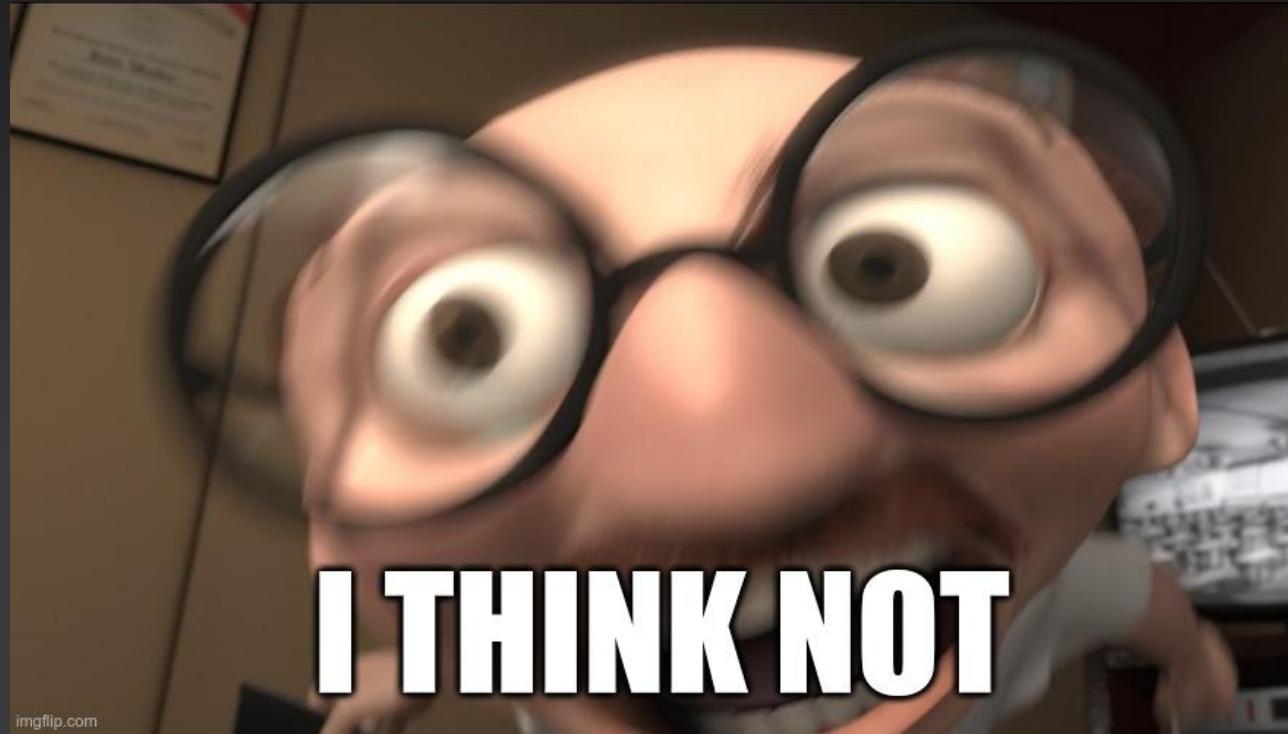


- How can it be mitigated?
 - Regular audits
 - Follow least privilege
 - Password rotation



Pass-The-Hash

- Similar-ish concept to Kerberoasting
- You need a password to access a service yeah?



Pass-The-Hash

- Obtain a user's NTLM hash
- Use the hash directly for authentication

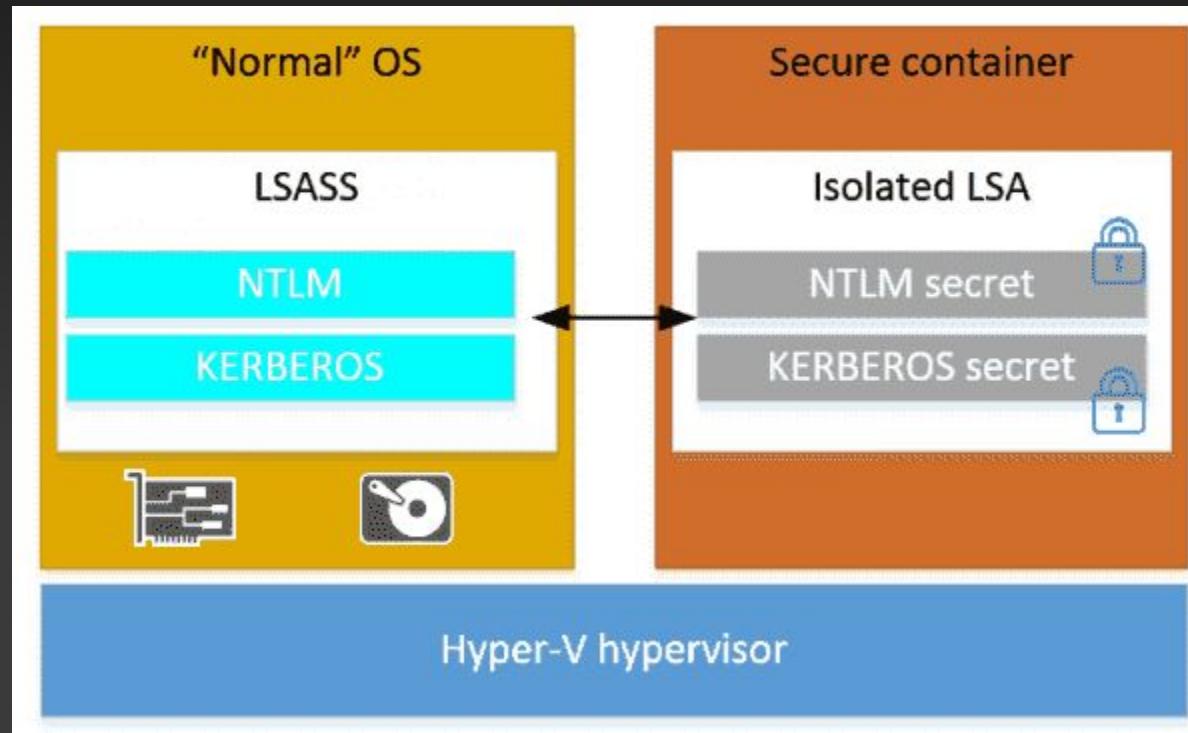


That's literally it!



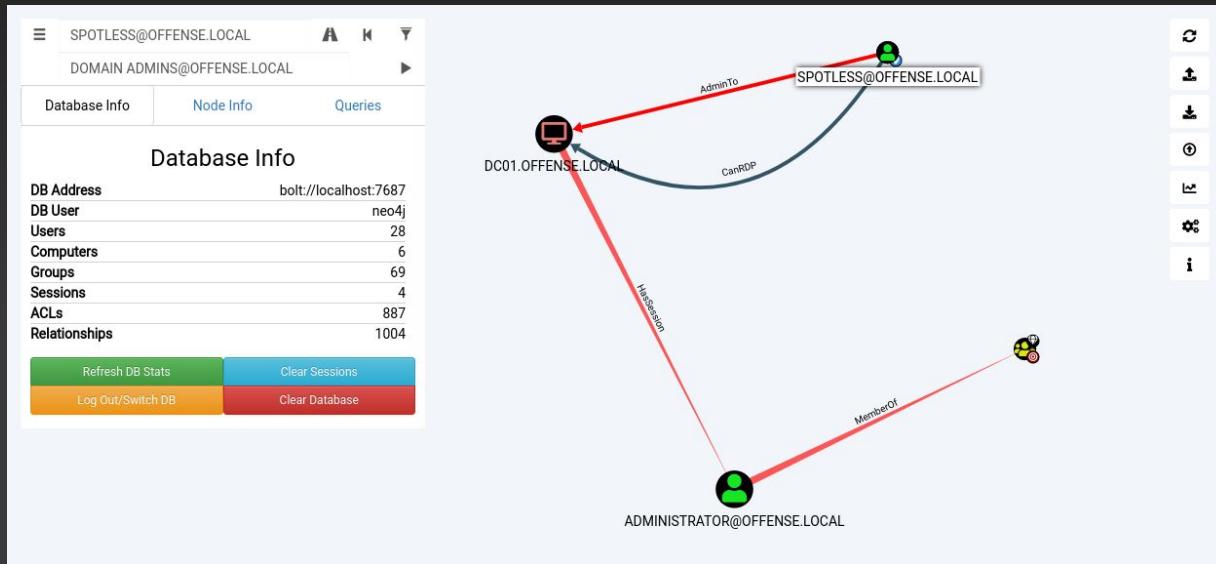
Pass-The-Hash

- Mitigation strategies
 - Credential Guard



Bloodhound

- A pentesting tool for AD environments (both cloud/on prem)
- Maps relationships between:
 - Users
 - PCs
 - Groups



A note on Azure AD (AAD)

- Becoming a lot more popular
- Used to be a lot of hybrid environments, seeing a lot of orgs go 100% cloud-based
- Interestingly enough, some people are going the other way - back to on-prem!



A note on AD)

 Microsoft 365 Status  @MSFT365Status · Follow

We're investigating an issue with users accessing or experiencing degraded functionality when using Exchange Online and [outlook.com](#) services. More details are available in your admin center under EX401976 and OL401977.

4:55 PM · Jul 18, 2022

42 Reply Copy link

[Read 4 replies](#)

 Microsoft 365 Status  @MSFT365Status

We're investigating an issue where some users in the EMEA region are unable to connect to some Microsoft 365 services. More details are available in the admin center under the SI MO411804.

 Microsoft 365 Status  @MSFT365Status · 9 Std.

Antwort an @MSFT365Status

Our investigation is focused on a potential issue where legitimate Microsoft traffic is being blocked across multiple regions. More details are available in your admin center under the SI MO411804.

 Microsoft 365 Status  @MSFT365Status · 4 Std.

We're working with our firewall partners to investigate snort rule 1-60381. We've received confirmation from some affected users that disabling the rule provides immediate relief. Additional information can be found in the admin center under MO411804.

 Microsoft 365 Status  @MSFT365Status

We're investigating an issue with accessing Outlook on the web. Further details can be found under EX571516 in the admin center.

8:27 PM · Jun 5, 2023 · 336.1K Views

286 Retweets 123 Quotes 647 Likes 36 Bookmarks

 Microsoft 365 Status  @MSFT365Status

We're investigating an issue where customers may be unable to connect to the **Exchange Online** service on their mobile devices. Please see **EX223053** in the admin center for details.

10:15 AM · Sep 29, 2020 · TweetDeck

86 Retweets 20 Quote Tweets 128 Likes

 Microsoft 365 Status  @MSFT365Status

We're investigating issues impacting multiple Microsoft 365 services. More info can be found in the admin center under MO502273.

2:31 AM · Jan 25, 2023 · 1.6M Views

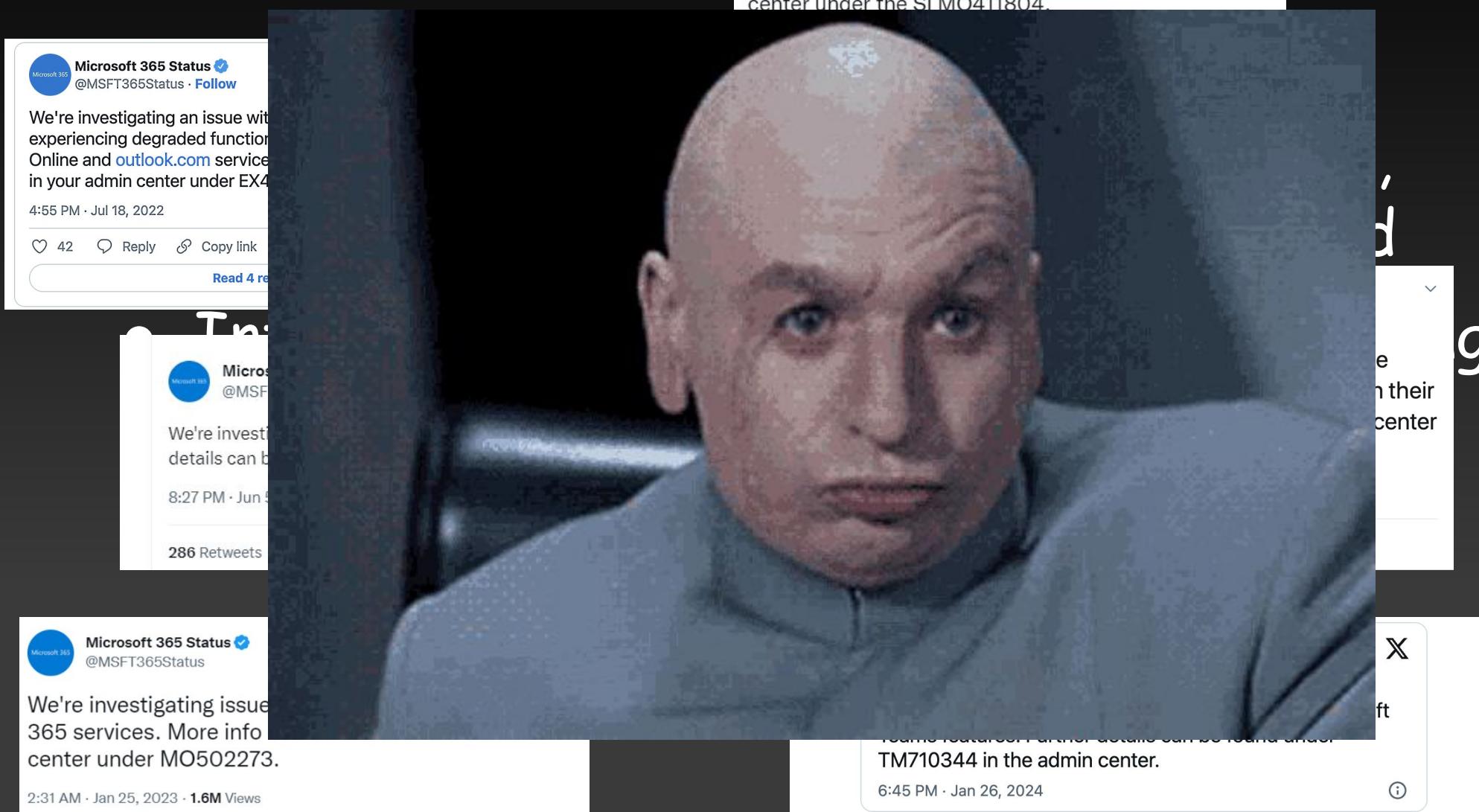
 Microsoft 365 Status  @MSFT365Status · Follow

We're investigating an issue impacting multiple Microsoft Teams features. Further details can be found under TM710344 in the admin center.

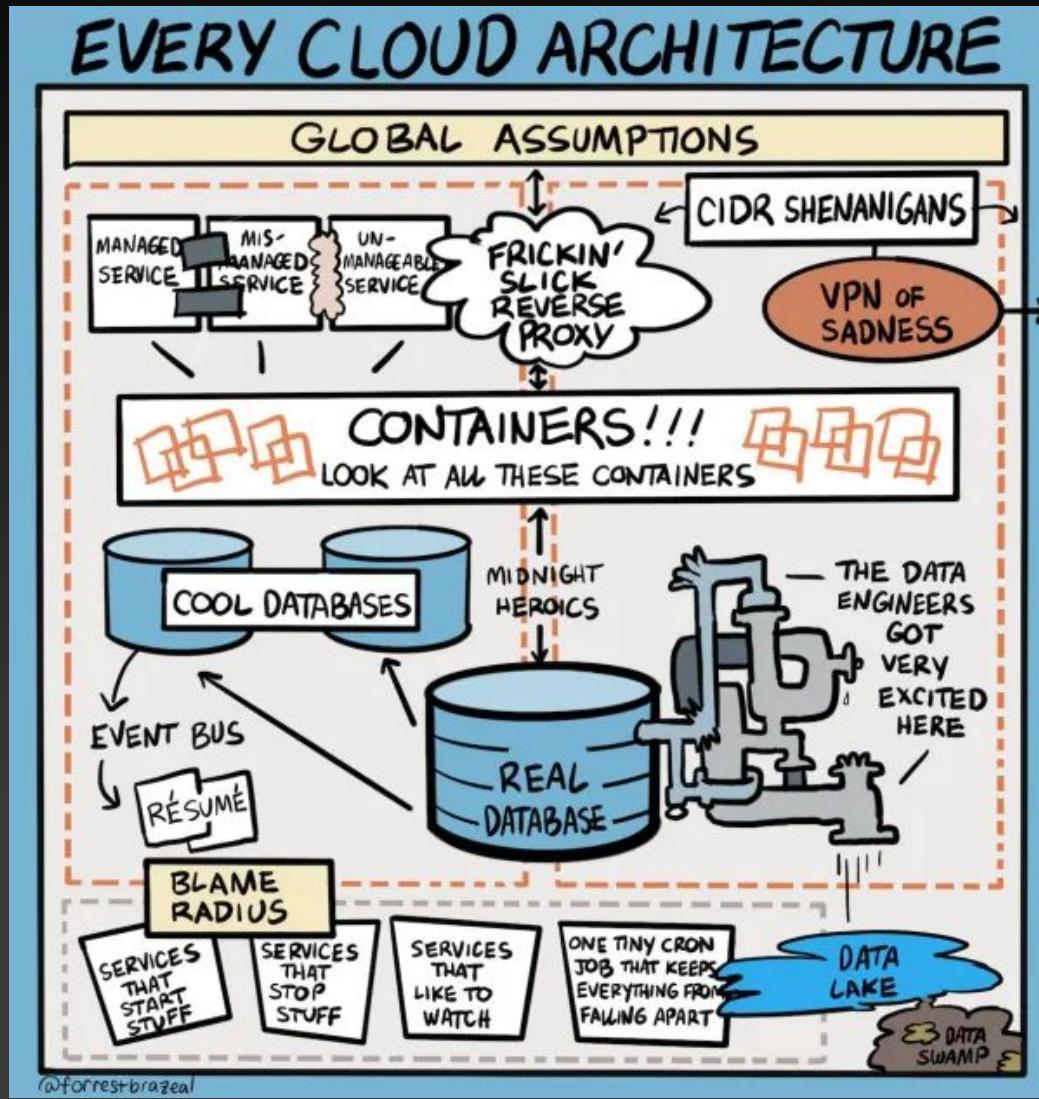
6:45 PM · Jan 26, 2024



A note on AD)



A note on Azure AD (AAD)



A note on Azure AD (AAD)



The folks are rioting about not being able to see gifs, lol
5d Like Reply



17

I always love hearing problems with MicroShaft.

To the internet "Teams is down, we can't communicate" to Microsoft its....tuesday LOL!



Good. I hate when people message me.

Not here damnit. I just got a teams message for a "critical" paper jam...

Sadly ours is still working.



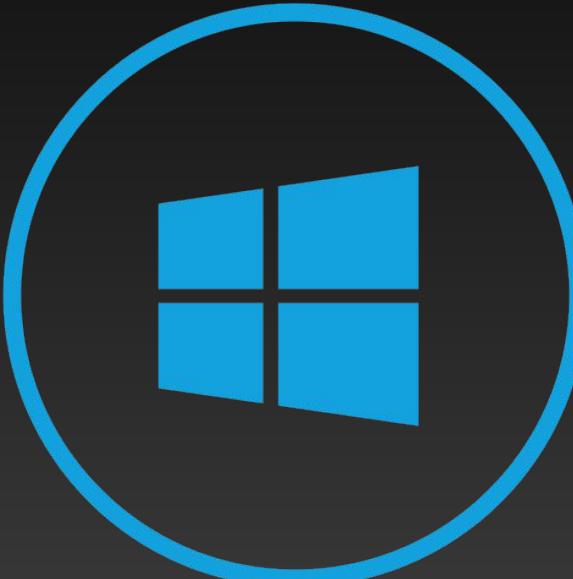
So glad i am not at work this week.



Demo time!



Today's Task...



Attacktive Directory

<https://tryhackme.com/room/attacktivedirectory>



Resources

- <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-with-bloodhound-on-kali-linux>
- <https://blog.netwrix.com/2017/04/20/tutorial-learn-the-basics-of-active-directory/>
- <https://tryhackme.com/room/attackingkerberos>



Before you go...



Guest Speaker Announcement

6pm on Discord
(Virtual
Session)



MightyGlens
Former Chairman, DMU Hackers

Working in a Security Operations Centre (SOC) + his
pathway to getting there



**COME TO THE
WARM PUB YOU WILL.**

**LOTS TO
DRINK YOU HAVE.**

imgflip.com

