
OMU
HACKERS

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!

DMU HACKERS PRESENTS

free!

KARAOKE NIGHT

MONDAY 12TH FEBRUARY

STARTING AT 8 PM

FIREBUG (UPSTAIRS)

Bring your aunts and uncles!

Bring your second cousin twice removed!

Bring your partners!


hackers.dmu
@dmuhackers
DMU
HACKERS
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

OMU HACKERS

~16%

~73% Market share

3.83%

Source: [Desktop Operating System Market Share Worldwide | Statcounter Global Stats]

Mac OS

~16%

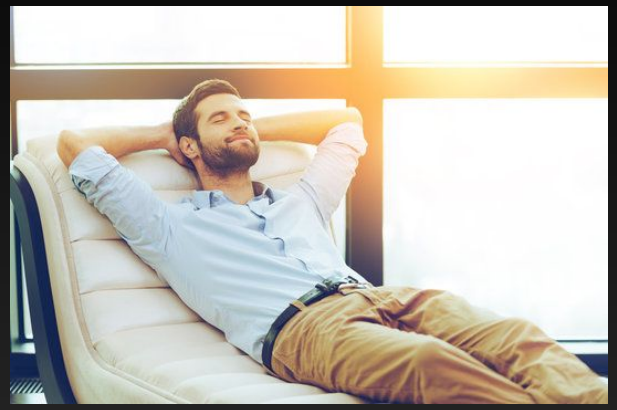
GNU/Linux

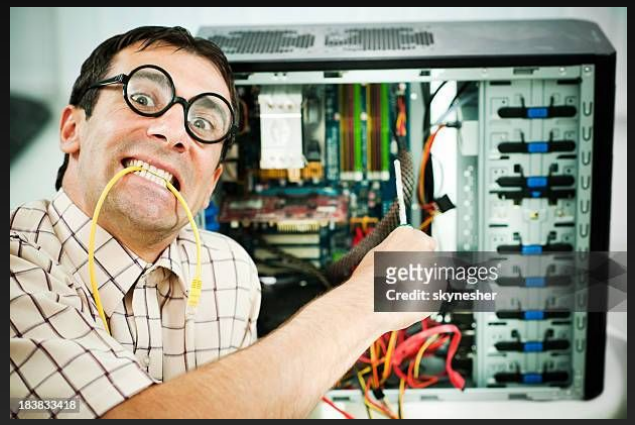
3.83%

Source: Desktop Operating System Market Share Worldwide | Statcounter Global Stats

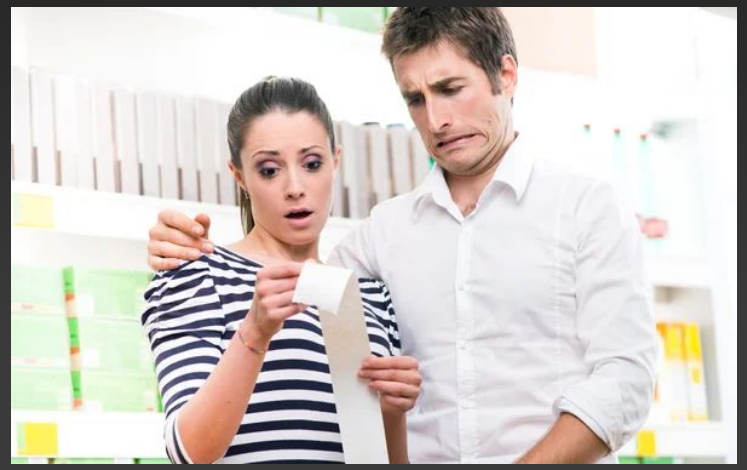

2025 WILL BE THE
YEAR OF THE LINUX DESKTOP
sure grandma let's
get you to bed
imgflip.com

Why Windows?





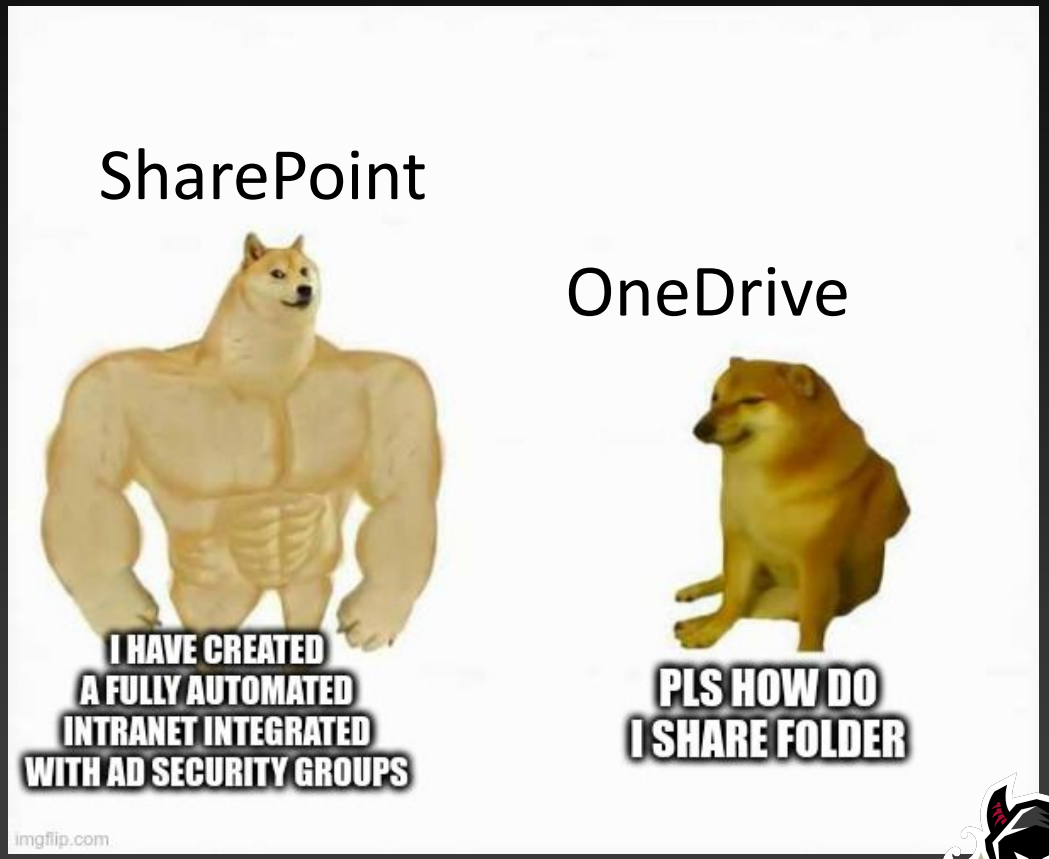

```
Dealer: J21              DEALER BUSINESS SYSTEM                DS300041
Store: 02                                          Release ID:  2.3  004
                                                 Function Name:
(Enter  S  to select function;   CF12 to Return; CF24 to SIGNOFF with joblog)
 FUNCTION      DESCRIPTION              FUNCTION      DESCRIPTION
_ OPMENU     Order Processing          _ CIMENU     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 Parms
_ EMMENU     Equipment Management      _ CPMENU     Customer Purchases
_ WPMENU     Warranty                  _ AAMENU     Alternate Applications
_ PMMENU     Planned Maintenance       _ CTMENU     Contract Tracking
_ RNMENU     Rental Menu               _ INMENU     Invoicing
_ FPMENU     CAT Financial Products    _ EDMENU     Project Menu
                                       _ ADMENU     Administrator Menu

  --- USER FUNCTIONS ---                --- USER FUNCTIONS ---
_ UPMENU     Parts (USR)               _ UMMENU     Merchandising (USR)
_ USMENU     Service (USR)             _ UJMENU     Project Mgmt (USR)
CF7: Change Break Mode                                          More...
UDS1104: No function specified: Please enter function
```



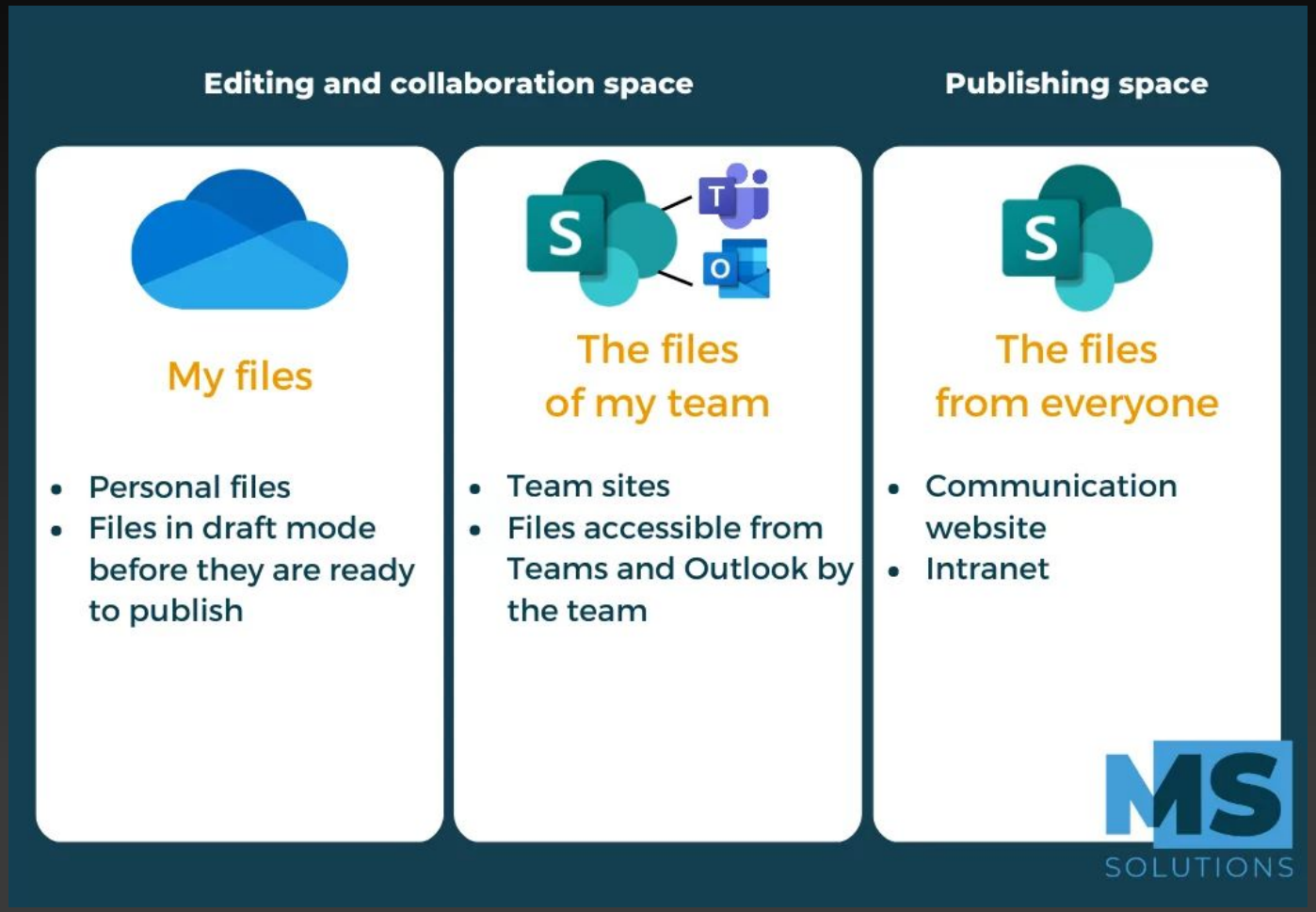
OMU HACKERS

Honourable mentions

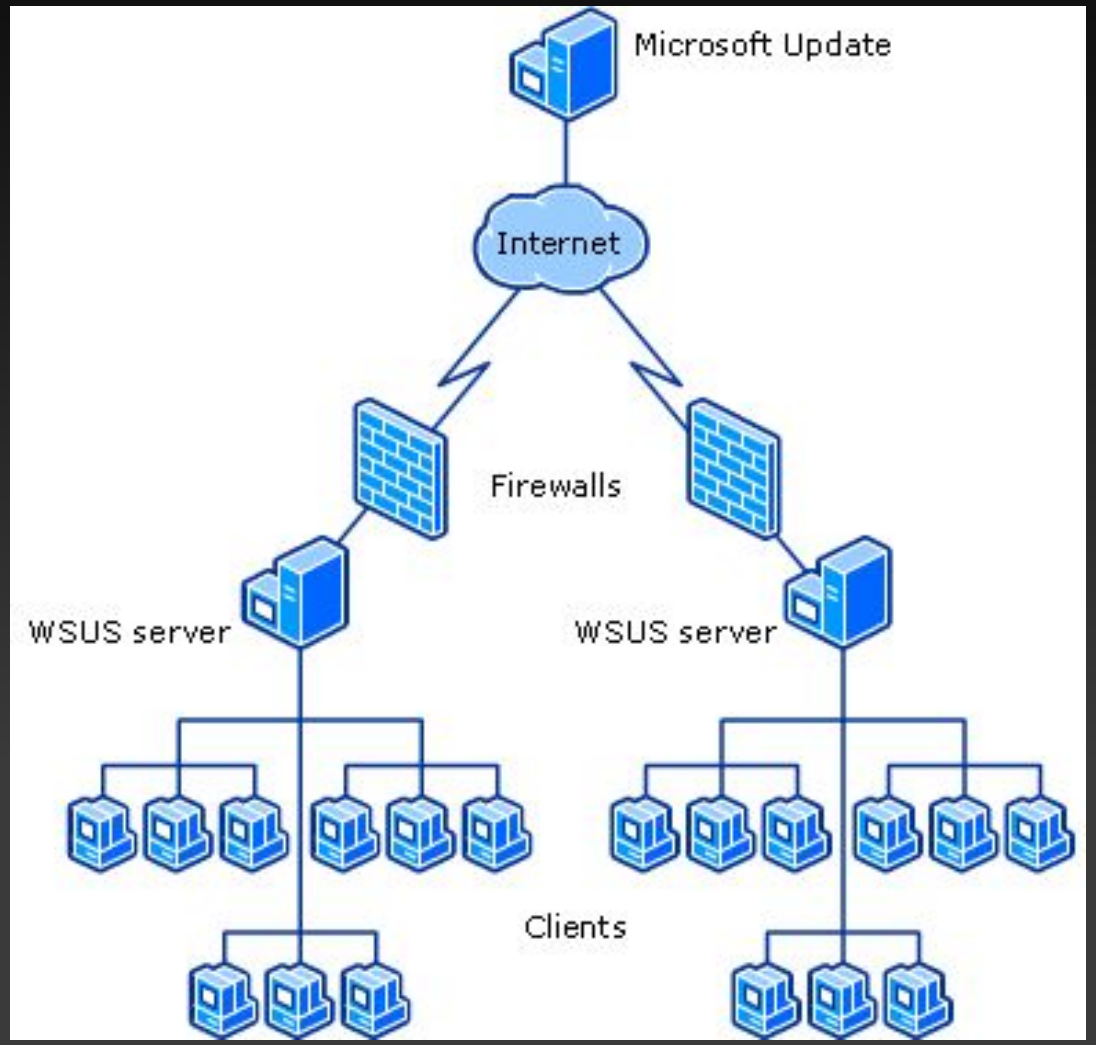
SharePoint vs OneDrive



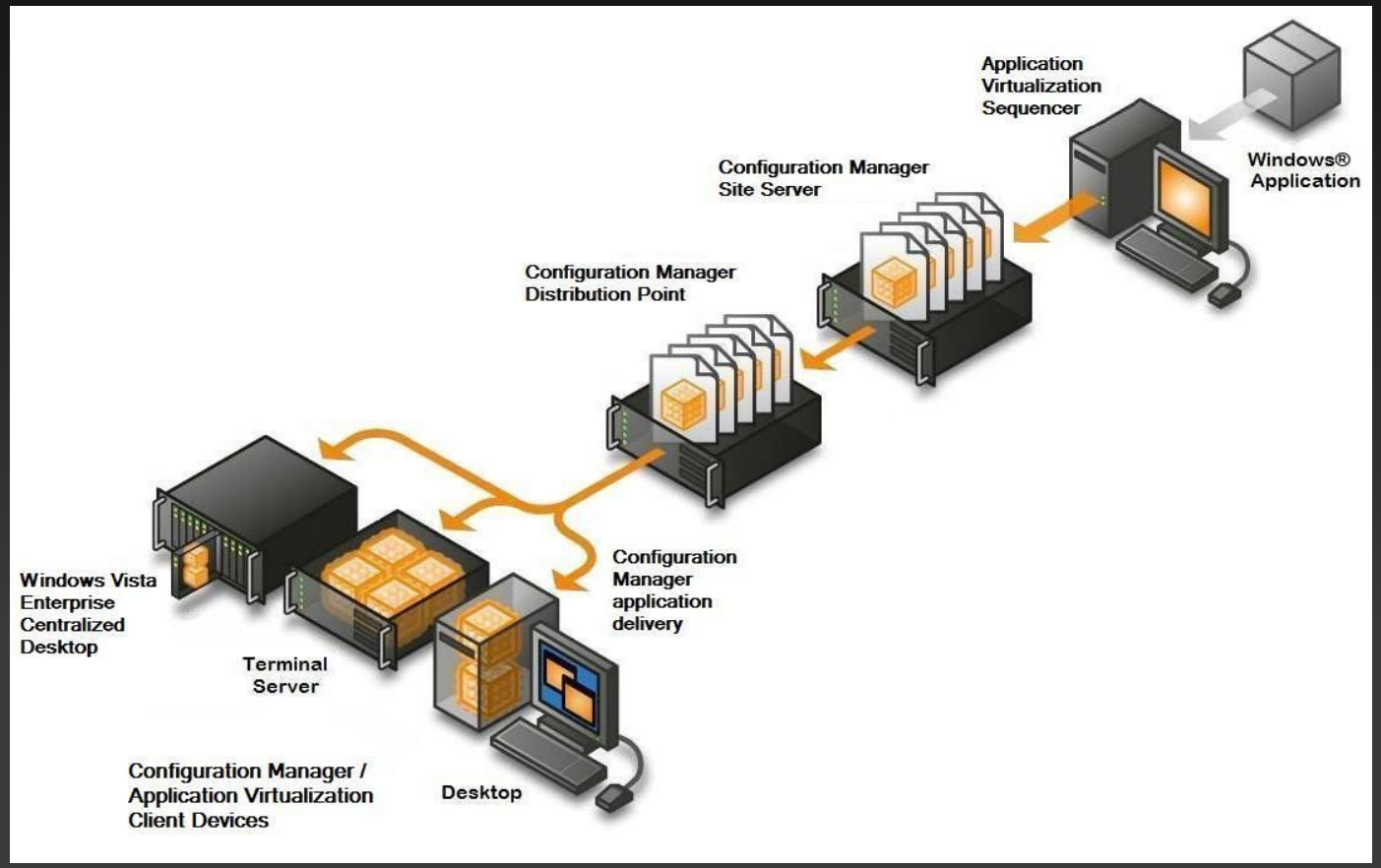
SharePoint vs OneDrive



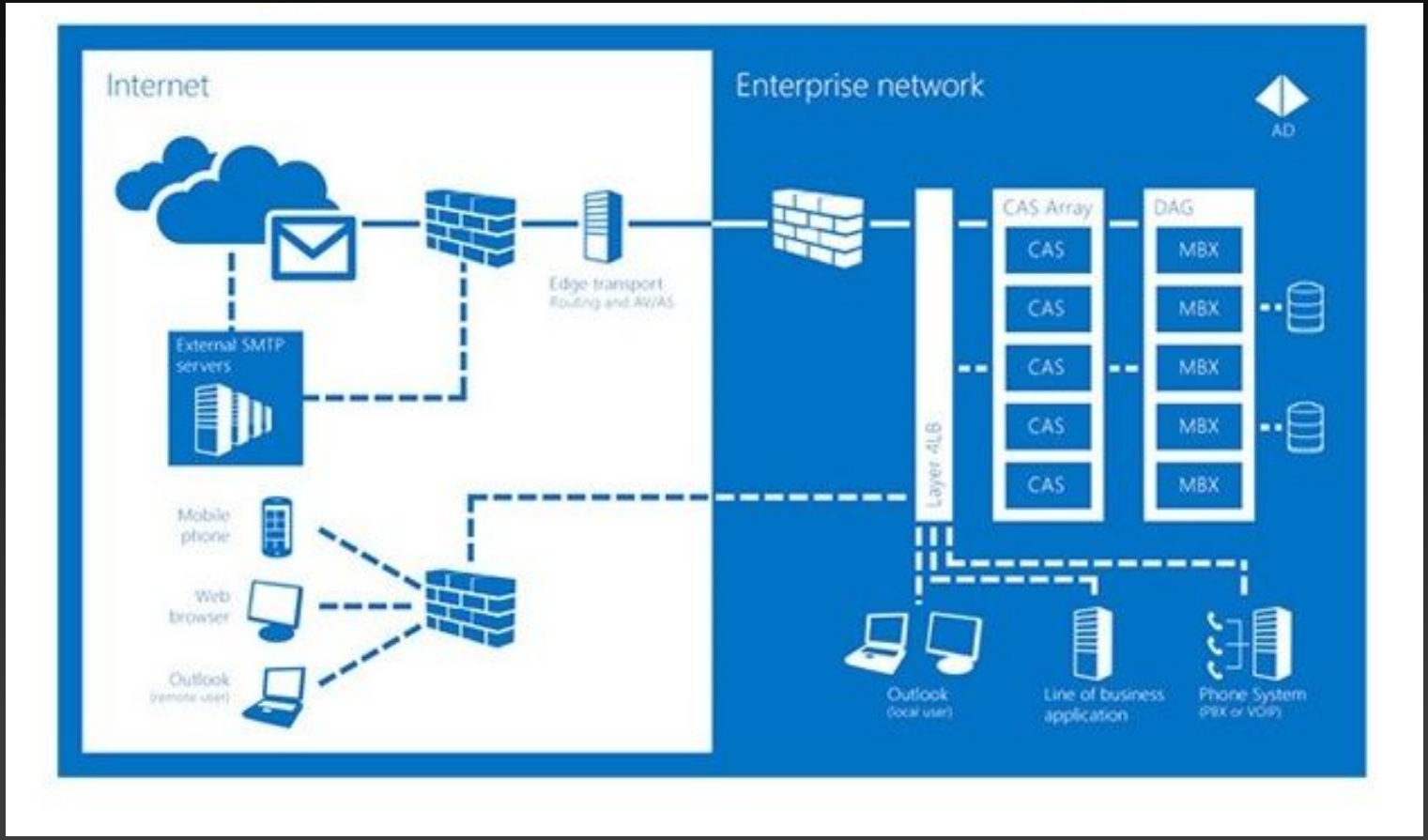
WSUS (Windows Server Update Services)



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



Microsoft Exchange



Heavily integrates with our good friend…

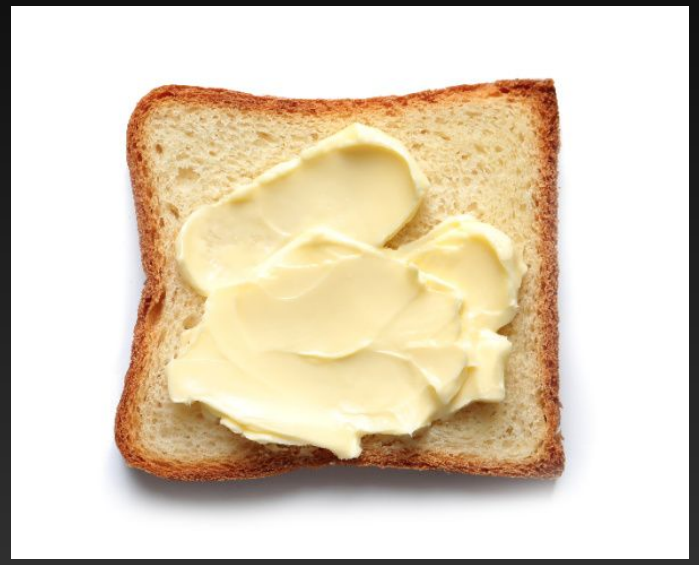
Active Directory
(the proper cool stuff)

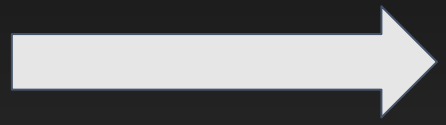
OMU HACKERS

Active Directory

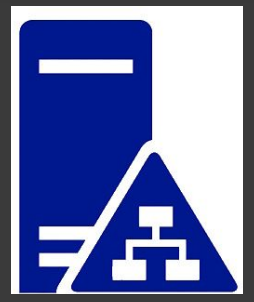
- Microsoft's proprietary directory services
- Connects everything in a corporate network

Active Directory





Domain Controller



But why?

Domain Controllers

Authentication + Authorisation

Single Sign On

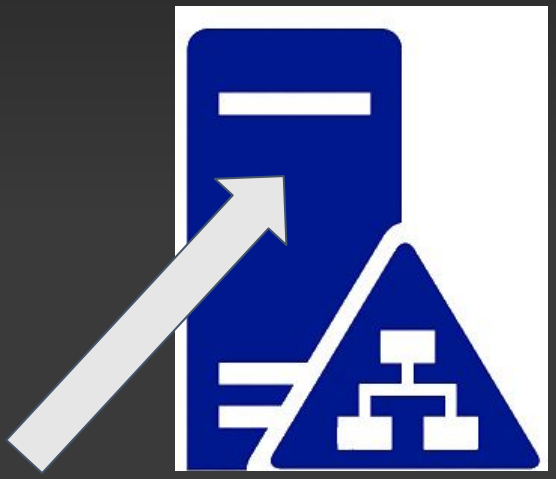
Manage resource access

Redundancy

Also…

Read-only

Global Catalog

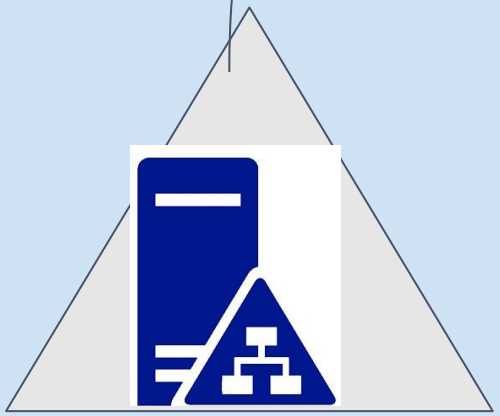


All objects, only some attributes

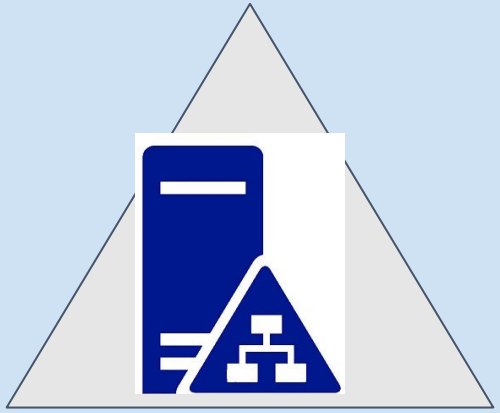
OMU HACKERS

Forest

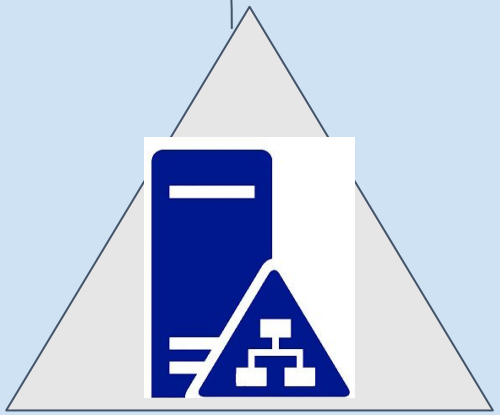
DMU



Domain 1:
DMU UK



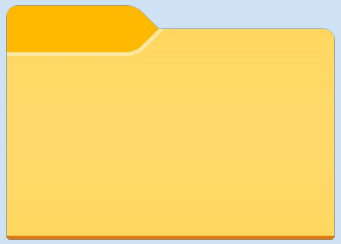
Domain 2:
DMU Kazakhstan



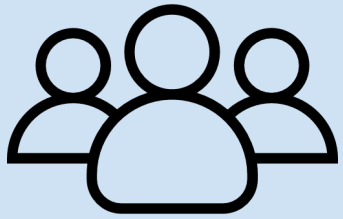
Domain 3:
DMU Dubai

Container Objects

Organizational Units (OUs)

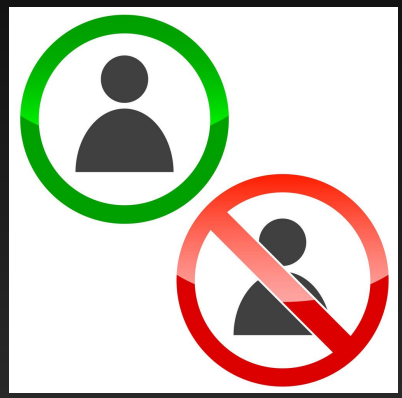


Groups



Leaf Objects

Security Groups



Security Groups

HR

1 3

Managers

1 4

Leicester

1 4

Legal

2 4 5

GDPR Group

1 2

Dubai

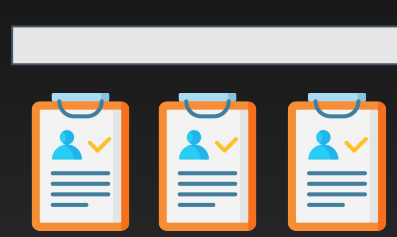
2 3 5

“Group Policy”

Group Policy Objects

IT Administrator

Group Policies



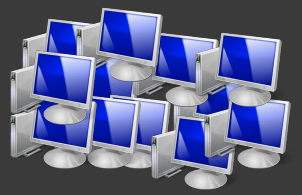
Active Directory

Container Objects

Organizational Units (OUs)

Groups

Users



Computers

Leaf Objects

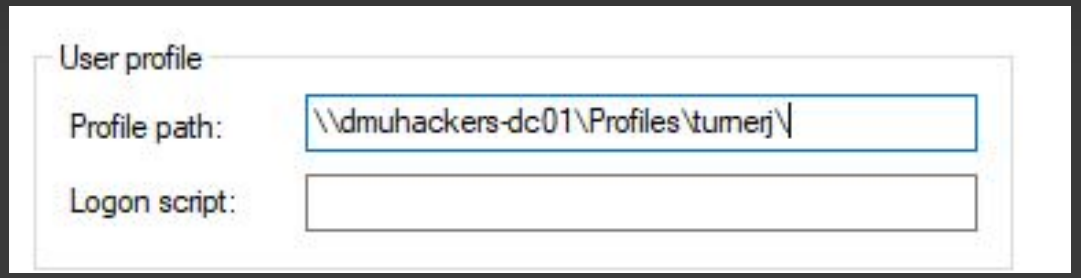
PCs

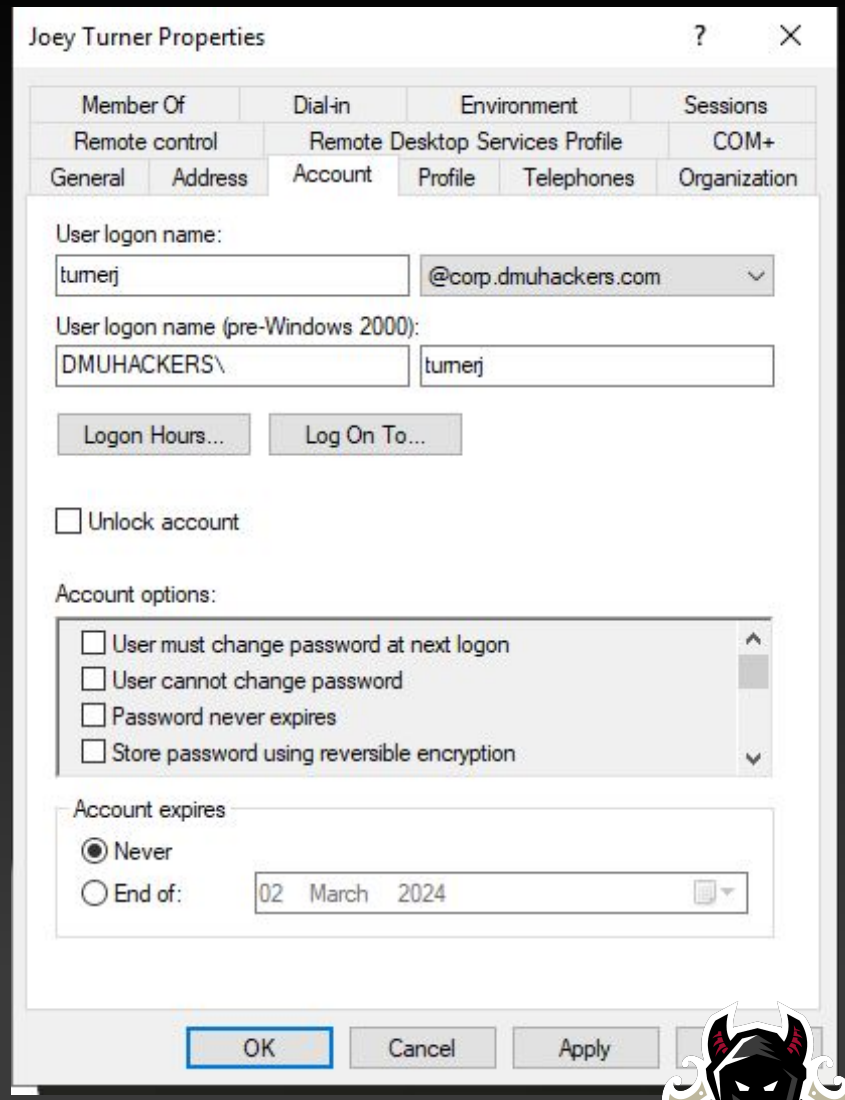
- 'Join the domain'
- Can be placed in OUs
- Either add beforehand or move from default container

domain\Computers

Users

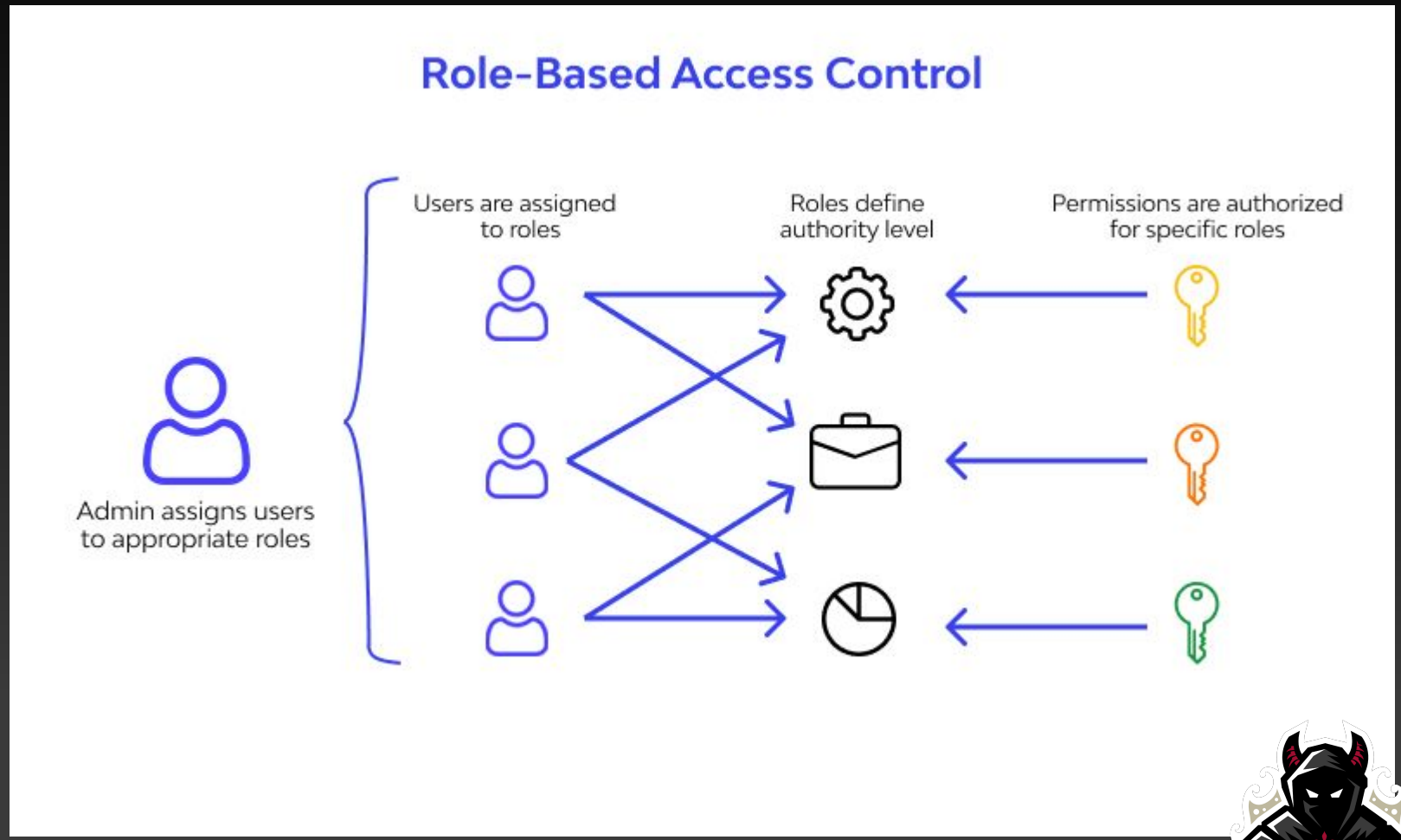
- Authentication/Authorisation
- Manage security groups
- User management facilities
- Roaming/Local Profiles





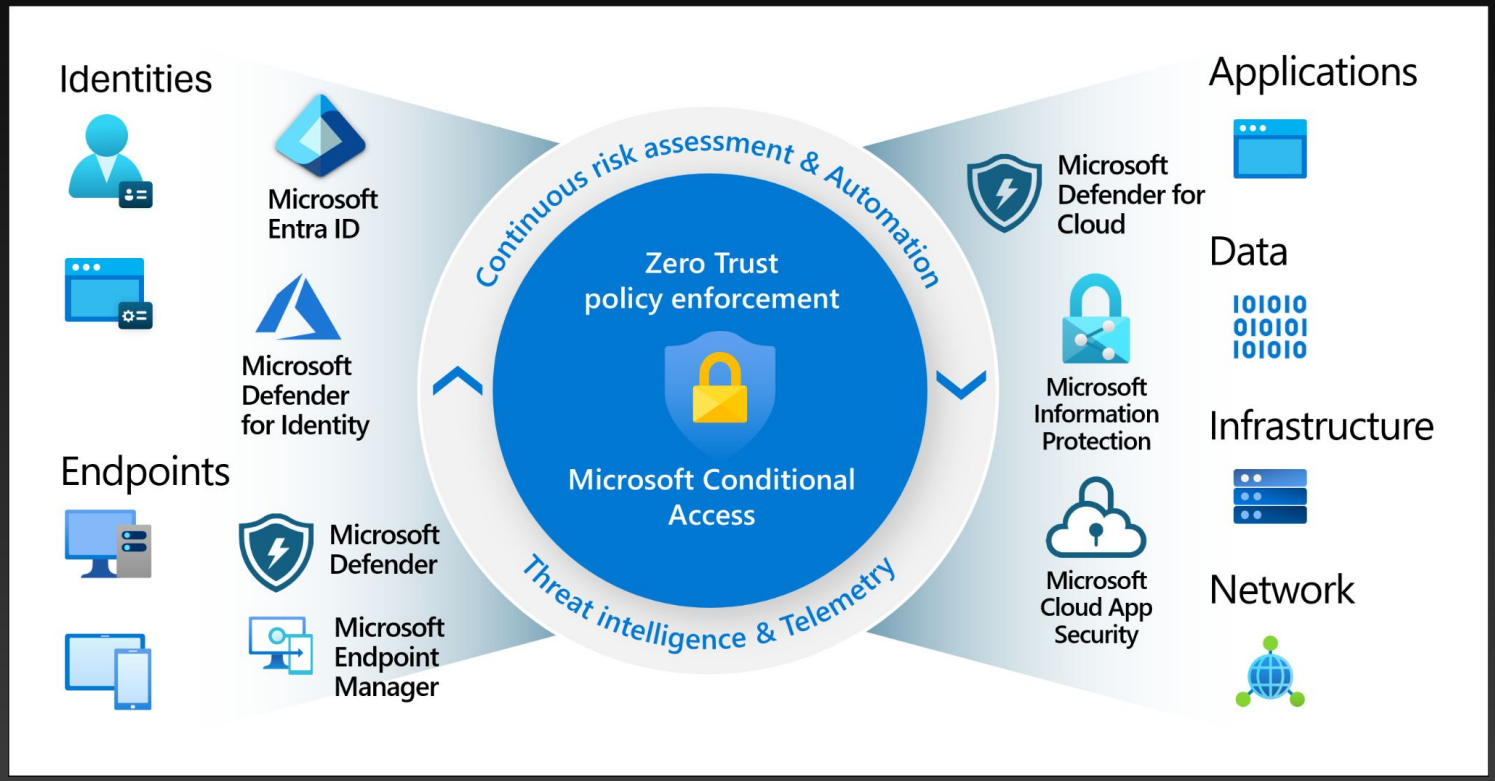
A note on RBAC

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



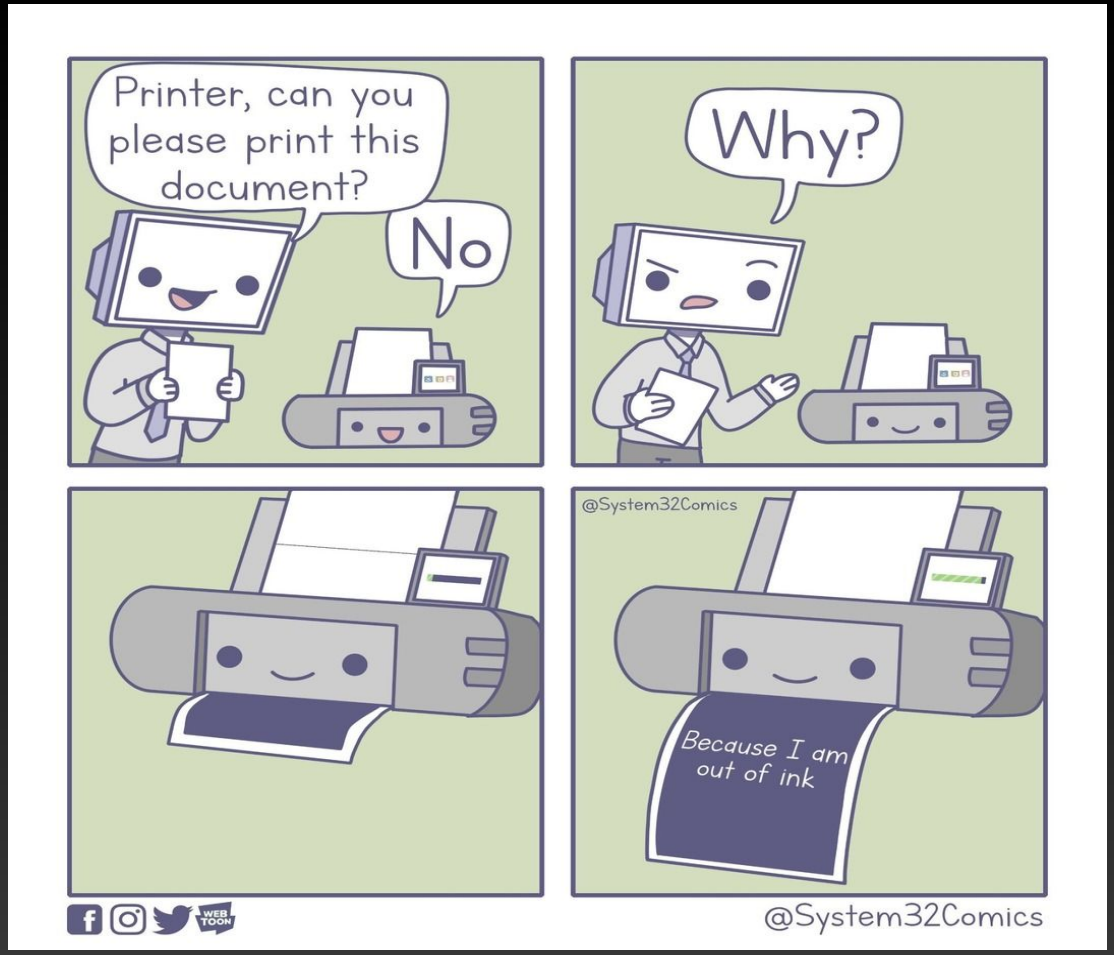
Conditional Access

- 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



HR


HR Printer

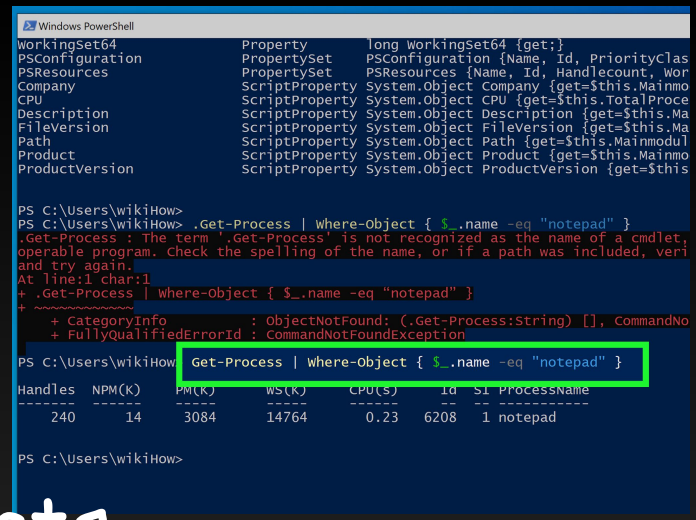
General Printer

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

Security Considerations of Active Directory

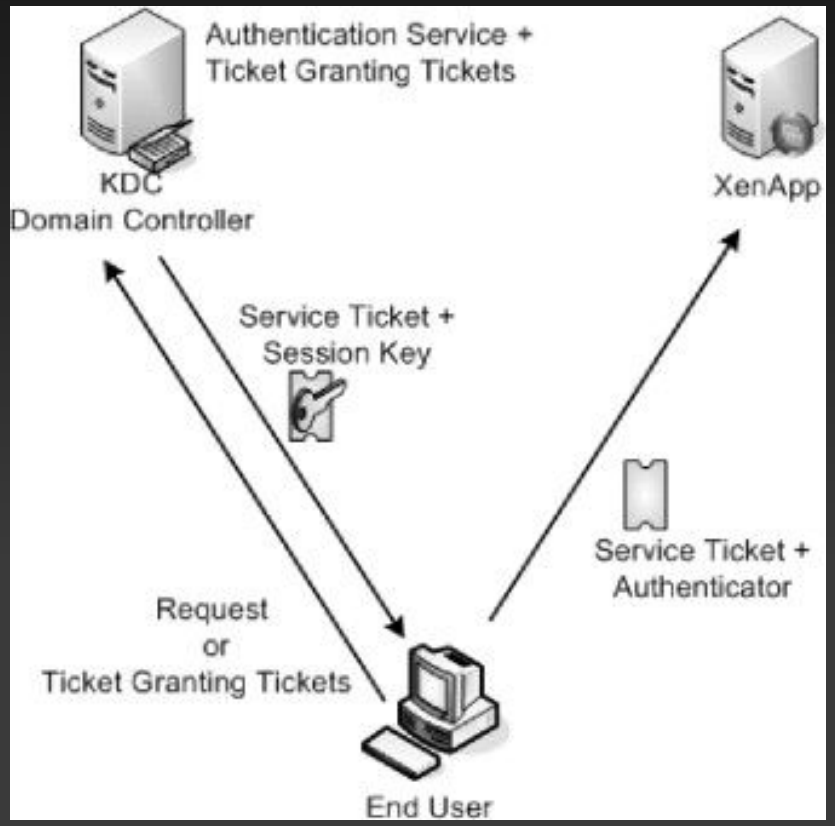
AD Security

- 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)
sammy            (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

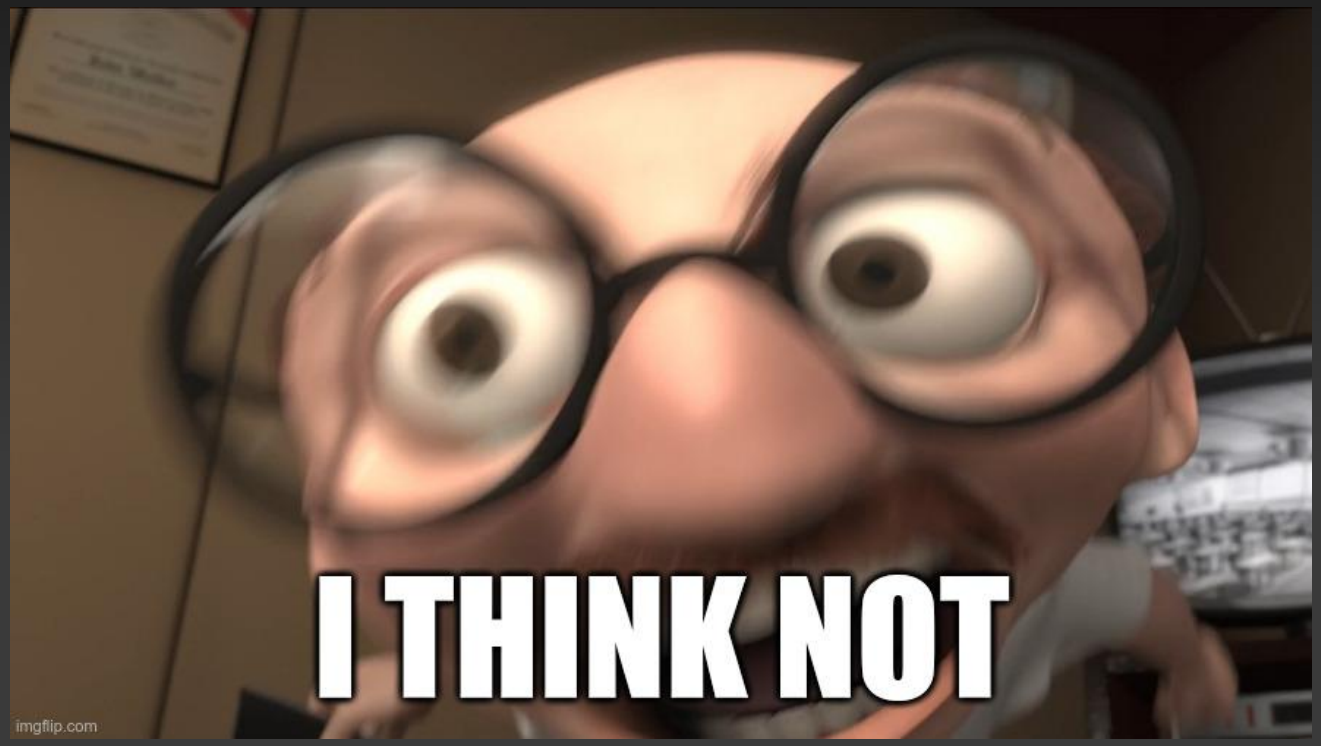
- Why is it so dangerous?
  - Service accounts often highly privileged but seldom audited
  - Highly lucrative PrivEsc methodology
  - Can be done offline, so doesn't create much noise

Kerberoasting

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

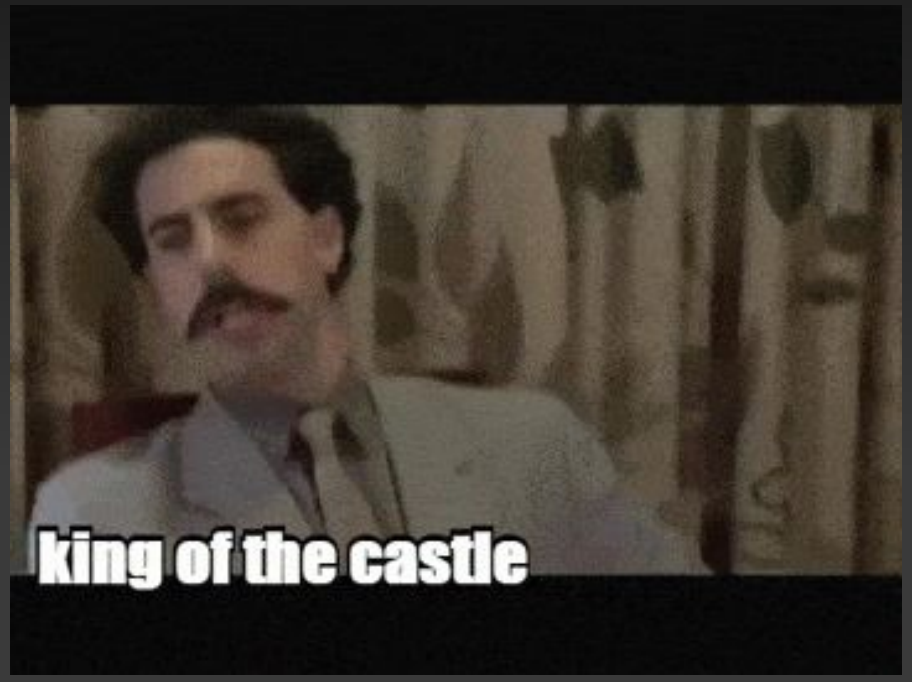
Pass-The-Hash

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



Pass-The-Hash

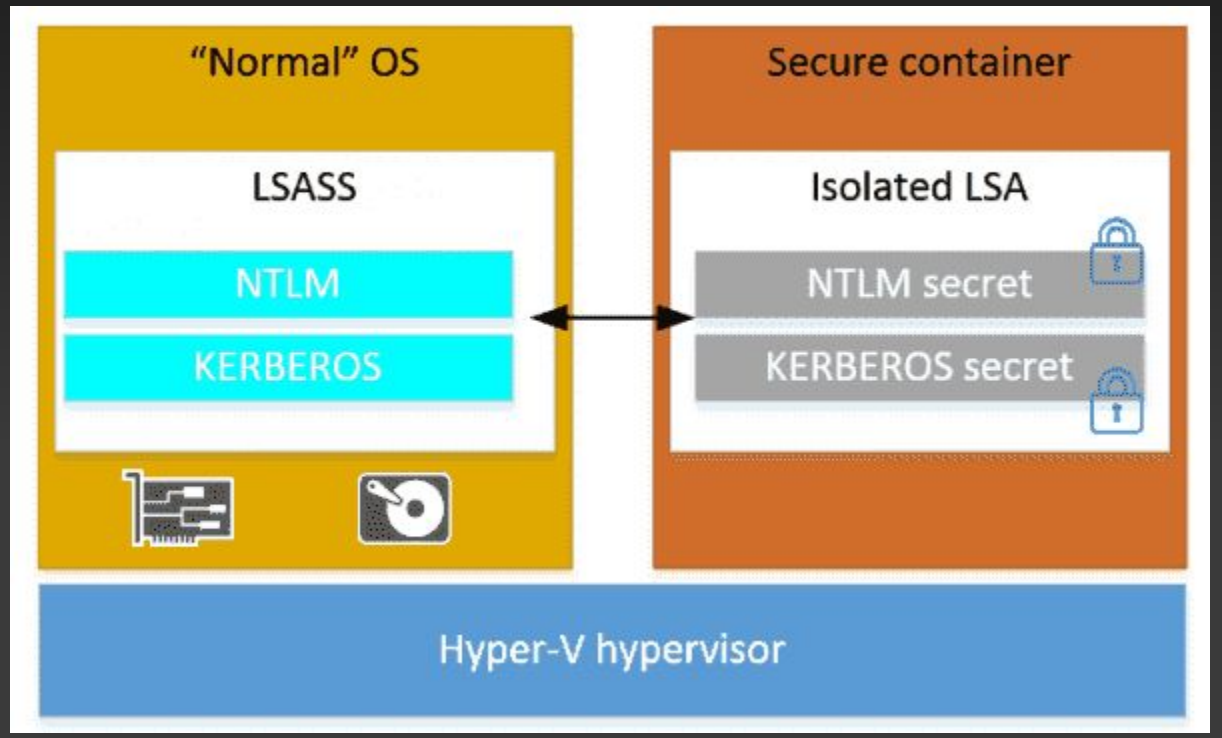
- Obtain a user's NTLM hash
- Use the hash directly for authentication



That's literally it!

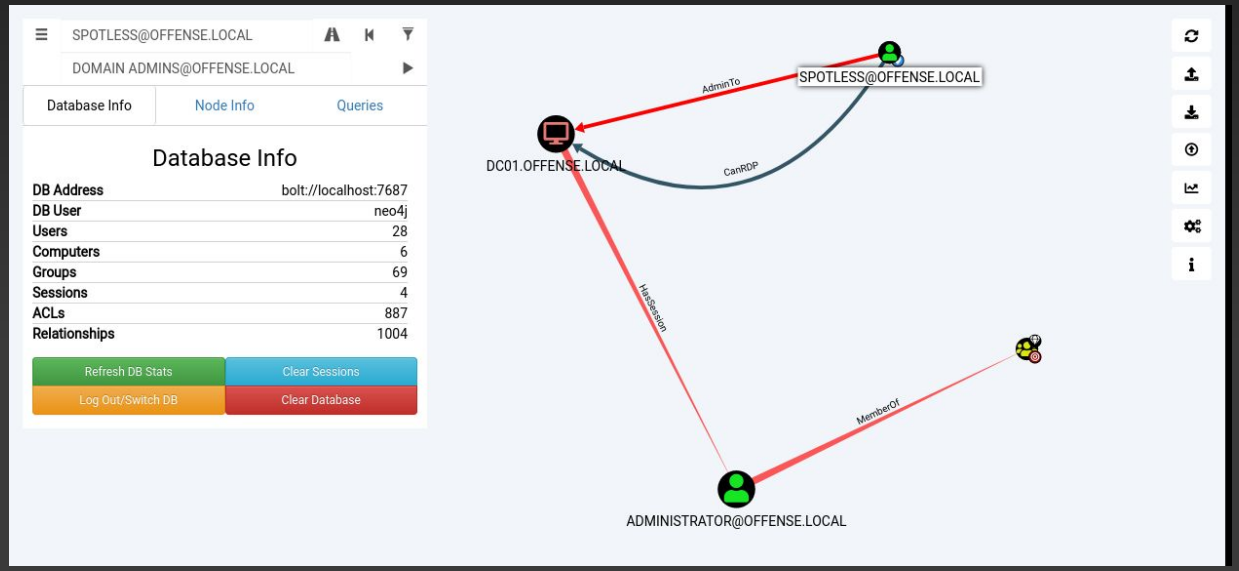
Pass-The-Hash

- Mitigation strategies
  - Credential Guard



Bloodhound

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

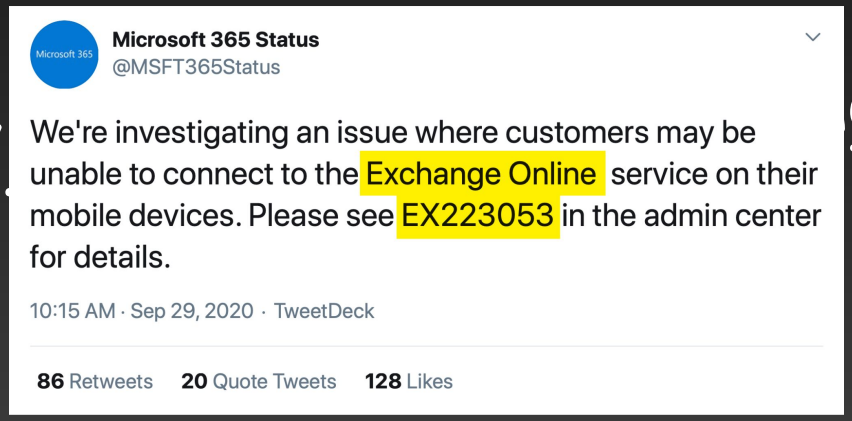


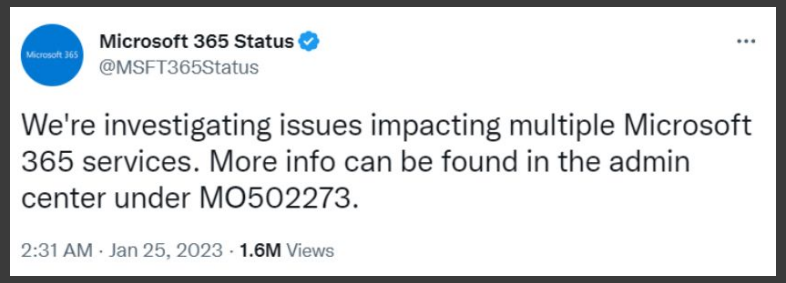
A note on Azure AD (AAD)

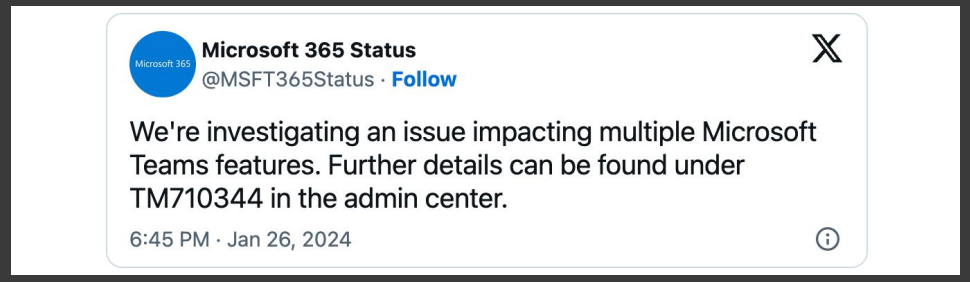
- Becoming a lot more popular
- Used to be a lot of hybrid environments, seeing a lot of orgs go 100% cloud-based
- Interestingly enough, some people are going the other way - back to on-prem!

A note on A… AD)

- …a lot mor…
- …e a lot of… nts,
- …t of orgs go 100% cloud based
- Interestingly enough, …g
- …ck …







A note on A AD)

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 · Follow

We're investigating an issue wit
experiencing degraded functio
Online and outlook.com service
in your admin center under EX4

4:55 PM · Jul 18, 2022

42 Reply Copy link

Read 4 re

Micros
@MSF

We're investi
details can b

8:27 PM · Jun

286 Retweets

their
center

Microsoft 365 Status
@MSFT365Status

We're investigating issue
365 services. More info
center under MO502273.

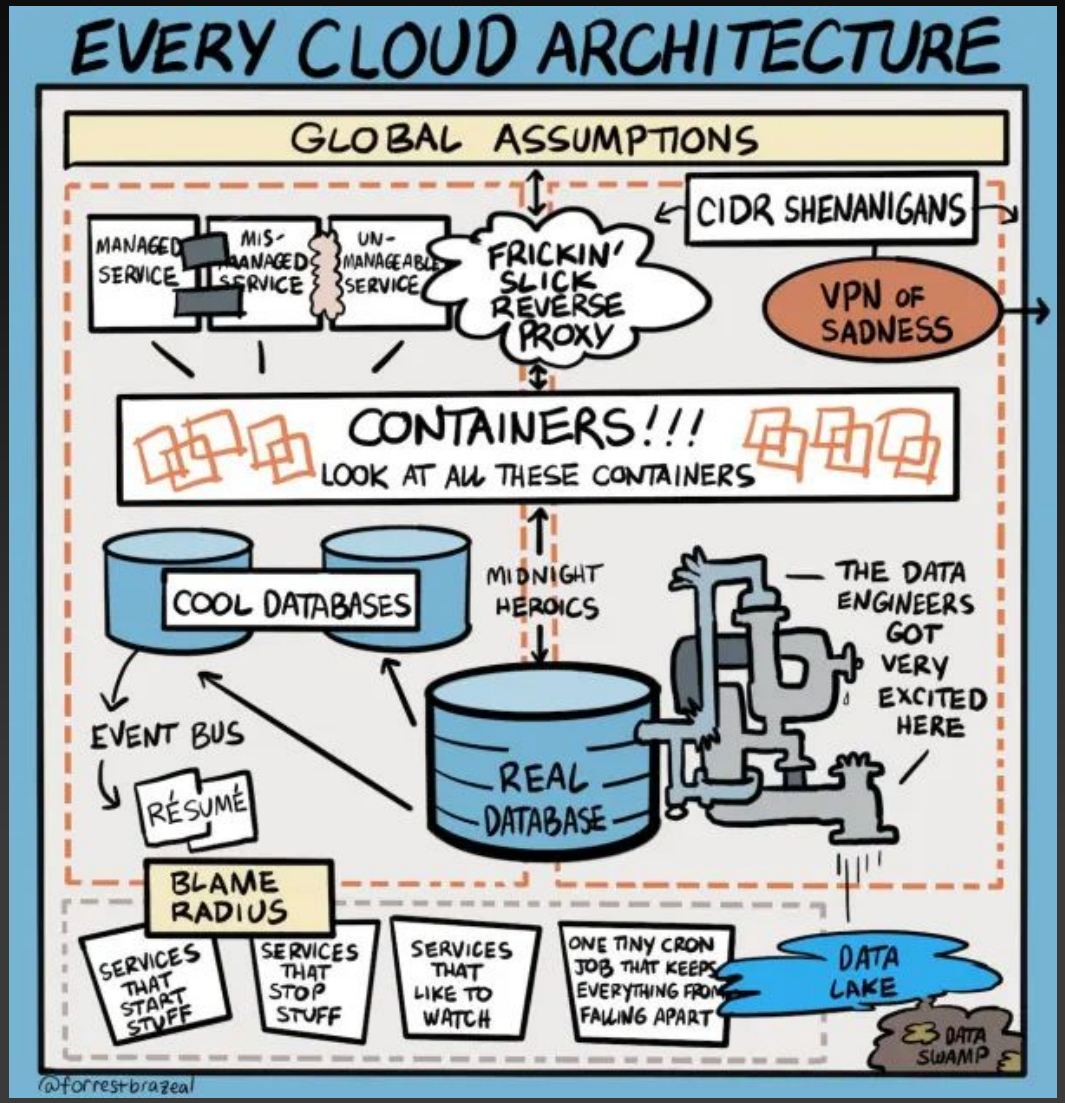
2:31 AM · Jan 25, 2023 · 1.6M Views

ft

TM710344 in the admin center.

6:45 PM · Jan 26, 2024

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