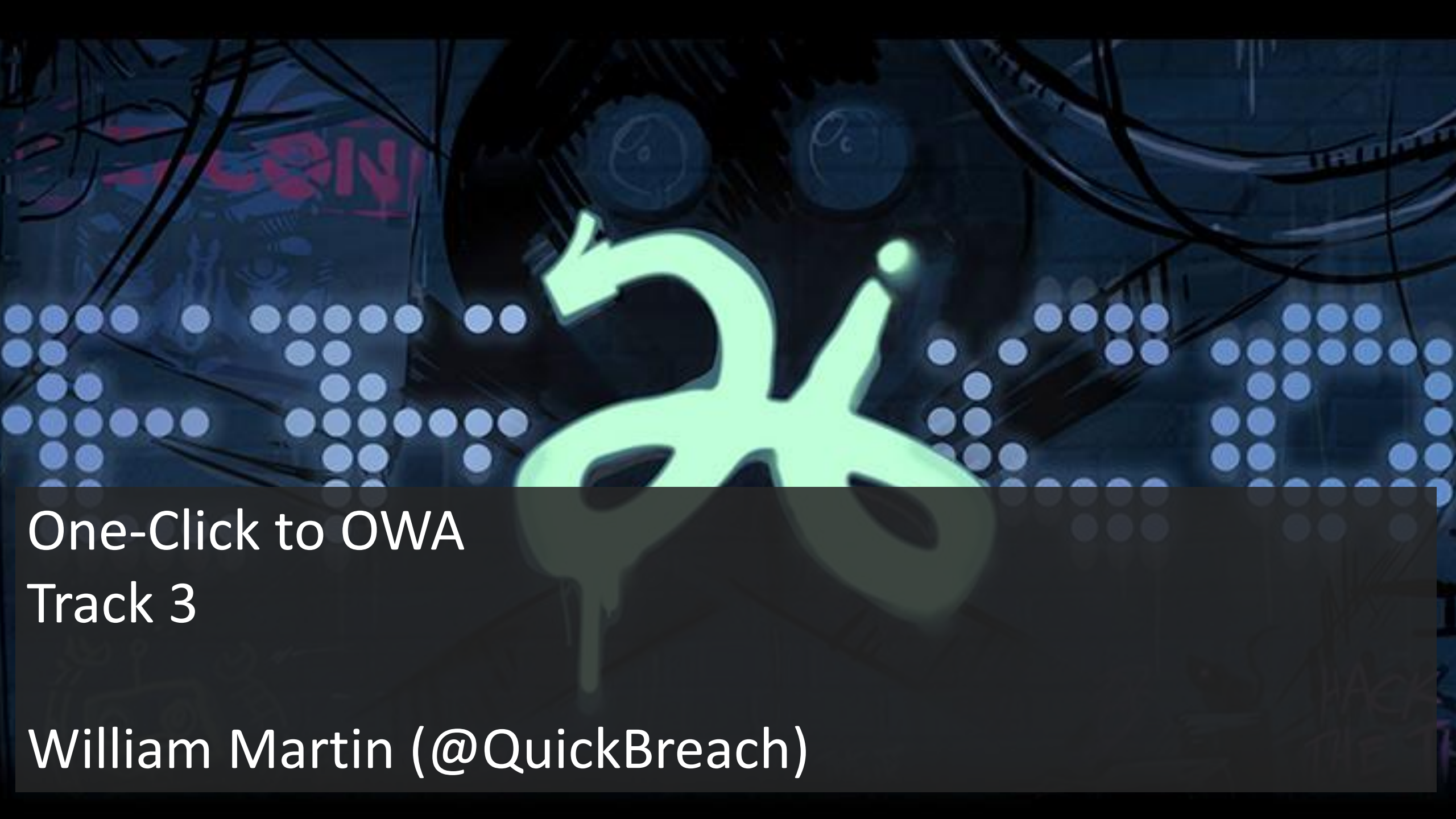


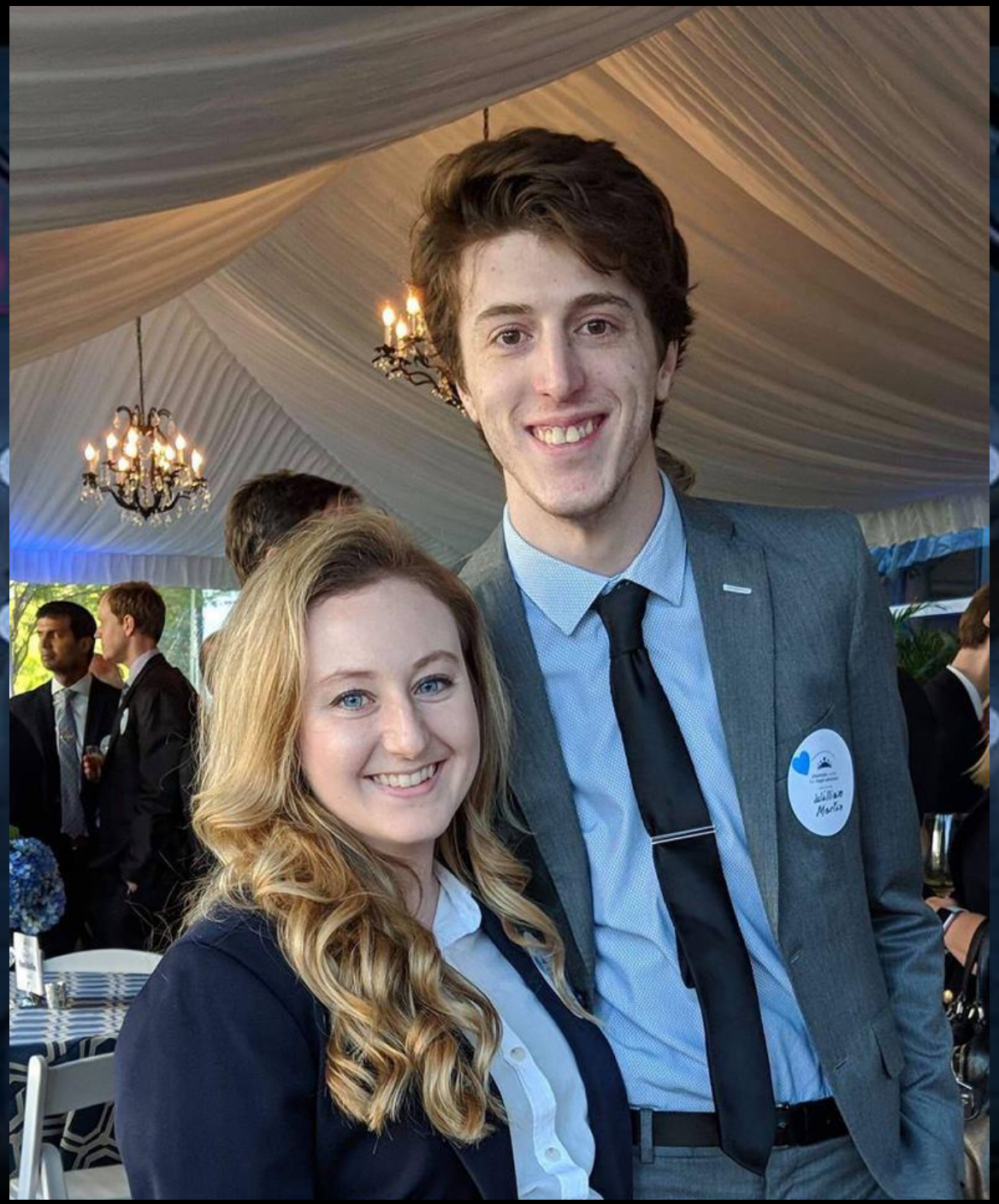
One-Click to OWA
Track 3

William Martin (@QuickBreach)

> whoami

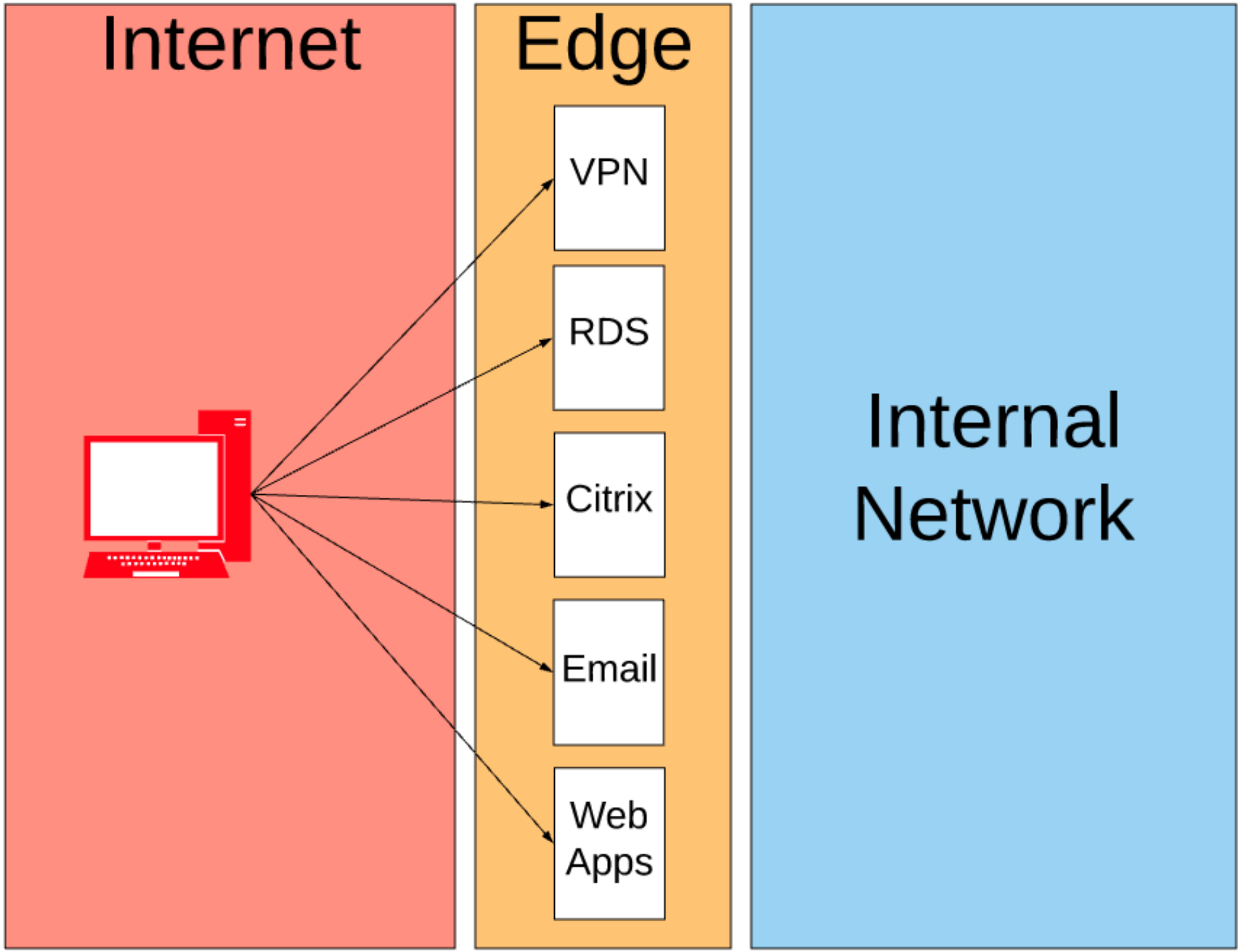
- William Martin
- OSCP
- Penetration Tester
- Supervisor at RSM US LLP in Charlotte, NC
- First time presenting at DEFCON

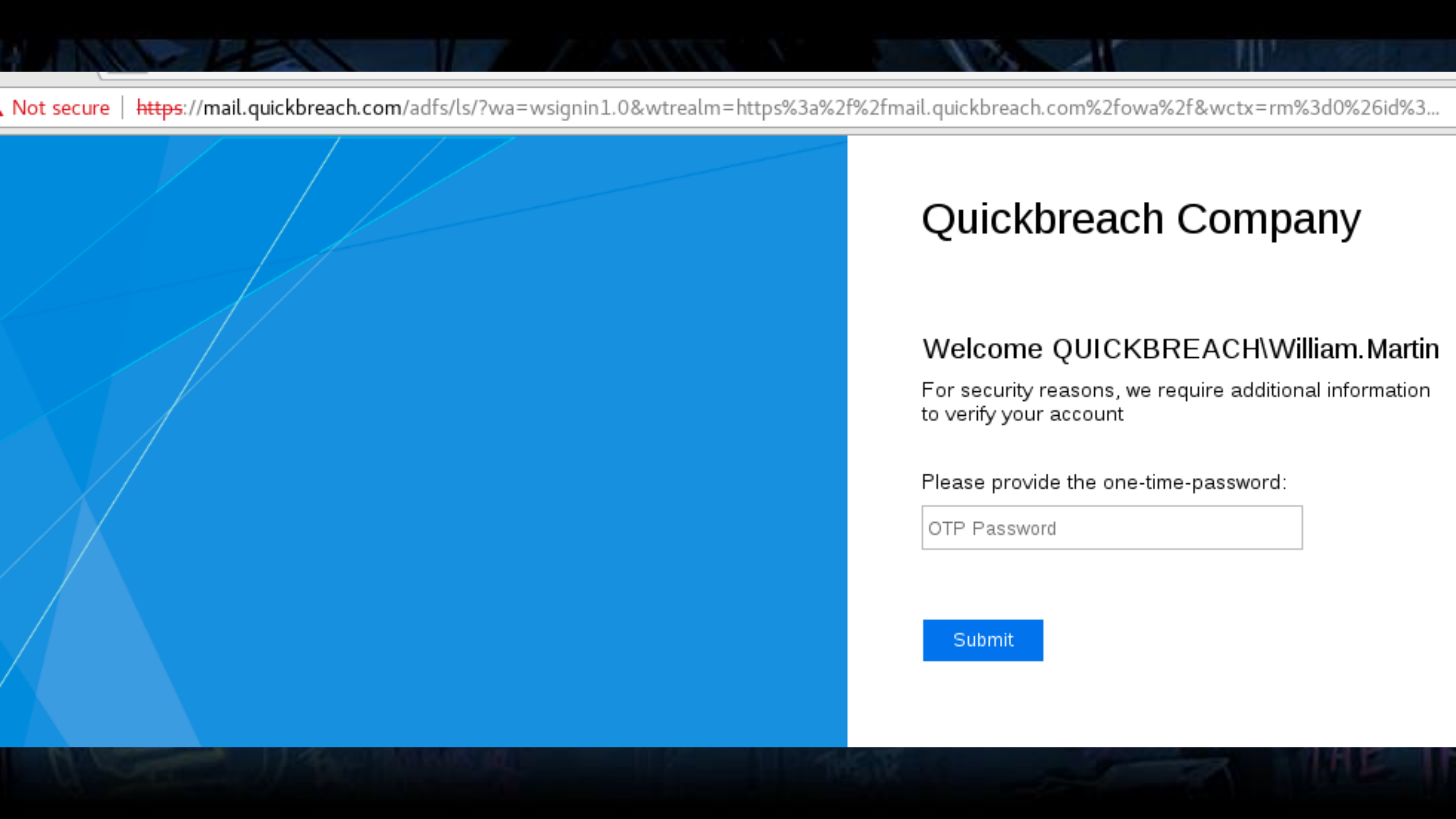
- Twitter: @QuickBreach

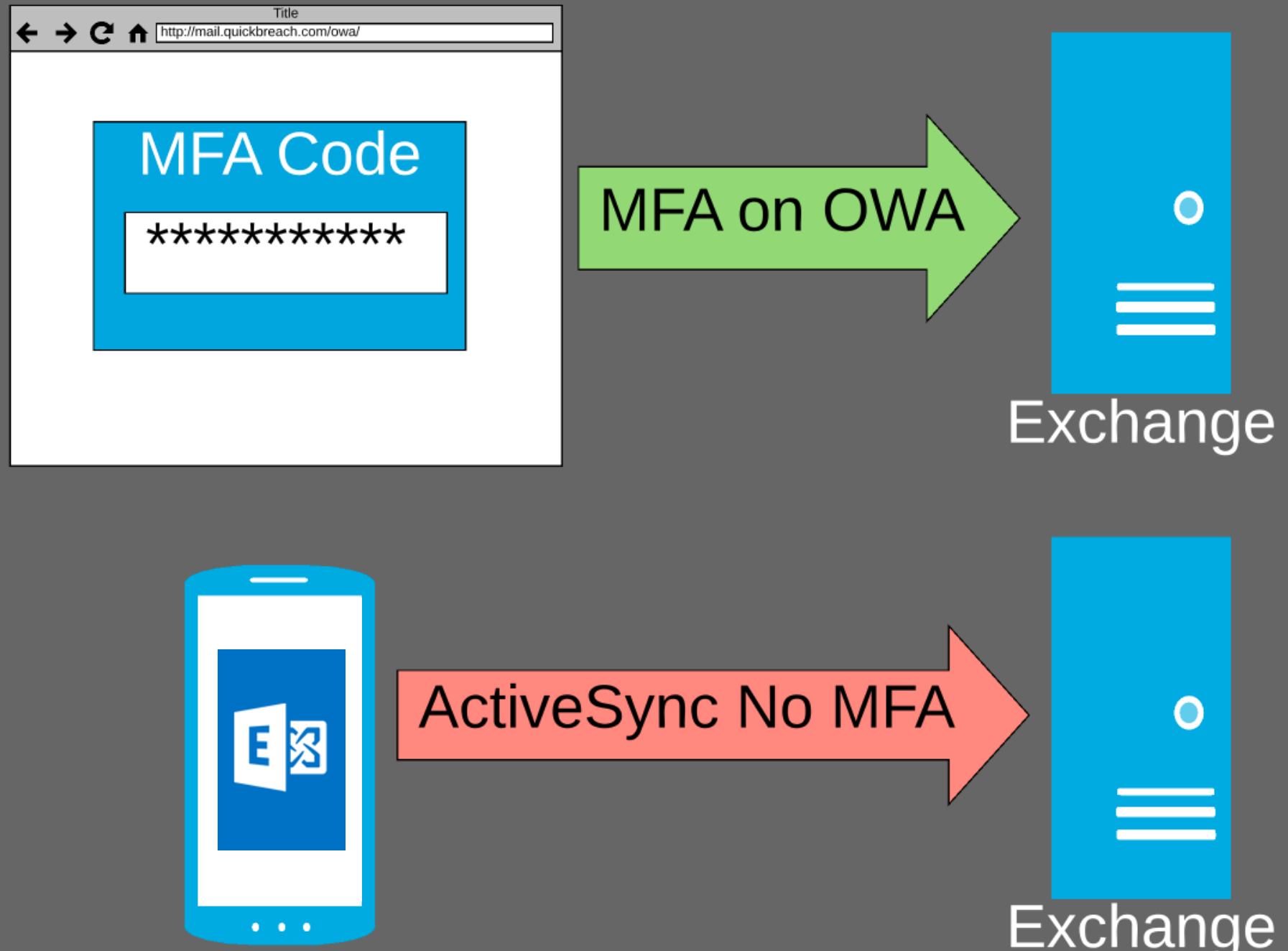


> What We Will Cover

- Basics on Exchange and endpoints on Exchange
- MFA crash course
- Recap on NTLM relay
- Background on ExchangeRelayX
- Demo & release
- Countermeasures

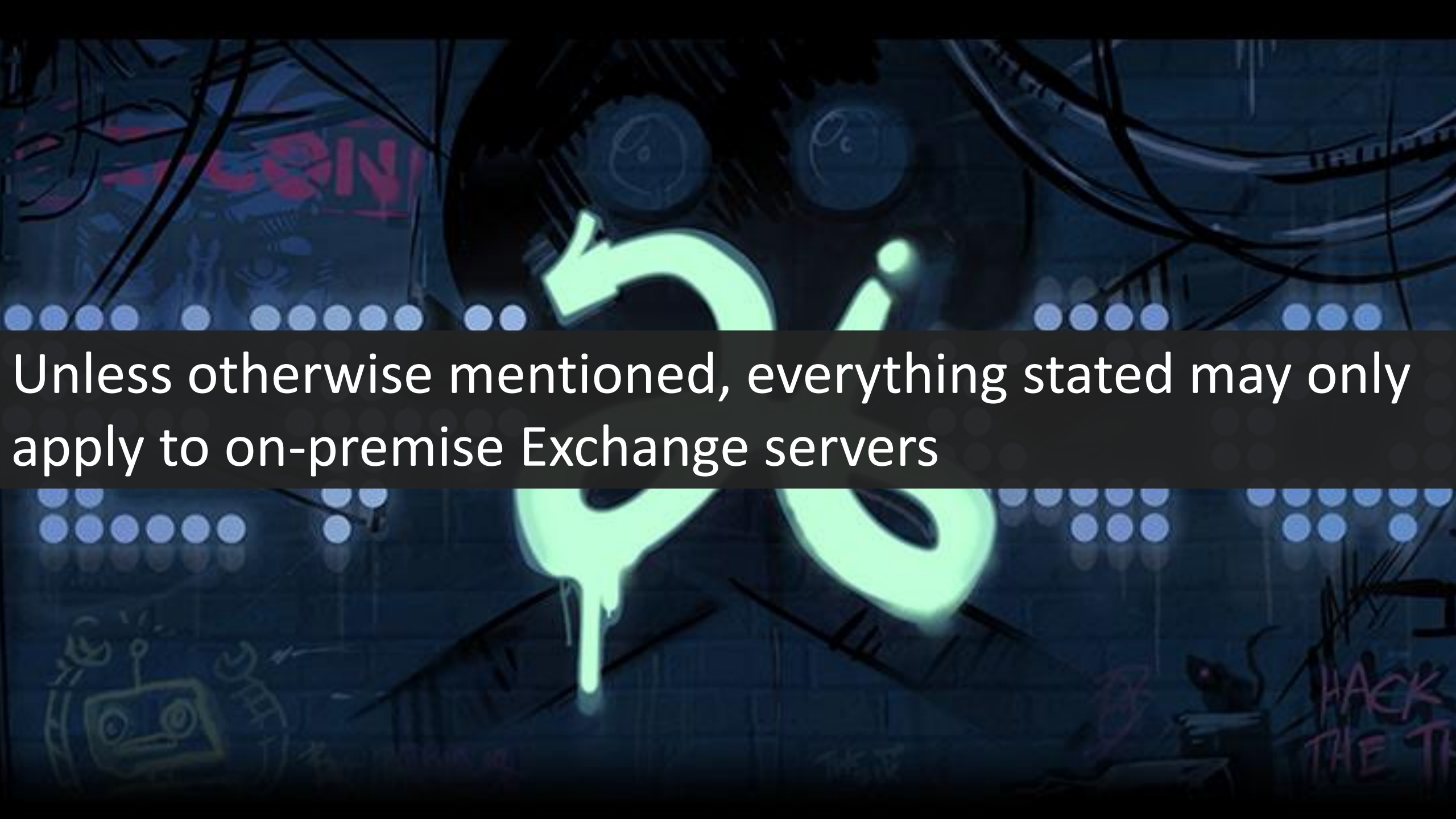

Internet
Edge
VPN
RDS
Citrix
Email
Web Apps
Internal Network


Not secure | https://mail.quickbreach.com/adfs/ls/?wa=wsignin1.0&wtrealm=https%3a%2f%2fmail.quickbreach.com%2fowa%2f&wctx=rm%3d0%26id%3...
Quickbreach Company
Welcome QUICKBREACH\William.Martin
For security reasons, we require additional information to verify your account
Please provide the one-time-password:
OTP Password
Submit


Title
http://mail.quickbreach.com/owa/
MFA Code
****
MFA on OWA
Exchange
ActiveSync No MFA
Exchange

Getting to know Microsoft Exchange




Unless otherwise mentioned, everything stated may only apply to on-premise Exchange servers

> Exchange Anatomy

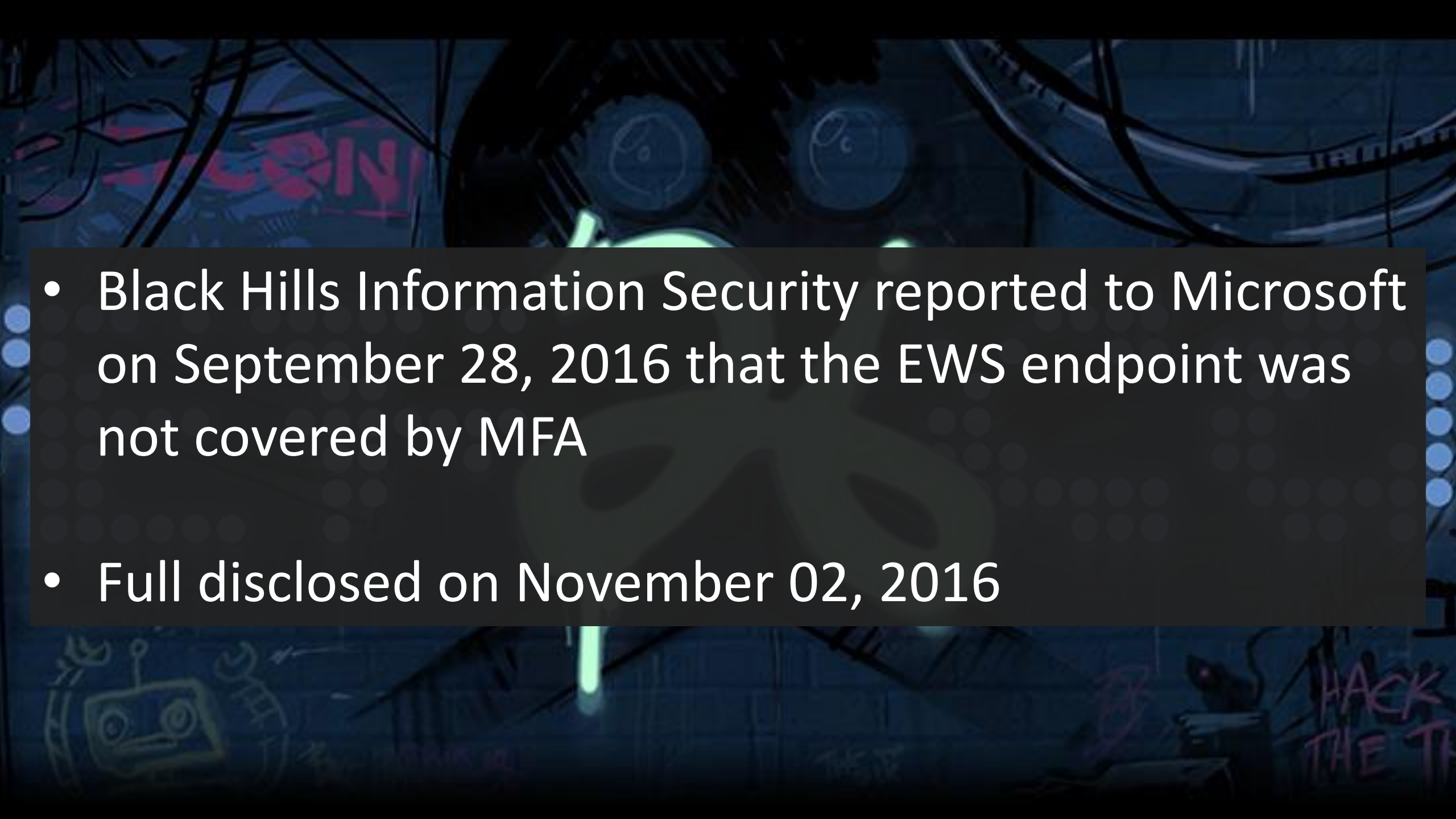
- Exchange Client Access Servers (CAS) are the OWA servers we are all familiar with and are how we, and our applications, interact with Exchange (Autodiscover, MAPI, Exchange Control Panel, etc)
- CAS servers operate essentially as a large Web App on top of IIS


https://ExchangeServer/AutoDiscover/
https://ExchangeServer/Mapi/
https://ExchangeServer/Rpc/
https://ExchangeServer/OAB/
https://ExchangeServer/OWA/
https://ExchangeServer/ECP/
https://ExchangeServer/Powershell/
https://ExchangeServer/EWS/
https://ExchangeServer/Microsoft-Server-ActiveSync/
Exchange

Endpoints	
/Powershell	Used for the Exchange Management Console for server administration
/Autodiscover	Provides clients the configuration details to use when connecting to the various endpoints, such as MAPI/HTTP
/Mapi	MAPI/HTTP Default way modern Outlook connects to Exchange
/Rpc	“Outlook Anywhere” – How previous versions of Outlook connected to Exchange
/Microsoft-Server-ActiveSync	Leveraged by mobile applications to access email
/OAB “Offline Address Book”	Can provides Outlook clients with a copy of the address book, eases the burden on Exchange
/ECP “Exchange Control Panel”	For users, manage their OWA. For admins, manage the server.
/OWA “Outlook Web App”	Email, Calendar, Tasks, and Contacts access via web app
/EWS “Exchange Web Services”	SOAP API to Exchange Web Services

Endpoints with access to user email or settings
/Mapi
/Rpc
/Microsoft-Server-ActiveSync
/ECP “Exchange Control Panel”
/OWA “Outlook Web App”
/EWS “Exchange Web Services”

Endpoints typically protected with MFA
/Mapi
/Rpc
/Microsoft-Server-ActiveSync
/ECP “Exchange Control Panel”
/OWA “Outlook Web App”
/EWS “Exchange Web Services”



- Black Hills Information Security reported to Microsoft on September 28, 2016 that the EWS endpoint was not covered by MFA
- Full disclosed on November 02, 2016

Multi-Factor Authentication (MFA), which includes Two-factor authentication (2FA), in Exchange Server and Office 365, is designed to protect against account and email compromise.

Microsoft has evaluated recent reports of a potential bypass of 2FA. We have determined that the technique described is not a vulnerability and the potential bypass does not exist on properly configured systems.

The reported technique does not pose a risk to Exchange Server or Office 365:

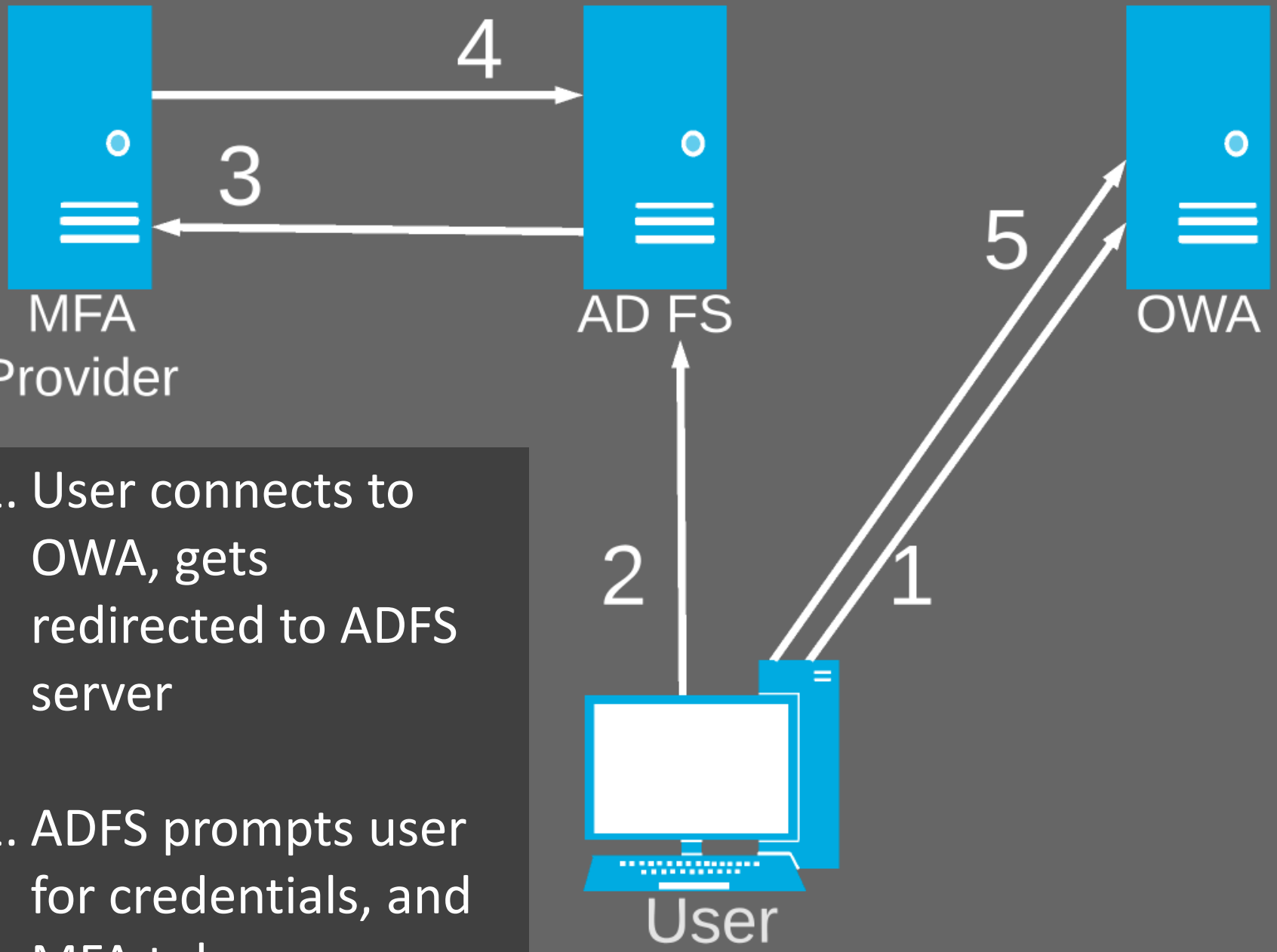
- In Exchange Server, authentication configuration settings for client endpoints are not shared across protocols. Supported authentication mechanisms are configured independently on a per protocol endpoint basis. Multi-Factor Authentication in Exchange Server can be enabled in multiple ways, including OAuth. Before implementing MFA with Exchange Server it is important that all client protocol touchpoints are identified and configured correctly.
- In Office 365, when Azure MFA is enabled within a tenant, it is applied to all supported client protocol endpoints. Exchange Web Services (EWS) is an Office 365 client endpoint which is enabled. Outlook on the Web (OWA) and Outlook client access are also enabled in Office 365. Office 365 users may experience a small delay in activation of MFA on all protocols due to propagation of configuration settings and credential cache expiration.

Source: https://blogs.technet.microsoft.com/exchange/2016/11/04/multi-factor-authentication-in-exchange-and-office-365/

> Cause of the Gap

- No mention of EWS or MAPI in popular MFA installation documentation

- Typical vendor solutions implement MFA on OWA and ECP through SSO web based solutions such as Active Directory Federation Services (AD FS) – which can’t be used by Outlook to directly authenticate to Exchange 2013/2016, so requests for /EWS and /MAPI are passed straight to Exchange



1. User connects to OWA, gets redirected to ADFS server

2. ADFS prompts user for credentials, and MFA token

3. AD FS forwards token to MFA provider to verify

4. MFA provider returns result of validity. If valid, the user has logged in and ADFS gives them a claim as a cookie

5. User is redirected back to OWA and uses the claim to SSO into the app

> Cause of the Gap

Vendors are aware of the gap, but the capabilities required to integrate their products with the authentication mechanisms of thick client protocols depends heavily on the environment and it’s support for “Modern Authentication”

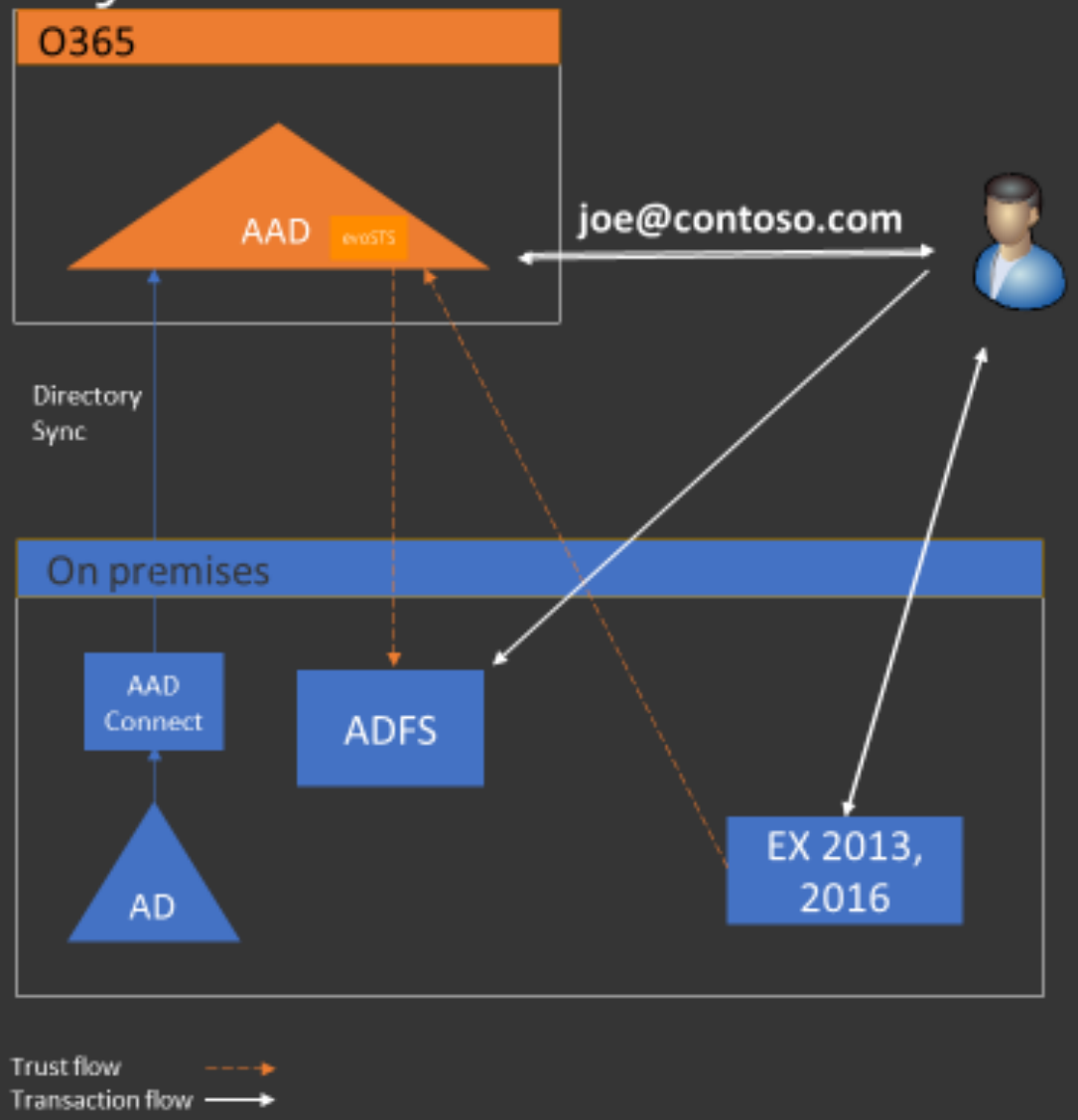
> Modern Authentication

- It is Microsoft's implementation of OAuth 2.0, introduced ~November of 2015
- Allows Outlook to authenticate to EWS, MAPI, and other endpoints with OAuth tokens issued by Azure Active Directory.
- In Modern Authentication, Exchange no longer handles authentication and thus Outlook clients may use MFA through AD FS as part of the OAuth authentication process. Exchange only receives the resulting "access" and "refresh" tokens provided to Outlook from Azure.

> Modern Authentication

- Three types of set up:
  - Pure on-premise (*coming in Exchange 2019*): Requires AD FS 2016, Outlook 2016, EX 2013/2016
  - Hybrid: Requires On-premise AD FS, Outlook 2013/2016, and O365 Azure Active Directory
  - Pure O365: Modern Auth is automatically enabled for Office 2016 clients, and can work with 2013

Hybrid Modern Auth – Federated Domain

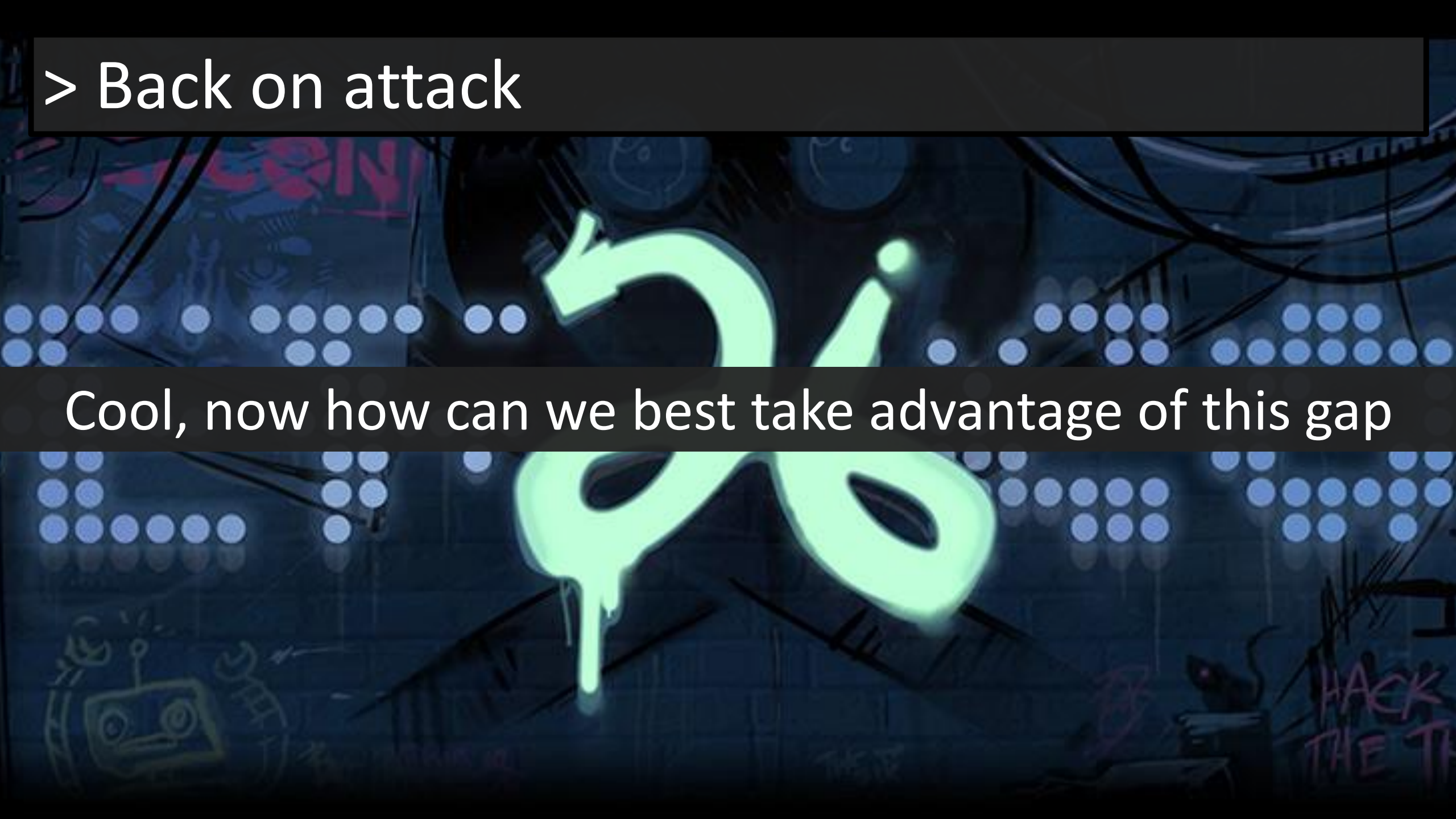


Outlook login (no cached tokens or Integrated Auth)

1. Outlook attempts to connect to Exchange
2. Exchange responds with "get token from AAD"
3. Outlook connects to URI provided by Exchange
4. User provides username to AAD
5. AAD redirects to on-prem AD FS
6. User enters password/certificate/drop of blood
7. AD FS redirects back to AAD
8. AAD returns Access and Refresh tokens to Outlook
9. Outlook gives client Access token to Exchange

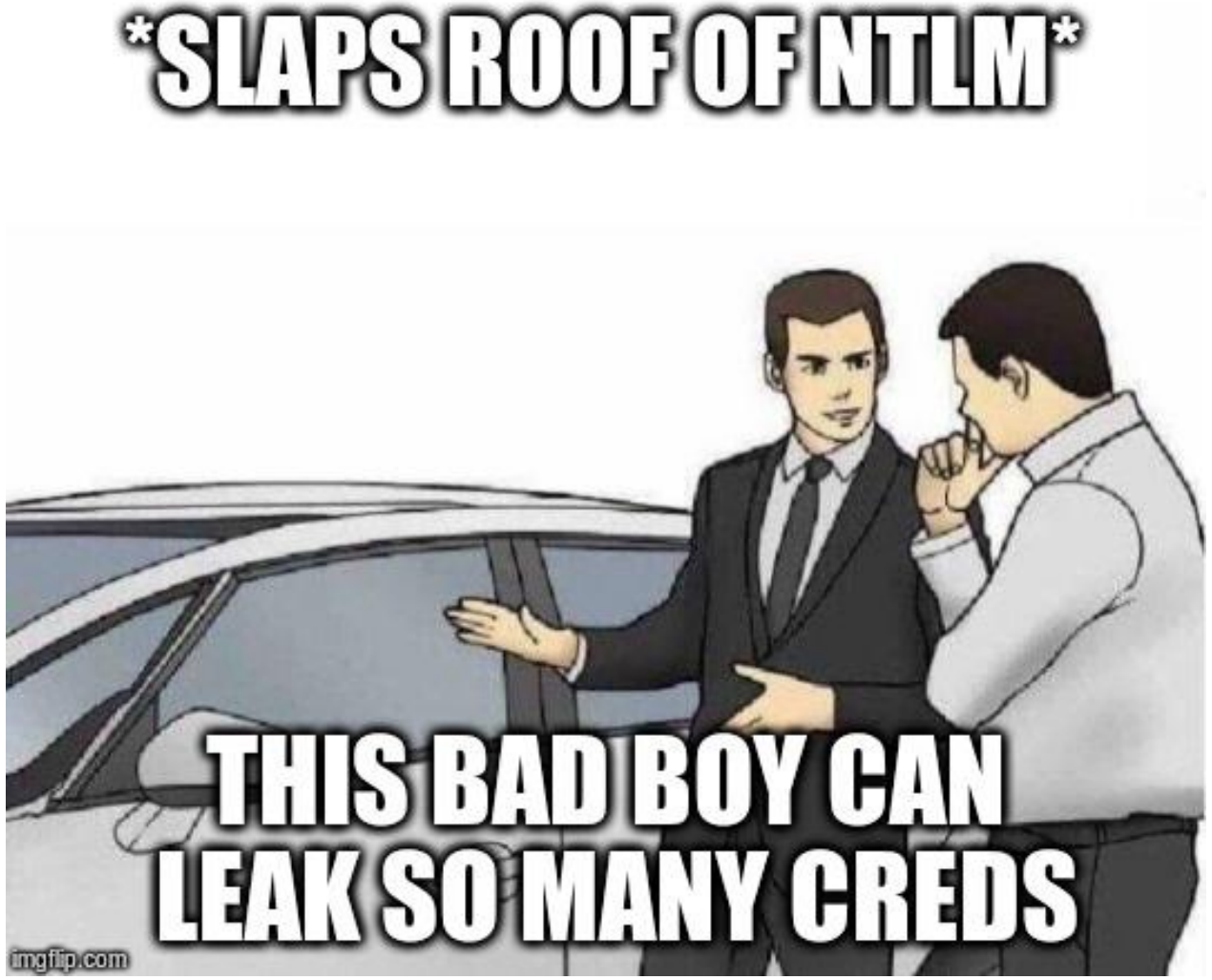
https://blogs.technet.microsoft.com/exchange/2017/12/06/announcing-hybrid-modern-authentication-for-exchange-on-premises/

> Back on attack



Cool, now how can we best take advantage of this gap

Endpoints not typically protected with MFA	Default Authentication Mechanisms
/Mapi	Kerberos, **NTLM**
/Rpc	Basic, **NTLM**
/Microsoft-Server-ActiveSync	Basic
/EWS “Exchange Web Services”	Kerberos, **NTLM**


SLAPS ROOF OF NTLM
THIS BAD BOY CAN
LEAK SO MANY CREDS
imgflip.com

> NTLM Relay: A tale as old as time

- A pseudo MiTM type attack to leverage the authentication in process of a victim
- Evidence of exploitation as early as 2001 by the Cult of the Dead Cow
- First step of compromise in 90% of my internal penetration tests

> NTLM Relay: A tale as old as time

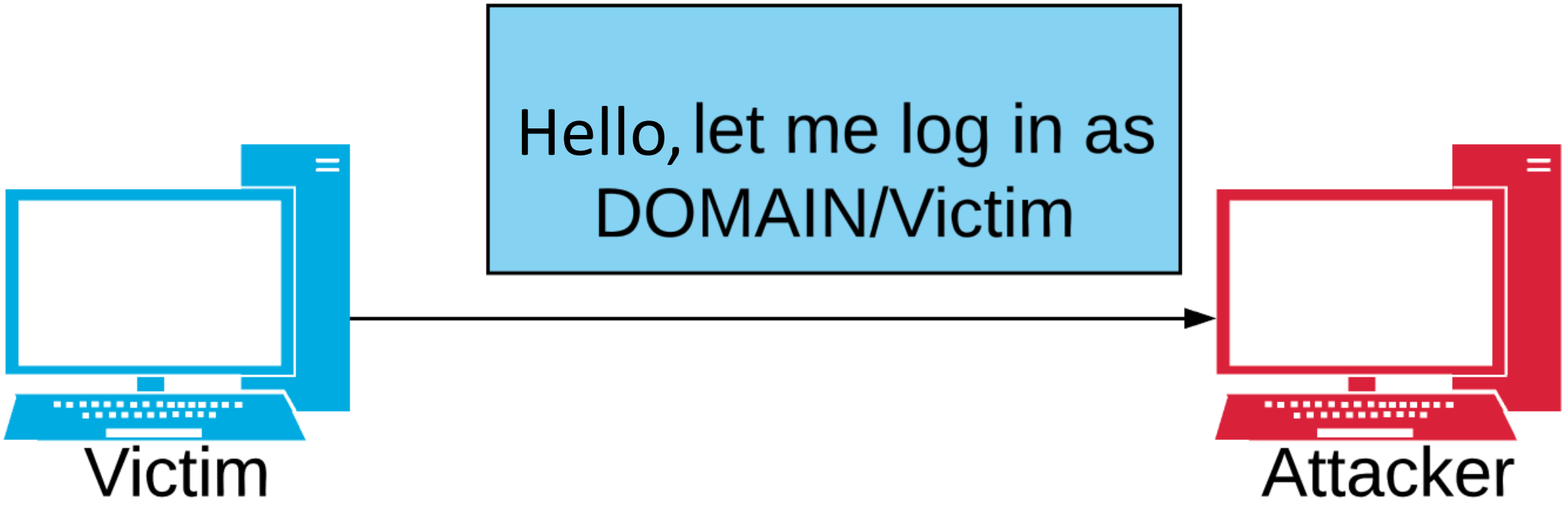
NTLM auth works by these three messages:

Client to Server: NTLM Negotiate

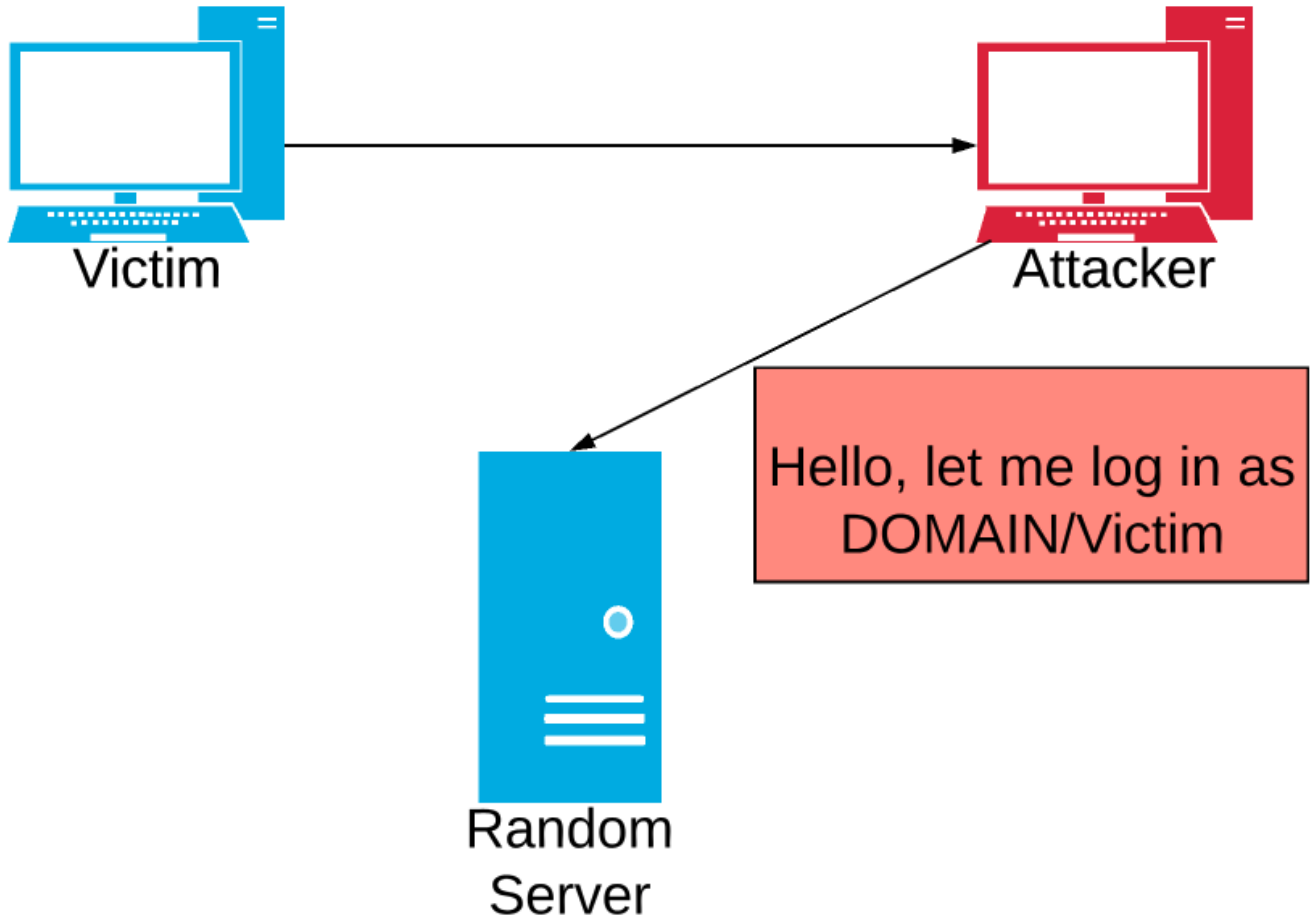
Server to Client: NTLM Challenge

Client to Server: NTLM Challenge-Response

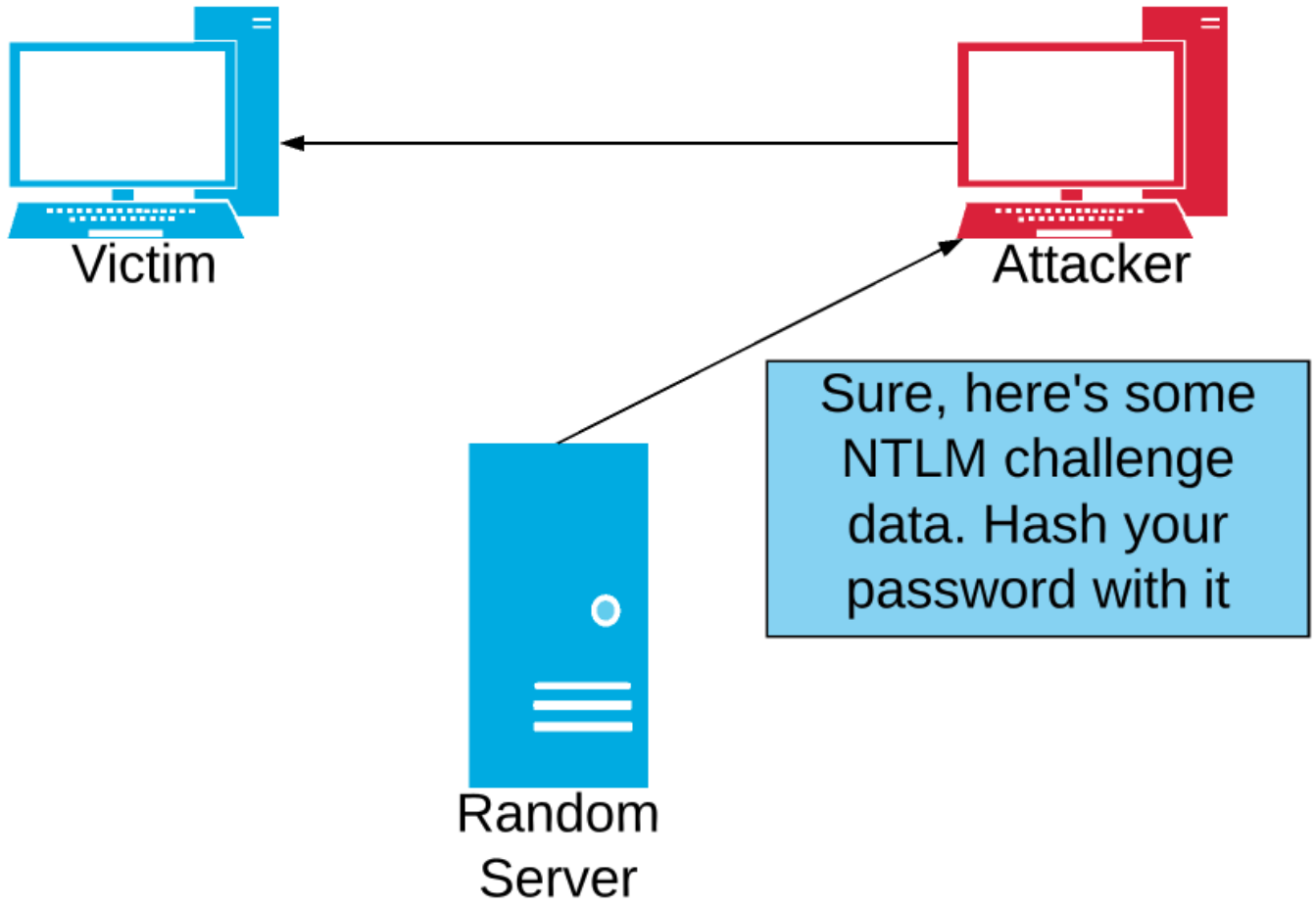
NTLM Relay Attack



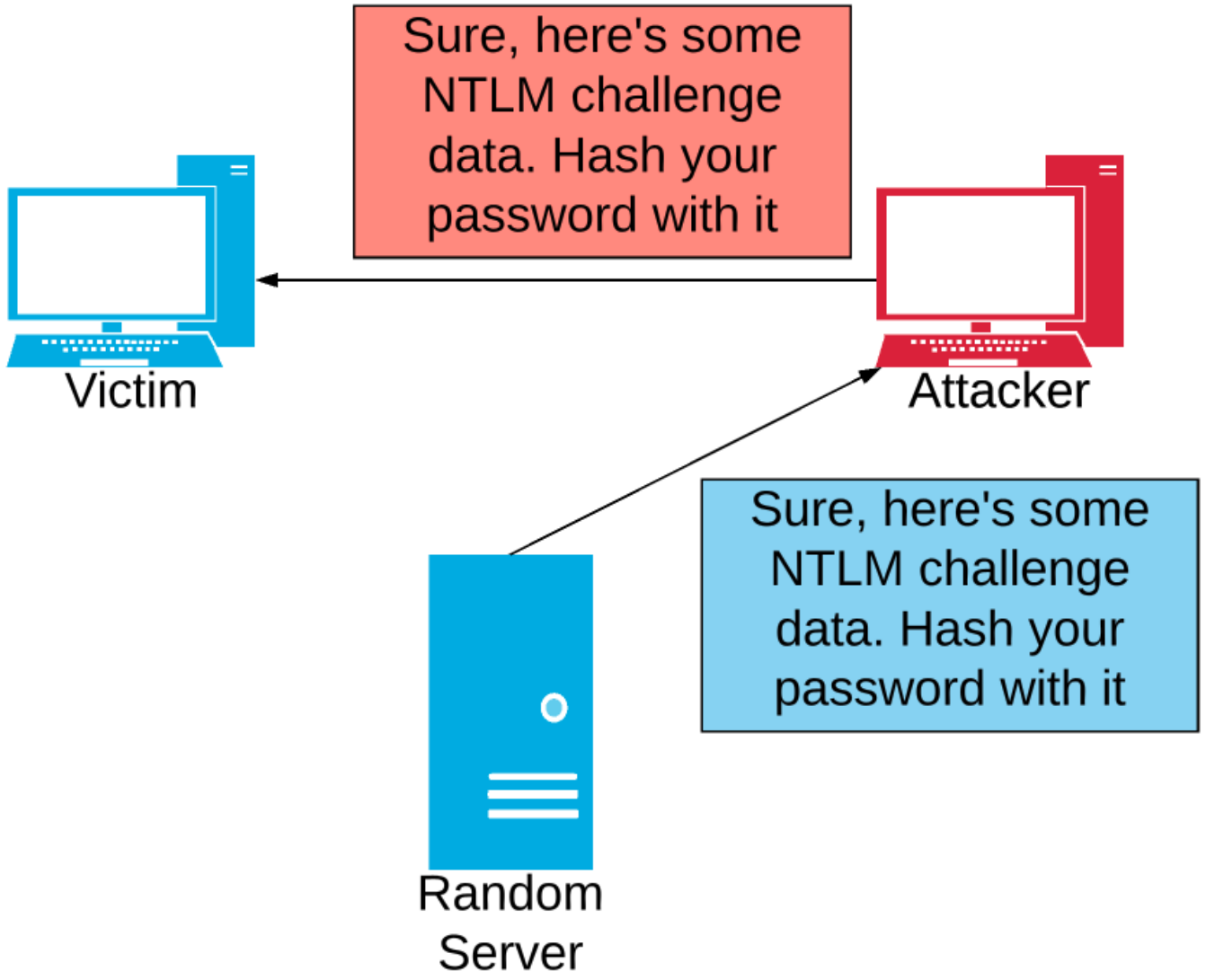
NTLM Relay Attack



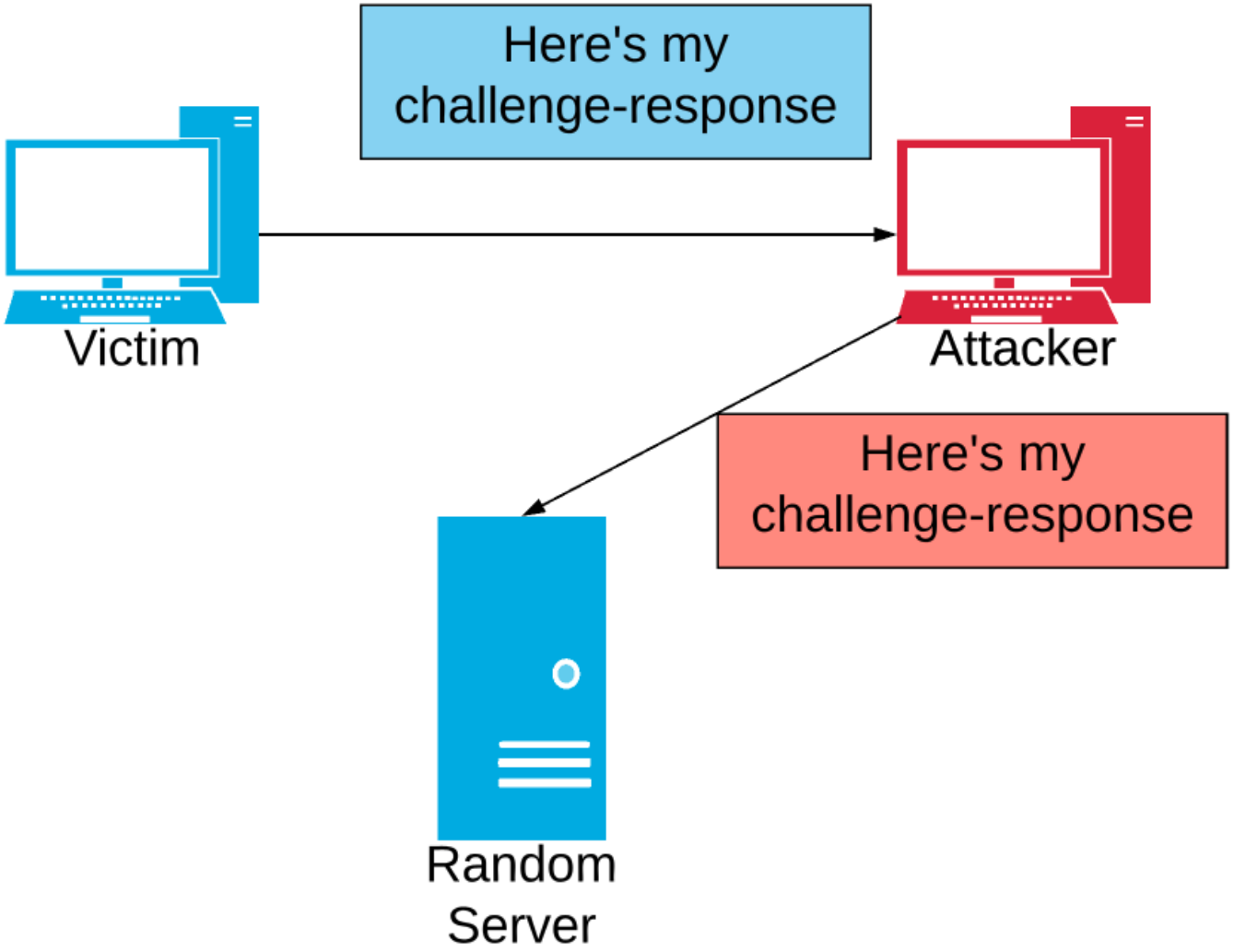
NTLM Relay Attack



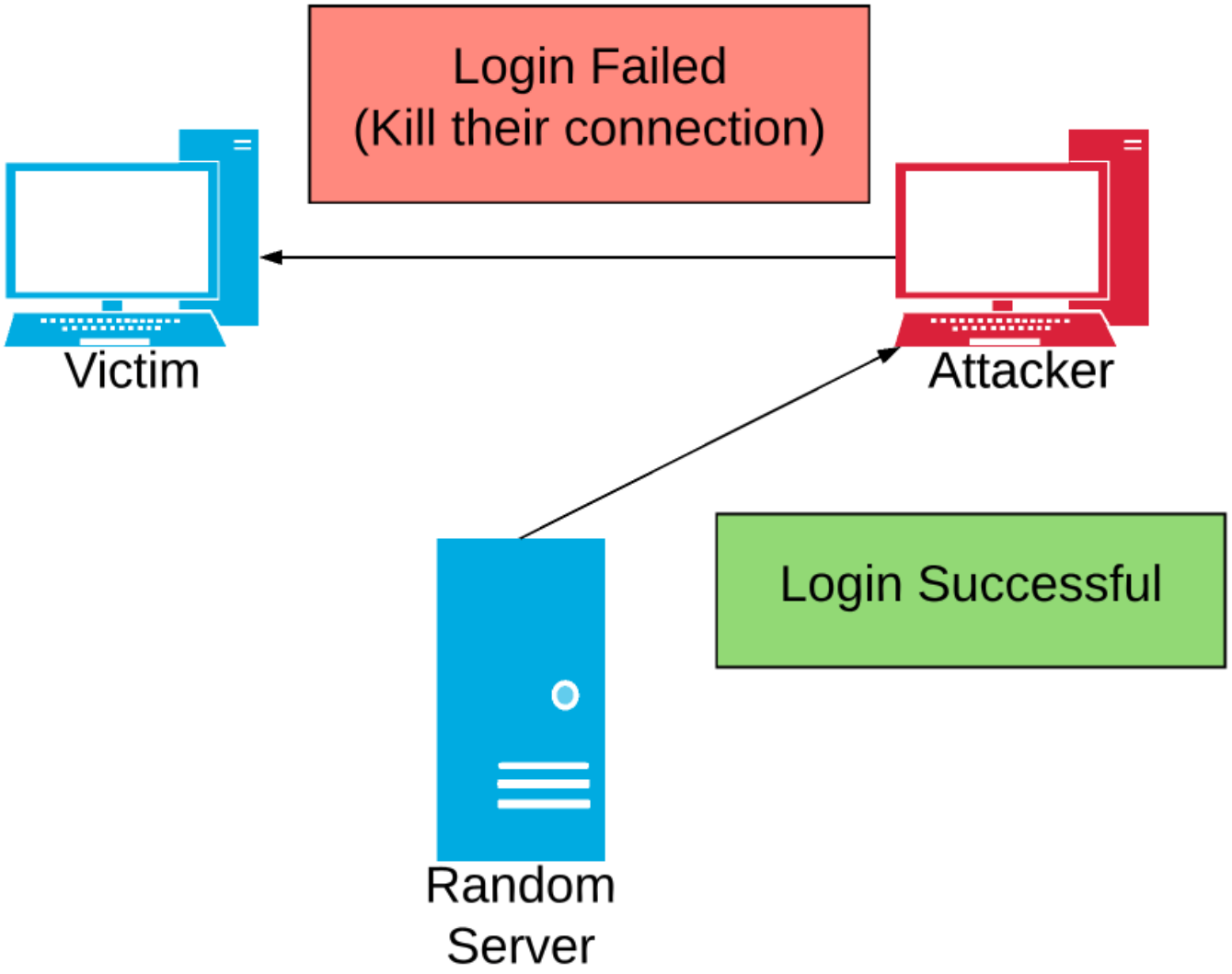
NTLM Relay Attack



NTLM Relay Attack



NTLM Relay Attack




> Common ways to trigger NTLM authentication

> UNC link in an email clicked in Outlook

Good afternoon DefCon,

<Insert standard phishing language here>

file://\\10.0.0.7\somefileshare\demo.png
Click or tap to follow link.

You should watch this video: https://www.youtube.com/watch?v=dQw4w9WgXcQ

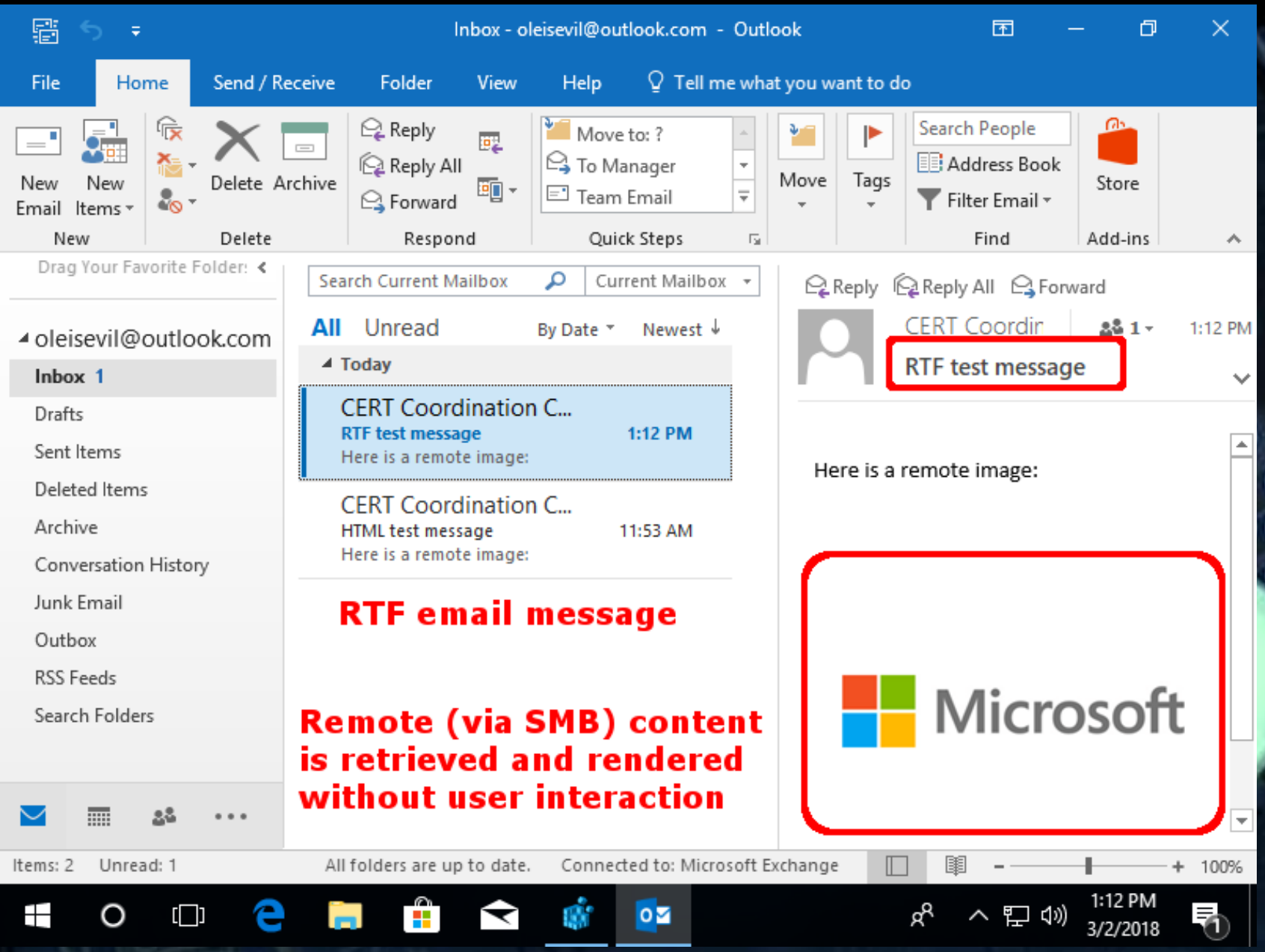
Best regards,

William

> NBT-NS & LLMNR poisoning

```
[*] [LLMNR]  Poisoned answer sent to 169.254.244.62 for name CLIENT-PC
[*] [LLMNR]  Poisoned answer sent to 169.254.244.62 for name dc02
[*] [LLMNR]  Poisoned answer sent to 10.0.0.15 for name CLIENT-PC
[*] [LLMNR]  Poisoned answer sent to 10.0.0.15 for name CLIENT-PC
[*] [LLMNR]  Poisoned answer sent to 10.0.0.15 for name CLIENT-PC
 [*] [LLMNR]  Poisoned answer sent to 10.0.0.15 for name CLIENT-PC
[*] [NBT-NS] Poisoned answer sent to 10.0.0.15 for name QUICKBREACH (se
[*] [LLMNR]  Poisoned answer sent to 10.0.0.15 for name somenetworkshar
[*] [NBT-NS] Poisoned answer sent to 10.0.0.15 for name DC02 (service:
[*] [LLMNR]  Poisoned answer sent to 10.0.0.15 for name afileshare
[*] [NBT-NS] Poisoned answer sent to 10.0.0.15 for name AFILESHARE (ser
[SMBv2] NTLMv2-SSP Client   : 10.0.0.15
[SMBv2] NTLMv2-SSP Username : QUICKBREACH\William.Martin
[SMBv2] NTLMv2-SSP Hash     : William.Martin::QUICKBREACH:d61eb942fd8cf
4D00420033000100 1E00570049004E002D0050005200480034003900320052005100410
52005100410046005 6002E0053004D00420033002E006C006F00630061006C0005001400
0000000000200000822EF1E35BC638E423744DBC052D19B8BCDC1209B853CC4718E6E76
610072006500000000000000000000000
```


> Slicker ways to trigger NTLM authentication



CVE-2018-0950 by Will Dormann

Outlook can render RTF email messages, and if they included remotely hosted OLE, used to automatically load the OLE from the remote resource – including from an SMB server.

Source: https://insights.sei.cmu.edu/cert/2018/04/automatically-stealing-password-hashes-with-microsoft-outlook-and-ole.html

> UNC path in office document framesets



Source: https://pentestlab.blog/2017/12/18/microsoft-office-ntlm-hashes-via-frameset/

Mike Felch @ustayready

An attacker can modify the "Websettings.xml" within a docx file, and include a new "websettings.xml.rel" in that same docx file to create a word document that will automatically attempt to authenticate to a given SMB share upon opening - without user interaction.

> Back to picking a target

Endpoints typically protected with MFA	Default Authentication Mechanisms
/Mapi	Kerberos, **NTLM**
/Rpc	Basic, **NTLM**
/EWS “Exchange Web Services”	Kerberos, **NTLM**



```
A tool by @_staaldraad from @sensepost to abuse Exchange Services.

AUTHOR:
   Etienne Stalmans <etienne@sensepost.com>, @_staaldraad

COMMANDS:
     add, a      add a new rule
     delete, r   delete an existing rule
     display, d  display all existing rules
     check, c    Check if the credentials work and we can interact with the mailbox
     send, s     Send an email to trigger an existing rule. This uses the target user's own account.
     brute, b    Do a bruteforce attack against the autodiscover service to find valid username/passwords
     abk         Interact with the Global Address Book
     form        Interact with the forms function.
     help, h     Shows a list of commands or help for one command

GLOBAL OPTIONS:
   --domain value, -d value    A domain for the user (optional in most cases. Otherwise allows: domain\username)
   --o365                      We know the target is on Office365, so authenticate directly against that.
   --username value, -u value  A valid username
   --password value, -p value  A valid password
   --hash value                A NT hash for pass the hash
   --email value, -e value     The target's email address
   --cookie value              Any third party cookies such as SSO that are needed
   --url value                 If you know the Autodiscover URL or the autodiscover service is failing. Requires full URI, htt
ps://autodisc.d.com/autodiscover/autodiscover.xml
   --insecure, -k              Ignore server SSL certificate errors
   --noencrypt                 Don't use encryption the RPC level - some environments require this
```

Source: http://seclist.us/wp-content/uploads/2017/05/ruler.png



staaldraad commented on Apr 9, 2017 Collaborator

I've looked into this and it would require a decent amount of work. Each NTLM authenticated request would need to be done through the relay (as far as I can see). So this would require sending a redirect or similar to cause a new "relay" request for each endpoint. For RPC/HTTP this would likely be 3+ requests.

1.) POST /autodiscover/autodiscover.xml
2.) RPC_IN_DATA /rpcproxy.dll
3.) RPC_OUT_DATA /rpcproxy.dll

2 and 3 would then need to be repeated for each action, such as `display`, `add` `delete` .
I'm adding this to future features list 👍

 **staaldraad** added the **help wanted** label on Apr 9, 2017

> Picking a target

Endpoints not typically protected with MFA	Default Authentication Mechanisms
~~*/Mapi*~~	~~*Kerberos, NTLM*~~
~~*/Rpc*~~	~~*Basic, NTLM*~~
/EWS “Exchange Web Services”	Kerberos, NTLM

> What is EWS?

“Exchange Web Services (EWS) provides the functionality to enable client applications to communicate with the Exchange server. EWS provides access to much of the same data that is made available through Microsoft Office Outlook.”

Source: https://docs.microsoft.com/en-us/previous-versions/office/developer/exchange-server-2010/dd877045%28v%3dexchg.140%29

> EWS

The three things we care about:

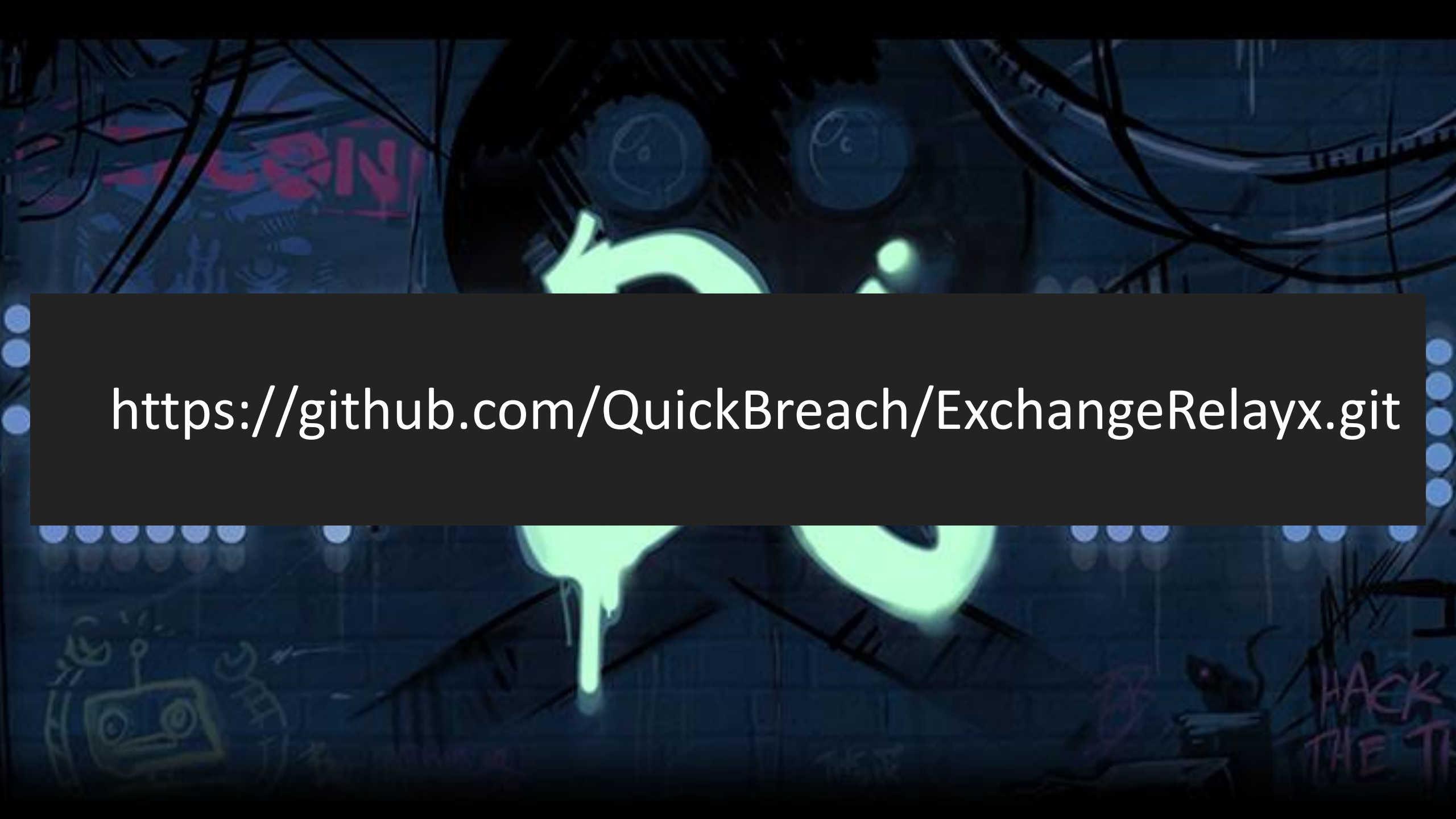
- Enabled by default on Exchange Client Access Servers
- On-Premise Exchange EWS support NTLM authentication by default
- Provides access to most things Outlook has access to

> Objectives with ExchangeRelayX

- Read/Send/Delete/Forward emails
- Download attachments
- Add forward rules to backdoor an email
- Scrape as much data as we can from AD
- Launch spear phishing from within the organization, potentially avoiding typical attachment filters


Demo




https://github.com/QuickBreach/ExchangeRelayx.git


Countermeasures

> Countermeasures: Modern Authentication

Organizations must push for Modern Authentication in order to have MFA covered on all Exchange endpoints

- Catch: RPC/HTTP (aka “Outlook Anywhere”) does not support OAuth, and thus will still not be covered. If logs support that this endpoint is not used, then disable/block access to it

- Catch: Exchange 2010 cannot exist anywhere in an environment with modern authentication

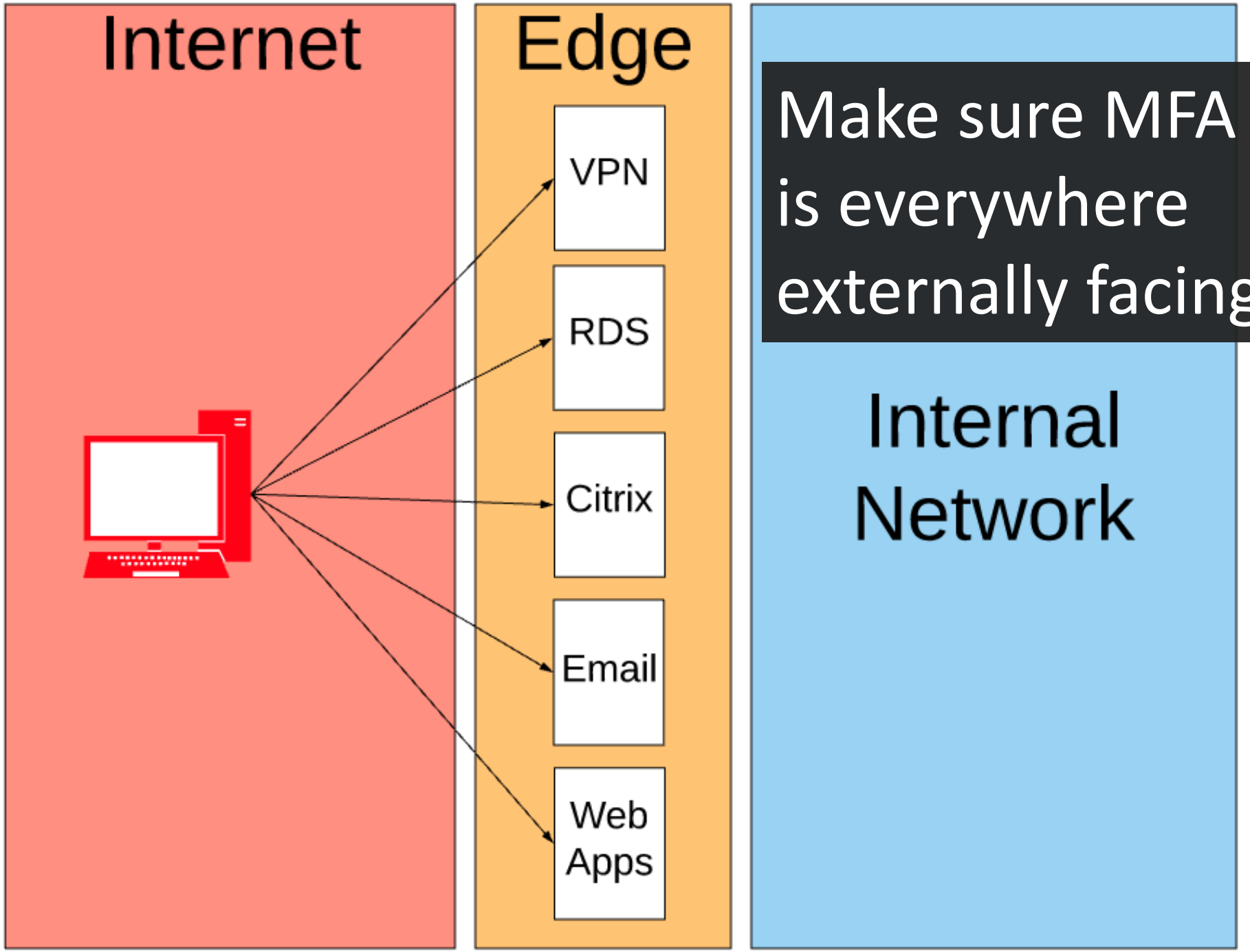
> Countermeasures: Modern Authentication

- Three types of set up:
  - Pure on-premise (*coming in Exchange 2019*): AD FS 2016, Outlook 2016, EX 2013/2016
  - Hybrid: On-premise AD FS, Outlook 2013/2016, and O365 Azure Active Directory
  - Pure O365: Modern Auth is automatically enabled for Office 2016 clients, and can work with 2013

> Countermeasures: Use it or lose it

- Modern Windows Outlook clients use MAPI/HTTP, and most mobile devices use ActiveSync. RPC/HTTP is only used by older versions of Outlook, and can be disabled if not used.

- EWS is used by Outlook for Mac, if there are no Mac's in the organization using EWS then disable/restrict it.


Internet
Edge
VPN
RDS
Citrix
Email
Web Apps
Make sure MFA is everywhere externally facing
Internal Network

> Countermeasures: Firewall spot check

- Ensure TCP 139/445 and UDP 137/138 are blocked outbound at the perimeter
- Split tunnel VPNs leave a gap, as well as any lack of requirement on VPN use to access web
- It is not uncommon for IPv6 to be forgotten

> Contributors

Jeremy Young
MSP Partner Manager @ Duo

Scott MacDonald
Sales engineer, MSP @ Duo

Tom Gallagher
Principal Group Engineering Manager @ MSFT

> \x00

Thank you DEFCON 26!

https://github.com/QuickBreach/ExchangeRelayx.git

William Martin
@QuickBreach