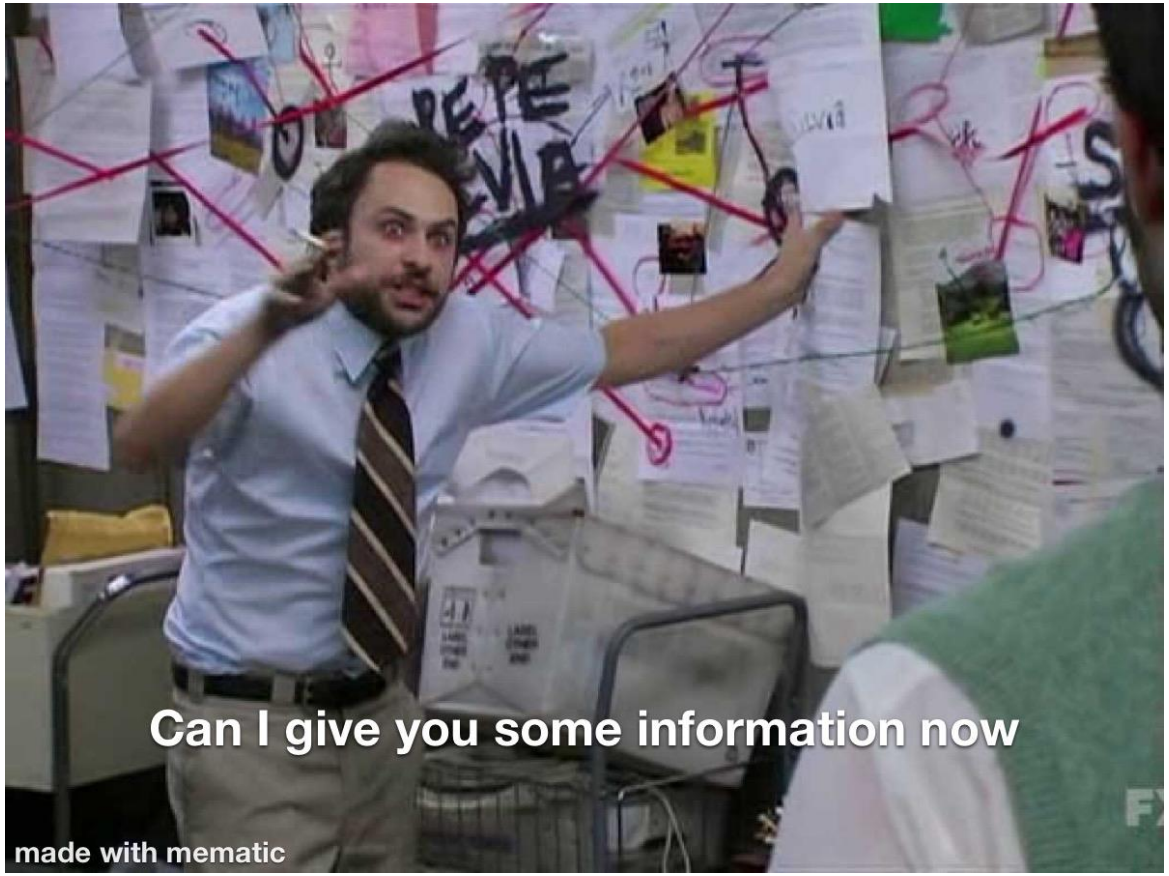
Securing Your Azure Cloud

Secrets From a Cloud Penetration Tester

Slides will be on Github
https://github.com/rootsecdev/Presentations

Insecure by Default: The hidden complexity of cloud security
https://www.youtube.com/watch?v=MPlRh8K1Igo



WHOAMI: Hacking Your Cloud

Boldy Exploring All Cloud Misconfigurations

WHOAMI

Edwin David
Security Consultant for TrustedSec (Force Cloud Practice)
Azure Cloud Penetration Testing
Twitter: @rootsecdev

Background/Certifications:
System Administrator 12+ years with focus on Active Directory/Azure Security

- M365 Security Administrator (MS500)
- Azure Security Engineer Associate (AZ500)
- Security Operations Analyst Associate (SC200)
- Azure Fundamentals (AZ900)

Adventures In Cloud Hacking

Adventures In Cloud Hacking

Who hacked my cloud?

Attack Phases:
- Recon
- Weak Password Spraying
- Bypassing MFA with Tokens
- I'm in Azure now what?
- SharePoint Online
- Finding insecure storage
- Conditional Access Policy Misconfigurations
- Pivoting with overly permissive Applications

Reconnaissance

Reconnaissance

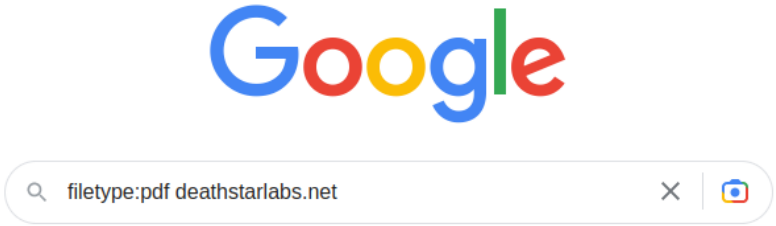
Looking at Azure Tenants with AADInternals

```
PS C:\Users\pentest> Invoke-AADIntReconAsOutsider -Domain skywalkerlabs.net | Format-Table
Tenant brand:       skywalkerlabs
Tenant name:        skywalkerlabs
Tenant id:          c77f09a5-4134-4cff-a600-5d8faa906a95
Tenant region:      NA
DesktopSSO enabled: True
MDI instance:       skywalkerlabs.atp.azure.com

Name                              DNS   MX  SPF DMARC Type    STS
----                              ---   --  --- ----- ----    ---
deathstarlabs.net                True True True False Managed
skywalkerlabs.mail.onmicrosoft.com True True True False Managed
skywalkerlabs.net                True True True  True Managed
skywalkerlabs.onmicrosoft.com    True True True False Managed
```

Reconnaissance

Determining email address formats
- Examine PDF's with Exiftool
- Dehashed
- Hunter.io

Social Media Hunting
- LinkedIn

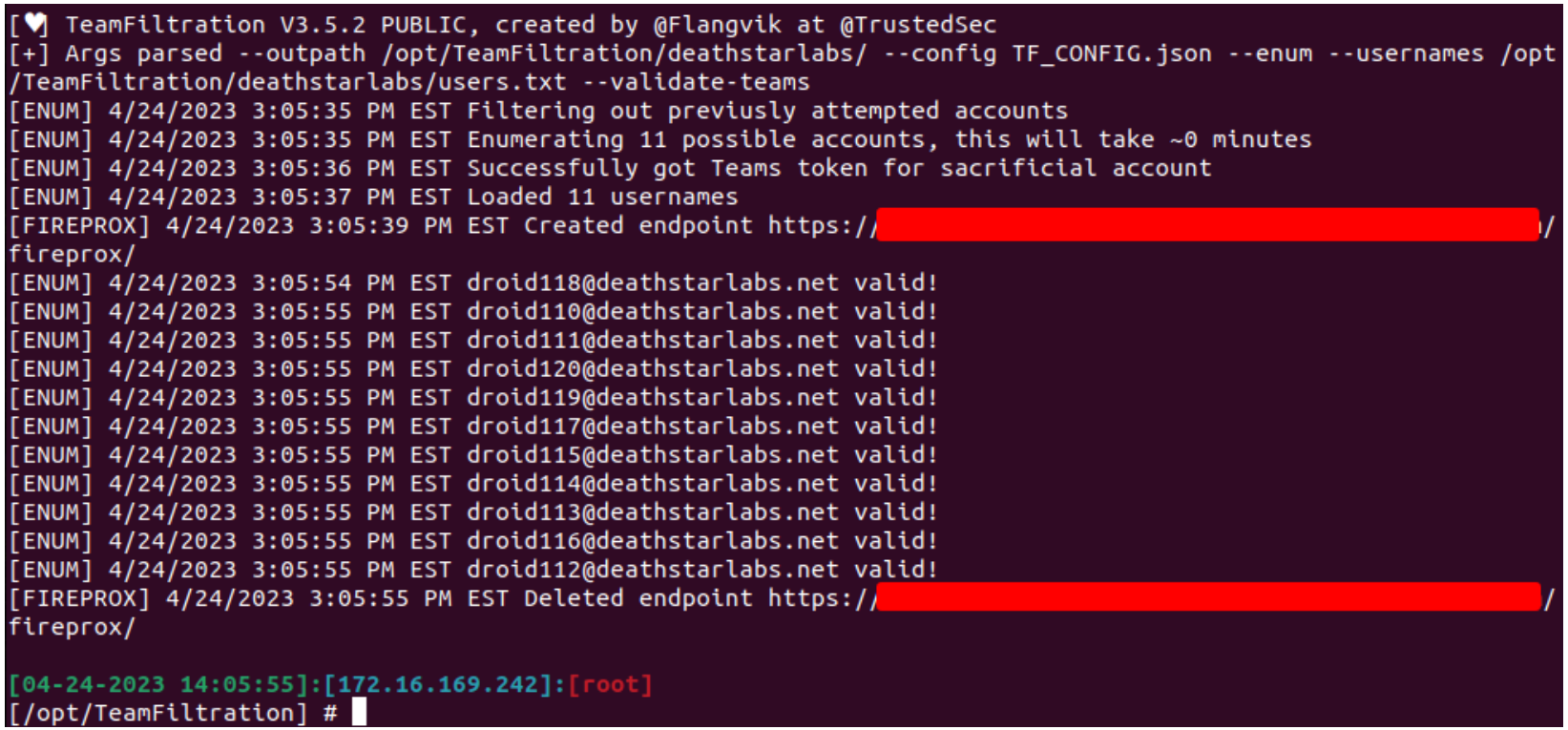



```
┌──(kali㉿hacklab)-[~/Downloads]
└─$ exiftool Droid\ 112\ Notes.pdf
ExifTool Version Number         : 12.57
File Name                       : Droid 112 Notes.pdf
Directory                       : .
File Size                       : 46 kB
File Modification Date/Time     : 2023:04:28 07:38:15-05:00
File Access Date/Time           : 2023:04:28 07:39:41-05:00
File Inode Change Date/Time     : 2023:04:28 07:39:41-05:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 1
Language                        : en-US
Tagged PDF                      : Yes
XMP Toolkit                     : 3.1-701
Producer                        : Microsoft® Word for Microsoft 365
Creator                         : Droid112
Creator Tool                    : Microsoft® Word for Microsoft 365
Create Date                     : 2023:04:28 05:35:21-07:00
Modify Date                     : 2023:04:28 05:35:21-07:00
Document ID                     : uuid:872072DE-1FED-41C0-8627-CDE83C3C5B87
Instance ID                     : uuid:872072DE-1FED-41C0-8627-CDE83C3C5B87
Author                          : Droid112
```

Reconnaissance

TeamFiltration
Github:
https://github.com/Flangvik/TeamFiltration

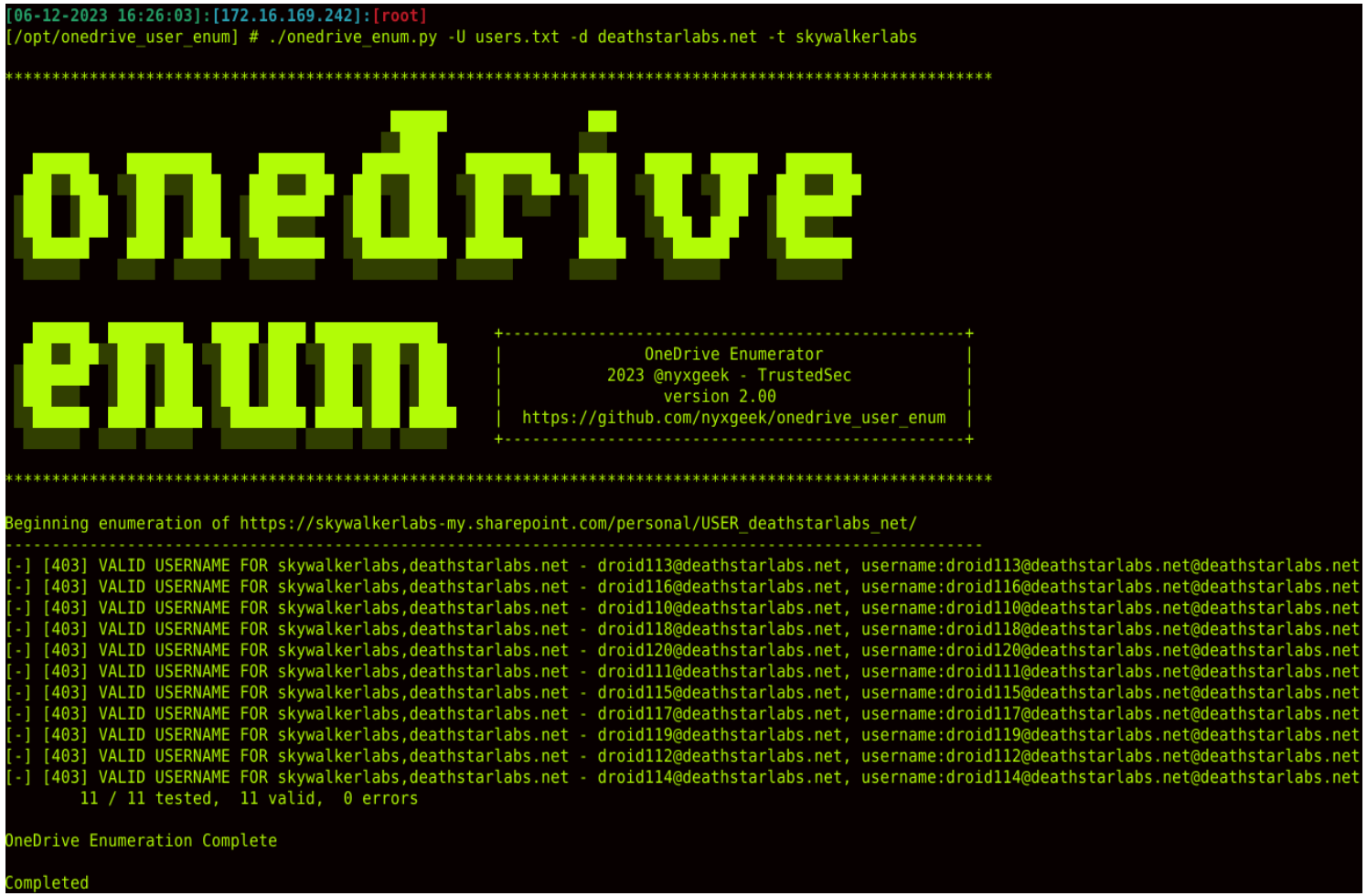
- Enumerate Valid accounts with MS Teams (no logs)
- Password Spray over Fireprox
- Automatically creates and breaks down fireprox endpoints
- Wordlist capabilities on user enumeration
- Exfil modules
- Interactive Database capabilities
- validate-msol (if all else fails)



Reconnaissance

One Drive User Enumeration (2.0)
Github:
https://github.com/nyxgeek/onedrive_user_enum

- Enumerate users with OneDrive for Business Accounts
- Produces no logs in the AAD tenant that recon activities are occurring
- Can add additional sanity checks with TeamFiltration Usage
- Supports wordlist functionality



Reconnaissance

Hard Truths on Recon:

- Very little blue teams can do to stop this activity
- Produces no logs depending on enumeration methods used
- Can be used to conduct both phishing/password spraying after valid account retrieval
- Shines spotlight on insecure MFA Methods/weak passwords

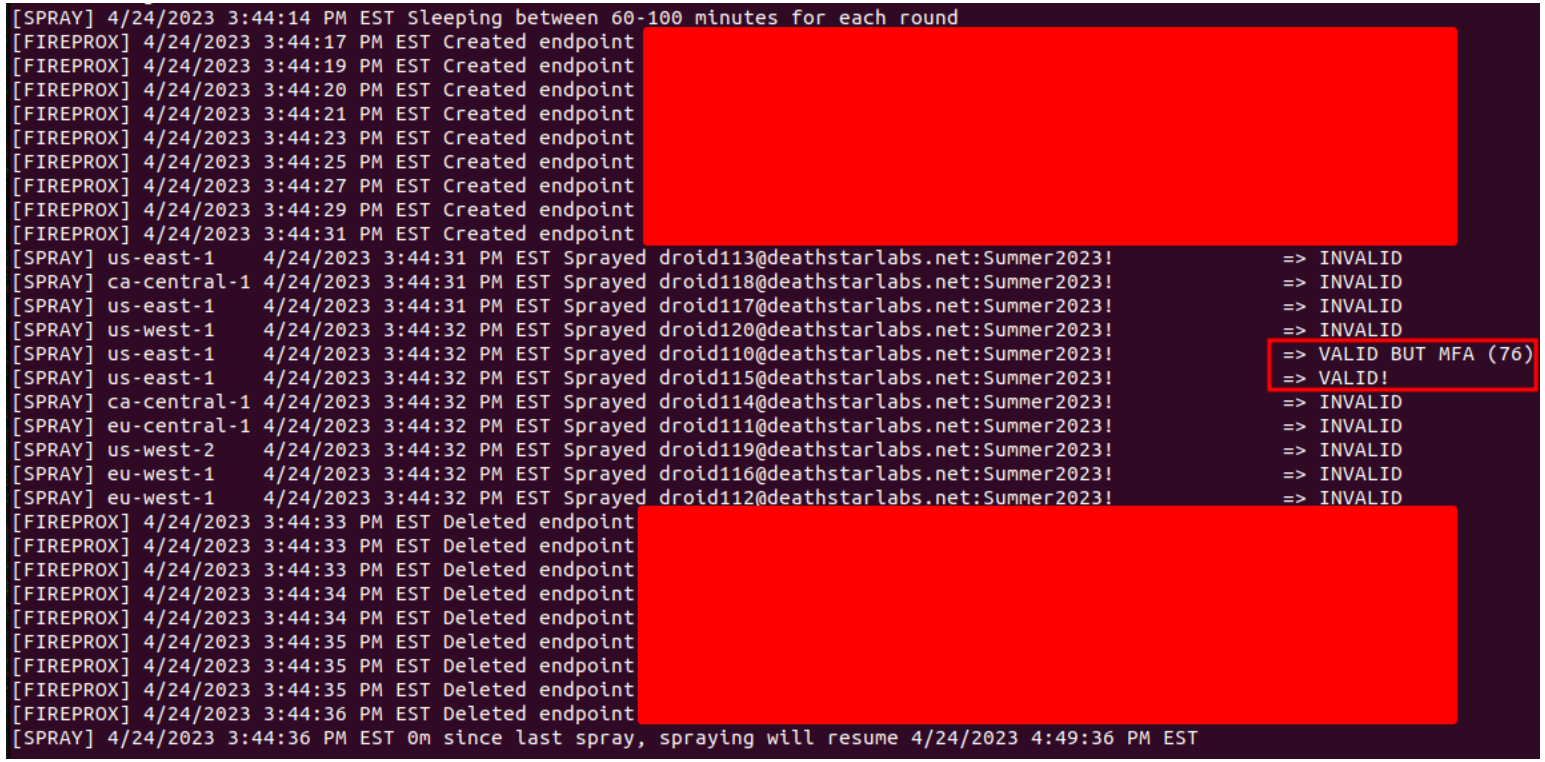
Weak Password Spraying

Mutilple Toolsets to conduct password spraying

- TeamFiltration
- MSOLSpray
- O365Spray
- Credmaster

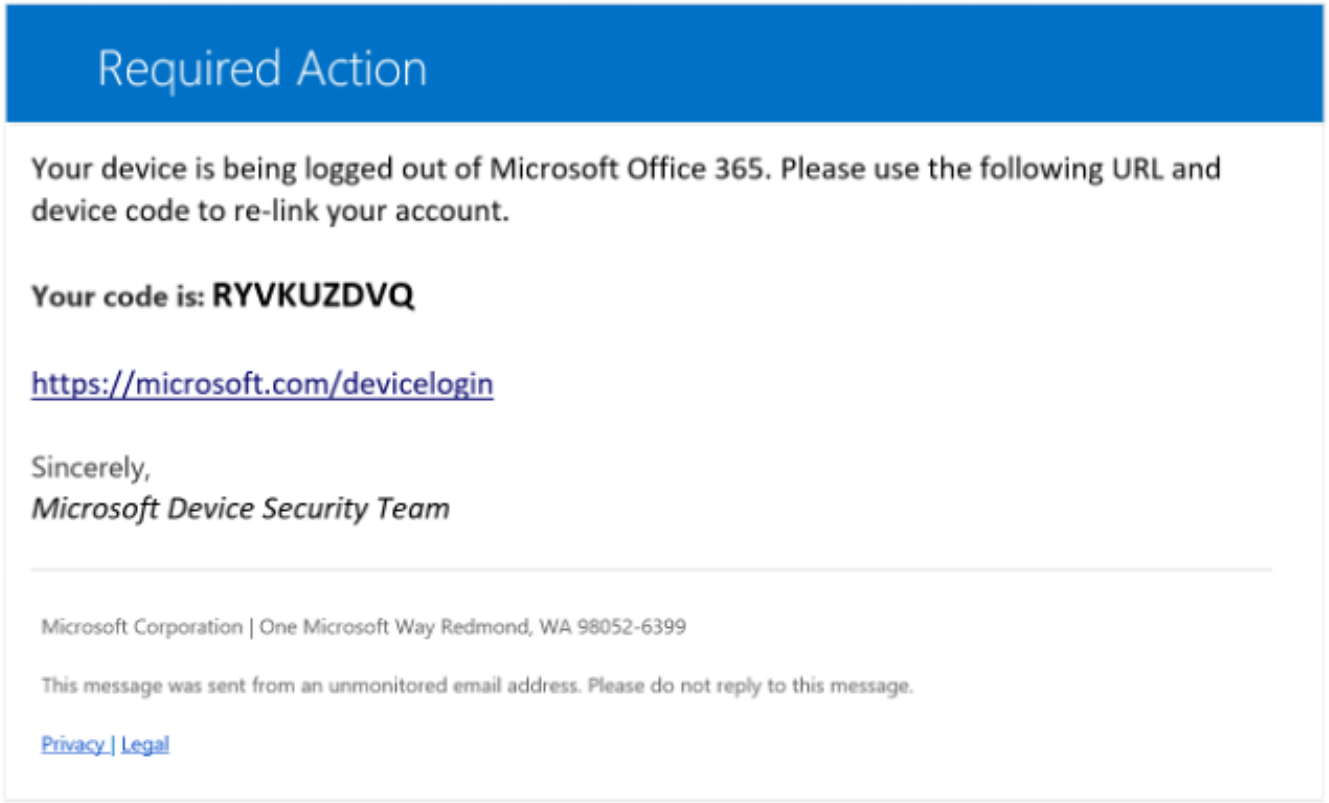
Password Spraying OPSEC

- All tools mentioned above support fireprox for Azure Smart Lockout avoidance (within limits)
- Ideal toolsets will let you randomize user agent strings
- Mobile device agents are ideal because of atypical travel dismissal
- Time Limited. Azure machine learning will eventually pick up on password spraying activities and block you.

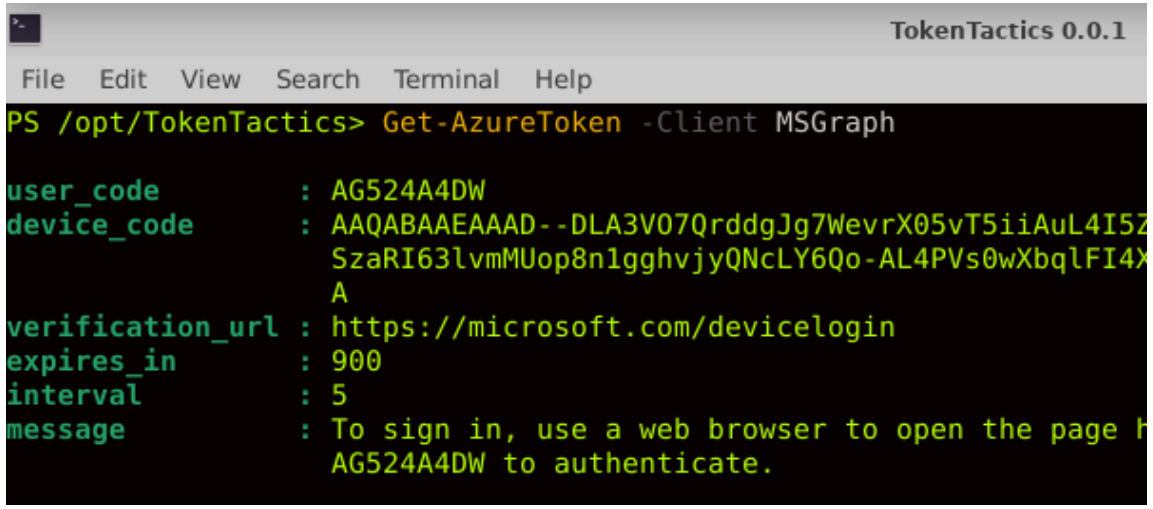


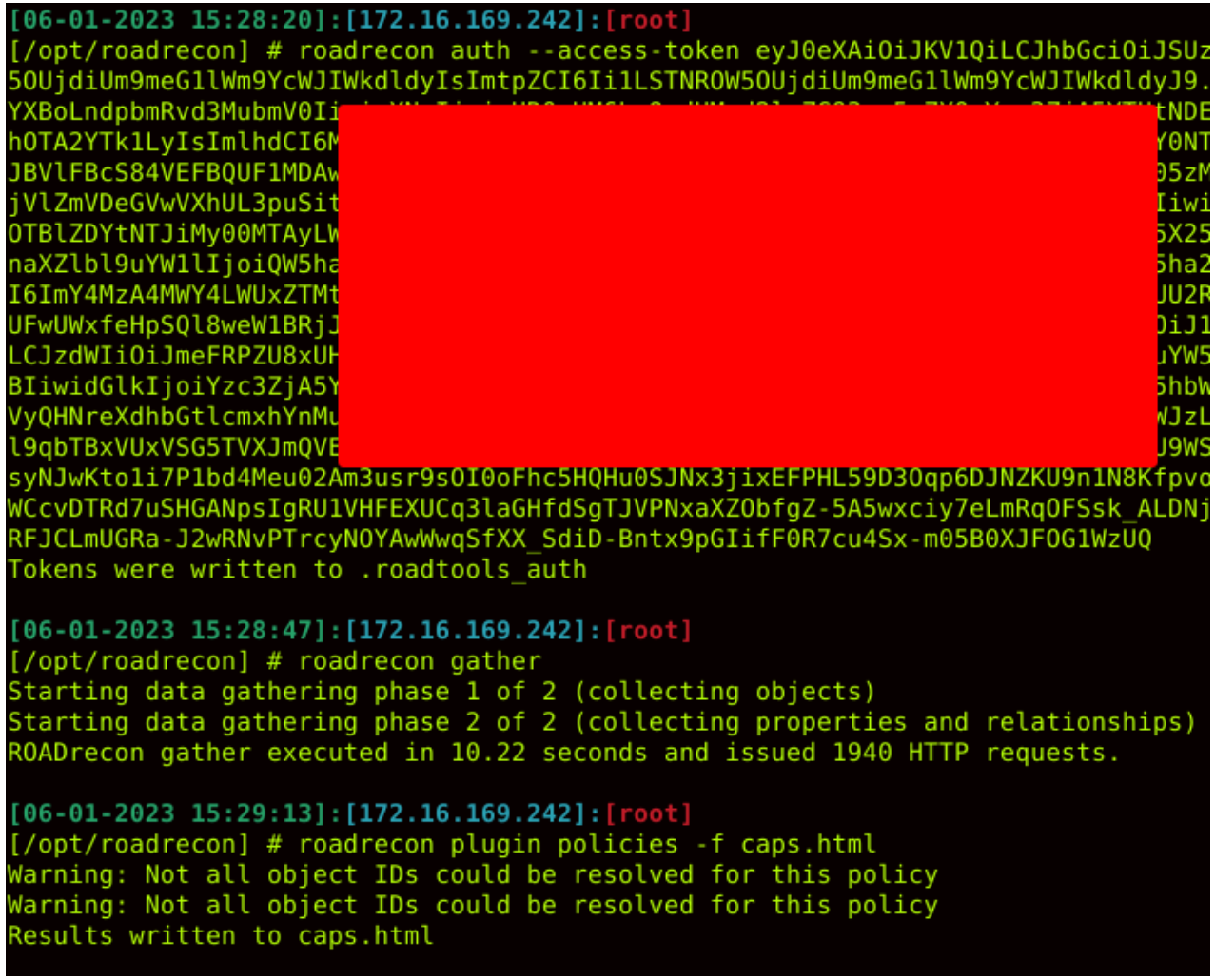
Bypassing MFA/Token Stealing

Sample Scenario: Device Code Phishing



Bypassing MFA/Token Stealing





Bypassing MFA/Token Stealing

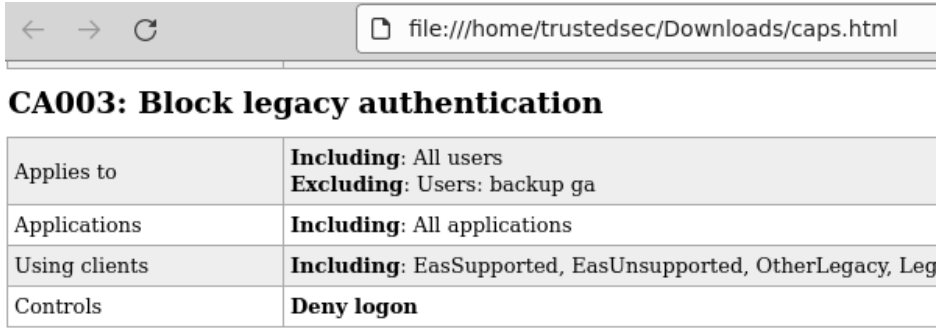
Tools and Techniques to Steal Tokens

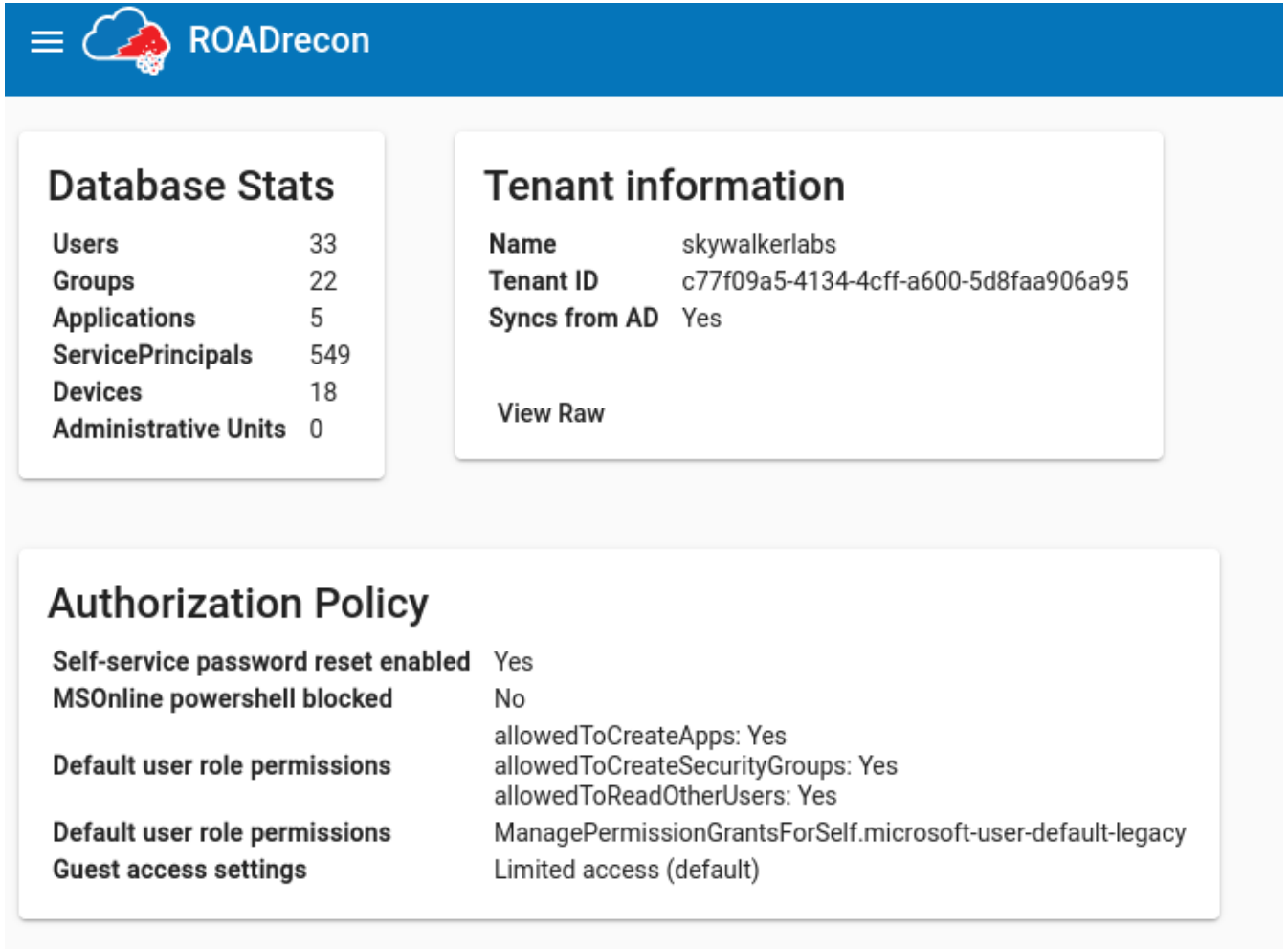
- TokenTactics: https://github.com/rvrsh3ll/TokenTactics
- TokenTacticsV2: https://github.com/f-bader/TokenTacticsV2
- Cobalt Strike BoF: https://github.com/trustedsec/CS-Remote-OPs-BOF

Active Recon with Tokens

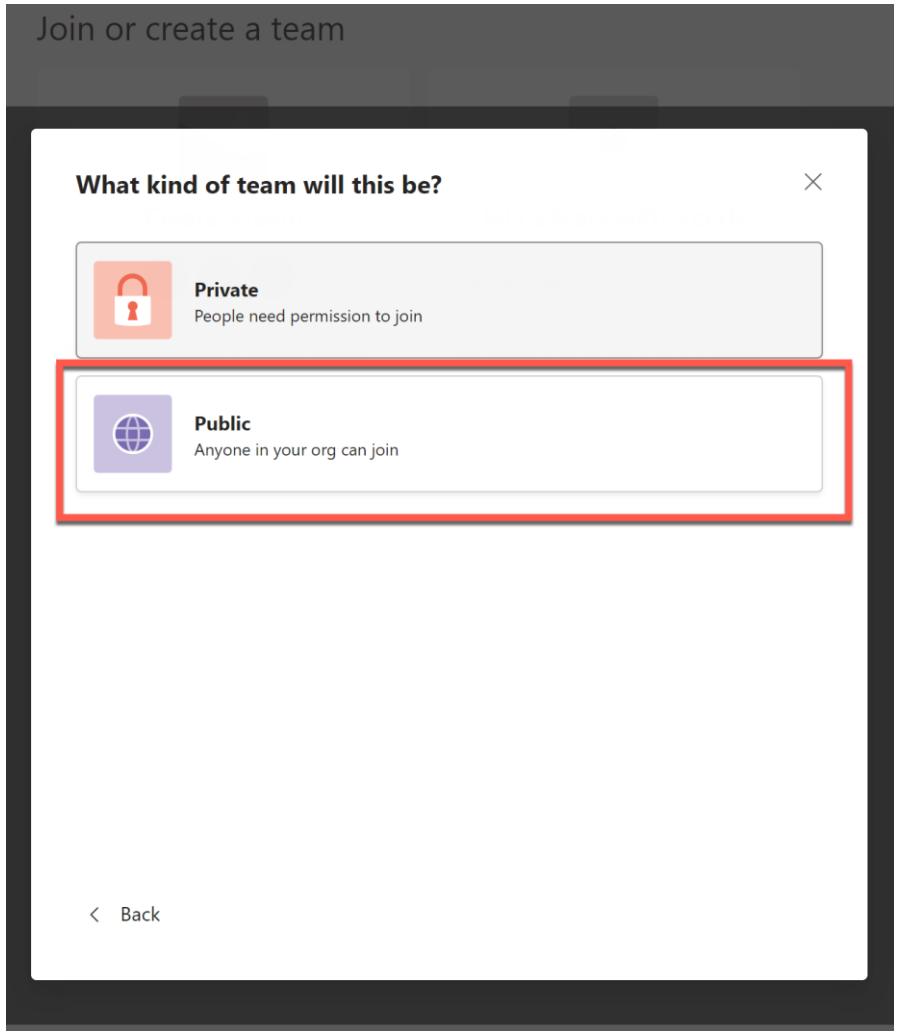
ROADRecon
Github:
https://github.com/dirkjanm/ROADtools

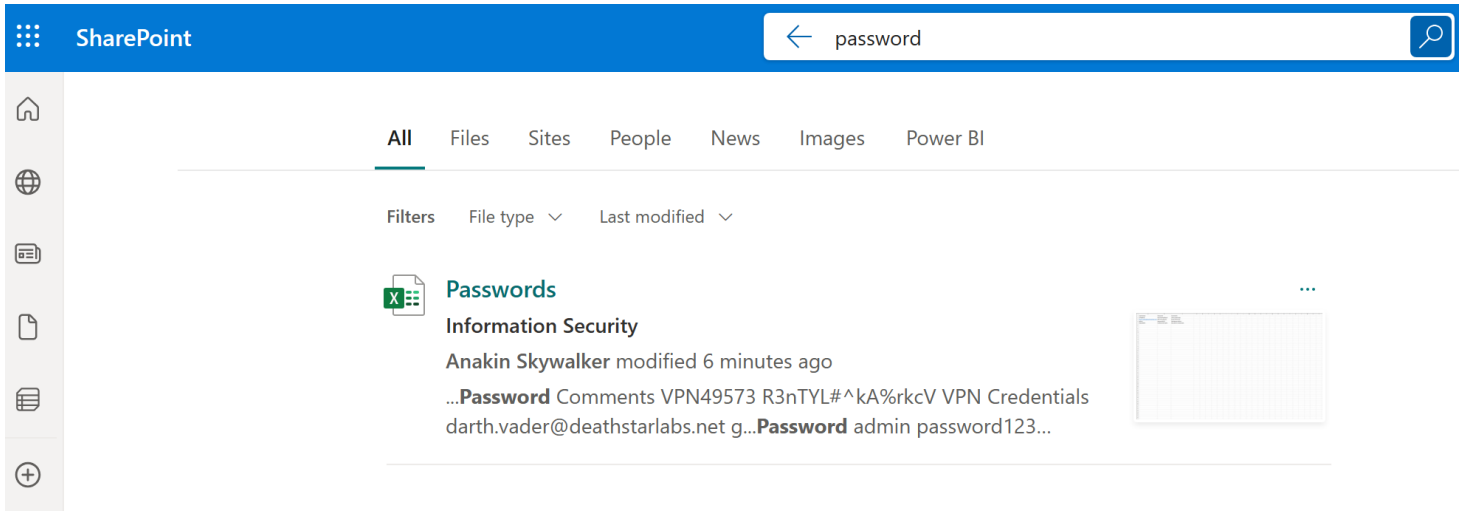
- ROADrecon can be used with MS Graph Tokens
- Will pull out Users, Groups, RBAC roles, Applications
- Database can be used to parse out Conditional Access Policies
- Requires low level end user access
- Rarely encounter conditional access resistence





Pivoting With SharePoint Online





- Public Teams channels create public SharePoint Online Sites
- Authenticated Users have access to any files that are shared in the Teams channel or on SharePoint site
- Creates confusion among teams when they start collaborating on data that should remain private
- SharePoint Online is a data goldmine for penetration testers and red team operators

Pivoting With Azure Storage Accounts

Detecting Public Storage Blobs
- Google Searches
- **Microburst (Tooling - Requires Authentication)**
- Github Searches
- Inspecting Code on target website

```
VERBOSE:  Listing out public blob files for the nsagov1 storage account...
VERBOSE:   Writing available containers to nsagov1-Containers.csv
VERBOSE:   Found Public Container - secrets
VERBOSE:    Public File Available: Confidential.docx
VERBOSE:    Public File Available: DeathStar Plans.docx
VERBOSE:    Public File Available: Rebel Base Locations.docx
VERBOSE:    Public File Available: secrets.yaml
```

This page is a partial list of the Azure domains in use. Some of them are REST API endpoints.

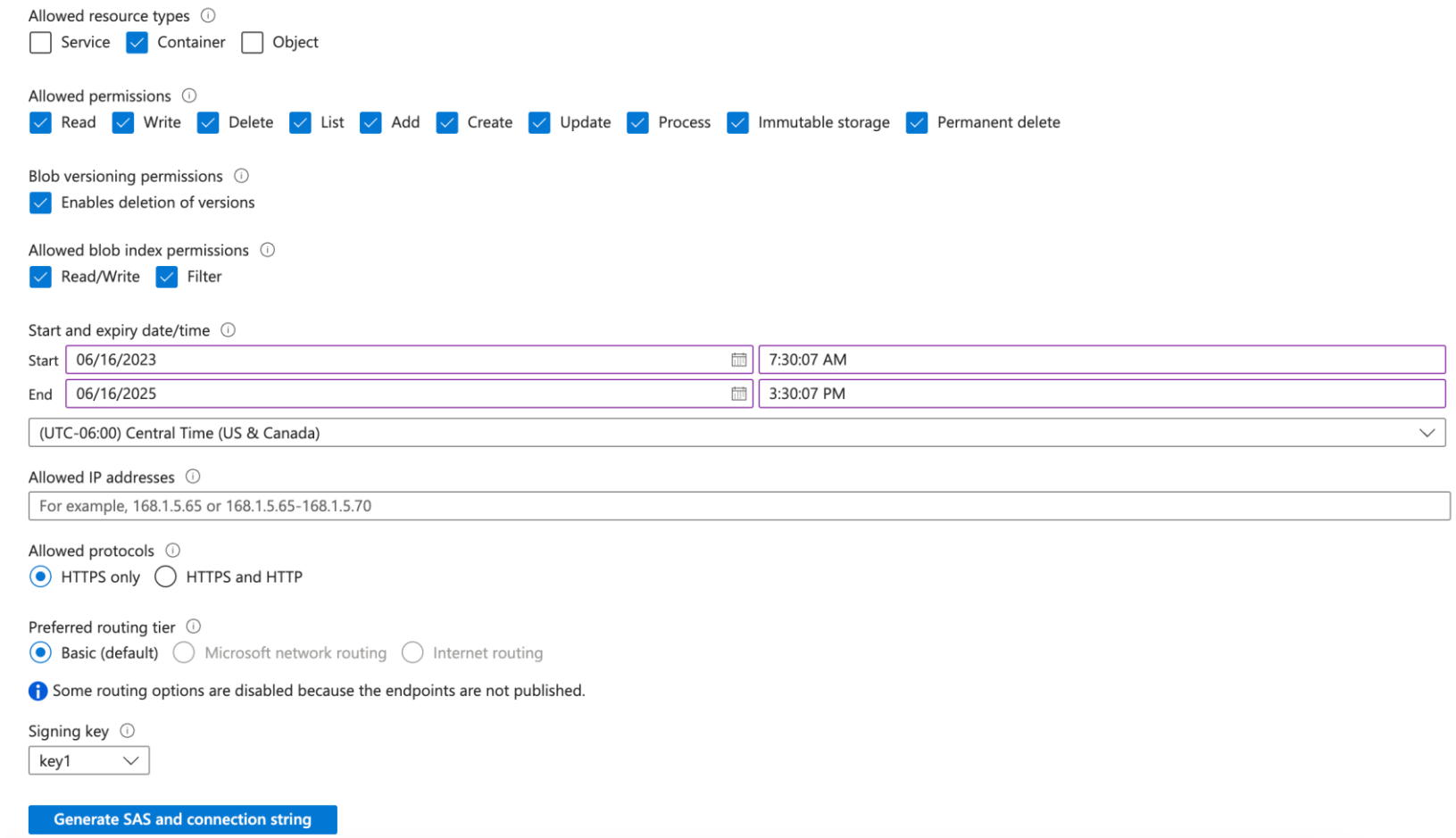
Service	Subdomain
Azure Access Control Service (retired)	*.accesscontrol.windows.net
Azure Active Directory	*.graph.windows.net / *.onmicrosoft.com
Azure API Management	*.azure-api.net
Azure BizTalk Services (retired)	*.biztalk.windows.net
Azure Blob storage	*.blob.core.windows.net
Azure Cloud Services and Azure Virtual Machines	*.cloudapp.net
Azure Cloud Services and Azure Virtual Machines	*.cloudapp.azure.com

Source: https://learn.microsoft.com/en-us/azure/security/fundamentals/azure-domains

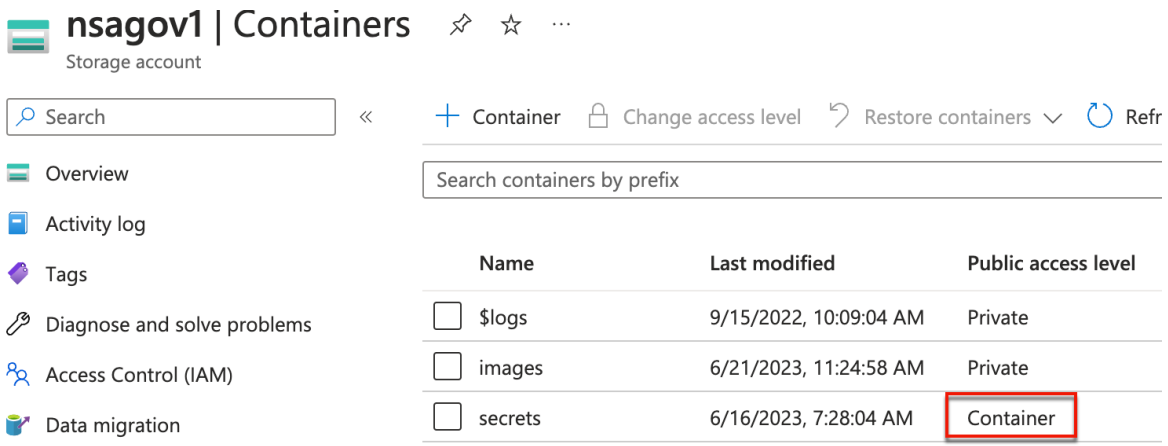
Pivoting With Azure Storage Accounts

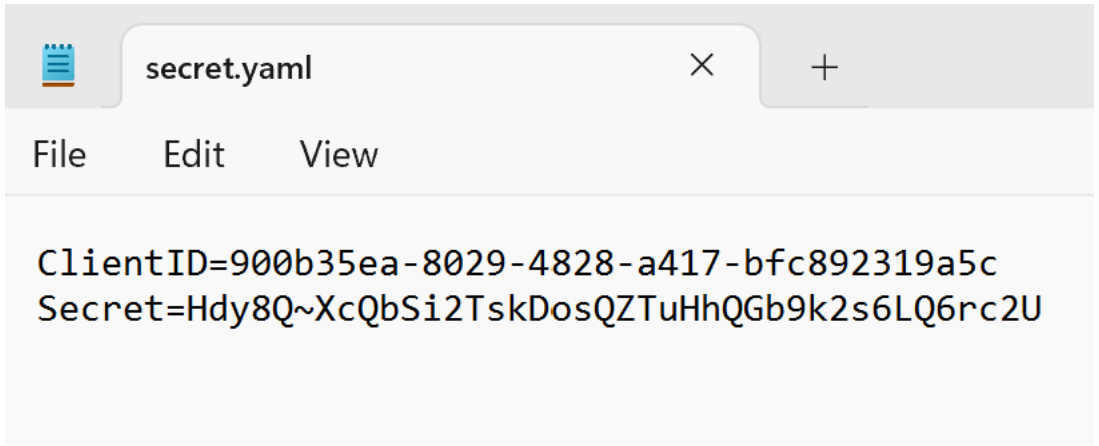
Two Main Threats
- Storage Public Blobs
- **SAS Tokens**

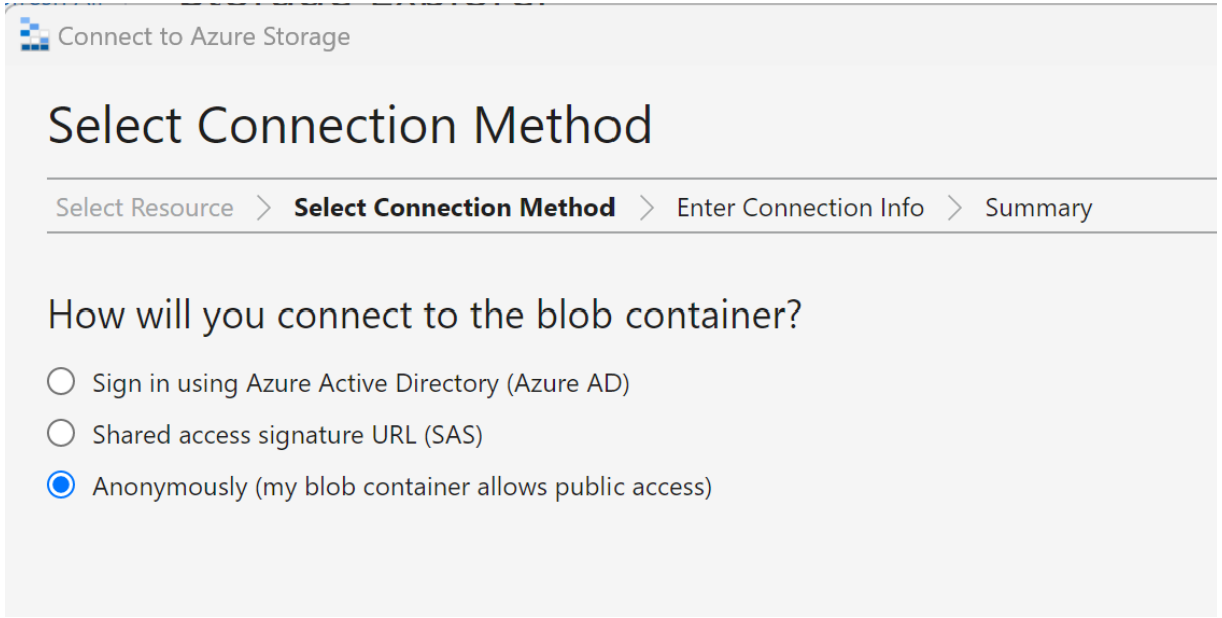
SAS Tokens
- Tracking issues: who has them?
- Azure Deployment logs
- Github Code repositories
- Incorrectly deployed azure keyvaults



Pivoting With Azure Storage Accounts







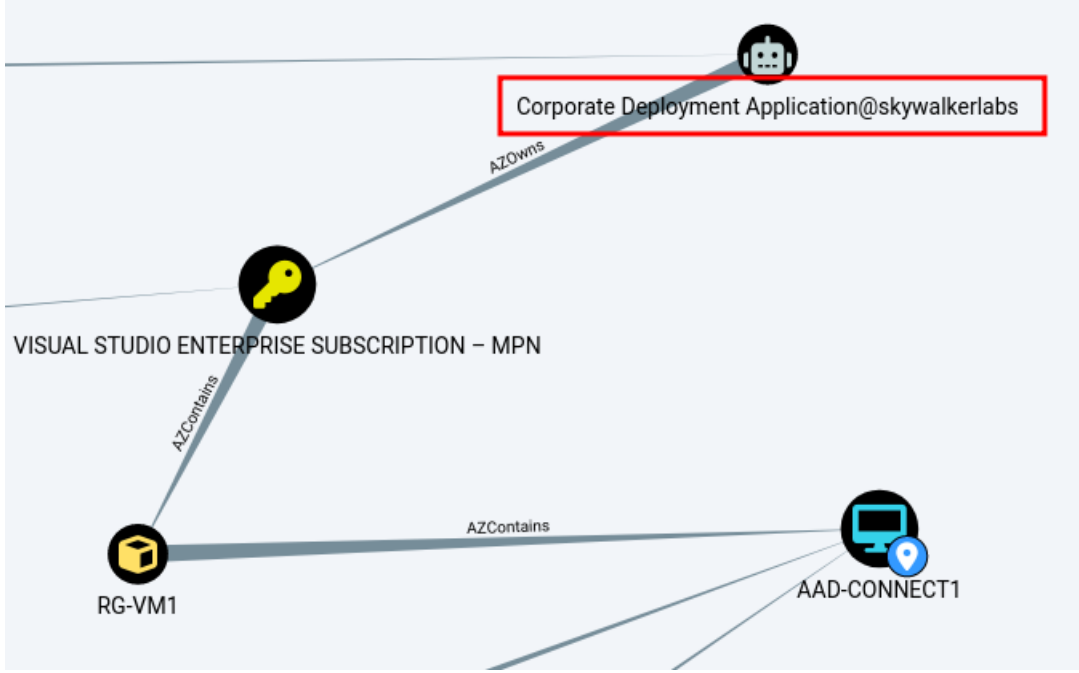
ClientID Hunting

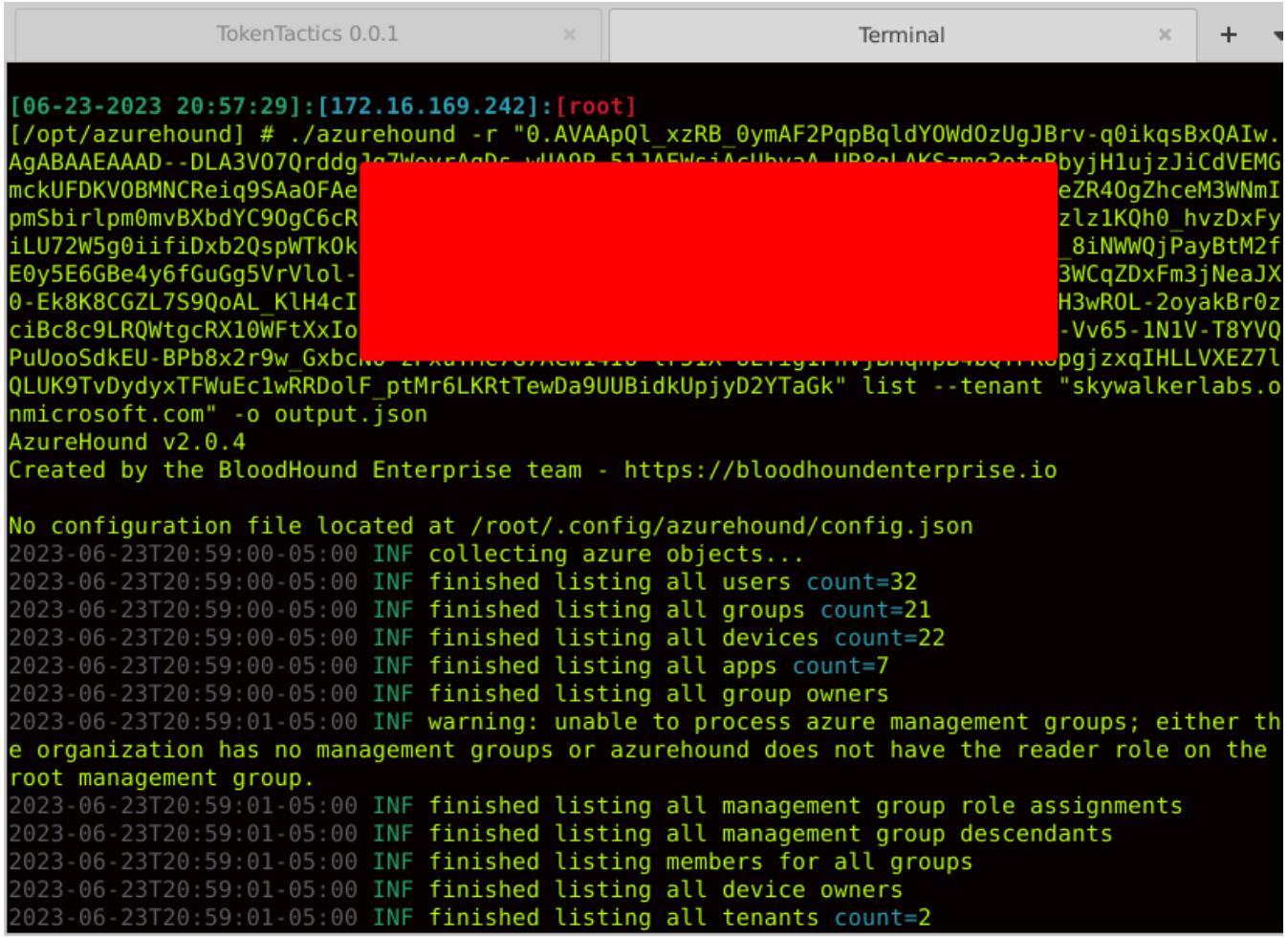
```
PS C:\Users\pentest> az login --allow-no-subscription
A web browser has been opened at https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize. Please continue
the login in the web browser. If no web browser is available or if the web browser fails to open, use device code flow w
ith `az login --use-device-code`.
The following tenants don't contain accessible subscriptions. Use 'az login --allow-no-subscriptions' to have tenant lev
el access.
c77f09a5-4134-4cff-a600-5d8faa906a95 'skywalkerlabs'
[
  {
    "cloudName": "AzureCloud",
    "id": "c77f09a5-4134-4cff-a600-5d8faa906a95",
    "isDefault": true,
    "name": "N/A(tenant level account)",
    "state": "Enabled",
    "tenantId": "c77f09a5-4134-4cff-a600-5d8faa906a95",
    "user": {
      "name": "droid115@deathstarlabs.net",
      "type": "user"
    }
  }
]
PS C:\Users\pentest> $graphAccessUserAsAll = az account get-access-token --scope="https://graph.microsoft.com/Directory.
AccessAsUser.All" | ConvertFrom-Json
PS C:\Users\pentest> Connect-MgGraph -AccessToken $graphAccessUserAsAll.accessToken
Welcome To Microsoft Graph!
PS C:\Users\pentest> Get-MgApplication

Id                                   DisplayName                          AppId                                SignIn
                                                                                                                  Audien
                                                                                                                  ce
--                                   -----------                          -----                                ---
[redacted]                                                                                                        Azu
                                                                                                                  Azu
                                                                                                                  Azu
                                                                                                                  Azu
                                                                                                                  Azu
653c22a4-45bb-4d2e-9fbb-041210ce4ede Corporate Deployment Application     900b35ea-8029-4828-a417-bfc892319a5c Azu
83601106-928e-451c-a76c-67a1e93fa634 Test3                                e5973f12-ccee-4754-805e-9c6e1a0ba389 Azu
```

TrustedSec

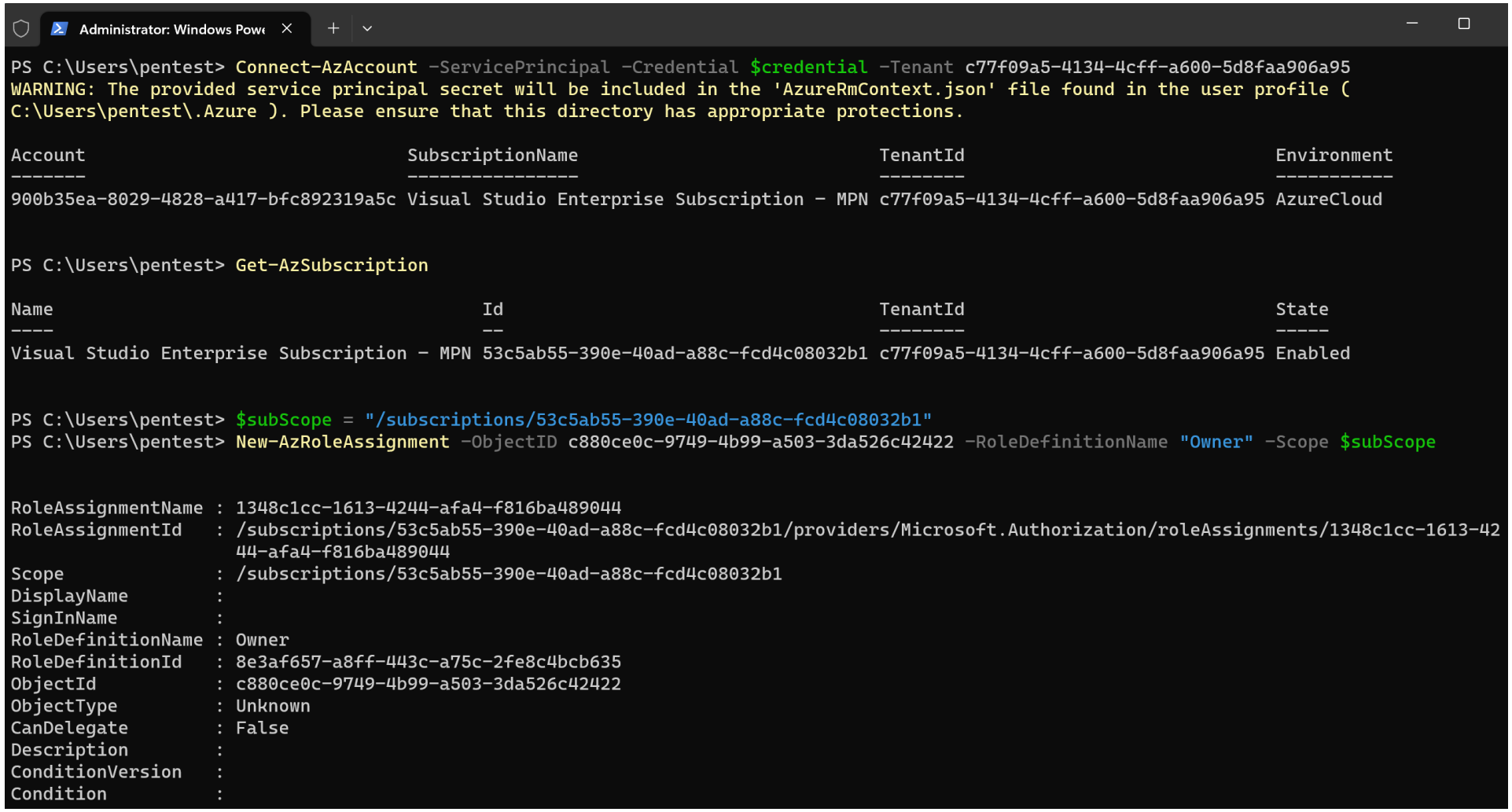
Privileged Account Takeover

Contributor/Owner Resources





Privileged Account Takeover



TrustedSec

Pivoting to Azure VM's

Home > CreateVm-MicrosoftWind

AAD-Connect1 |

Virtual machine

Search

- Backup
- Disaster recovery
- Updates
- Inventory
- Change tracking
- Automanage
- Configuration management (Preview)
- Policies
- Run command

Monitoring

- Insights
- Alerts
- Metrics

Run Command Script

RunPowerShellScript

Script execution complete

PowerShell Script

```
1  whoami
```

Run

Output

```
nt authority\system
```

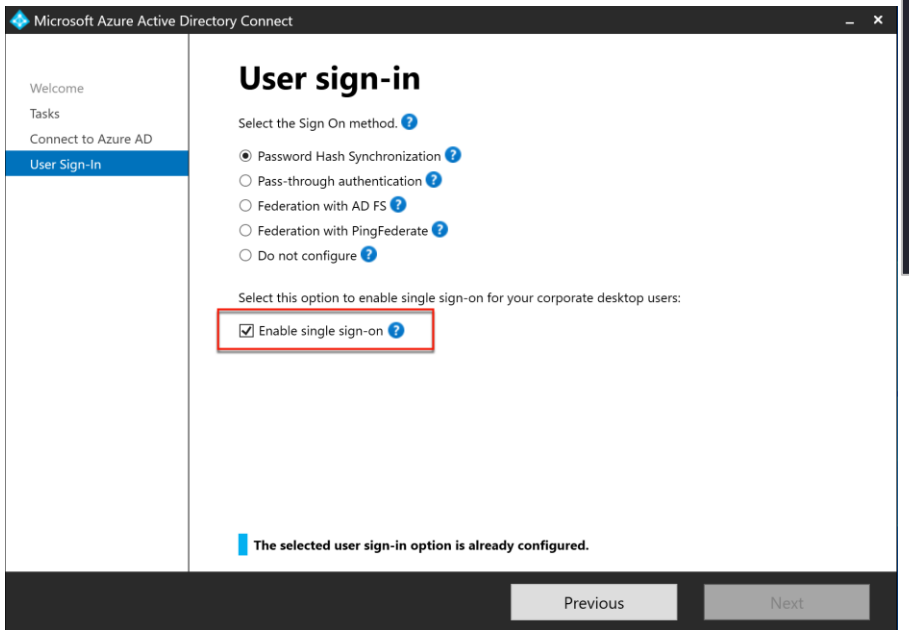
```
PS C:\projects> .\ADSyncDecrypt.ps1
AD Connect Sync Credential Extract v2 (@_xpn_)
        [ Updated to support new cryptokey storage method ]

[*] Querying ADSync localdb (mms_server_configuration)
[*] Querying ADSync localdb (mms_management_agent)
[*] Using xp_cmdshell to run some Powershell as the service user
[*] Credentials incoming...

Domain: SKYWALKERLABS.NET
Username: MSOL_d8dea9a764ab
Password: [redacted]
PS C:\projects>
```

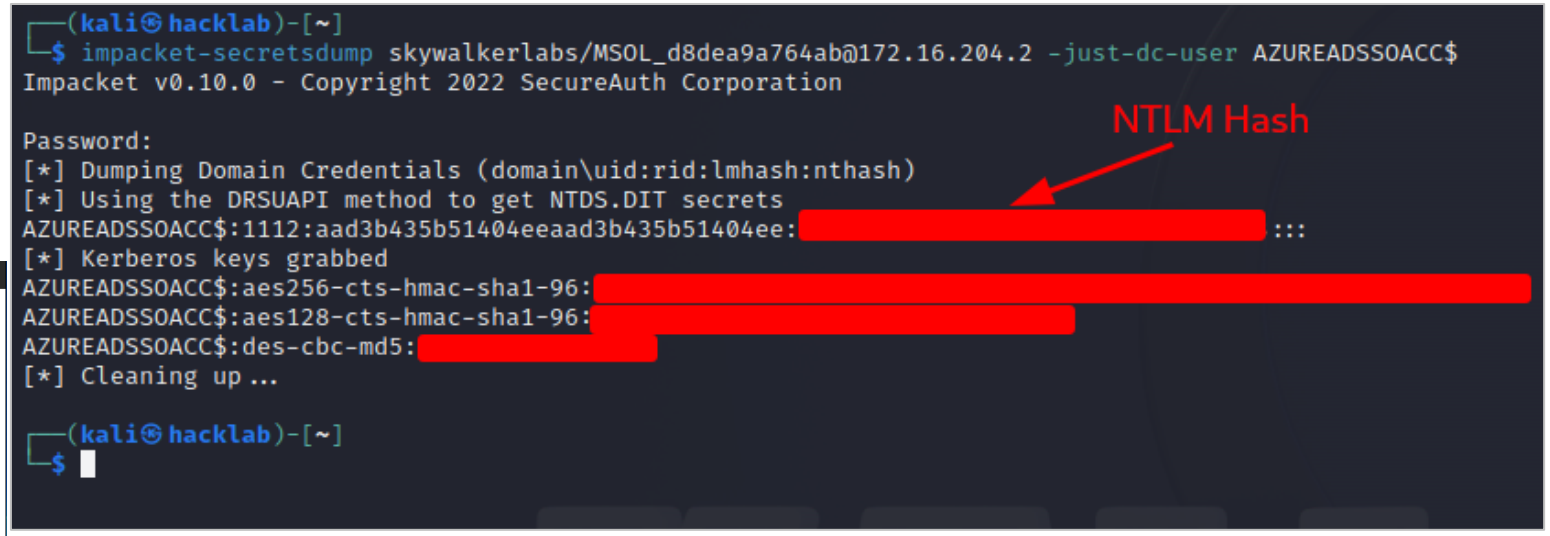
TrustedSec

Abusing Seamless SSO

How it works

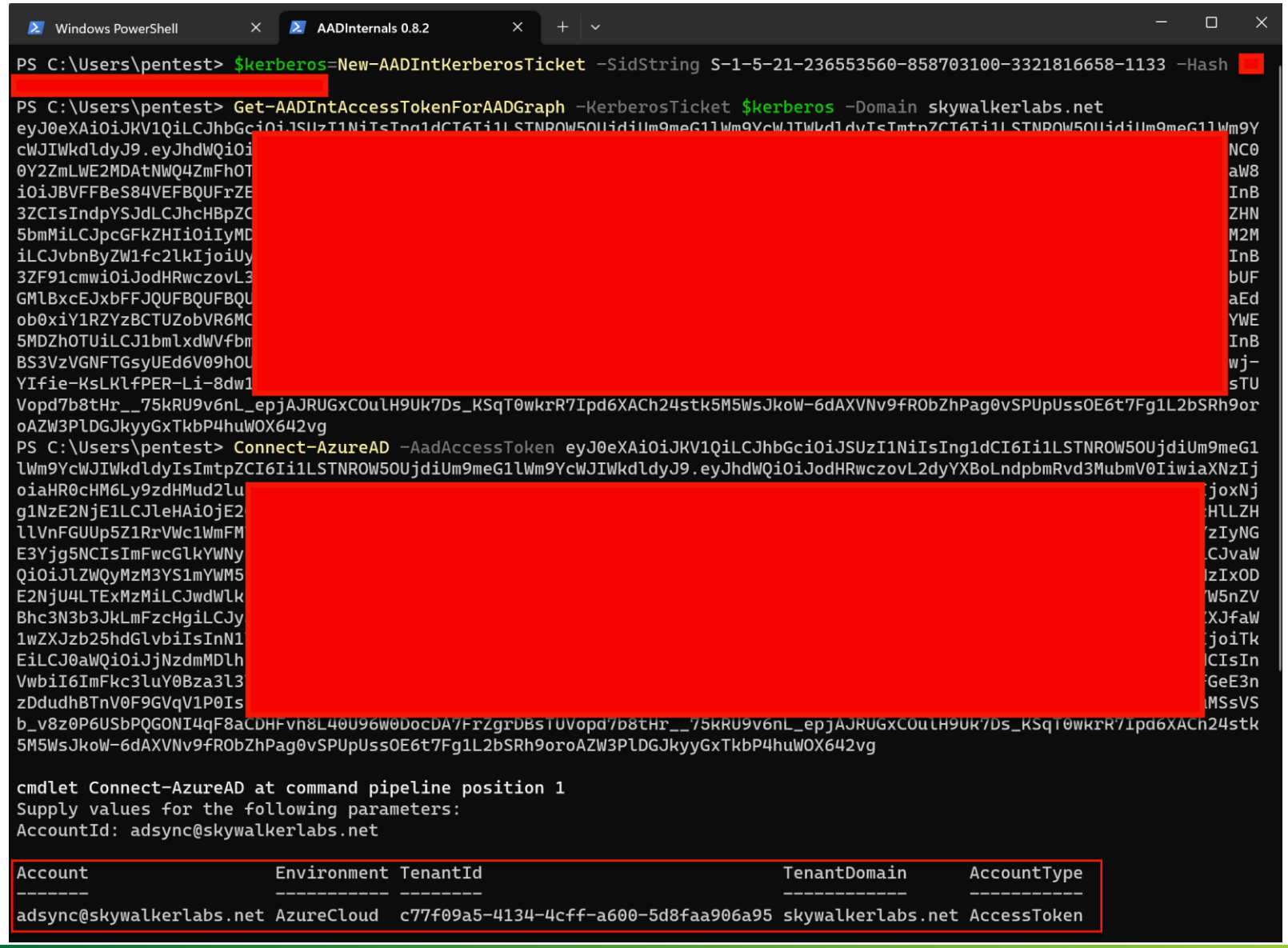
- Starts by Internal AD Compromise
- AZUREADSSOACC$ machine account hash is stolen
- Requires SSO to be turned on in Azure AD Connect





TrustedSec

Abusing Seamless SSO

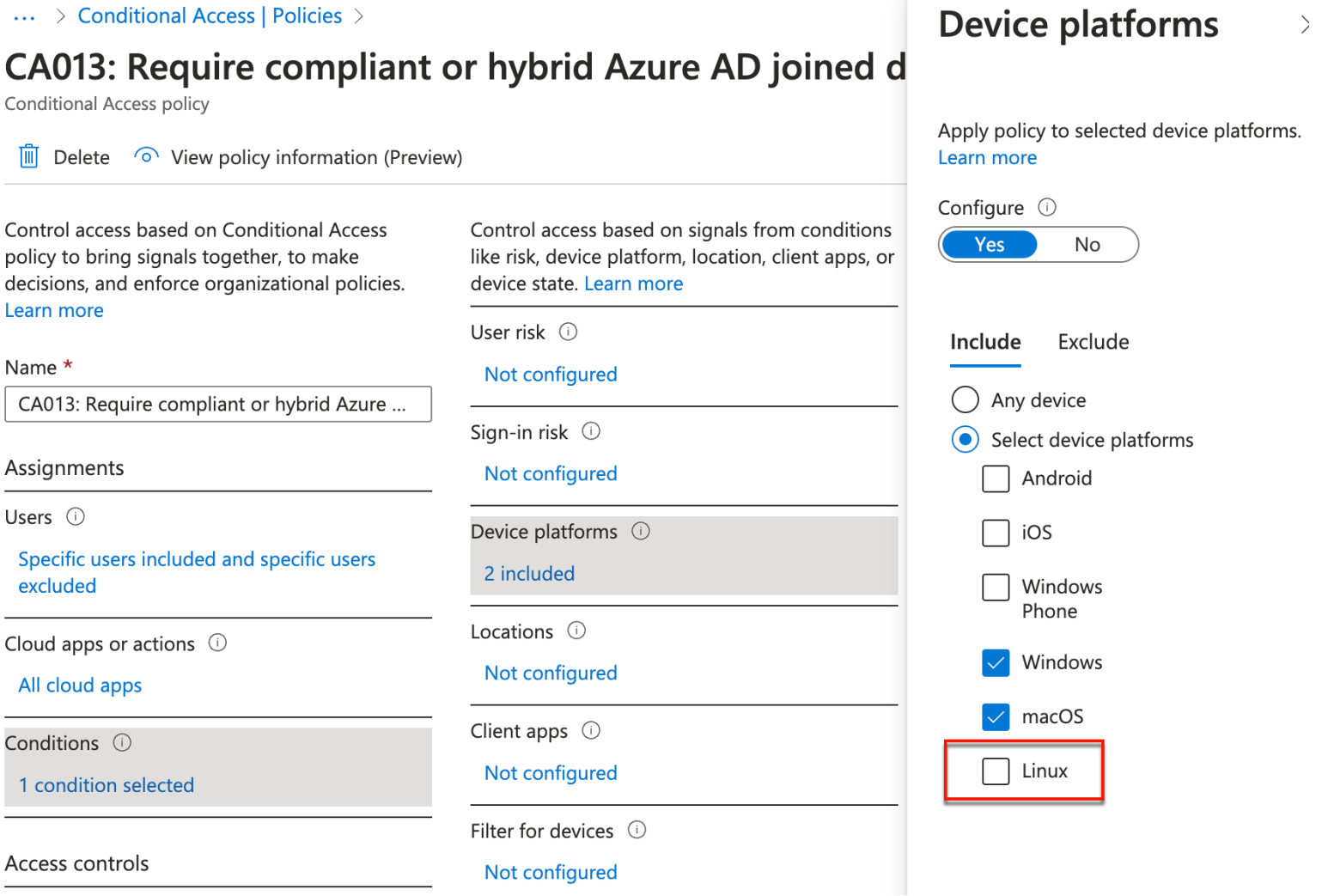


- Account Impersonation by abusing Desktop SSO
- Can request Kerberos tickets using AADInternals
- Works with any account sync'd to the cloud with exceptions around MFA
- Service Accounts are ideal to abuse since they are not enrolled into MFA

TrustedSec

Common Conditional Access Issues

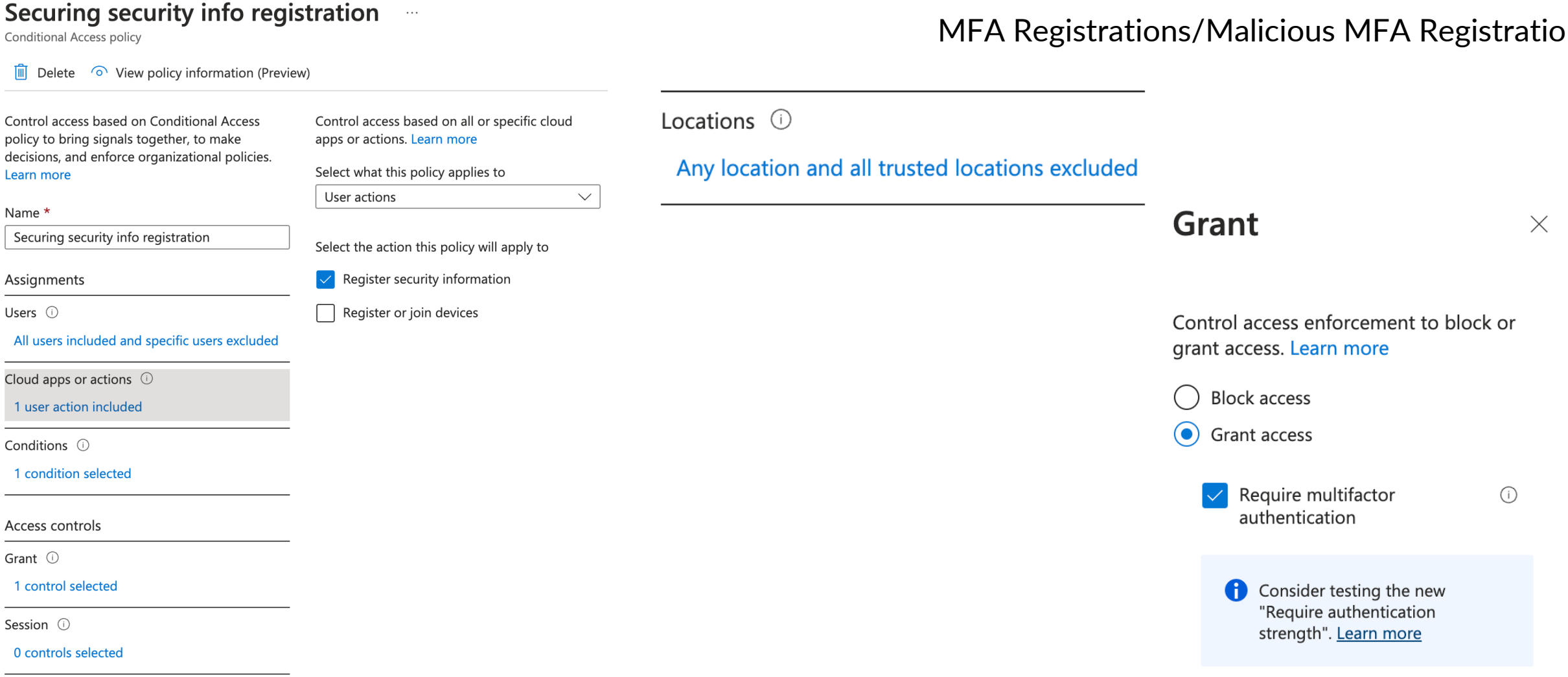
Device Platform Filtering
- Easily bypassed by switching user agent
- Linux is the most common platform that is missed



TrustedSec

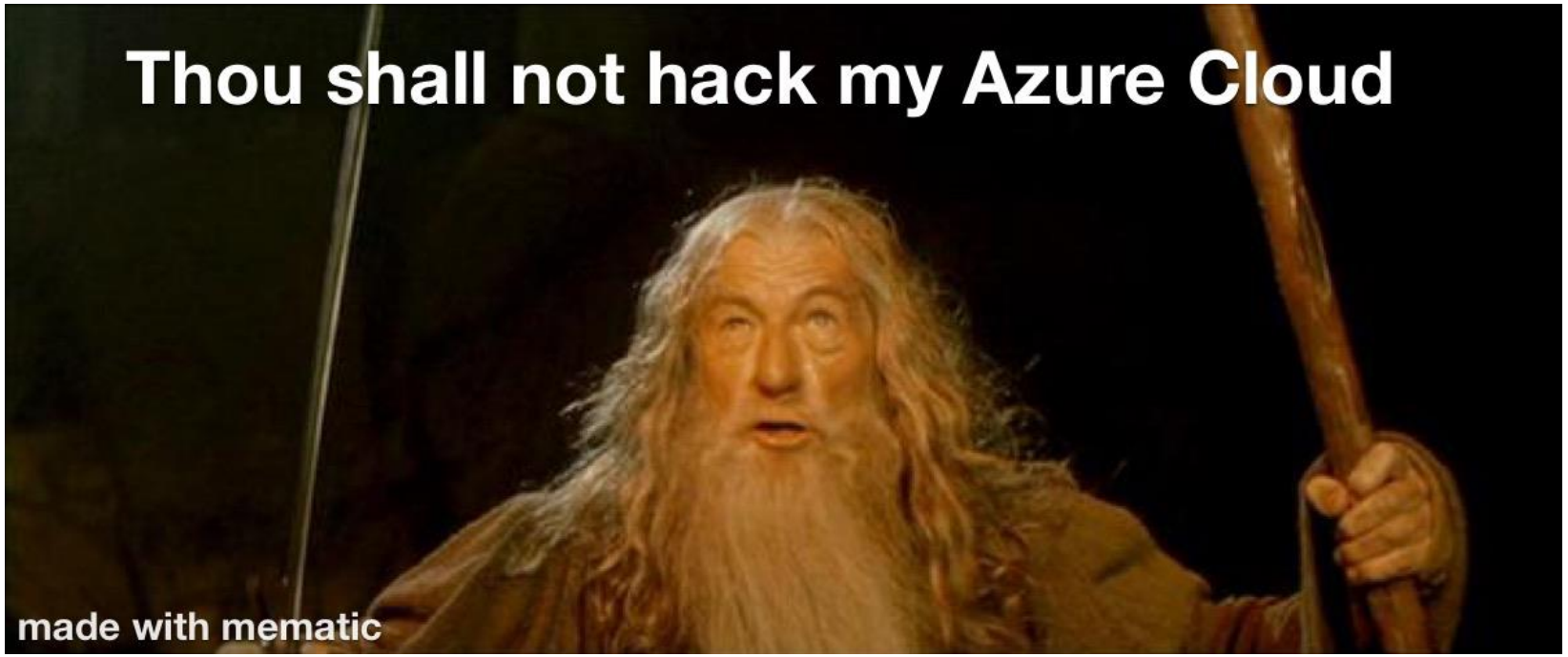
Common Conditional Access Issues

MFA Registrations/Malicious MFA Registrations



TrustedSec

Defensive Tactics



Early Warning IOC's

Active rules | **Rule templates** | Anomalies

spray | Add filter

Severity	Name	Rule type
Medium	IN USE Password spray attack against Azure AD Seamless SSO	Scheduled
Medium	IN USE Potential Password Spray Attack (Uses Authentication Normalization)	Scheduled
Medium	IN USE Password spray attack against Azure AD application	Scheduled
Medium	Password spray attack against ADFSSignInLogs	Scheduled

Strategies for password spraying detection

- Print external PDF's on company sites with honeytoken account
- Use Azure Sentinel to create a custom KQL rule query for attempted logons to honeytoken account.
- Account has to exist in Azure AD but can be disabled
- Sentinel has out of the box detections for password spraying activity

Blocking Powershell

https://learn.microsoft.com/en-us/schooldatasync/blocking-powershell-for-edu

Blocking PowerShell for EDU Tenants

Article • 02/20/2023 • 4 contributors

Feedback

In this article

- Works for Regular Enterprise Tenants

Creates Enterprise Applications
- Azure Active Directory Powershell
- Microsoft Graph Command Line
- Can control Access with users and groups

Preventing Malicious Recon

```
PS C:\Users\pentest> Disable-AADIntTenantMsolAccess

PS C:\Users\pentest> Get-AADIntTenantAuthPolicy


id                                                : authorizationPolicy
allowInvitesFrom                                  : everyone
allowedToSignUpEmailBasedSubscriptions            : True
allowedToUseSSPR                                  : True
allowEmailVerifiedUsersToJoinOrganization         : True
allowUserConsentForRiskyApps                      : False
blockMsolPowerShell                               : True
description                                       : Used to manage authorization related settings across the company.
displayName                                       : Authorization Policy
enabledPreviewFeatures                            : {}
guestUserRoleId                                   : 10dae
permissionGrantPolicyIdsAssignedToDefaultUserRole : {Mana
defaultUserRolePermissions                        : @{all
                                                    allow
                                                    allow
                                                    allow
```

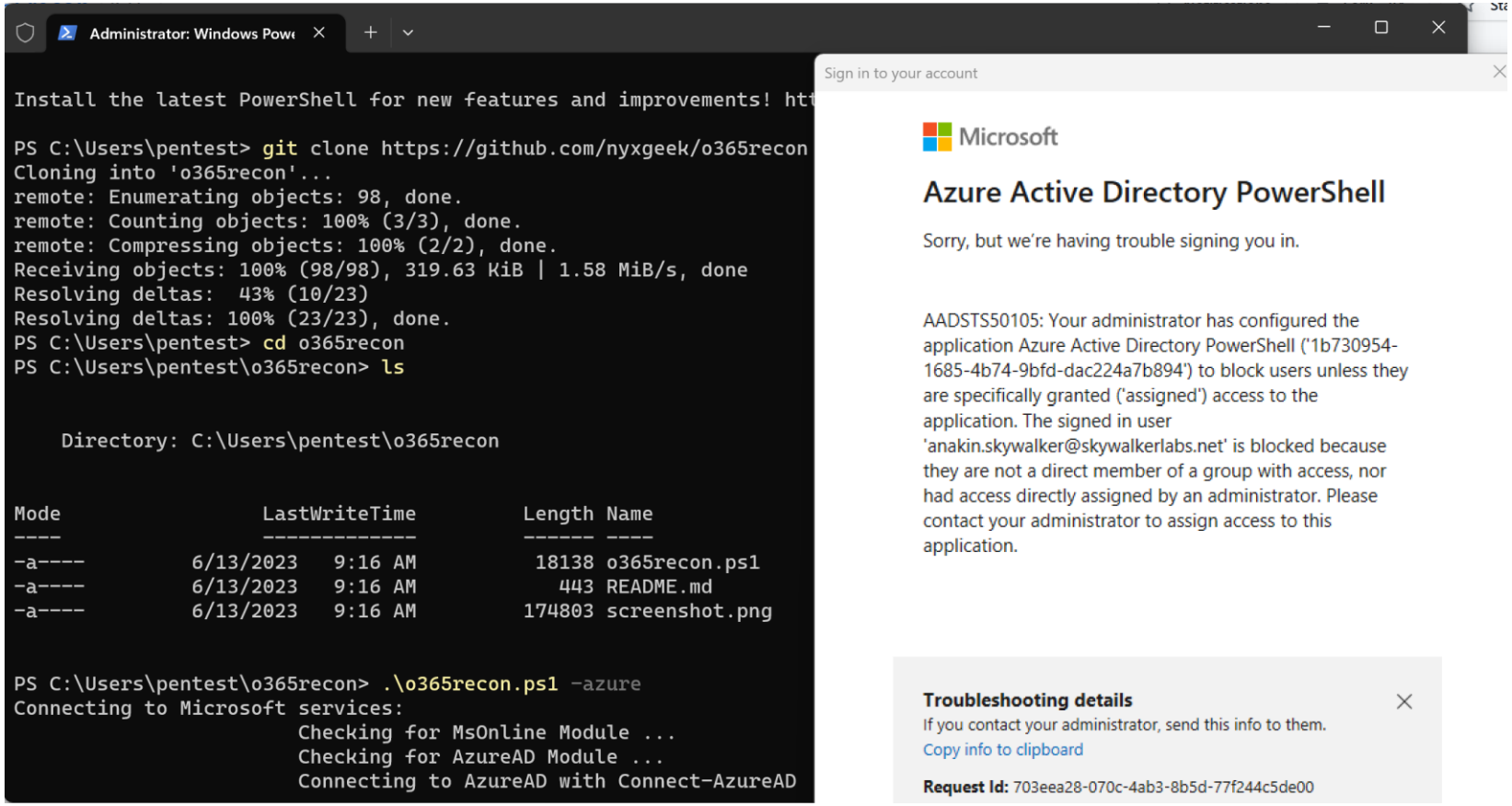
- Disable MSOLPowershell tenant wide with care
- Impacts Azure AD Connect Upgrades

An error occurred while executing the An error occurred while executing the 'Get-MsolUserRole' command. Access Denied. You do not have permissions to call this cmdlet. command. Learn more

Previous Next

Reference:
https://aadinternals.com/post/limit-user-access/

Preventing Malicious Recon

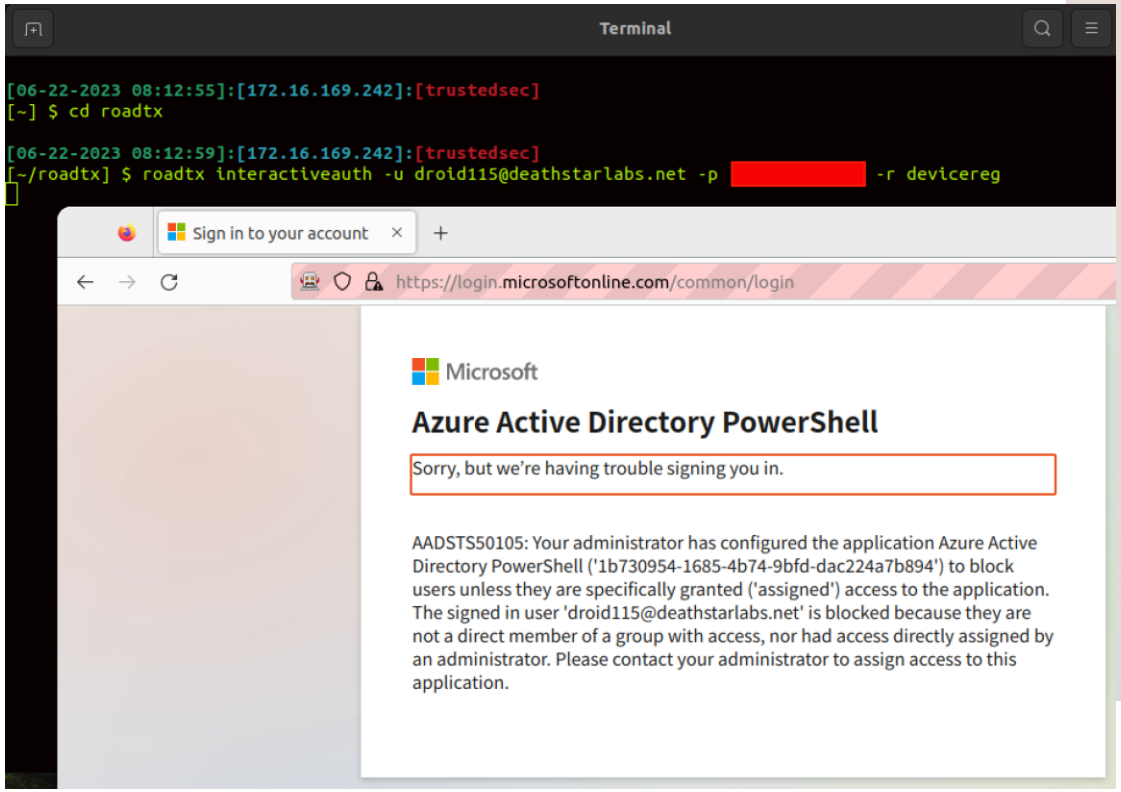


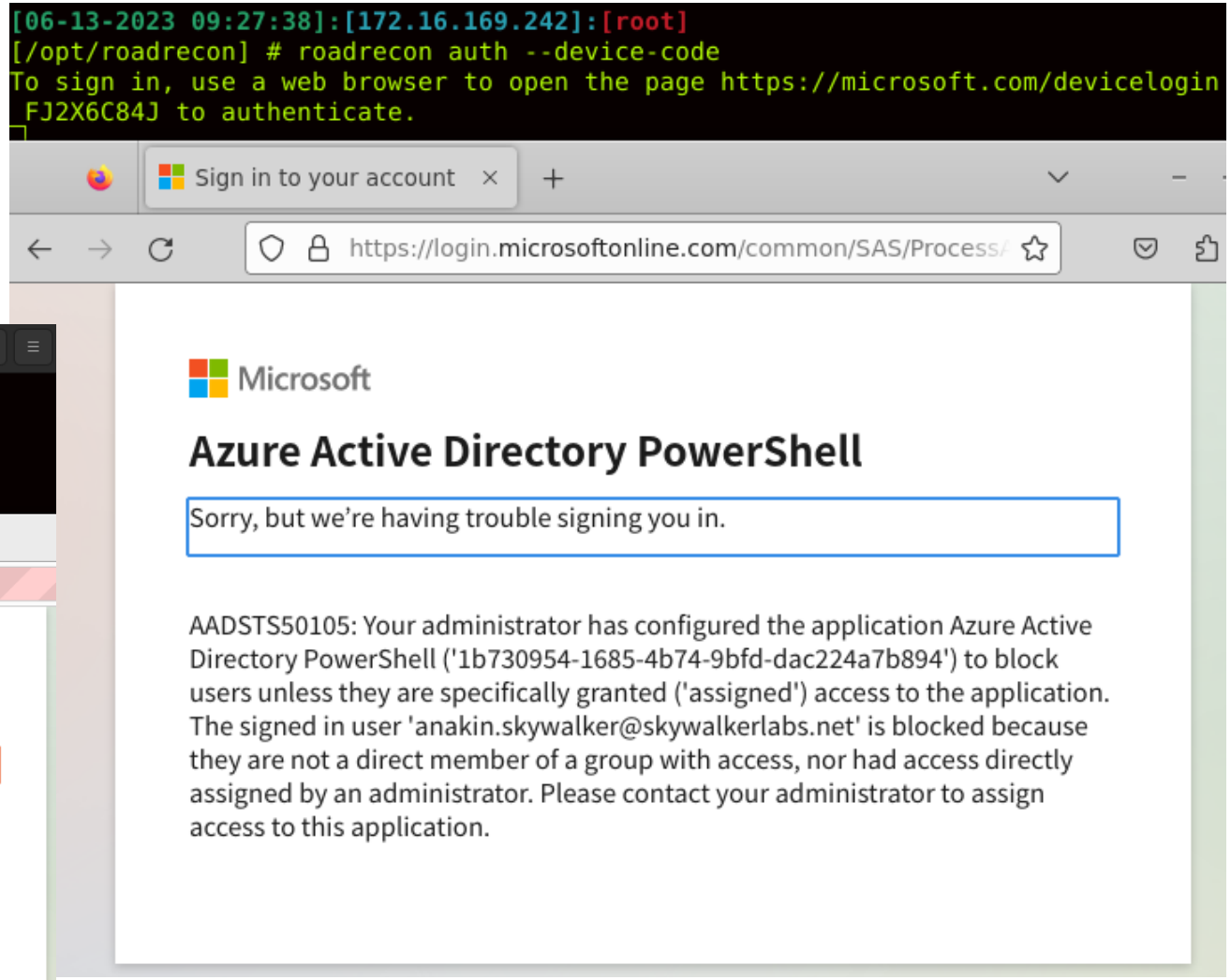
TrustedSec

Preventing Malicious Recon

Roadrecon
- Auth through device codes will be blocked
- Still works if using a Graph Access Token

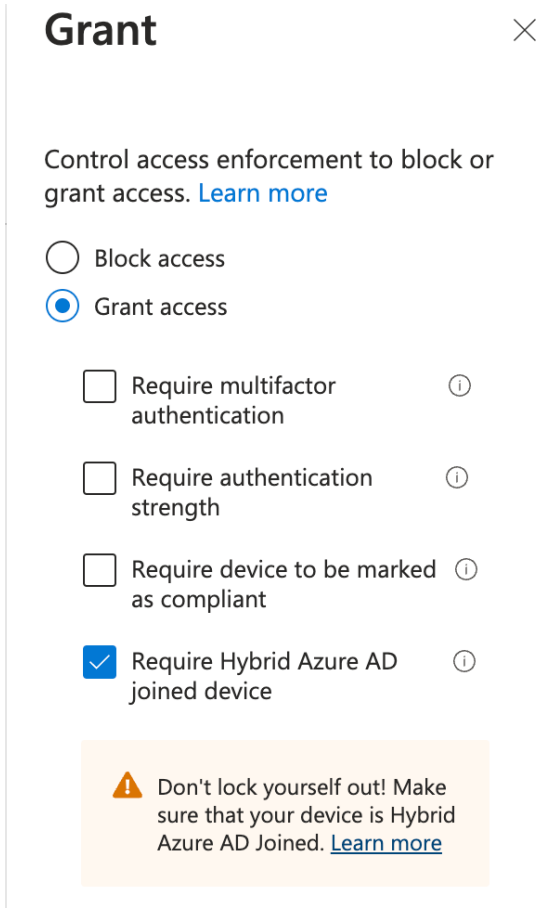
Roadtx
- Stops device registrations with roadtx

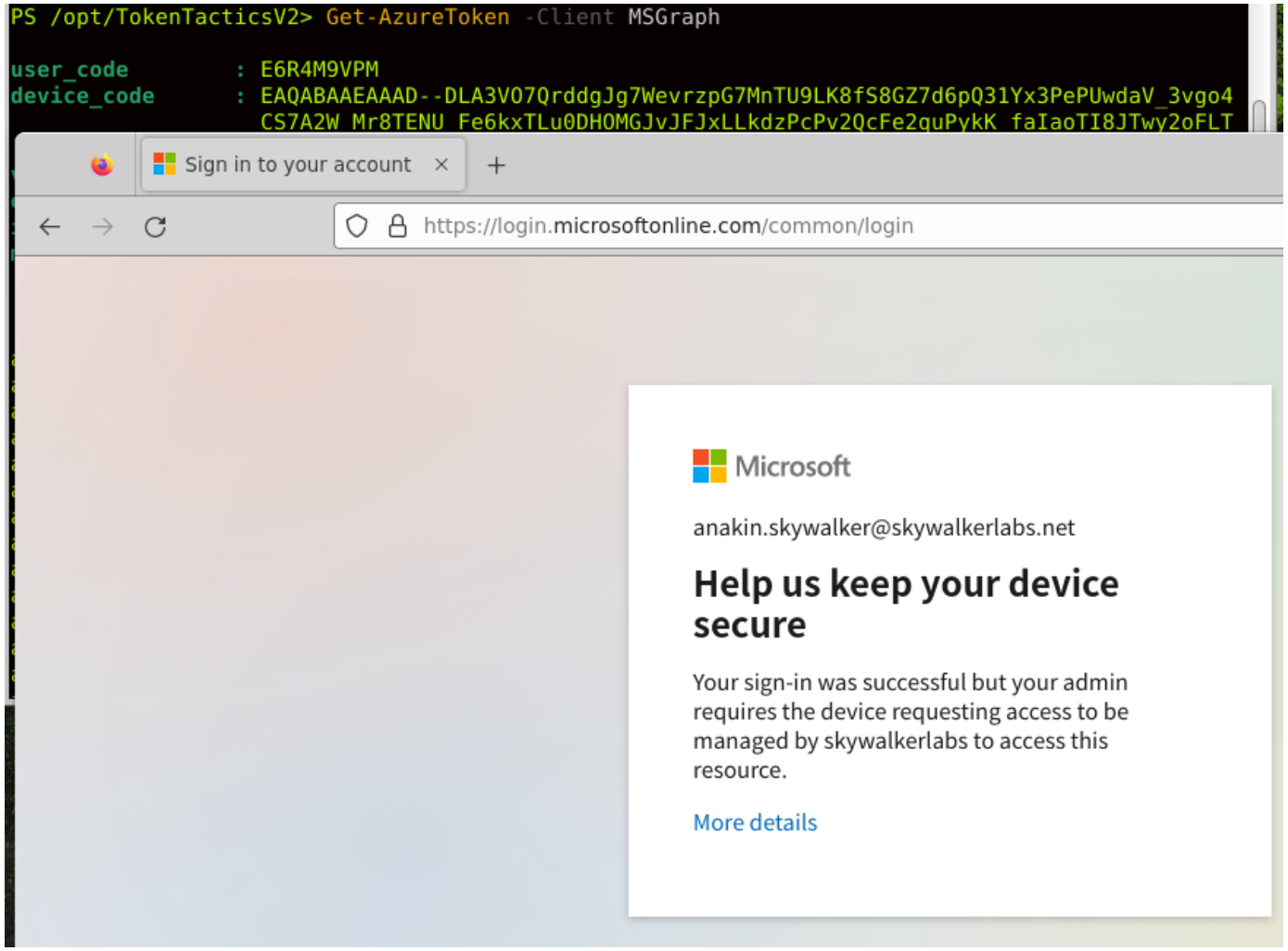




Preventing Malicious Recon

Token Stealing Prevention
- Hybrid Azure AD Join Enforcement





Other Conditional Access Suggestions

Block Access to Azure Management

Conditional Access policy

Delete | View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Block Access to Azure Management

Assignments

Users

All users included and specific users excluded

Target resources

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Control access based on all or specific network access traffic, cloud apps or actions. Learn more

Select what this policy applies to

Cloud apps

Include | Exclude

- None
- All cloud apps
- Select apps

Edit filter (Preview)

None

Select

Microsoft Azure Management

MA Microsoft Azure Management
797f4846-ba00-4fd7-ba43-dac1f8f63013

Don't lock yourself out! This policy

Block Access to Azure Management

Conditional Access policy

Delete | View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Block Access to Azure Management

Assignments

Users

All users included and specific users excluded

Target resources

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

Include | Exclude

Select the users and groups to exempt from the policy

- [ ] Guest or external users
- [x] Directory roles

15 selected

- [x] Users and groups

Select excluded users and groups

1 user, 1 group

AZ Azure_AD_MGMT

OD On-Premises Directory Synchr...
Sync_DC1_d8dea9a764ab@sk...

Other Conditional Access Suggestions

Zero Trust

Securing security info registration

Secure when and how users register for Azure AD multifactor authentication and self-service password. Learn more

View | Download JSON file (Preview)

Require multifactor authentication for guest access

Require guest users perform multifactor authentication when accessing your company resources. Learn more

View | Download JSON file (Preview)

Require multifactor authentication for risky sign-ins

Require multifactor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License) Learn more

View | Download JSON file (Preview)

Require password change for high-risk users

Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License) Learn more

View | Download JSON file (Preview)

No persistent browser session

Protect user access on unmanaged devices by preventing browser sessions from remaining signed in after the browser is closed and setting a sign-in frequency to 1 hour.
Learn more

View | Download JSON file (Preview)

TrustedSec

Alerts on role assignments

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-alert

Alert on privileged Azure role assignments

Article • 10/30/2022 • 1 contributor

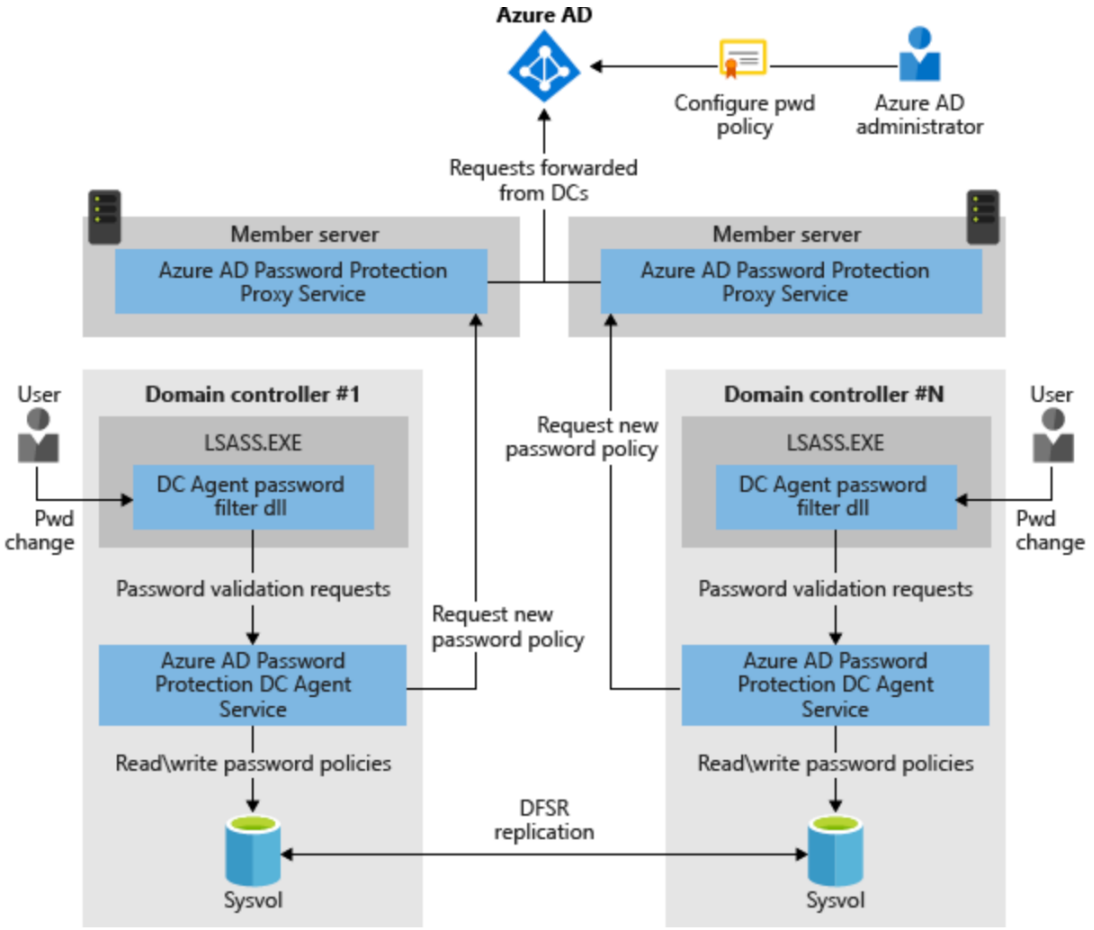
Feedback

In this article

Privileged Azure roles, such as Contributor, Owner, or User Access Administrator, are powerful roles and may introduce risk into your system. You might want to be notified by email or text message when these or other roles are assigned. This article describes how to get notified of privileged role assignments at a subscription scope by creating an alert rule using Azure Monitor.

Weak Password Prevention

Azure AD Password Protection
- Supported on Azure AD free, P1 and P2.
- Free Tier Supports Cloud only accounts
- If using Active Directory for on premises synchronization, requires additional setup
- Setup custom password lists is highly recommended
- Can do reporting on failing password compliance before switching to enforcement mode

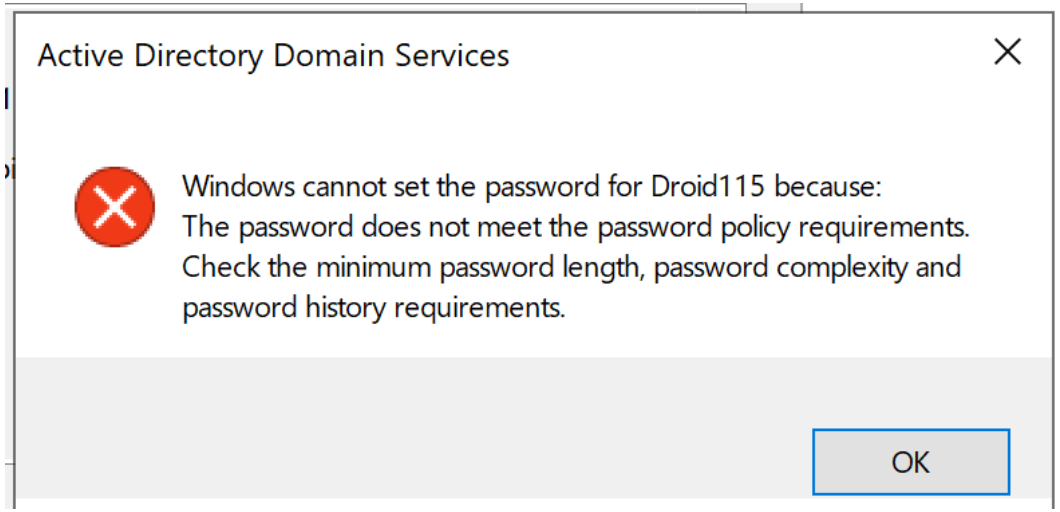


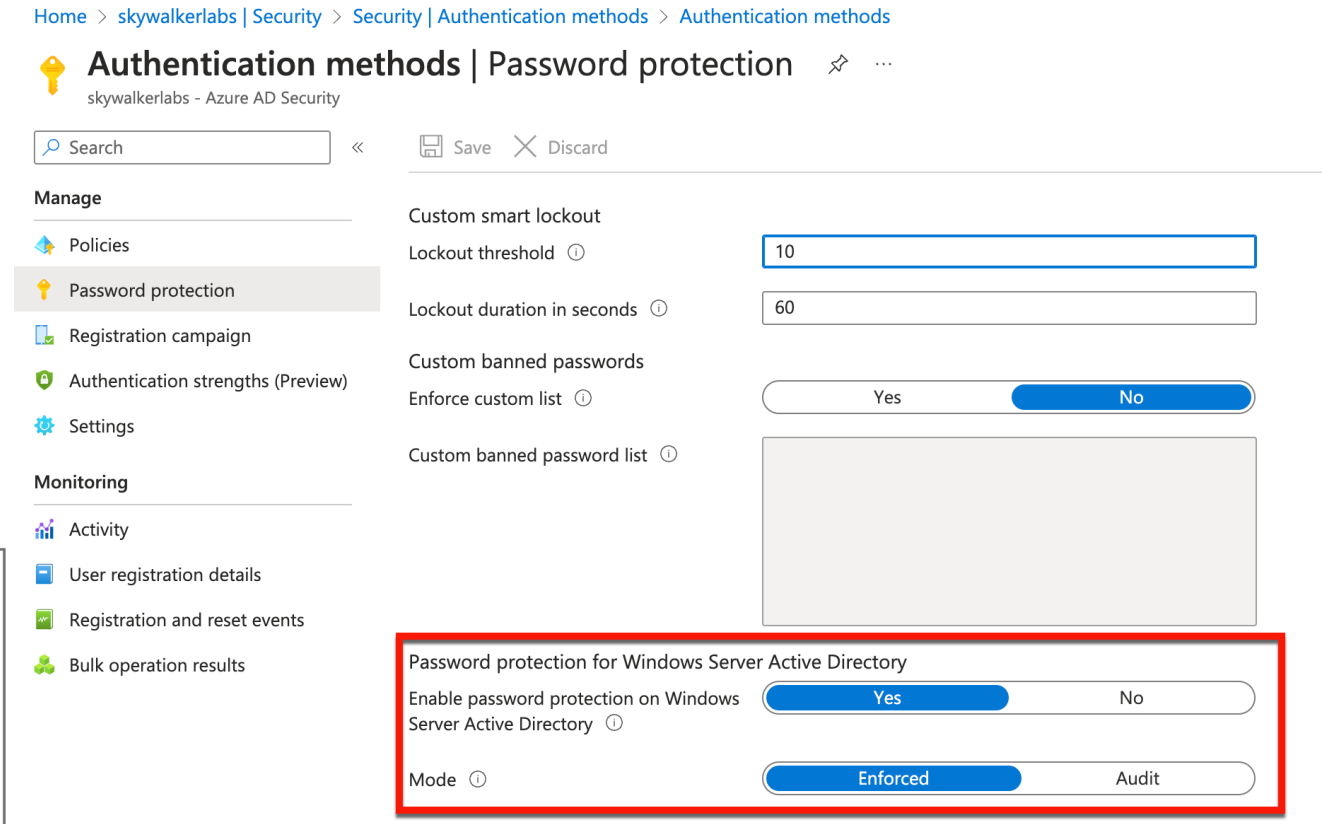
Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Weak Password Prevention

Azure AD Password Protection Tips

- Put in Audit Mode First!!!!!
- Communicate to your End Users on changes
- Utilize Reporting Features
- Help Desk can no longer reset passwords with weak ones.





Azure AD Connect Protection

- Treat as Tier 0 Asset
- Only Domain Admins should have access
- EDR will alert for private key extraction attempts

EDR alert detections/MDE

Alerts

Export 1 Week

Alert name	Tags	Severity	Investigation state
Suspicious User Account Discovery		Low	
AAD Connect private key extraction attempt		High	
Suspicious process executed PowerShell command		Medium	
Suspicious LDAP query		Medium	
Suspicious service launched		Medium	

Tips for MFA Excellence

MFA Methods to avoid
- Phone Calls
- Text SMS

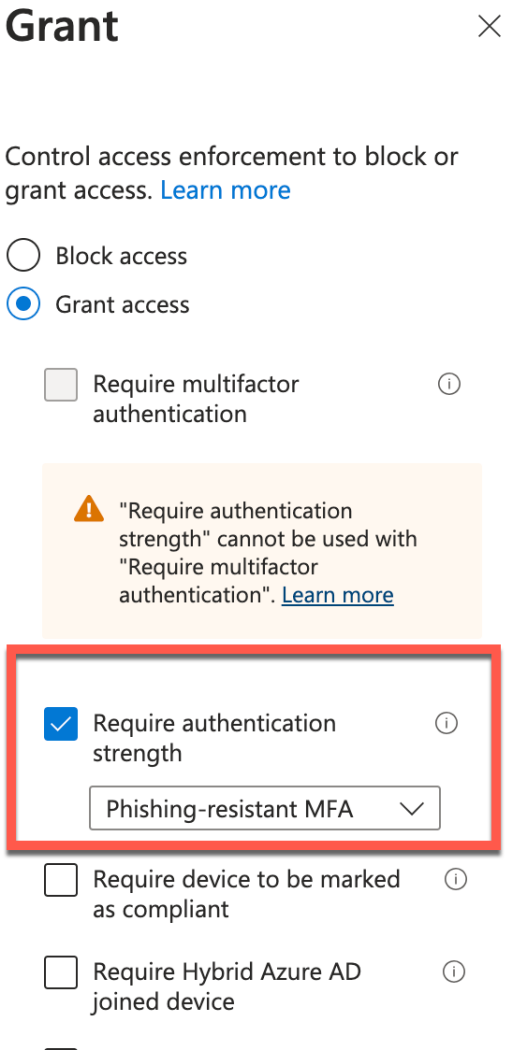
Better MFA Methods
- Authenticator App w/Number Matching
- Authenticator App w/Codes
- Passwordless MFA

Most Secure MFA Methods
- FIDO2 Hardware keys
- Certificate-based Authentication
- Both options are Phishing resistant MFA methods

Tips for MFA Excellence

Conditional Access Authentication Strength
- https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths

Give Someone an MFA nudge
- https://aka.ms/nudge



Tools

Azure Hound
https://github.com/BloodHoundAD/AzureHound

ROADtools
https://github.com/dirkjanm/ROADtools

Microburst
https://github.com/NetSPI/MicroBurst

TeamFiltration
https://github.com/Flangvik/TeamFiltration

One_drive_enum
https://github.com/nyxgeek/onedrive_user_enum

TokenTactics
https://github.com/rvrsh3ll/TokenTactics

O365recon
https://github.com/nyxgeek/o365recon

References

Azure Security fundamentals documentation:
https://learn.microsoft.com/en-us/azure/security/fundamentals/

Azure Security Documentation:
https://learn.microsoft.com/en-us/azure/security/

CIS Workbench:
https://workbench.cisecurity.org/

Microsoft Security Compliance Toolkit:
https://www.microsoft.com/en-us/download/details.aspx?id=55319

Hybrid Azure AD Join Targeted Deployments:
https://learn.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-control

Thank You!

TrustedSec