Secureworks®

Azure AD OSINT

@DrAzureAD

https://linkedin.com/in/nestori

https://aadinternals.com

Dr Nestori Syynimaa

Senior Principal Security Researcher

Secureworks® CTU™

Twitter/*Mastodon/BlueSky:*

@DrAzureAD *@infosec.exchange*
.bsk.social

MVP
Microsoft®
Most Valuable
Professional

MICROSOFT
MOST VALUABLE
Security
Researcher
ESTD. 2022
VOLUME

Secureworks®

AADInternals

- Admin & hacking toolkit for Azure AD & Microsoft 365
- Open source:
  - https://github.com/gerenios/aadinternals
  - https://aadinternals.com/aadinternals
- MITRE ATT&CK
  - https://attack.mitre.org/software/S0677/

Groups That Use This Software

ID	Name	References
G0016	APT29	[5]

Azure AD is being renamed to Entra ID

James Casey

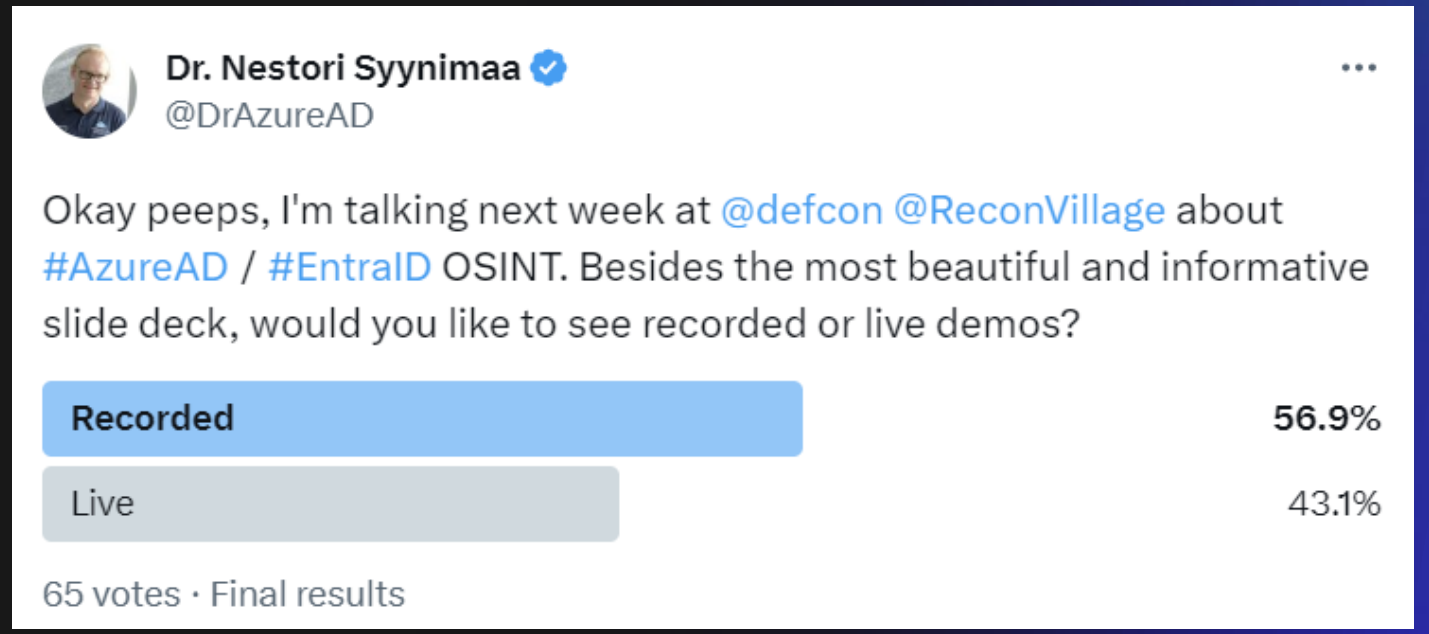
July 11th, 2023 | 4 | 3

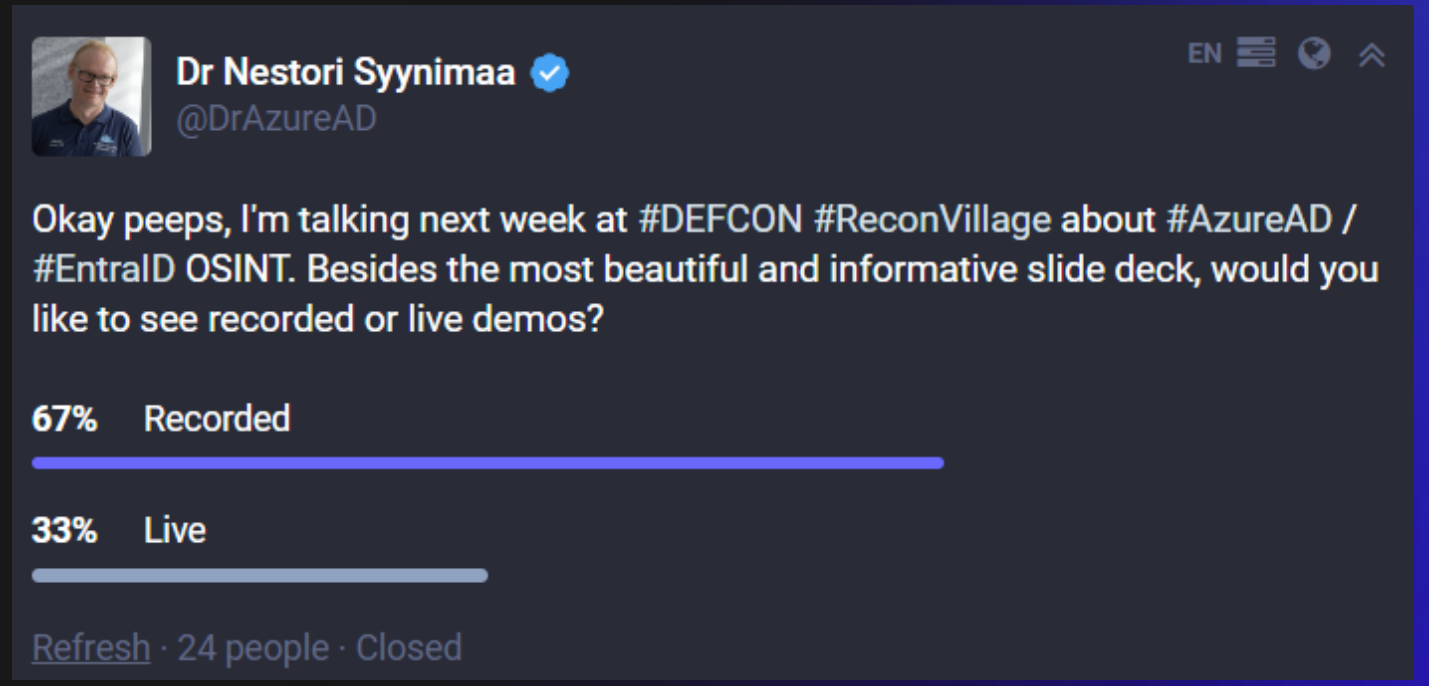
Today, one of the key announcements at *Reimagine secure access with Microsoft Entra* is that Azure Active Directory (Azure AD) is being renamed to Microsoft Entra ID as part of our commitment to simplify secure access experiences for everyone.

Secureworks

Contents

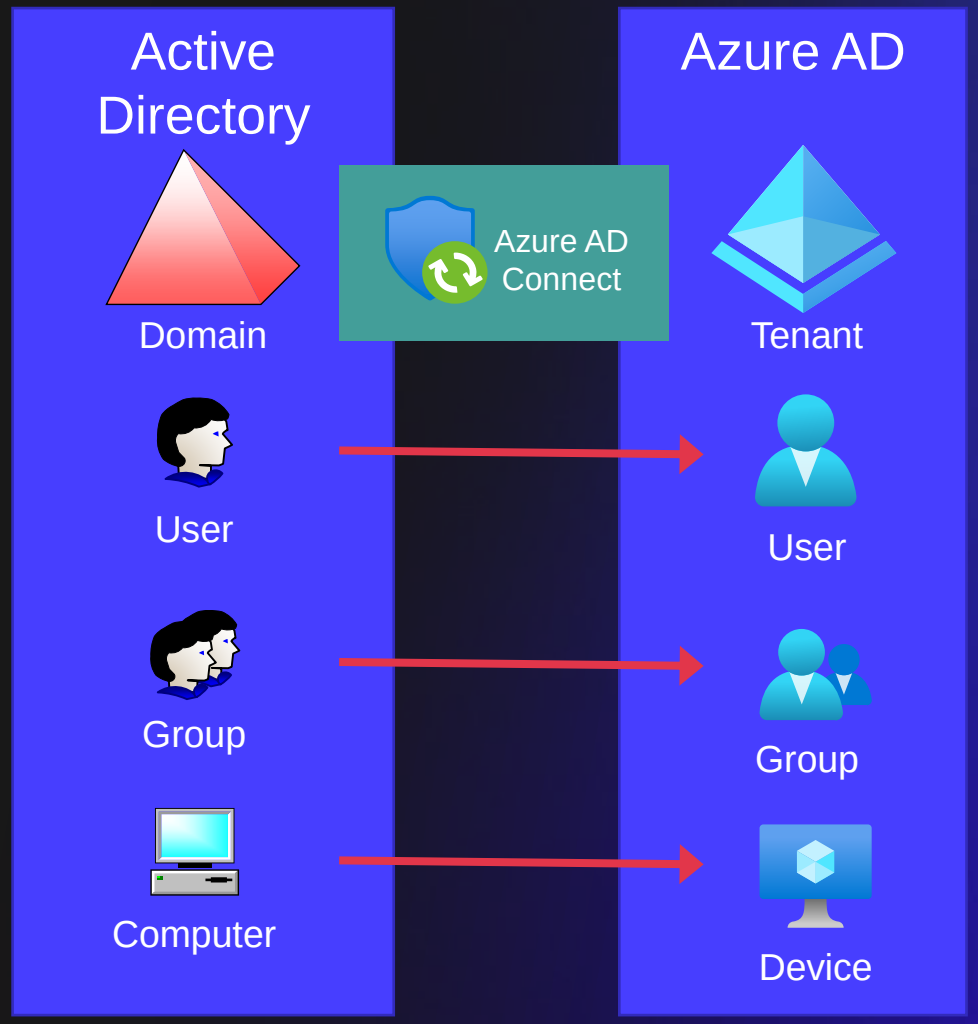
- Slides
- Demos





Introduction to Azure Active Directory (Azure AD)

- Microsoft's cloud-based IAM
- Used by M365 & Azure & thousands of 3rd party apps
- Multiple authentication options
- Usually objects synced from on-prem AD (=hybrid identity)



Azure AD adoption/usage statistics

Fortune 500 *		
Has Azure AD Tenant	441	88 %
Has federated domains (*n*=441)	293	68 %
Uses Seamless SSO (*n*=441)	118	27 %

Finland 500		
Has Azure AD Tenant	492	98 %
Has federated domains (*n*=492)	160	35 %
Uses Seamless SSO (*n*=492)	191	39 %

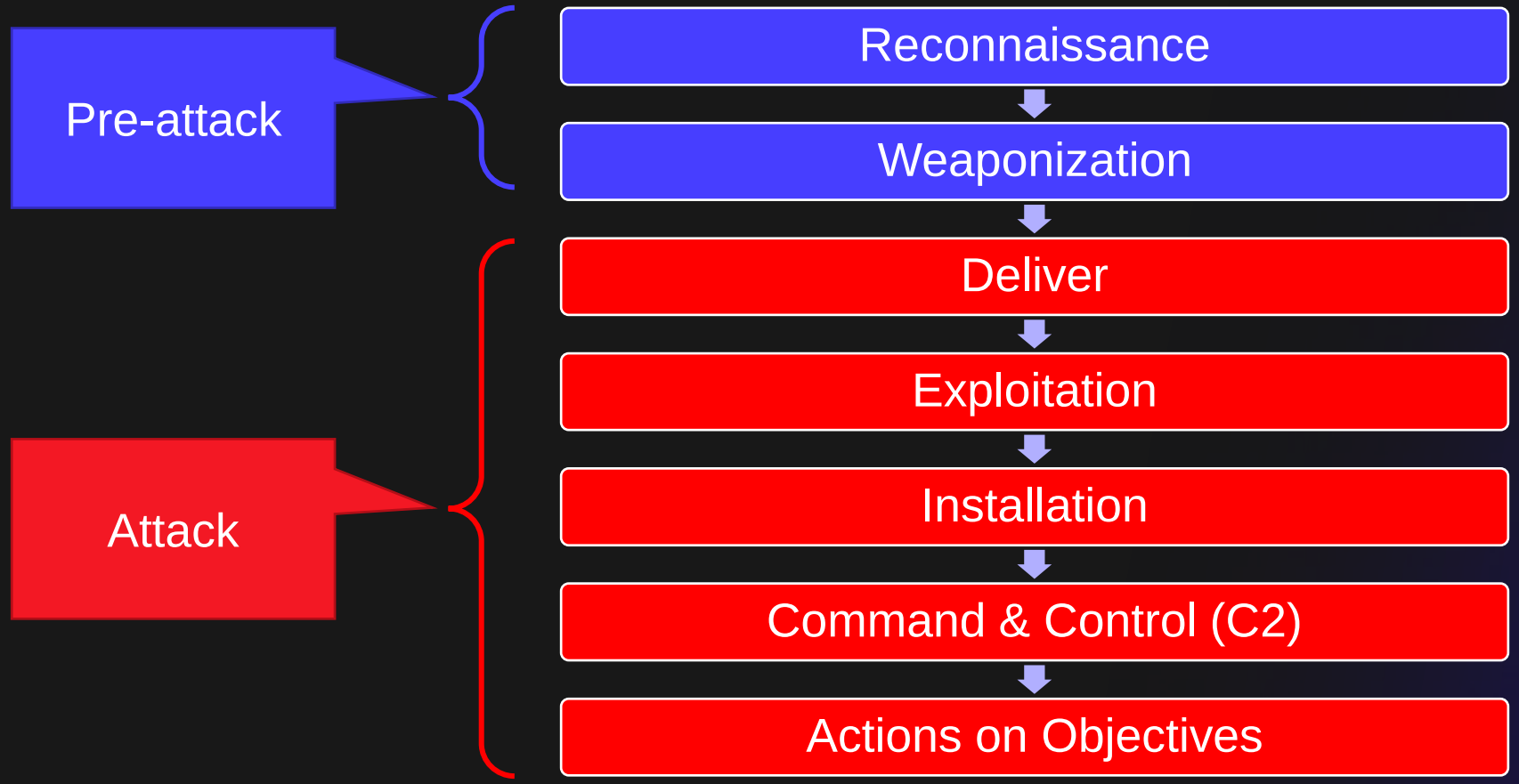
Top Universities (*n*=2000) *		
Has Azure AD Tenant	1892	95 %
Has federated domains (*n*=1892)	293	28 %
Uses Seamless SSO (*n*=1892)	258	14 %

Finnish municipalities (*n*=302)		
Has Azure AD Tenant	301	100 %
Has federated domains (*n*=301)	78	26 %
Uses Seamless SSO (*n*=301)	94	31 %

* Syynimaa, N. (2022). Exploring Azure Active Directory Attack Surface : Enumerating Authentication Methods with Open-Source Intelligence Tools. In J. Filipe, M. Smialek, A. Brodsky, & S. Hammoudi (Eds.), *ICEIS 2022 : Proceedings of the 24th International Conference on Enterprise Information Systems : Volume 2* (pp. 142-147). SCITEPRESS Science And Technology Publications. https://doi.org/10.5220/0011077100003179

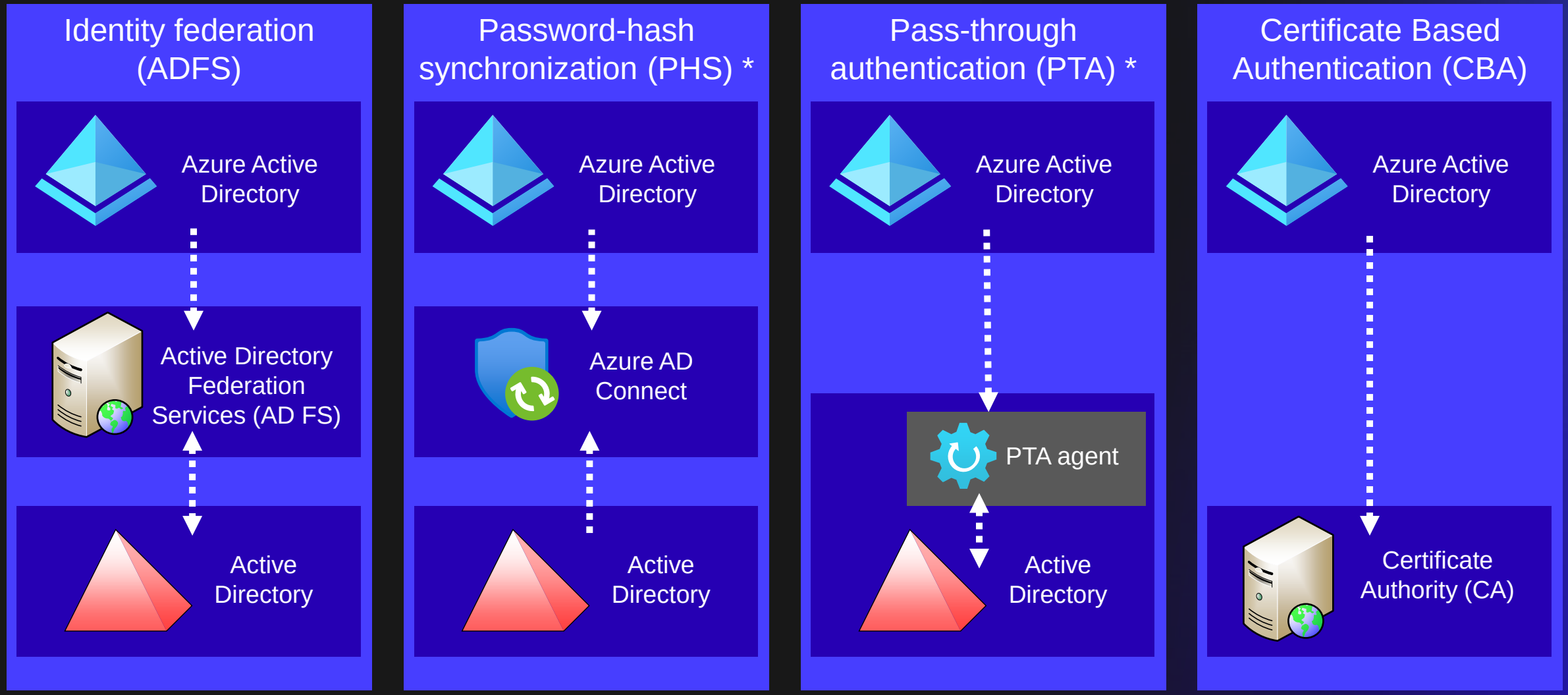
Cyber Kill chain

What the adversaries must complete in order to achieve their objectives



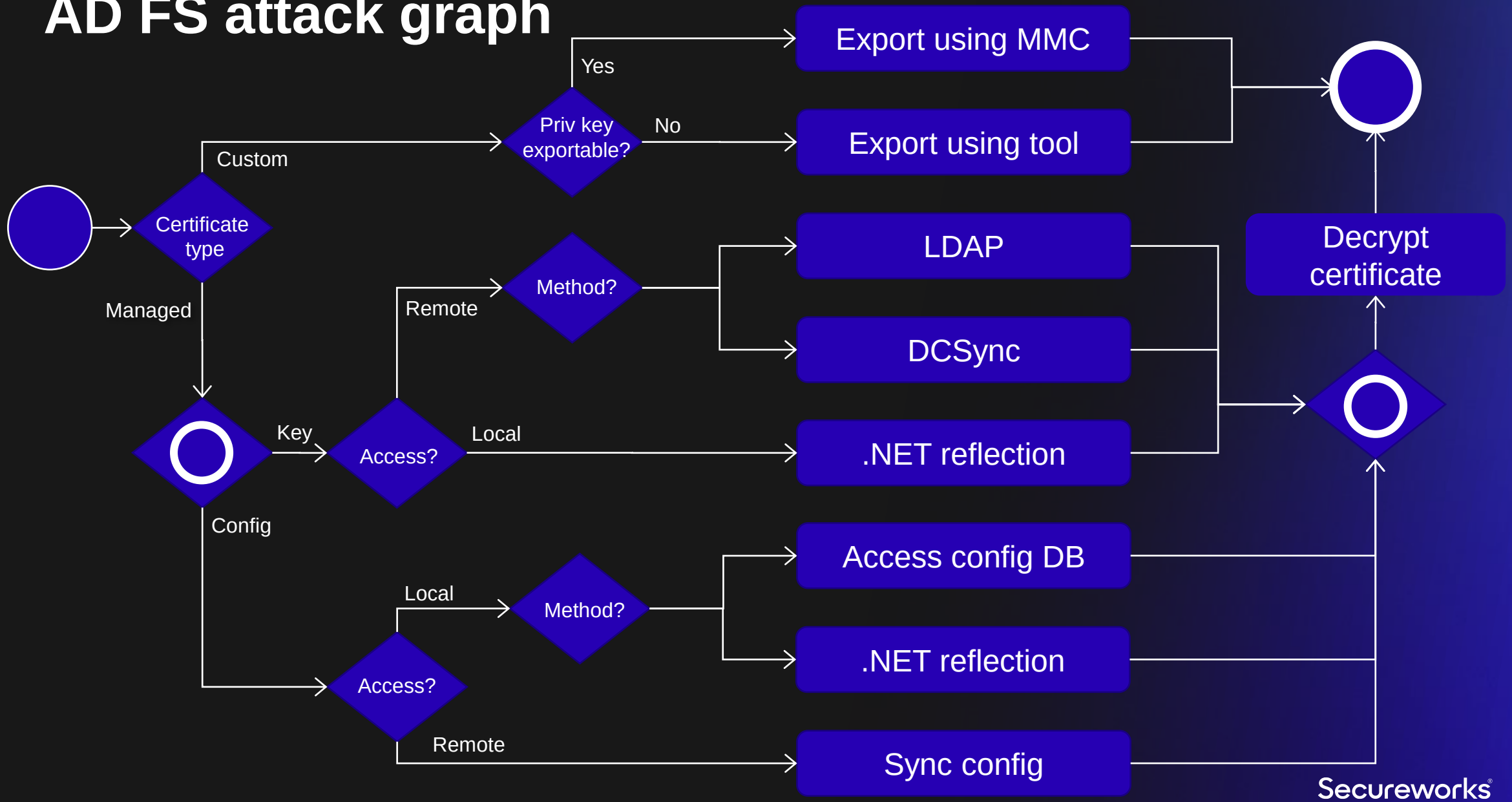
Adopted from Lockheed Martin Cyber Kill Chain® framework

Hybrid Authentication Options



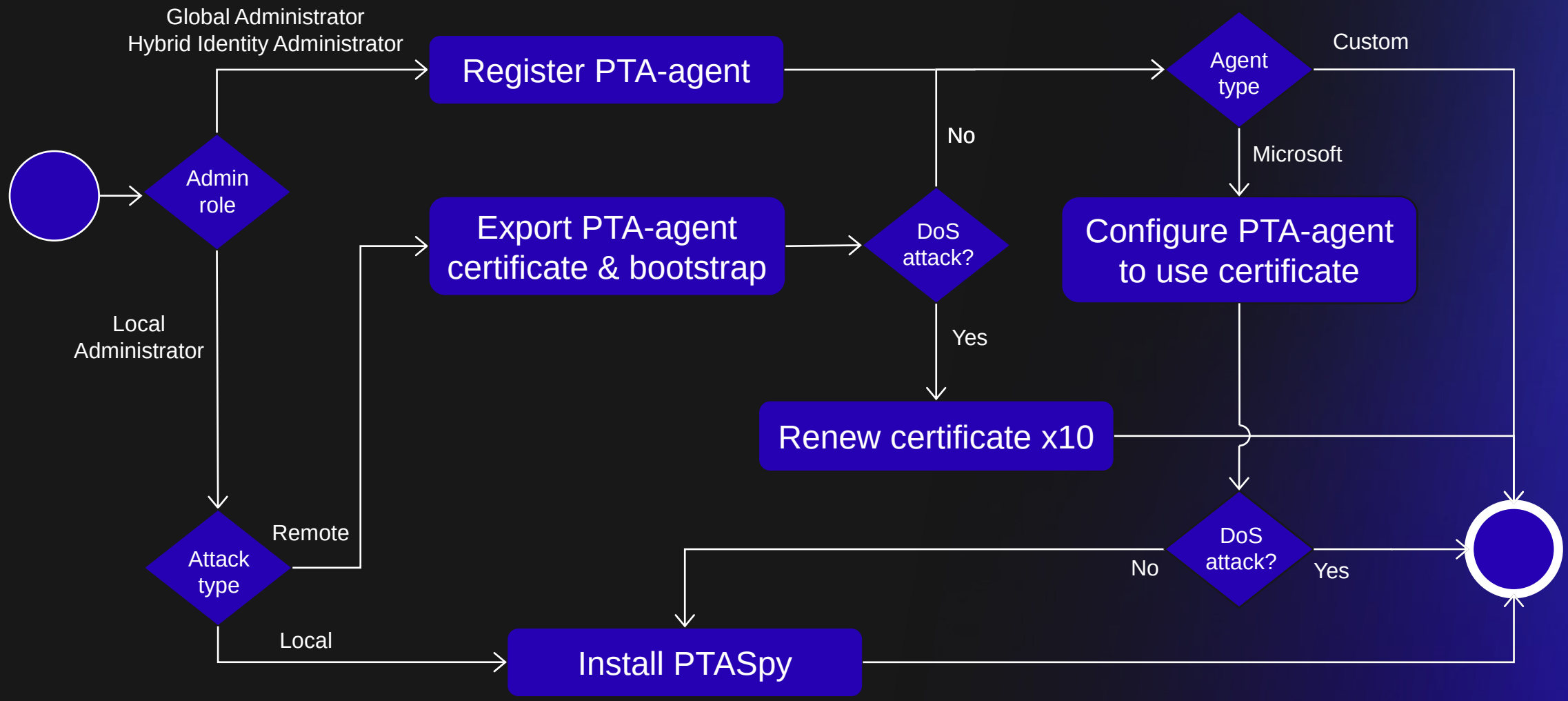
* Supports seamless single sign-on

AD FS attack graph

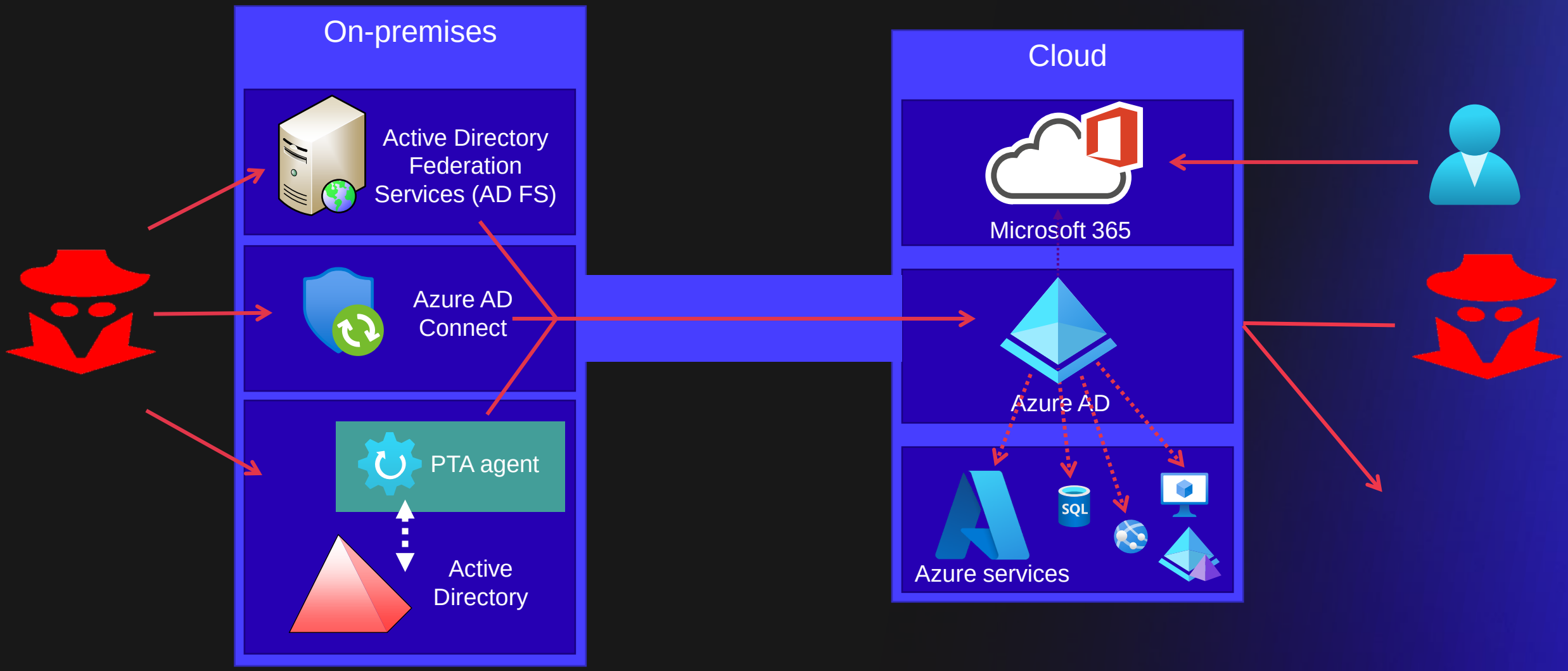


Secureworks

PTA attack graph



(Hybrid) Cloud Security



Reconnaissance goals

- Enumerate authentication options
- Find valid accounts / domains
- Don’t leave traces

How to get OSINT?

- Anonymous API calls
  - For everyone
- Authenticated API calls
  - Requires Azure AD tenant

Anonymous API calls

- All registered domain names
  - Domain type (managed/federated)
  - DNS information (MX, SPF, DMARC, etc.)
- Tenant ID with domain name
- Does the user exist
- Is tenant using (or used) Azure AD Connect Cloud sync
- Is tenant using Microsoft Defender for Identity (MDI)

Domain names 1/2

- Exchange Online Autodiscover service
- Post SOAP envelope to:

  `https://autodiscover-s.outlook.com/autodiscover/autodiscover.svc`

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:exm="http://schemas.microsoft.com/exchange/services/2006/messages" xmlns:
    <soap:Header>
        <a:Action soap:mustUnderstand="1">http://schemas.microsoft.com/exchange/2010/Autodisco
        <a:To soap:mustUnderstand="1">https://autodiscover-s.outlook.com/autodiscover/autodisc
        <a:ReplyTo>
            <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
        </a:ReplyTo>
    </soap:Header>
    <soap:Body>
        <GetFederationInformationRequestMessage xmlns="http://schemas.microsoft.com/exchange/2
            <Request>
                <Domain>company.com</Domain>
            </Request>
        </GetFederationInformationRequestMessage>
    </soap:Body>
</soap:Envelope>
```

Domain names 2/2

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" xmlns:a="http://www.w3.org/2005/08/a
    <s:Header>
        <a:Action s:mustUnderstand="1">http://schemas.microsoft.com/exchange/2010/Autodiscover/Autod
        <h:ServerVersionInfo xmlns:h="http://schemas.microsoft.com/exchange/2010/Autodiscover" xmlns
            <h:MajorVersion>15</h:MajorVersion>
            <h:MinorVersion>20</h:MinorVersion>
            <h:MajorBuildNumber>6652</h:MajorBuildNumber>
            <h:MinorBuildNumber>22</h:MinorBuildNumber>
            <h:Version>Exchange2015</h:Version>
        </h:ServerVersionInfo>
    </s:Header>
    <s:Body>
        <GetFederationInformationResponseMessage xmlns="http://schemas.microsoft.com/exchange/2010/A
            <Response xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
                <ErrorCode>NoError</ErrorCode>
                <ErrorMessage/>
                <ApplicationUri>outlook.com</ApplicationUri>
                <Domains>
                    <Domain>company.com</Domain>
                    <Domain>company.net</Domain>
                    <Domain>company.mail.onmicrosoft.com</Domain>
                    <Domain>company.onmicrosoft.com</Domain>
                </Domains>
                <TokenIssuers>
                    <TokenIssuer>
                        <Endpoint>https://login.microsoftonline.com/extSTS.srf</Endpoint>
                        <Uri>urn:federation:MicrosoftOnline</Uri>
                    </TokenIssuer>
                </TokenIssuers>
            </Response>
        </GetFederationInformationResponseMessage>
    </s:Body>
```

Domain type

- Multiple endpoints

  `https://login.microsoftonline.com/common/GetCredentialType`

  `https://login.microsoftonline.com/common/userrealm/<username>`

  `https://login.microsoftonline.com/GetUserRealm.srf?login=<username>`

- Information
  - Domain type (managed / federated)
  - Does the user exist (gets easily throttled)
  - Is DesktopSSO (Seamless Single-Sign-On) enabled
  - Is CBA enabled

User enumeration 1/2

ONEDRIVE TO ENUM THEM ALL

June 6, 2023

By TrustedSec in Cloud Penetration Testing, Office 365 Security Assessment

THIS POST WAS WRITTEN BY @NYXGEEK

Greetings fellow hackers,

Today we'll be diving into the topic of user enumeration via OneDrive. I wrote a blog post on this topic a few years back when I first identified the technique. Since then, I've learned more about it, and the onedrive_enum.py tool has been updated and is more powerful than ever!

In short, OneDrive can be the best way to do user enumeration because:

- It doesn't require a login attempt
- It's completely silent (companies cannot see the requests)
- There's no rate-limiting

https://www.trustedsec.com/blog/onedrive-to-enum-them-all

User enumeration 2/2

1. Get tenant name (*e.g.*, **company**.onmicrosoft.com)
2. Normalize username: user@company.com → user_company_com
3. Make HTTP HEAD request:

```
https://company-my.sharepoint.com/personal/user_company_com
```

Tenant ID

- Make HTTP GET request:

`https://login.microsoftonline.com/<domain>/.well-known/openid-configuration`


```
{
  "token_endpoint": "https://login.microsoftonline.com/63067c3a-238c-46f5-9f22-ad8e3dc85778/oauth2/token",
  "token_endpoint_auth_methods_supported": [
    "client_secret_post",
    "private_key_jwt",
    "client_secret_basic"
  ],
  "jwks_uri": "https://login.microsoftonline.com/common/discovery/keys",
  "response_modes_supported": [
    "query",
    "fragment",
    "form_post"
  ],
  "subject_types_supported": [
    "pairwise"
  ],
```

Azure AD Connect Cloud sync

- Standard username:

  `ADToAADSyncServiceAccount@<tenant>.onmicrosoft.com`

Microsoft Defender for Identity

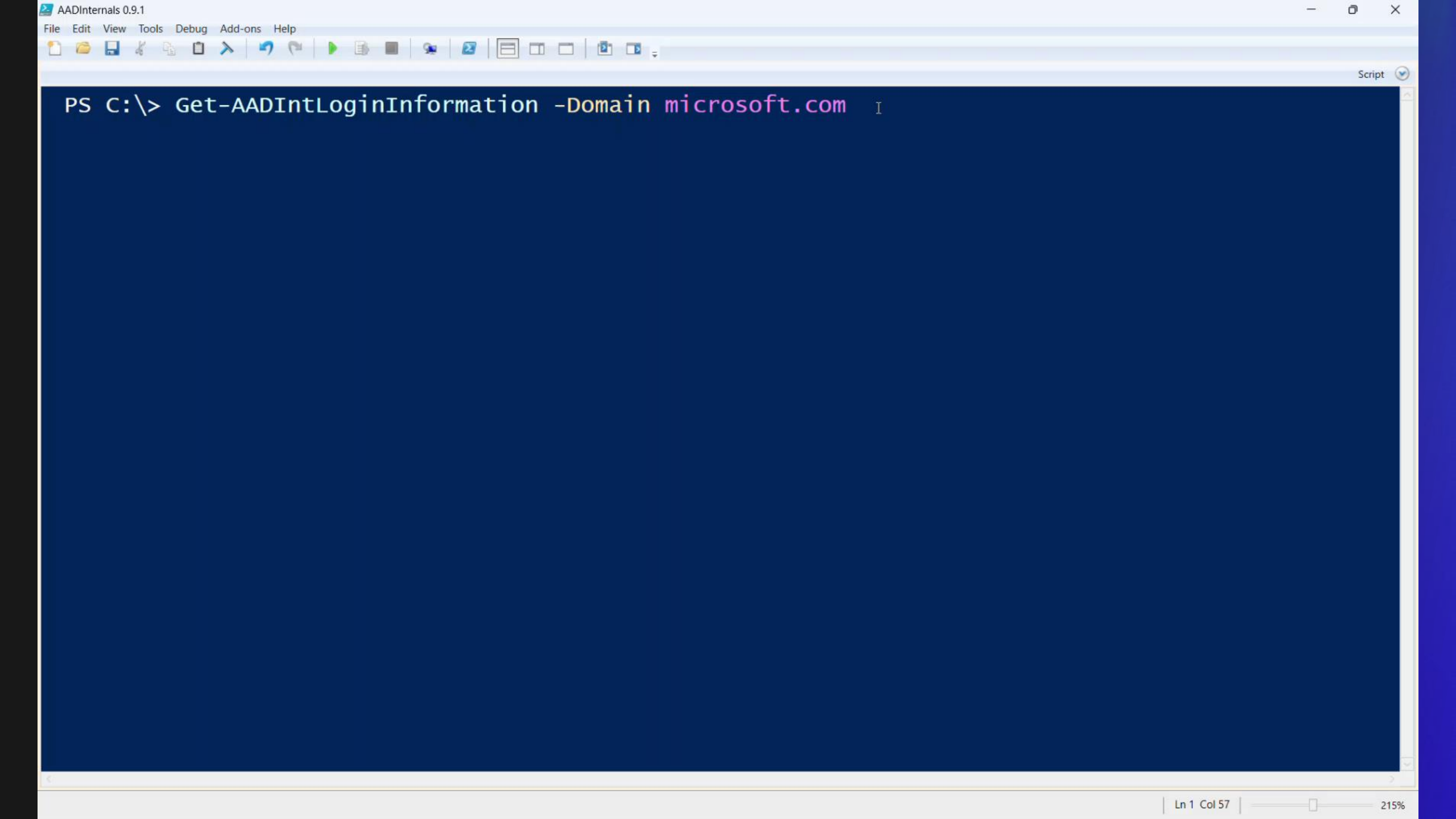
- Urls:

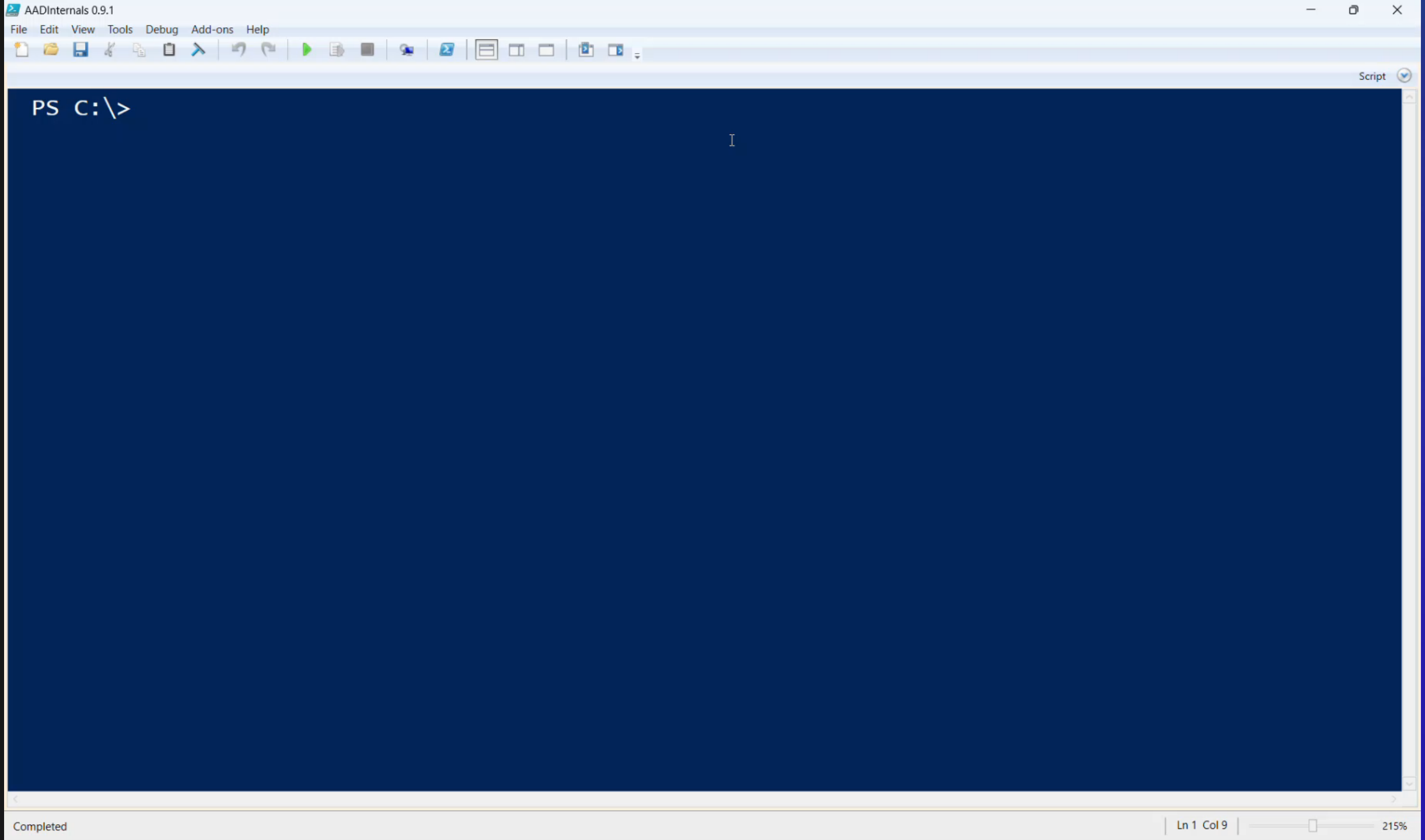
  `<tenant>.atp.azure.com`

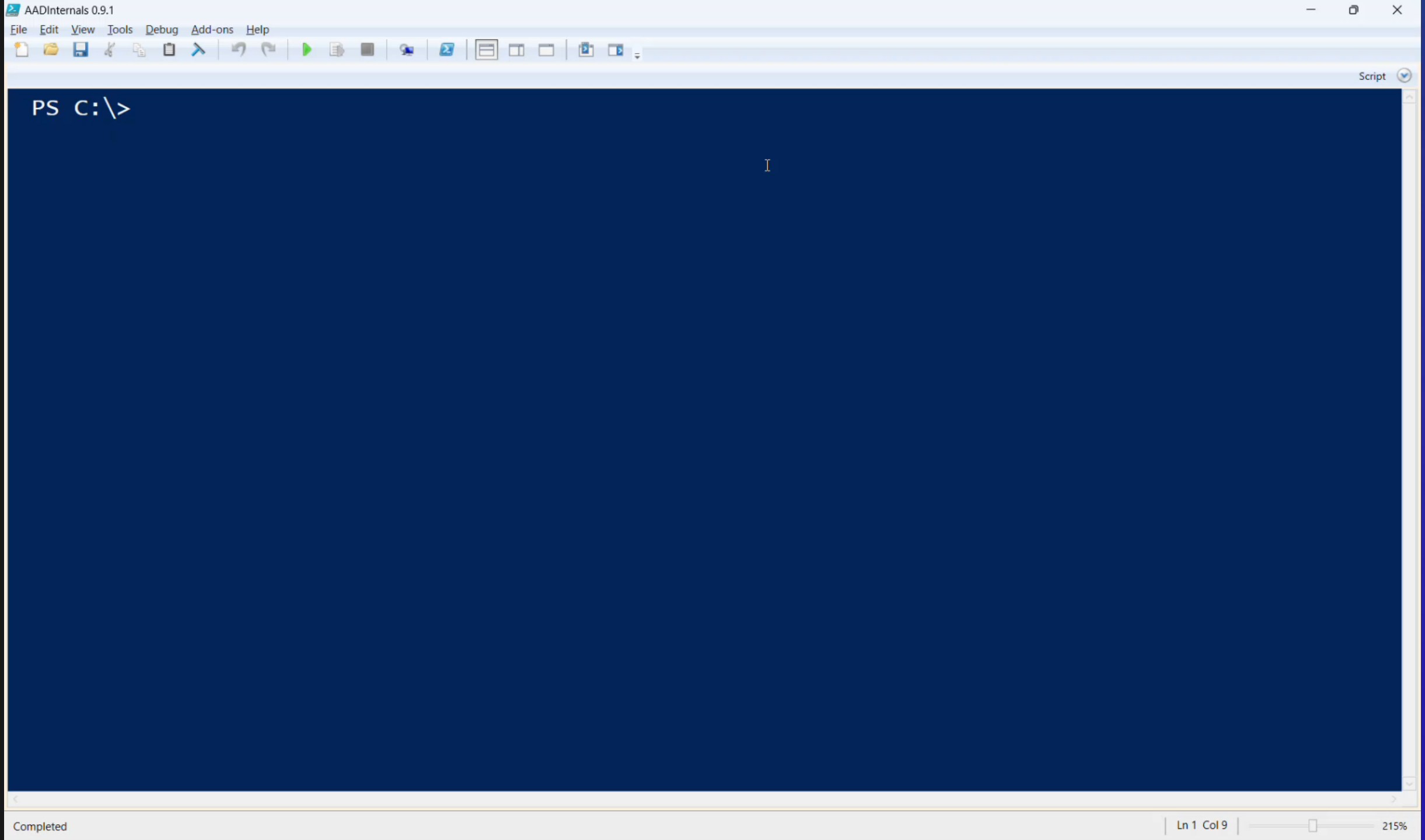
  `<tenant>-onmicrosoft-com.atp.azure.com`

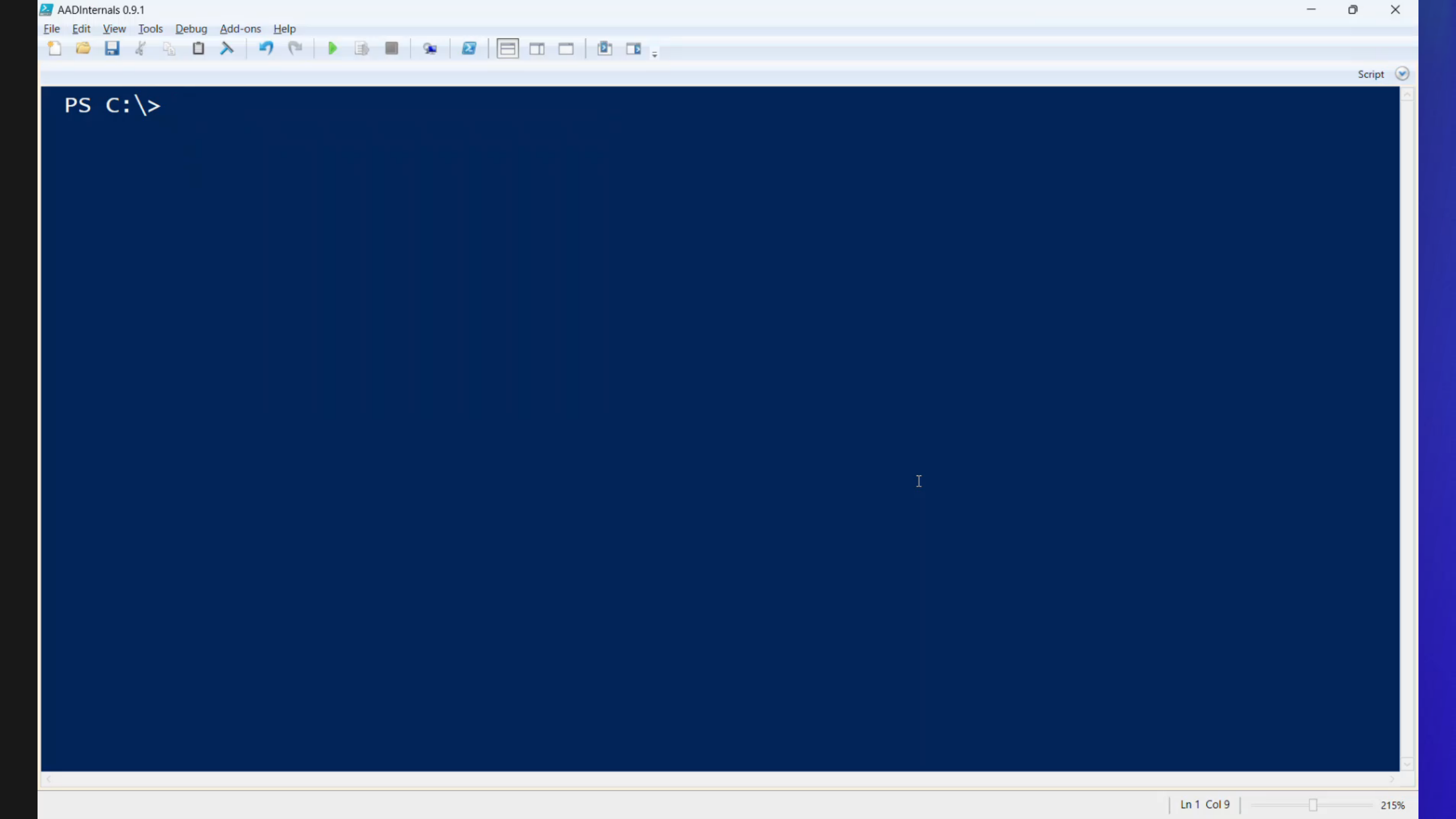
Anonymous Azure AD OSINT with AADInternals

- `Get-AADIntLoginInformation`
  - User/domain login information, including domain type & Seamless SSO (Desktop SSO)
- `Get-AADIntTenantID`
  - Azure AD Tenant ID of the given domain
- `Get-AADIntTenantDomains`
  - List all domains of the tenant of the given domain
- `Invoke-AADIntReconAsOutsider`
  - All above + DNS records


AADInternals 0.9.1
File Edit View Tools Debug Add-ons Help
Script
PS C:\> Get-AADIntLoginInformation -Domain microsoft.com
Ln 1 Col 57
215%


AADInternals 0.9.1
File Edit View Tools Debug Add-ons Help
Script
PS C:\>
Completed
Ln 1 Col 9
215%


AADInternals 0.9.1
File Edit View Tools Debug Add-ons Help
Script
PS C:\>
Completed
Ln 1 Col 9
215%

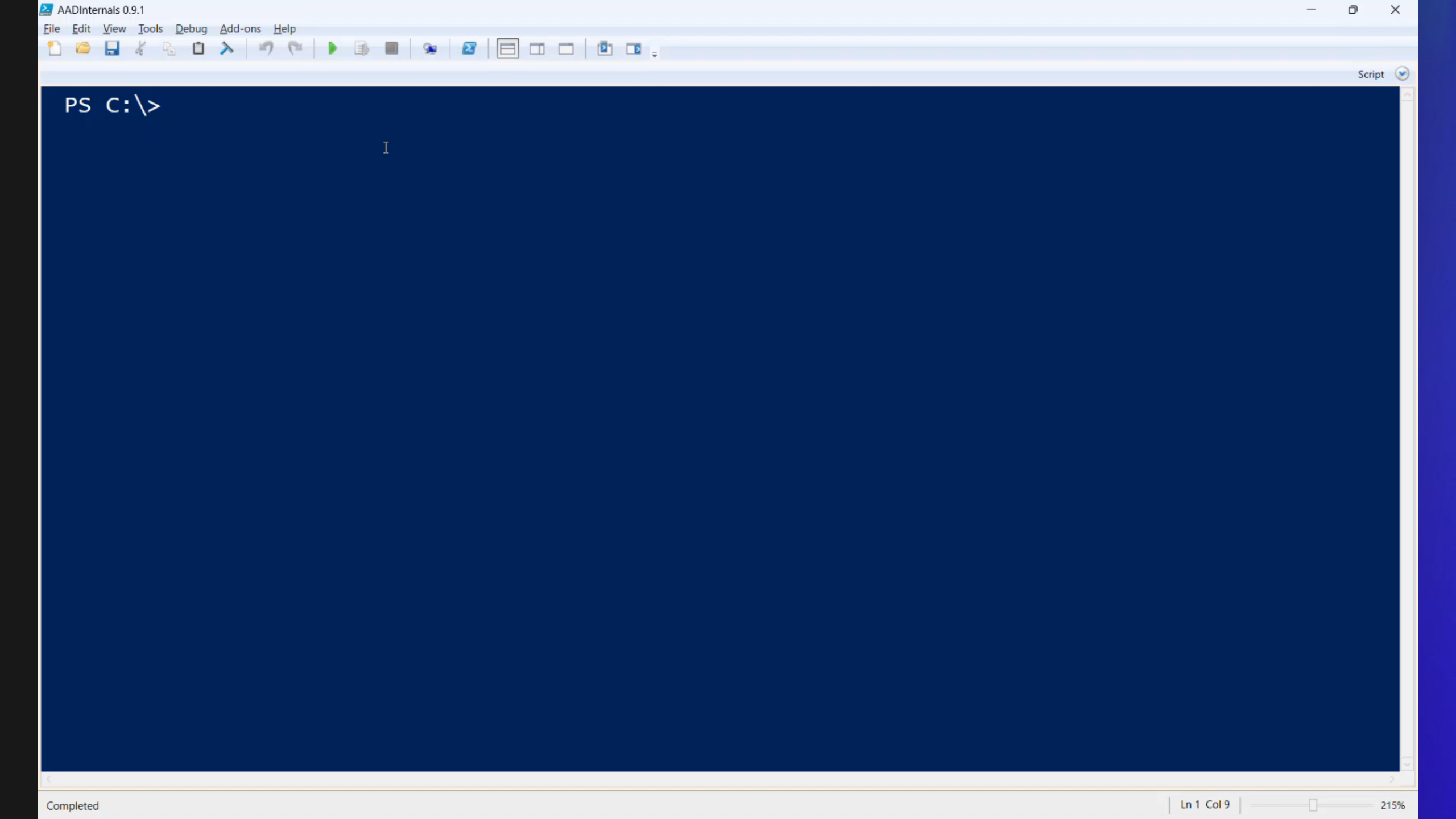

AADInternals 0.9.1
File Edit View Tools Debug Add-ons Help
Script
PS C:\>
Ln 1 Col 9
215%

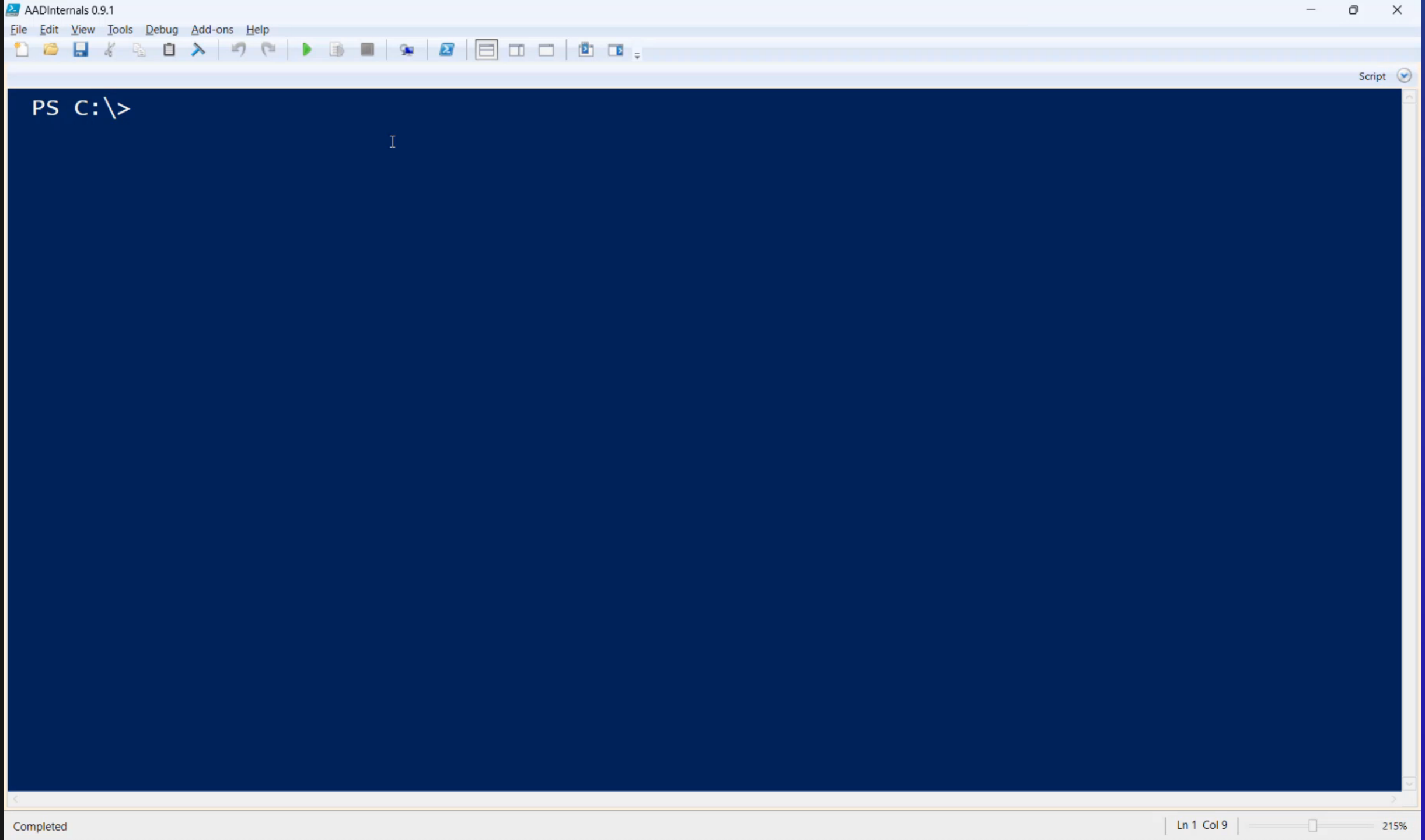
Authenticated API calls

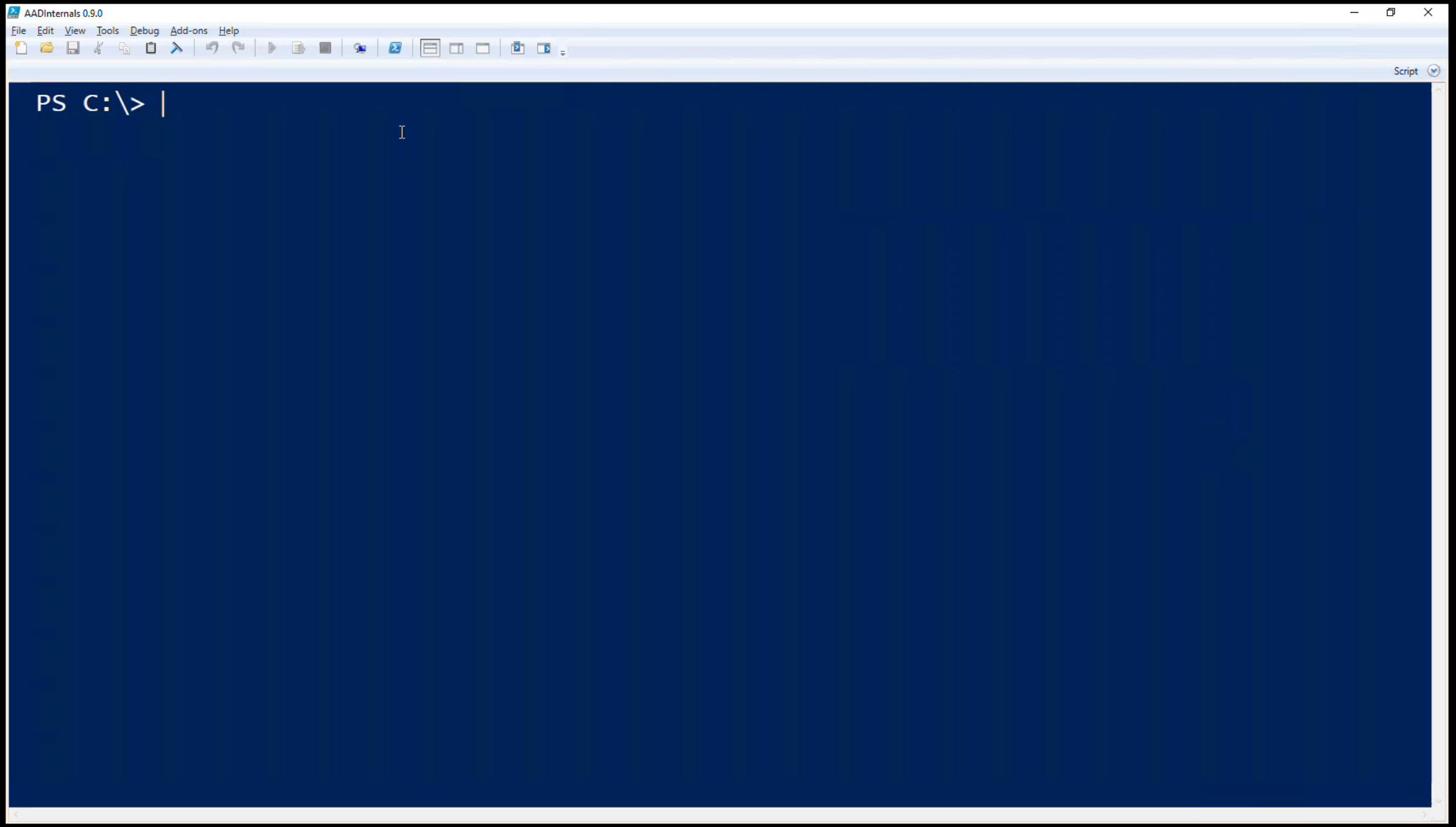
- Tenant name (domain) from Tenant ID
- User object ID from email
- User display name from email
- UPN from email
- Teams availability status

Authenticated Azure AD OSINT with AADInternals

- `Get-AADIntTenantDomain -TenantId`
  - Tenant name (*e.g.*, company.onmicrosoft.com)
  - Requires admin permissions
- `Find-AADIntTeamsExternalUser`
  - User object id, display name, and upn
- `Get-AADIntTeamsAvailability`
  - User team availability

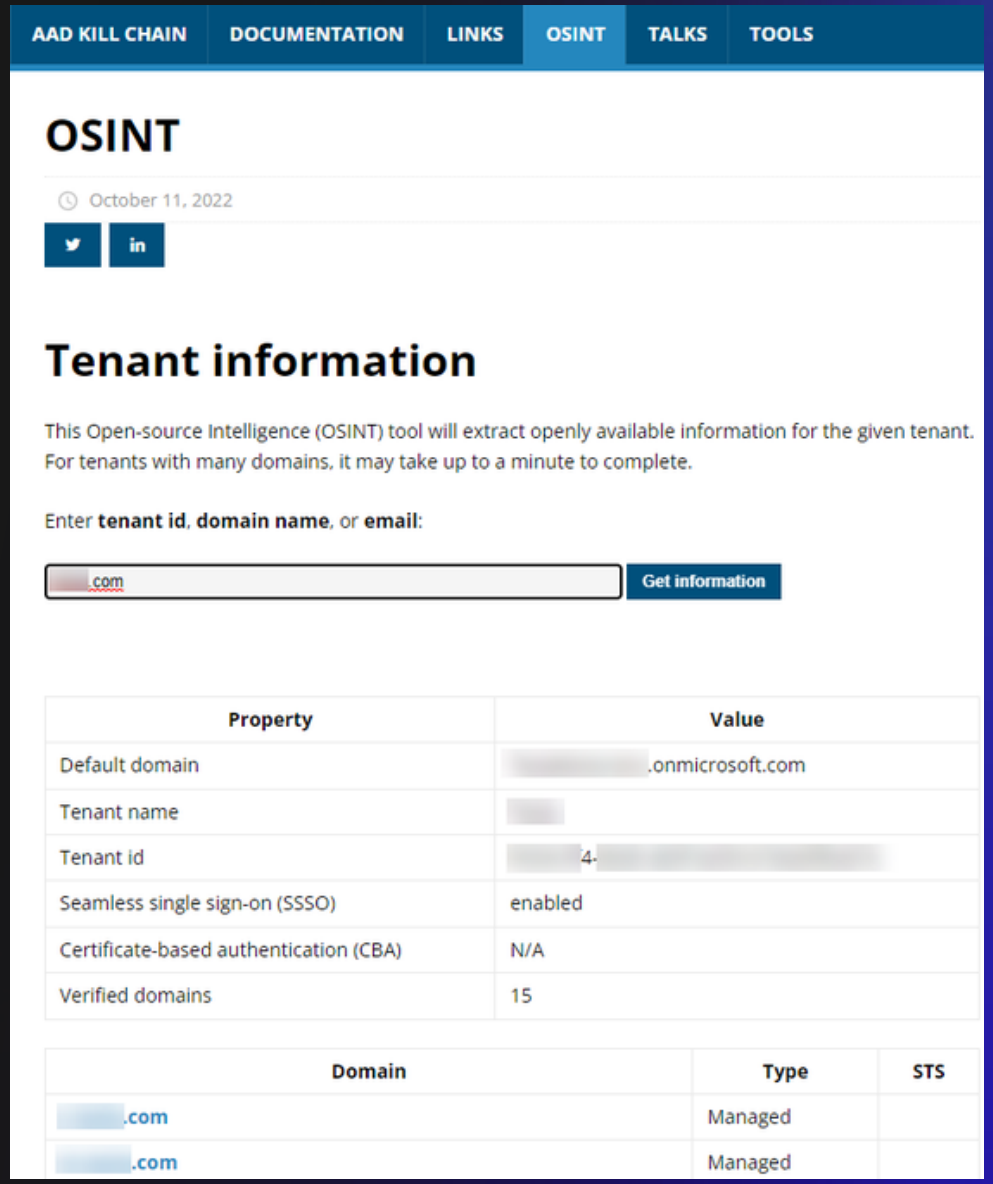

AADInternals 0.9.1
File Edit View Tools Debug Add-ons Help
Script
PS C:\>
Completed
Ln 1 Col 9
215%


AADInternals 0.9.1
File Edit View Tools Debug Add-ons Help
Script
PS C:\>
Completed
Ln 1 Col 9
215%


AADInternals 0.9.0
File Edit View Tools Debug Add-ons Help
Script
PS C:\>

AADInternals online OSINT tool

- https://aadinternals.com/osint
- Gathers basic OSINT information using various Azure AD APIs
  - Tenant name/id
  - Default domain
  - SSSO & CBA status
  - Teams status
  - Domain names
  - Domain details (type & STS)



Secureworks

Questions?

Secureworks®

Secureworks®