Speaker









AADInternals: How did I built the ultimate Azure AD hacking tool from the scratch



September 16th & 17th
Online Event

Powered By







Thank you to all our generous sponsors



Sponsored by





Supported by



Powered by

The Global Tech Community Platforn





Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @Secureworks
- Developer of AADInternals toolkit
- Microsoft MVPx2 (Identity and Access, Intune)
- Microsoft MVSR

Contact

- nsyynimaa@secureworks.com
- Twitter: <u>@DrAzureAD</u>
- https://linkedin.com/in/nestori
- https://o365blog.com













Agenda



- Introduction to AADInternals
- Why did I do it?
- Introduction to Microsoft APIs
- Examples:
 - Get-AADIntServiceLocations
 - Set-AADIntUserPassword



Introduction to AADinternals

AADInternals



- PowerShell module (>41000 lines of code)
- Admin & hacking toolkit for Azure AD & Office 365 (since Oct 2018)
- Open source:
 - https://github.com/gerenios/aadinternals
 - http://o365blog.com/aadinternals/
- Easy to install & use:



Why did I do it?

Background 1/2

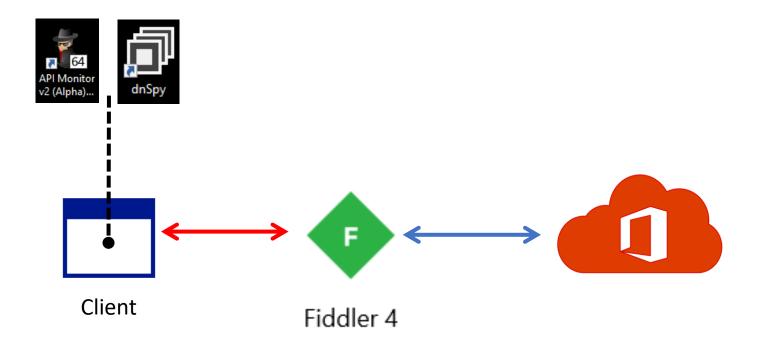


- Why AADInternals?
 - Easy way to contribute to the community
 - Increases the security awareness
 - No other tools for most functionality
- Why PowerShell?
 - Well, it is EASY to use
 - Most Microsoft administrative tasks use PowerShell

Background 2/2



- How?
 - Monitoring traffic between clients & cloud
 - Hours of reverse-engineering MS binaries



Results?



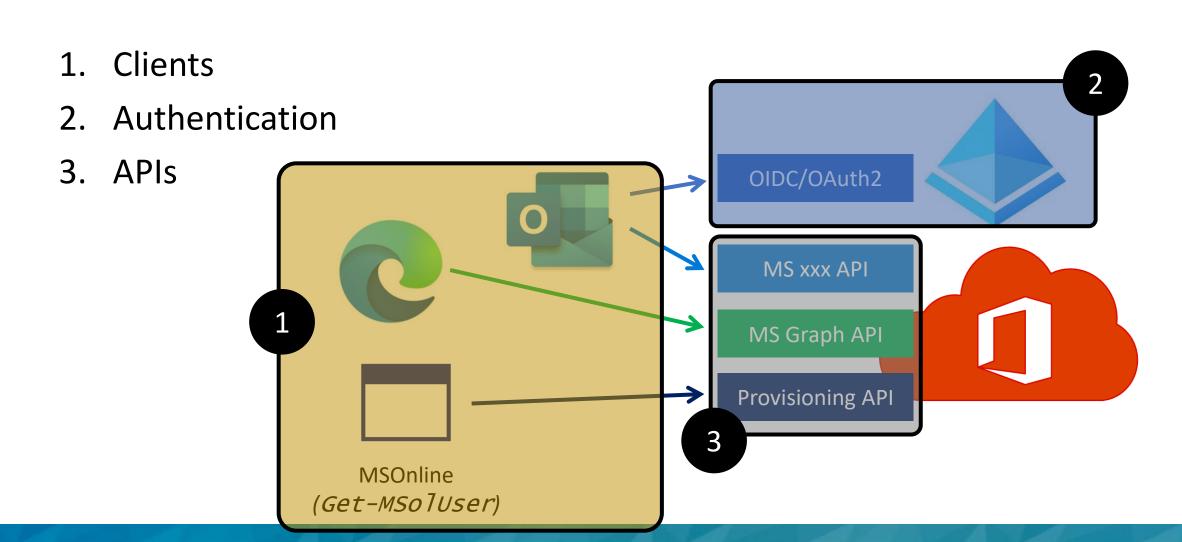
- Awarded MVP on Dec 2020 in Enterprise Mobility tech. area
 - Identity and Access
 - Intune
- Started as full-time security researcher on Apr 2021
- Awarded Most Valuable Security Researcher by MSRC on Aug 2021
- https://o365blog.com
 1 500+ weekly visitors
- 5 600+ AADInternals downloads from PSGallery



Introduction to MS APIs

How the cloud works 1/2



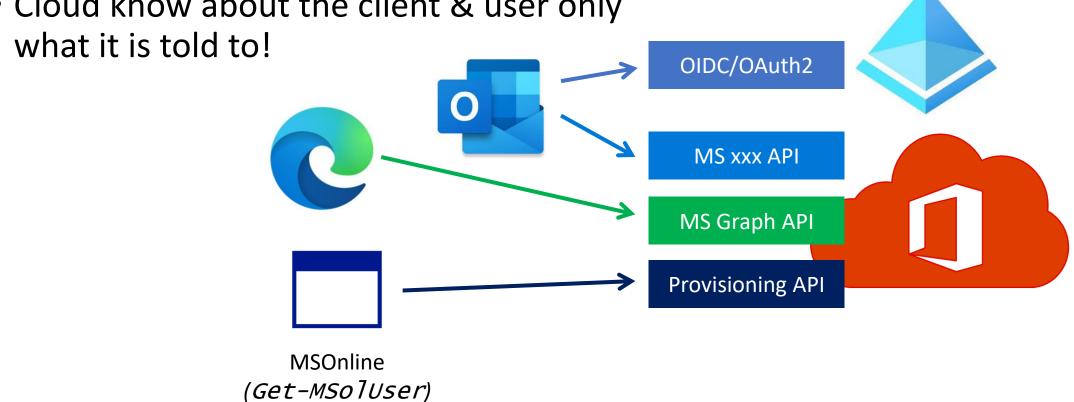


How the cloud works 2/2



Cloud (only) does what client tells it to do!

Cloud know about the client & user only



Some API endpoints



"Thing"	API	Address
MSOnline module	Provisioning API	https://provisioningapi.microsoftonline.com/ provisioningwebservice.svc
AzureAD module	<u>Azure AD Graph</u> (! <u>Microsoft Graph</u>)	https://graph.windows.net/ <tenant>/<command/></tenant>
Azure AD Connect	Sync provisioning service	https://adminwebservice.microsoftonline.com/ provisioningservice.svc



Examples

Get-AADIntServiceLocations



- Get-MsolCompanyInformation
 - Gets company wide settings from Azure AD
 - Content-Type: application/soap+xml
 - Only a subset of returned information is shown

```
DisplayName
                                          : Black Hat
PreferredLanguage
                                            en
Street
City
State
PostalCode
Country
CountryLetterCode
                                            US
TelephoneNumber
                                            8006427676
MarketingNotificationEmails
TechnicaĺNotificationEmails
                                            {admin@blackhat.myo365.site}
SelfServePasswordResetEnabled
                                            True
UsersPermissionToCreateGroupsEnabled
                                            True
UsersPermissionToCreateLOBAppsEnabled
                                            True
UsersPermissionToReadOtherUsersEnabled
                                            True
UsersPermissionToUserConsentToAppEnabled:
                                            True
DirectorySynchronizationEnabled
                                            True
                                            Sync_SERVER_2980bcb19aa3@M365x403056.onmicrosoft.com
DirSyncServiceAccount
LastDirSyncTime
                                            28.5.2020 7.08.53
LastPasswordSyncTime
                                            28.5.2020 7.12.06
PasswordSynchronizationEnabled
                                            True
```

```
<br/>

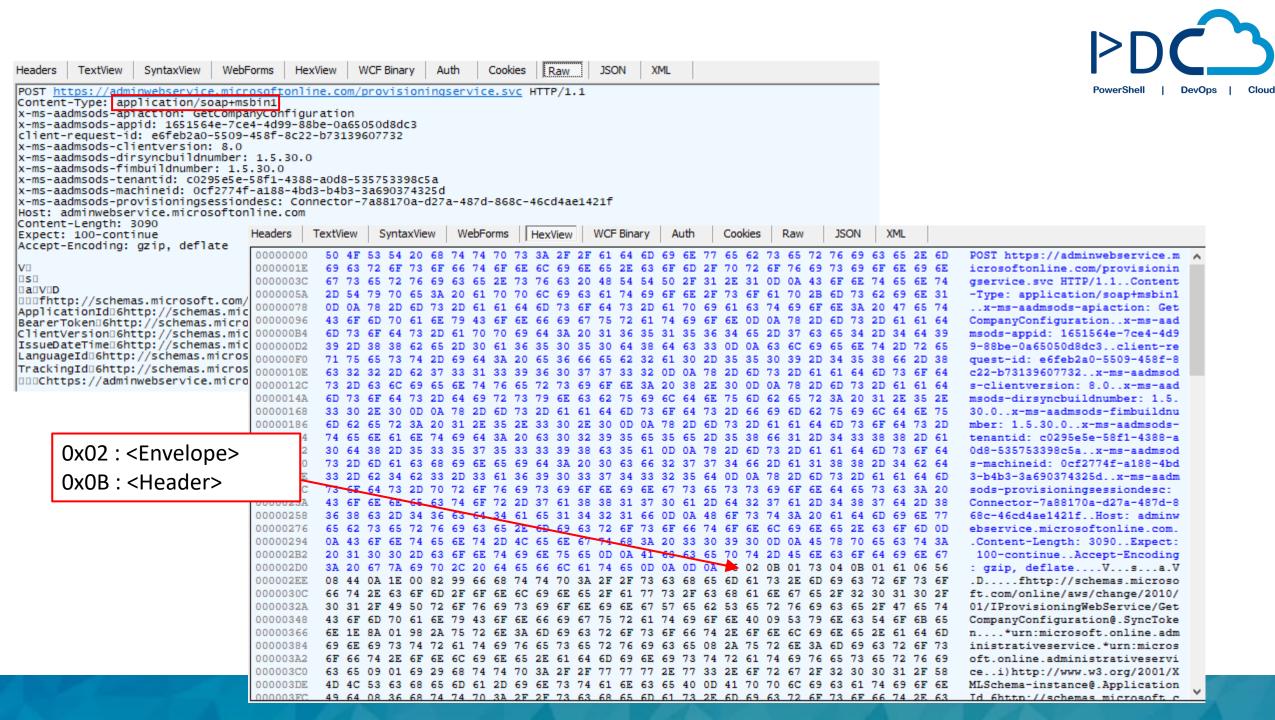
     <c:AllowAdHocSubscriptions>true</c:AllowAdHocSubscriptions>
     <c:AllowEmailVerifiedUsers>true</c:AllowEmailVerifiedUsers>
                                                                                                                             <c:ServiceInstanceInformation>
     <c:AuthorizedServiceInstances xmlns:d="http://schemas.microsoft.com/2003/10/Serialization"
                                                                                                                                     <c:ServiceInstanceInformation>
     <c:AuthorizedServices/>
     <c:City i:nil="true"/>
                                                                                                                                            <c:GeographicLocation>
     <c:CompanyDeletionStartTime i:nil="true"/>
                                                                                                                                                    <c:Country>US</c:Country>
     <c:CompanyTags xmlns:d="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
                                                                                                                                                    <c:Region>NA</c:Region>
     <c:CompanyType>CompanyTenant</c:CompanyType>
     <c:CompassEnabled i:nil="true"/>
                                                                                                                                                    <c:State i:nil="true"/>
     <c:Country i:nil="true"/>
                                                                                                                                            </c:GeographicLocation>
     <c:CountryLetterCode>US</c:CountryLetterCode>
     <c:DapEnabled i:nil="true"/>
                                                                                                                                            <c:ServiceInstance>Windows/SDF</c:ServiceInstance>
     <c:DefaultUsageLocation i:nil="true"/>
                                                                                                                                            <c:ServiceInstanceEndpoints i:nil="true"/>
     <c:DirSyncAnchorAttribute>mS-DS-ConsistencyGuid</c:DirSyncAnchorAttribute>
     <c:DirSvncApplicationTvpe>1651564e-7ce4-4d99-88be-0a65050d8dc3</c:DirSvncApplicationTv</pre>
                                                                                                                                     </c:ServiceInstanceInformation>
     <c:DirSyncClientMachineName>SERVER</c:DirSyncClientMachineName>
                                                                                                                                     <c:ServiceInstanceInformation>
     <c:DirSyncClientVersion>1.5.30.0</c:DirSyncClientVersion>
                                                                                                                                            <c:GeographicLocation>
     <c:DirSyncServiceAccount>Sync SERVER 2980bcb19aa3@M365x403056.onmicrosoft.com</c:DirSy</pre>
     <c:DirectorySynchronizationEnabled>true</c:DirectorySynchronizationEnabled>
                                                                                                                                                    <c:Country>US</c:Country>
     <c:DirectorySynchronizationStatus>Enabled</c:DirectorySynchronizationStatus>
                                                                                                                                                    <c:Region>NA</c:Region>
     <c:DisplayName>Black Hat</c:DisplayName>
     <c:InitialDomain>M365x403056.onmicrosoft.com</c:InitialDomain>
                                                                                                                                                    <c:State i:nil="true"/>
     <c:LastDirSyncTime>2020-05-28T09:39:08Z</c:LastDirSyncTime>
                                                                                                                                            </c:GeographicLocation>
     <c:LastPasswordSyncTime>2020-05-28T09:12:52Z</c:LastPasswordSyncTime>
                                                                                                                                            <c:ServiceInstance>SCO/PROD AMSUA0502 03</c:ServiceInstance>
     <c:MarketingNotificationEmails xmlns:d="http://schemas.microsoft.com/2003/10/Serializa
     <c:MultipleDataLocationsForServicesEnabled i:nil="true"/>
                                                                                                                                            <c:ServiceInstanceEndpoints i:nil="true"/>
     <c:ObjectId>c0295e5e-58f1-4388-a0d8-535753398c5a/c:ObjectId>
                                                                                                                                    </c:ServiceInstanceInformation>
     <c:PasswordSynchronizationEnabled>true</c:PasswordSynchronizationEnabled>
     <c:PortalSettings>
                                                                                                                                     <c:ServiceInstanceInformation>
     <c:PostalCode i:nil="true"/>
                                                                                                                                            <c:GeographicLocation>
     <c:PreferredLanguage>en</c:PreferredLanguage>
                                                                                                                                                    <c:Country>US</c:Country>
     <c:ReleaseTrack>FirstRelease</c:ReleaseTrack>
     <c:ReplicationScope>NA</c:ReplicationScope>
                                                                                                                                                    <c:Region>NA</c:Region>
     <c:RmsViralSignUpEnabled>true</c:RmsViralSignUpEnabled>
                                                                                                                                                    <c:State i:nil="true"/>
     <c:SecurityComplianceNotificationEmails xmlms:d="http://schemas.microsoft.com/2003/10/
     <c:SecurityComplianceNotificationPhones xmlns:d="http://schemas.microsoft.com/2003/10/</pre>
                                                                                                                                            </c:GeographicLocation>
     <c:SelfServePasswordResetEnabled>true/c:SelfServePasswordResetEnabled>
                                                                                                                                            <c:ServiceInstance>MultiFactorService/NA001</c:ServiceInstance>
     <c:ServiceInformation>
     <c:ServiceInstanceInformation>
                                                                                                                                            <c:ServiceInstanceEndpoints i:nil="true"/>
     <c:State i:nil="true"/>
                                                                                                                                     </c:ServiceInstanceInformation>
     <c:Street i:nil="true"/>
     <c:SubscriptionProvisioningLimited>false</c:SubscriptionProvisioningLimited>
     <c:TechnicalNotificationEmails xmlns:d="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
     <c:TelephoneNumber>8006427676</c:TelephoneNumber>
     <c:UIExtensibilityUris i:nil="true" xmlns:d="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/>
     <c:UsersPermissionToCreateGroupsEnabled>true</c:UsersPermissionToCreateGroupsEnabled>
     <c:UsersPermissionToCreateLOBAppsEnabled>true</c:UsersPermissionToCreateLOBAppsEnabled>
     <c:UsersPermissionToReadOtherUsersEnabled>true</c:UsersPermissionToReadOtherUsersEnabled>
     <c:UsersPermissionToUserConsentToAppEnabled>true</c:UsersPermissionToUserConsentToAppEnabled>
     <c:WhenCreated>2019-07-14T07:03:20Z</c:WhenCreated>
```

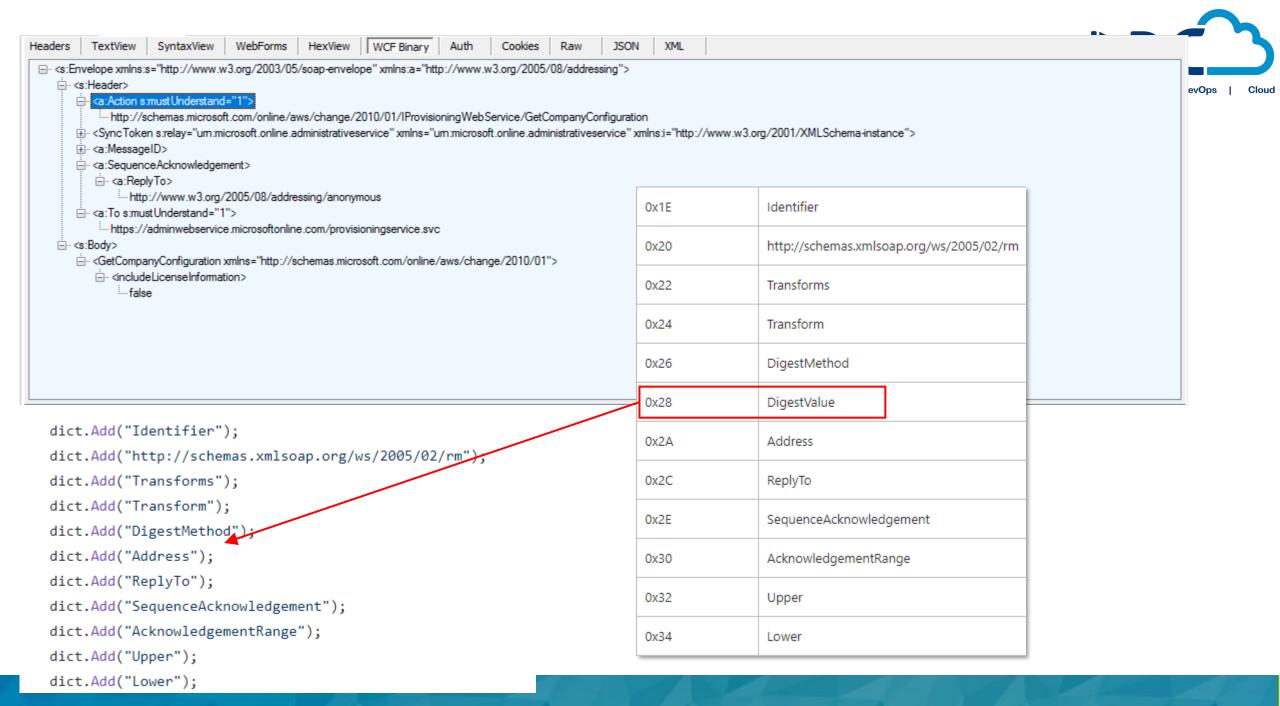
</b:ReturnValue>

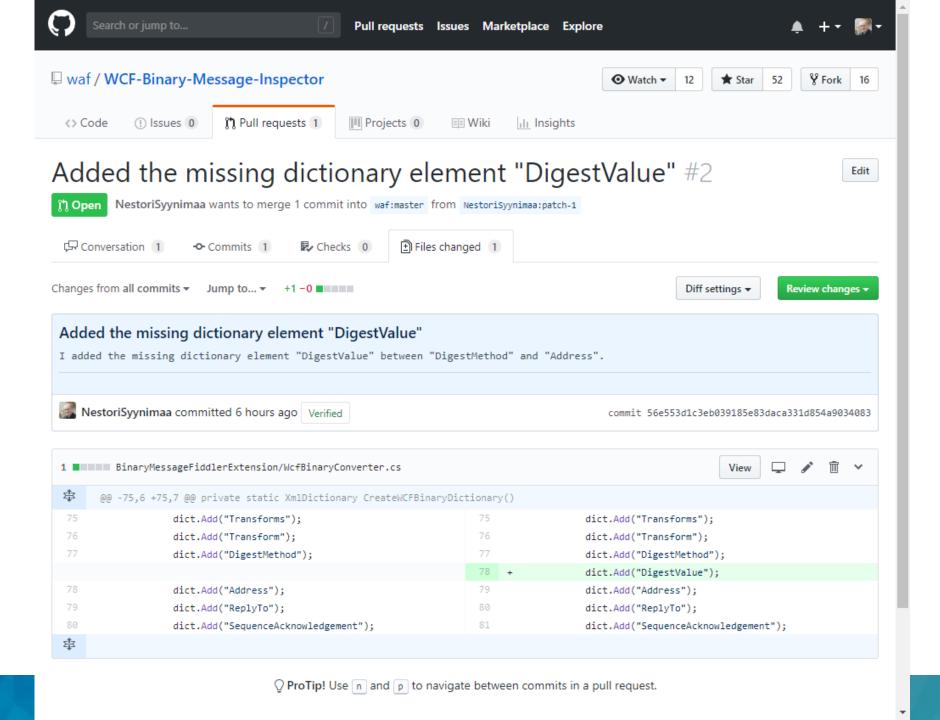
Set-AADIntUserPassword



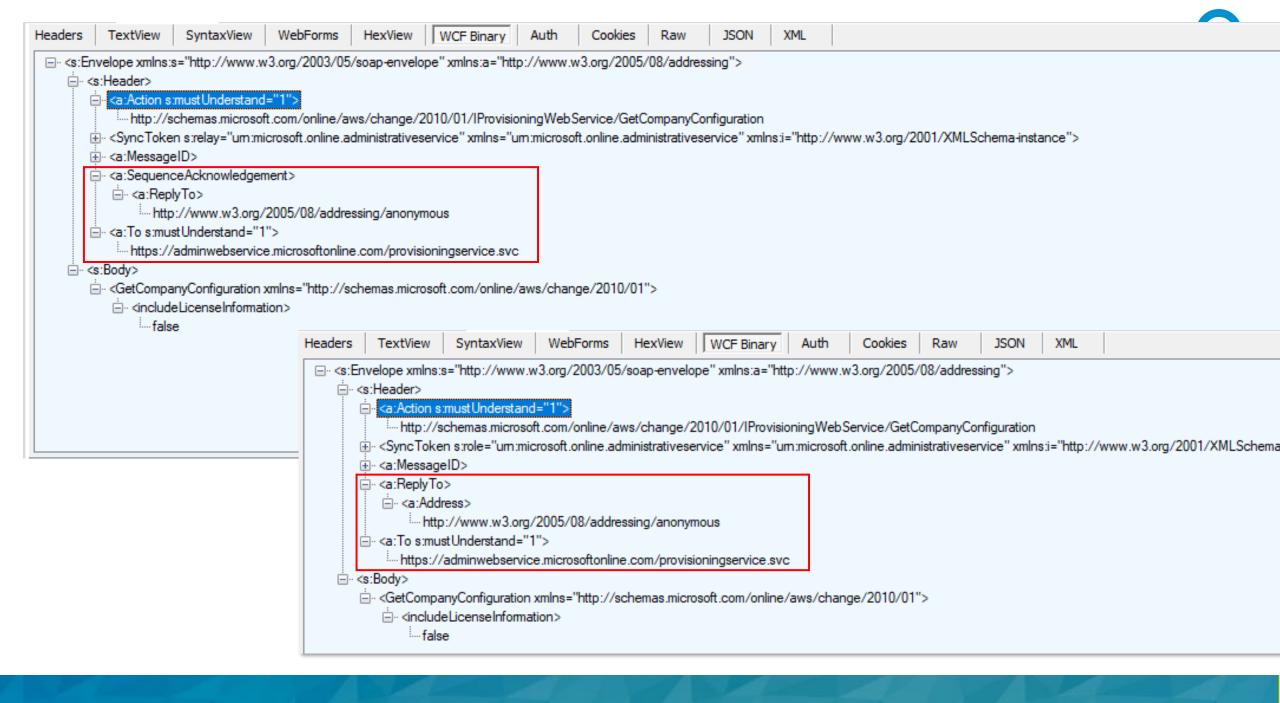
- Azure AD Connect (if configured) synchronises password hashes from Active Directory to Azure AD
- Content-Type: application/soap+msbin1 😸
- WCF Binary Message Inspector by Will Fuqua!







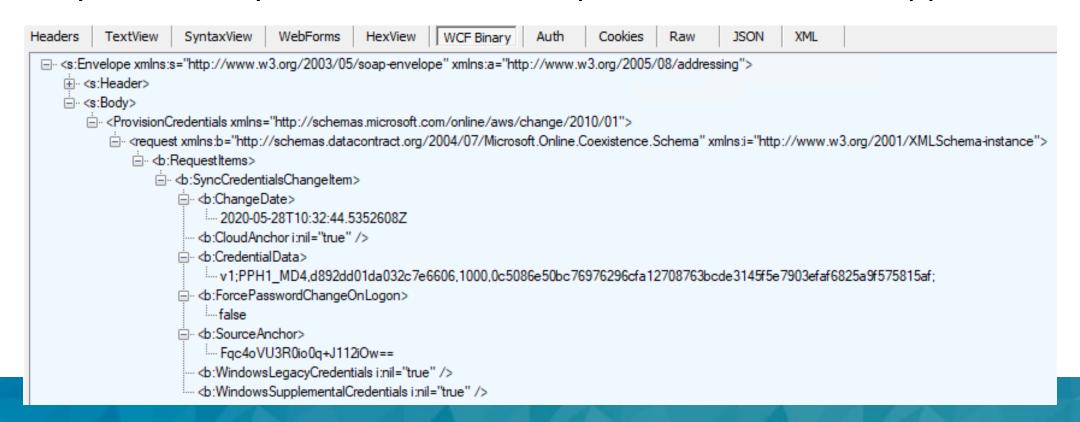




Set-AADIntUserPassword



- Password Hash, change timestamp, and force password change
- Hash is a PBKDF2 (Password-Based Key Derivation Function 2)
- Only a hash is synchronised -> cloud pwd restrictions not applied ☺



Summary



- PowerShell module is a great way to share your knowledge!
- Cloud changes all the time...

