



Cloud Pentesting Bootcamp





Phillip Wylie

Offensive Cyber Security Expert

✉ pwylie@ine.com

🐦 [@PhillipWylie](https://twitter.com/PhillipWylie)

in linkedin.com/in/phillipwylie





Penetration Testing of Azure





Slavi Parpulev

IT Security Expert

✉ sparpulev@ine.com

🐦 [@binary_raider](https://twitter.com/binary_raider)

in [linkedin.com/in/slavi-parpulev/](https://www.linkedin.com/in/slavi-parpulev/)





Tracy Wallace

Azure Solutions Architect Expert



twallace@ine.com



@TracyWallaceINE



linkedin.com/in/tracy-wallace-746482a



Course Outline

Initial Access

- Azure Kill Chain
- Phishing, Password guessing, On-prem to AAD
- Access to Azure and MFA Bypass options

Enumeration & Privilege Escalation

- Enumerating Azure & AzureAD from different roles
- Identifying and abusing escalation paths

On-Premise Attacks

- Abuse on-prem technologies to access Azure
 - Golden SAML
 - Pass the PRT
 - On-prem AD attacks to gain privileged access to Azure



Penetration Testing & Authorizations



Agenda

- + What is Penetration Testing (Pentesting)?
- + Rule of Engagement for Pentesting Azure

Penetration Testing

- + What is Penetration Testing?
- + What is the objective of a Penetration Test?



Customer Agreements

- + Penetration test preparation and agreement
 - + Scope
 - + Time
 - + Information from the customer (Highly recommended)
 - + Get Out of Jail card



Azure AD & Azure Kill Chain

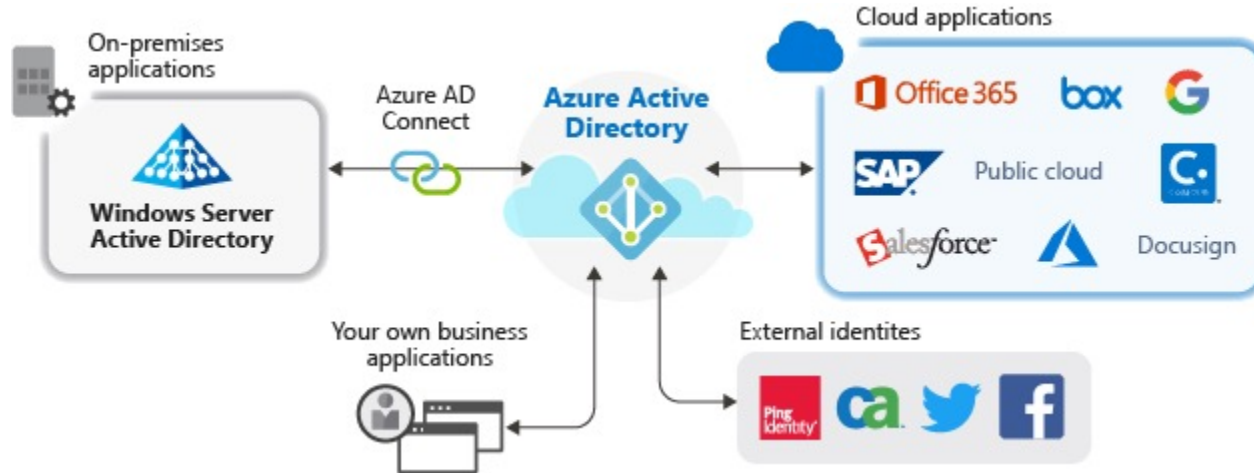


Agenda

- + Azure AD
- + Initial Access
- + Azure Kill Chain

Azure AD

+ Azure Active Directory



Azure AD

- + Azure Active Directory is not 'legacy' Active Directory in the cloud
- + Azure Active Directory Domain Services
- + Virtual Machines in Azure running legacy Active Directory

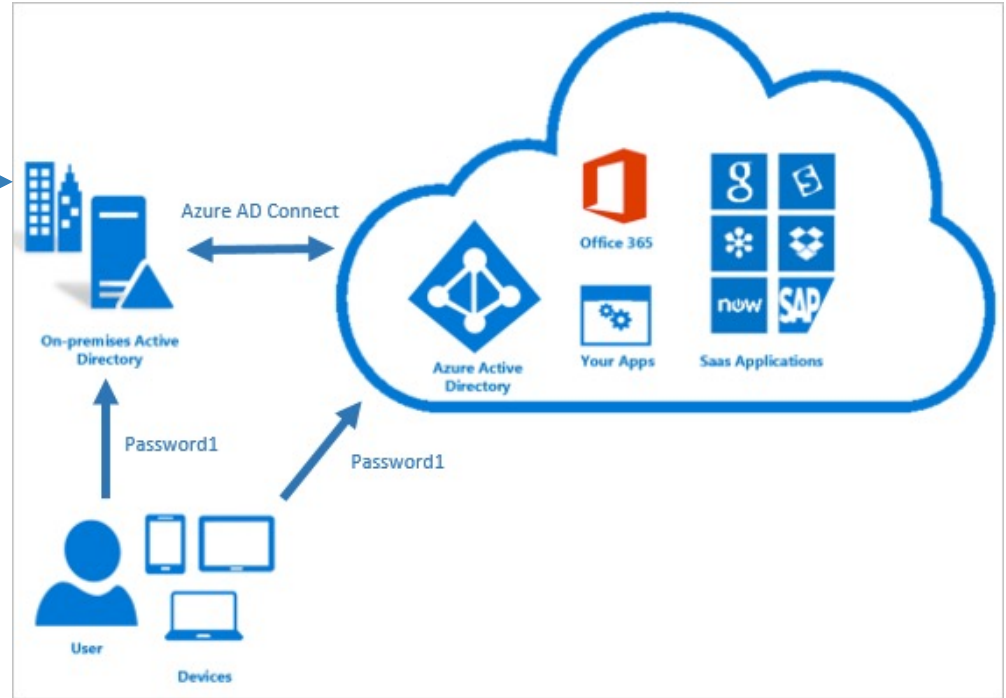
Azure AD

+ AD vs AAD

(Windows Server) Active Directory	Azure Active Directory
LDAP	REST API's
NTLM/Kerberos	OAuth/SAML/OpenID/etc
Structured directory (OU tree)	Flat structure
GPO's	No GPO's
Super fine-tuned access controls	Predefined roles
Domain/forest	Tenant
Trusts	Guests

Azure AD

- + AD to AAD Integration
- + Password hash synchronization
- + ADFS
- + Pass through authentication



+ Roles

Home > Default Directory - Roles and administrators

Default Directory - Roles and administrators

Azure Active Directory

Search (Ctrl+/)

Overview

Getting started

Manage

- Users
- Groups
- Organizational relationships
- Roles and administrators**
- Enterprise applications
- Devices
- App registrations
- App registrations (Preview)
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding

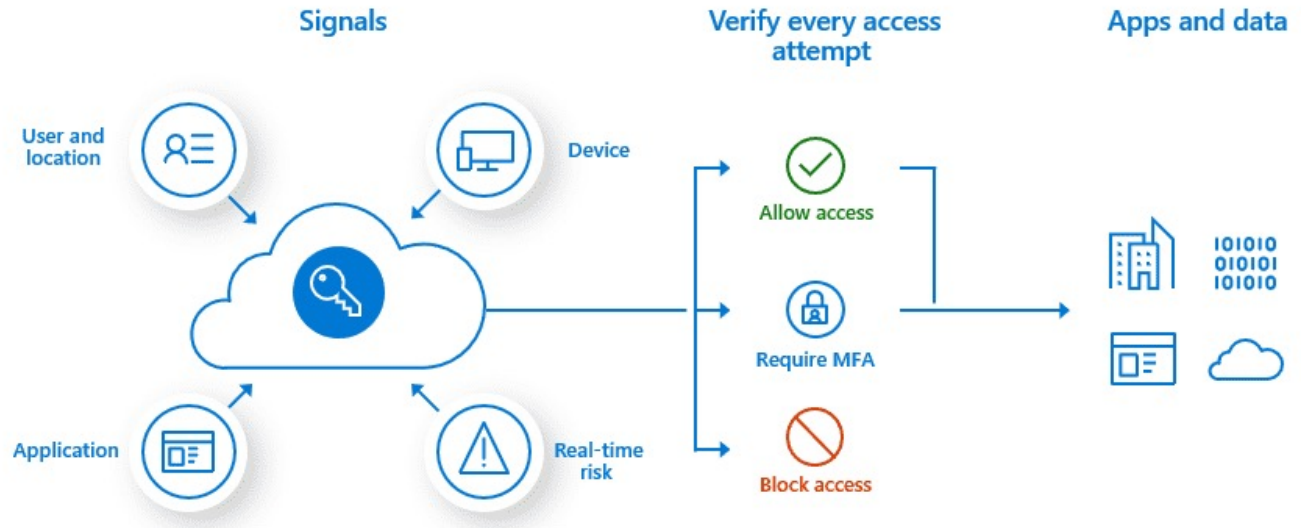
Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

Your Role: Global administrator and 2 other roles

ROLE	DESCRIPTION
Application administrator	Can create and manage all aspects of app registrations and enterprise...
Application developer	Can create application registrations independent of the 'Users can reg...
Billing administrator	Can perform common billing related tasks like updating payment info...
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise...
Cloud device administrator	Full access to manage devices in Azure AD.
Compliance administrator	Can read and manage compliance configuration and reports in Azure ...
Conditional Access administrator	Can manage conditional access capabilities.
Customer LockBox access approver	Can approve Microsoft support requests to access customer organiza...
Desktop Analytics administrator	Can access and manage Desktop management tools and services.
Dynamics 365 administrator	Can manage all aspects of the Dynamics 365 product.
Exchange administrator	Can manage all aspects of the Exchange product.
Global administrator	Can manage all aspects of Azure AD and Microsoft services that use A...
Guest inviter	Can invite guest users independent of the 'members can invite guests...
Information Protection administrator	Can manage all aspects of the Azure Information Protection product.

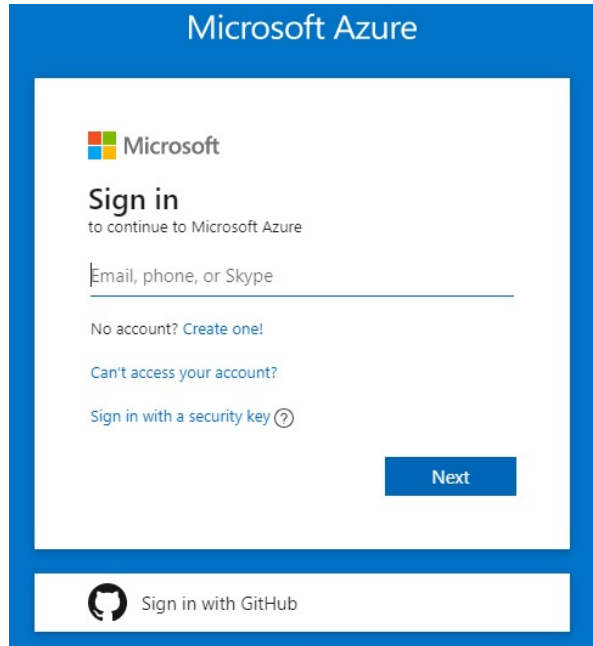
Azure AD

- + Protections
 - + Access Control Policies
 - + Identity Protection



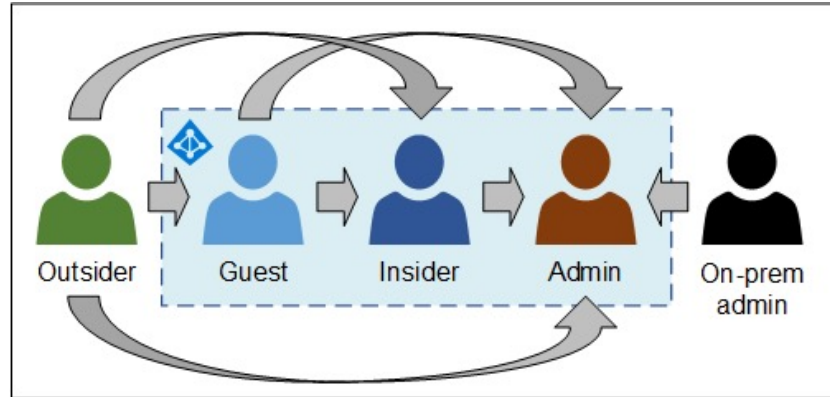
Initial Access

- + Initially – no access
 - + “Outsider” user role



The image shows a screenshot of the Microsoft Azure sign-in page. The page has a blue header with the text "Microsoft Azure". Below the header, there is a white box containing the Microsoft logo and the text "Microsoft". The main heading is "Sign in" followed by "to continue to Microsoft Azure". There is a text input field with the placeholder text "Email, phone, or Skype". Below the input field, there are three links: "No account? Create one!", "Can't access your account?", and "Sign in with a security key (?)". A blue "Next" button is located at the bottom right of the white box. At the bottom of the page, there is a white box with the GitHub logo and the text "Sign in with GitHub".

Azure Kill Chain





Phishing & MFA



Agenda

- + Initial Access through Phishing
- + MFA
- + Legacy Protocols
- + MFA Bypass (through Phishing)

Initial Access Through Phishing

- + Phishing username/password



Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

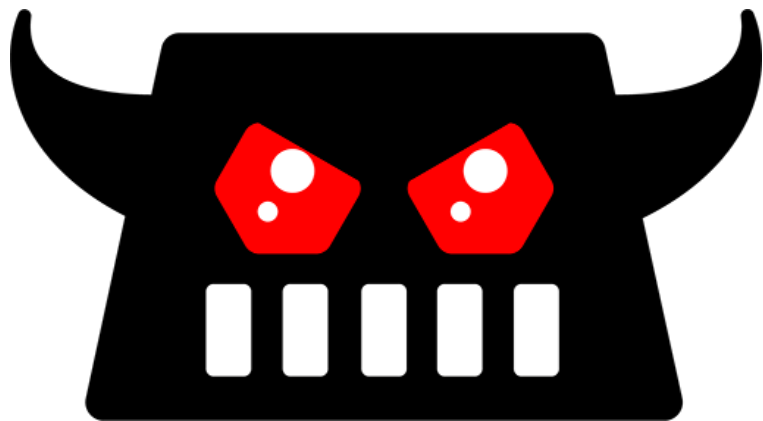
Back

Next



Initial Access Through Phishing

- + Evilginx2
 - + MiTM Framework for phishing credentials and session cookies



<https://github.com/kgretzky/evilginx2>



Password Spraying & Reuse

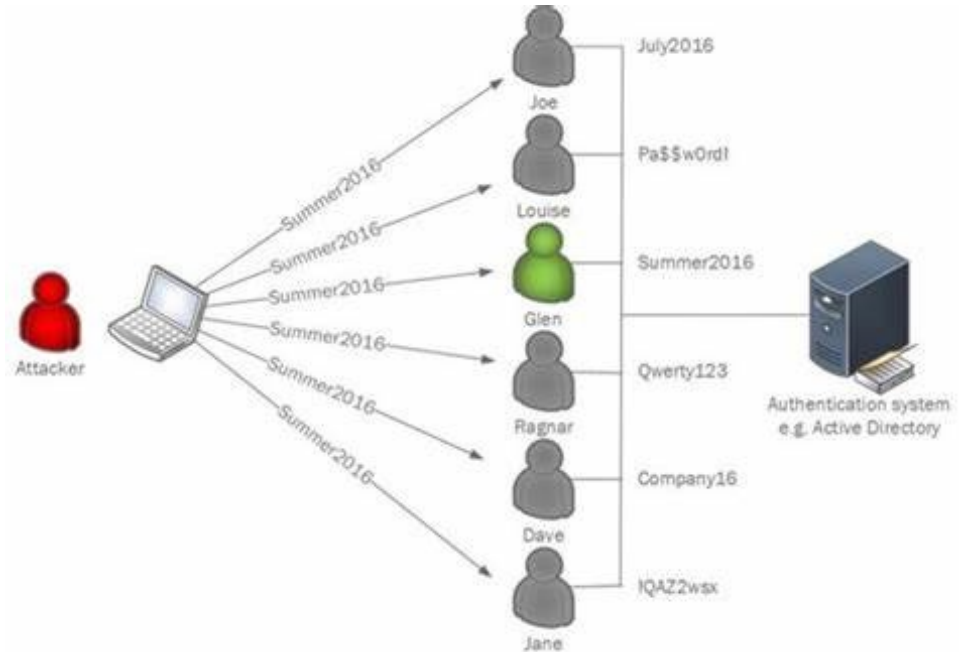


Agenda

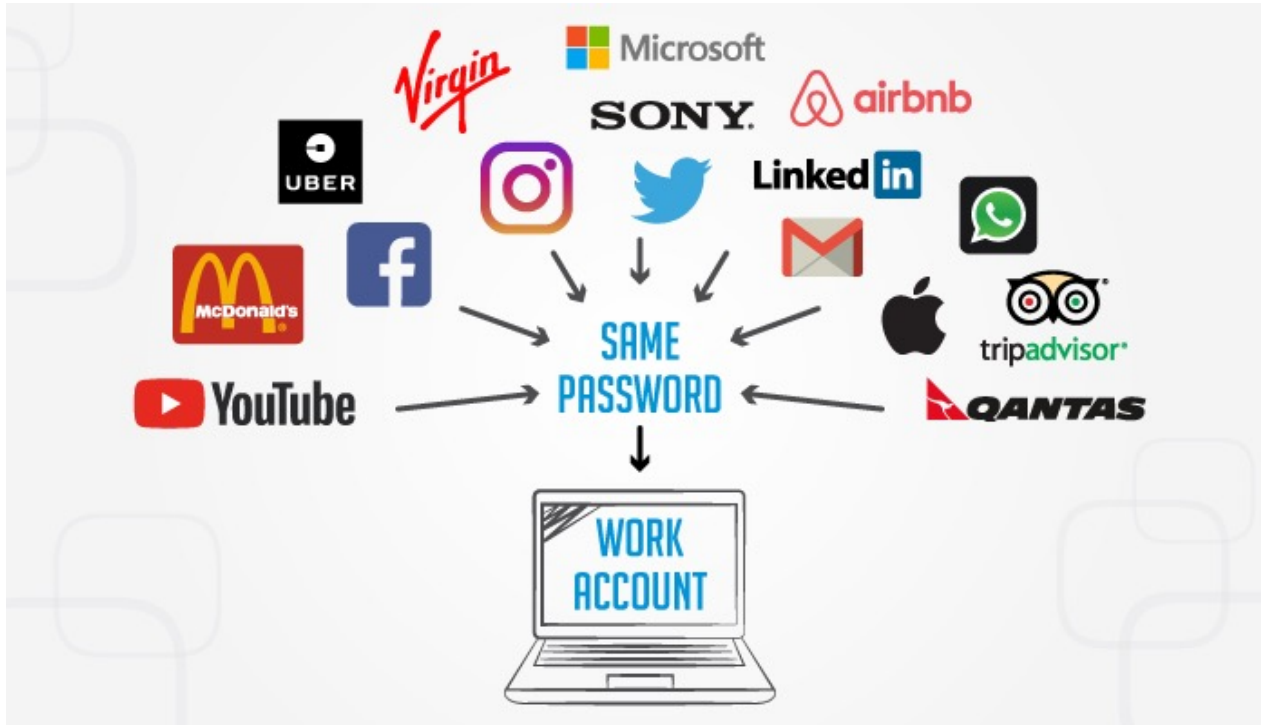
- + Password Spraying
- + Password Reuse
- + Passwords in Github

Password Spraying

- + Enumerating Azure
- + Spraying
- + Legacy protocols



Password Reuse



Passwords in Github

filename:.env MAIL_HOST=smtp.gmail.c / Pull requests Issues Marketplace Explore

Showing 6,630 available code results Sort: Best match

Repository Statistics:

- Repositories: 1
- Code: 6K+
- Commits: 532+
- Issues: 101
- Packages: 0
- Marketplace: 0
- Topics: 0
- Wikis: 10
- Users: 0

Languages:

PHP	61
Text	42
SQL	9
Shell	9
Roff	6
Elixir	4
HTML	2
INI	2
Java	1
JavaScript	1

Result 1: linares82/crm36

```
.env
37 #MAIL_ENCRYPTION=tls
38
39 #MAIL_DRIVER=smtp
40 #MAIL_HOST=smtp.gmail.com
41 #MAIL_PORT=587
42 #MAIL_USERNAME=linares82@gmail.com
43 #MAIL_PASSWORD=*****
44 #MAIL_ENCRYPTION=tls
45
46 MAIL_DRIVER=smtp
47 MAIL_HOST=smtp.gmail.com
48 MAIL_PORT=587
```

Showing the top 12 matches Last indexed on Jul 15, 2018

Result 2: AliaksandrHaurylenka/laravel-sport-kostukovka

```
.env
31 REDIS_HOST=127.0.0.1
32 REDIS_PASSWORD=*****
33 REDIS_PORT=6379
34
35
36
37 #====Mailtrap====
38 #MAIL_DRIVER=smtp
39 #MAIL_HOST=smtp.mailtrap.io
40
41
42 MAIL_DRIVER=smtp
43 MAIL_HOST=smtp.gmail.com
44 MAIL_PORT=587
45
46 MAIL_USERNAME=*****
47 MAIL_PASSWORD=*****
```





On-Prem to Azure

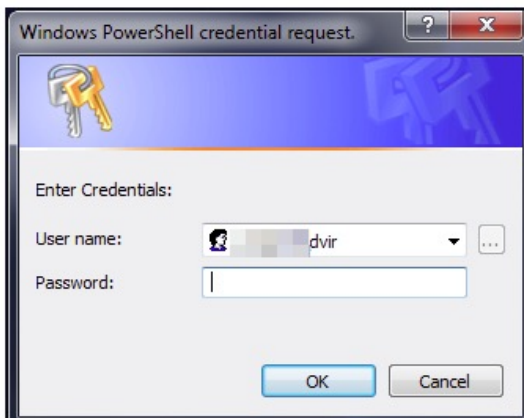


Agenda

- + Interacting with a Compromised User
- + Credential Dumping
- + Credentials in Files or AD Attributes
- + Browser Pivots & Cookies
- + Azure Service Principals

Interacting with a Compromised User

This script will display a powershell credentials box that will ask the user for his credentials.



The box cannot be closed (only by killing the process) will keeps checking the credentials against the DC. When validated, it will close and leak it to a web server outside.

```
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.28.1 - - [30/Aug/2017 07:36:23] code 404, message File not found
192.168.28.1 - - [30/Aug/2017 07:36:23] "GET /;dvir HTTP/1.1" 404
192.168.28.1 - - [31/Aug/2017 05:08:18] code 404, message File not found
```



Credential Dumping

```
Authentication Id : 0 ; 2594251 (00000000:002795cb)
Session          : Service from 0
User Name        : svc-SQLAnalysis
Domain           : ADSECLAB
SID              : S-1-5-21-1473643419-774954089-2222329127-1608
msv :
  [0000000021] Binary
    * Username : svc-SQLAnalysis
    * Domain   : ADSECLAB
    * NTLM     : 3c917b61c58c4cba165396aad7d140a2
    * SHA1     : f089edb437e1f455ac1ab65886ed51959df7dc30
  tspkg :
    * Username : svc-SQLAnalysis
    * Domain   : ADSECLAB
    * Password : ThisIsAnOKPassword99!
  wdigest :
    * Username : svc-SQLAnalysis
    * Domain   : ADSECLAB
    * Password : ThisIsAnOKPassword99!
  kerberos :
    * Username : svc-SQLAnalysis
    * Domain   : LAB.ADSECURITY.ORG
    * Password : ThisIsAnOKPassword99!
  ssp :
  credman :
```



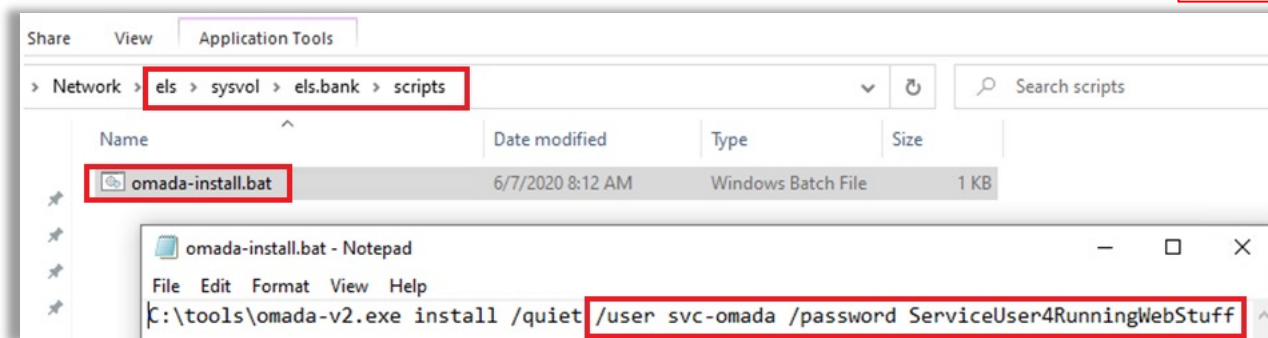
Credentials in Files or AD Attributes

+ Passwords in scripts placed on shares

+ Invoke-ShareFinder

```
findstr /s /i /m "pass" \\SHARE\PATH\*.*<FILEEXTENSION>  
findstr /s /i /m "pass" \\FileServer01\Scripts\*.ini
```

.ini
.conf
.config
.cmd
.bat
.vbs
.ps1



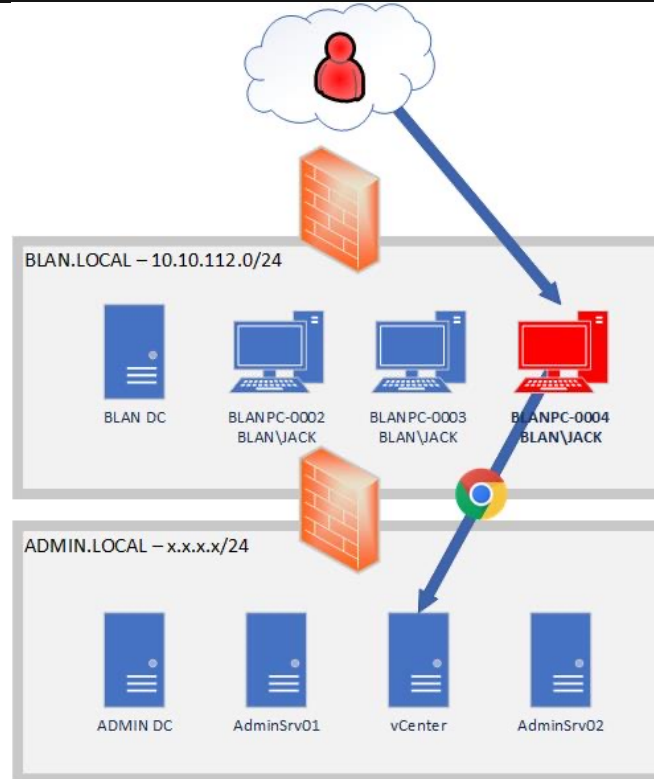
Credentials in Files or AD Attributes

```
C:\Users\analyst1\Desktop>SharpView.exe get-domainuser -SamAccountName slavi
[Get-DomainSearcher] search base: LDAP://BANK-DC.ELS.BANK/DC=ELS,DC=BANK
[Get-DomainUser] filter string: (&(samAccountType=805306368)(|(samAccountName=slavi)))
objectsid : {S-1-5-21-3192643952-2658629199-322554960-1602}
samaccounttype : USER_OBJECT
objectguid : 5696667b-8eb0-4334-bdd7-08a8a8f9c09d
useraccountcontrol : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
accountexpires : NEVER
lastlogon : 6/9/2020 9:00:07 AM
lastlogontimestamp : 6/7/2020 11:03:00 AM
pwdlastset : 6/8/2020 12:54:58 PM
lastlogoff : 12/31/1600 4:00:00 PM
badPasswordTime : 12/31/1600 4:00:00 PM
name : Slavi
distinguishedname : CN=Slavi,OU=Users,OU=Playground,DC=els,DC=bank
whencreated : 6/5/2020 7:08:17 PM
whenchanged : 6/18/2020 3:56:08 PM
samaccountname : slavi
memberof : {CN=SG_PIM,OU=Groups,OU=Playground,DC=els,DC=bank}
cn : {Slavi}
objectclass : {top, person, organizationalPerson, user}
displayname : Slavi
msds-supportedencryptiontypes : 0
givenname : Slavi
badpwdcount : 0
countrycode : 0
usnchanged : 75511
logoncount : 16
primarygroupid : 513
objectcategory : CN=Person,CN=Schema,CN=Configuration,DC=els,DC=bank
userprincipalname : slavi@els.bank
description : pass: Welcome123
uscorepropagationdata : {6/7/2020 1:55:34 PM, 6/7/2020 1:53:12 PM, 1/1/1601 12:04:17 AM}
usncreated : 57867
```

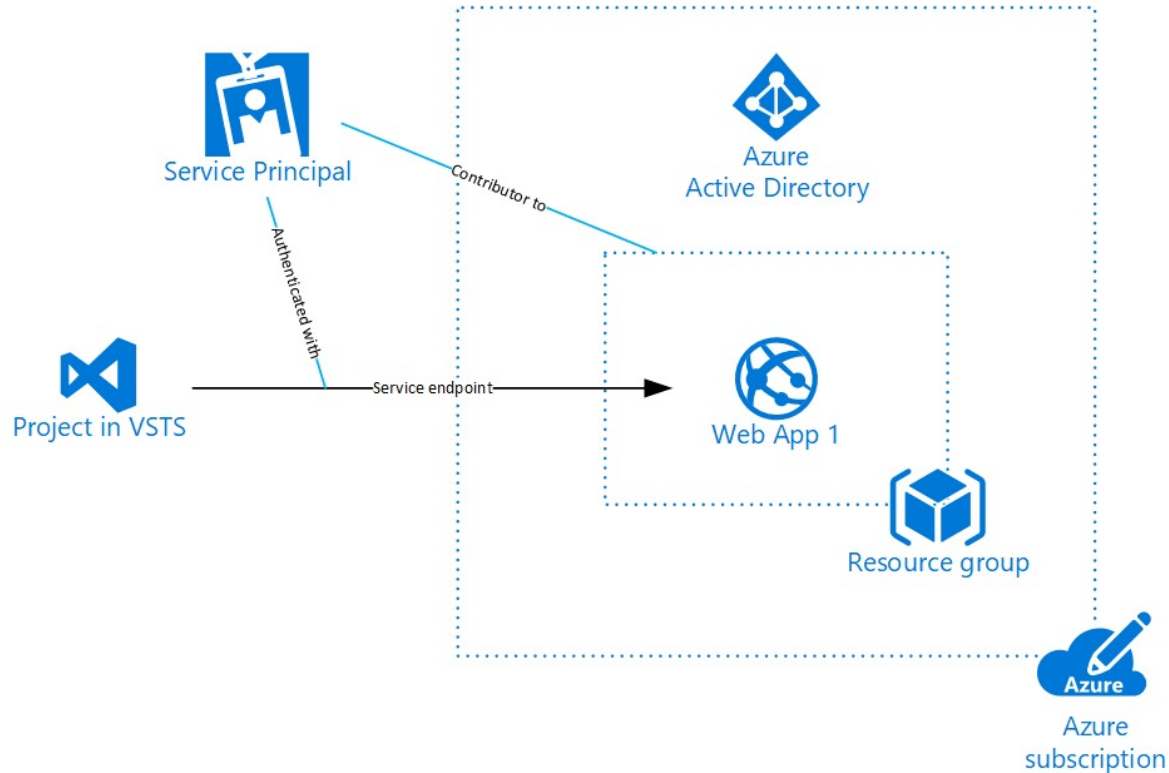
Active Directory state-of-the-art attacks

- + Kerberoasting
- + Asreproasting
- + Keberos Delegation attacks
 - + Unconstrained Delegation
 - + Constrained Delegation
 - + Resource-Based Delegation
- + Group Policy Preferences

Browser Pivots



Azure Service Principals





Cloud Pentesting Bootcamp Day 2





Enumeration & Privilege Escalation



Agenda

- + Enumerating Azure & AzureAD from different roles
- + Identifying and abusing escalation paths



Enumerating Azure & Azure AD from different roles



Agenda

- + Enumerating as Guest
- + Enumerating as Member

Azure AD Account Types

- + Account Types Overview

Azure AD Account Types

- + Guest
- + Member

Azure AD Guest

- + Azure Active Directory (Azure AD) business-to-business (B2B) collaboration is a feature within External Identities that lets you invite guest users to collaborate with your organization. With B2B collaboration, you can securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data. Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources. Developers can use Azure AD business-to-business APIs to customize the invitation process or write applications like self-service sign-up portals. For licensing and pricing information related to guest users, refer to [Azure Active Directory pricing](#).

Azure AD Member

+ Member

Azure AD User Enumeration

+ Get-AzureADUser



Identifying and abusing escalation paths



Identifying and abusing escalation paths

- + Abusing Dynamic Groups
- + Abusing Managed Identities

<https://www.mnemonic.no/blog/abusing-dynamic-groups-in-azure/>

<https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-privilege-escalation-using-managed-identities/>





Cloud Pentesting Bootcamp Day 3





On-Premise Attacks



Agenda

- + Abuse on-prem technologies to access Azure
 - + Golden SAML
 - + Pass the PRT
 - + On-prem AD attacks to gain privileged access to Azure

Golden SAML

- + The vector enables an attacker to create a golden SAML, which is basically a forged SAML “authentication object,” and authenticate across every service that uses SAML 2.0 protocol as an SSO mechanism. [1]
- + Not an Azure only attack vector
- + Golden SAML was used in Solarwinds

[1]<https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps>
<https://www.sygnia.co/golden-saml-advisory>
<https://attack.mitre.org/techniques/T1606/002/>



Pass the PRT

- + A Primary Refresh Token (PRT) is a key artifact of Azure AD authentication on Windows 10, iOS, and Android devices. It is a JSON Web Token (JWT) specially issued to Microsoft first party token brokers to enable single sign-on (SSO) across the applications used on those devices. [1]

[1] <https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-primary-refresh-token>
<https://o365blog.com/post/prt/>
<https://stealthbits.com/blog/lateral-movement-to-the-cloud-pass-the-prt/>

On-prem AD attacks to gain privileged access to Azure

- + Although on-prem administrators doesn't usually have admin rights to Azure AD, they can have access to crucial information, such as Azure AD Connect, ADFS, and Active Directory. Administrators of these services can easily get admin rights to Azure AD to manipulate and impersonate users. [1]

[1] https://o365blog.com/post/on-prem_admin/