NETSPI

ADVENTURES IN
AZURE PRIVILEGE ESCALATION

Karl Fosaaen

WHO AM I

- Karl Fosaaen
  - Pen Tester
  - Password Cracker
  - Social Engineer
  - Blogger
  - Cloud Enthusiast
  - Private Pilot

- https://github.com/netspi
- https://blog.netspi.com/
- Twitter - @kfosaaen

INTRODUCTION

- Everyone is moving to the cloud
  - Developers
  - Sys Admins
  - Pen Testers

- Azure Benefits
  - AzureAD
    - Integrated AD users/groups
  - One-stop licensing
  - Easy to integrate

INTRODUCTION

- For the folks at home, this will assume some level of Azure knowledge, feel free to pause here, watch the following talks, and come back when you're done
- Primer Talks:
  - You Moved to O365, Now What? - https://www.youtube.com/watch?v=1loGEPn_n7U
  - Attacking & Defending the Microsoft Cloud - https://adsecurity.org/?p=4179
  - I'm in your cloud… - https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Dirk-jan-Mollema-Im-in-your-cloud-pwning-your-azure-environment.pdf
  - Attacking Azure w/PowerShell - https://www.youtube.com/watch?v=IdORwgxDpkw

INITIAL ENTRY POINTS

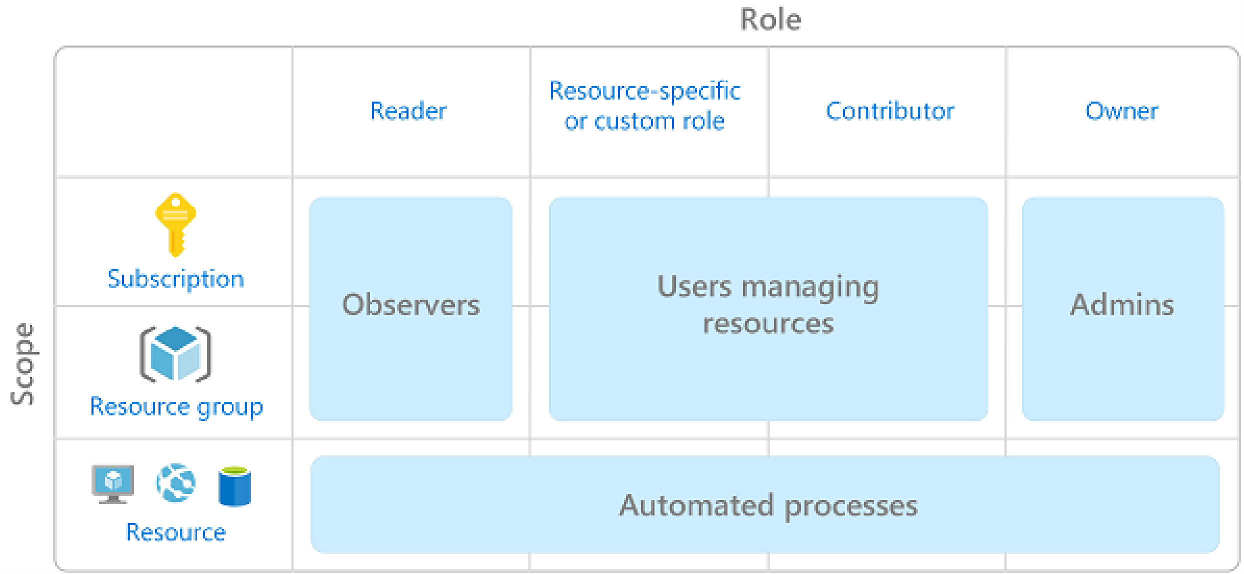
- How to get credentials in the first place
  - This talk is about privilege escalation, but first we need access

- Gathered Credentials
  - GitHub/PasteBin/etc.
- Guessed Creds
  - Summer2019
- How to access Azure
  - Azure Portal – portal.azure.com
  - Azure CLI
  - PowerShell - AzureRM /AZ CLI / MSOnline

AZURE PERMISSIONS MODEL

- Tenant Level
  - Global Admin
- Subscription Level
  - Owner
  - Contributor
  - Reader
- Special/Custom Roles
  - Multi-Level
  - Service Specific
  - Application Specific

- Application of Roles
  - Subscription/Resource Group/Asset Level



	Reader	Resource-specific or custom role	Contributor	Owner
Subscription	Observers	Users managing resources		Admins
Resource group				
Resource	Automated processes			

PRIVILEGE ESCALATION

- How to Access/List Your Permissions
  - AZ CLI
    - List Roles: az role assignment list
    - List your roles: az role assignment list –assignee YOUR_USERNAME
    - List the Readers: az role assignment list --role reader
    - List the Contributors: az role assignment list --role contributor
    - List the Owners: az role assignment list --role owner
  - Azure Portal – Search->Subscriptions
    - Review subscription IAM
  - Azure Portal – Search->Azure Active Directory
    - Roles and Administrators
      - Built-in Roles, Global Admins, etc.

MY ROLE

Contributor

Reader

Owner

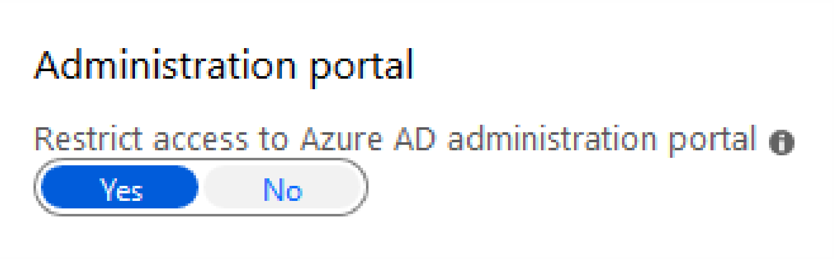
PRIVILEGE ESCALATION

- General Privilege Overview
  - Tenant/Global Admin
  - Owner
  - Contributor/Some Contributor Rights
  - Reader
  - No Azure Access

MY ROLE
Contributor
Reader
Owner

PRIVILEGE ESCALATION – NO ACCESS

- No Azure Access
  - Portal is available, but there's nothing there…
    - Common for users without a Subscription
- Positives
  - You have valid credentials and can pivot to other services
    - Office365
      - Outlook/SharePoint/Teams/etc.
    - Single Factor Auth Interfaces
    - https://myapps.microsoft.com
- Negatives
  - Not that much valuable information available from Azure



Administration portal

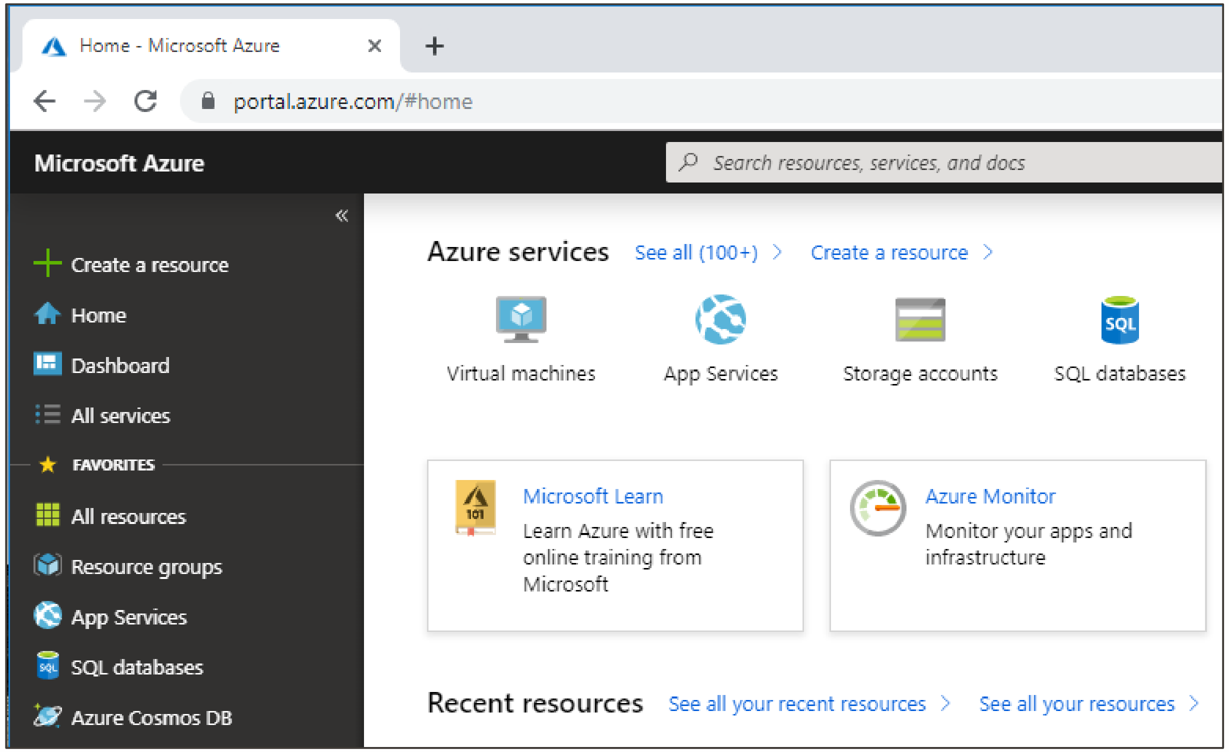
Restrict access to Azure AD administration portal

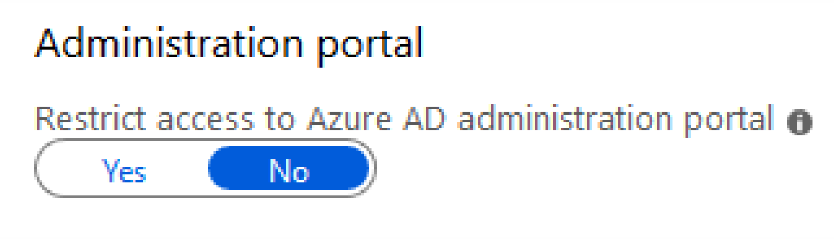
[✓ Yes] No

No Azure Access

PRIVILEGE ESCALATION - READER

- Reader Level Access
  - AzureAD Password Guessing with a full list of users
    - Summer2019, Company1, Password2, etc.




Administration portal

Restrict access to Azure AD administration portal

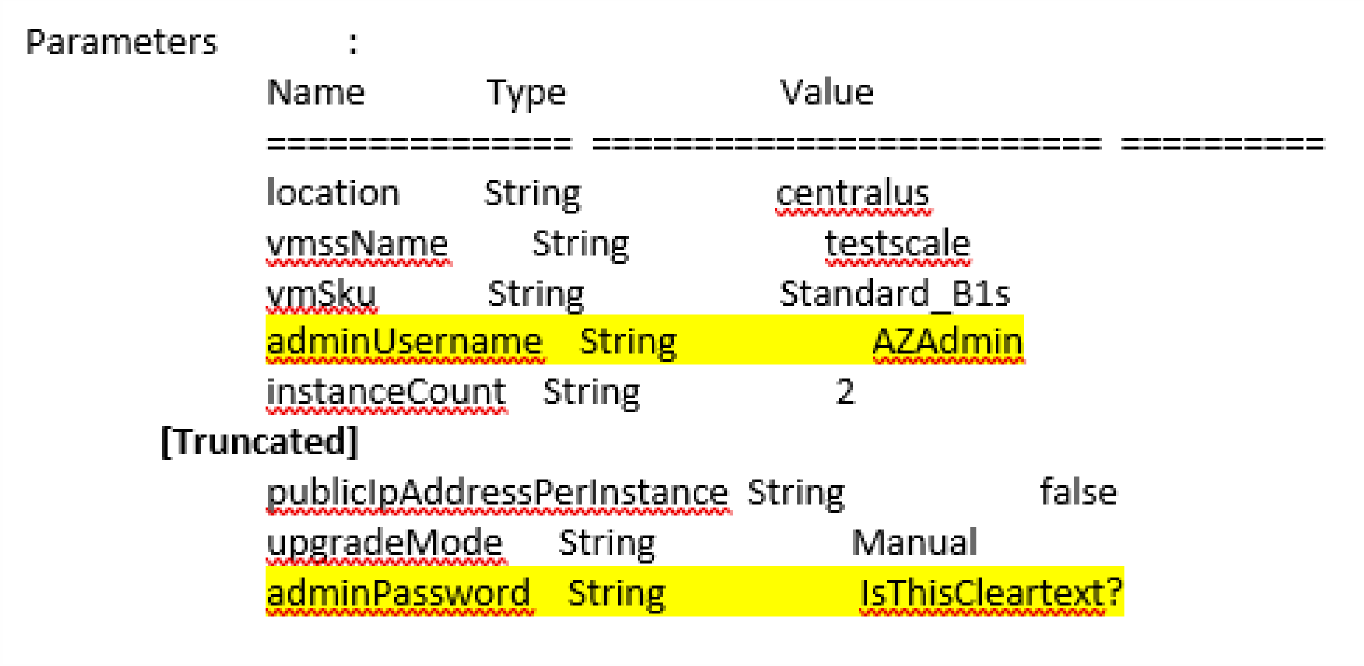
Yes [✓ No]

Reader

PRIVILEGE ESCALATION - READER

- Reading Deployment Parameters
  - All Resource Groups, All Deployments
  - Looking for config templates with Cleartext Credentials/Keys/Etc.

```
Get-AzureRmResourceGroup | Get-AzureRmResourceGroupDeployment >> ".\Deployments.txt"
```

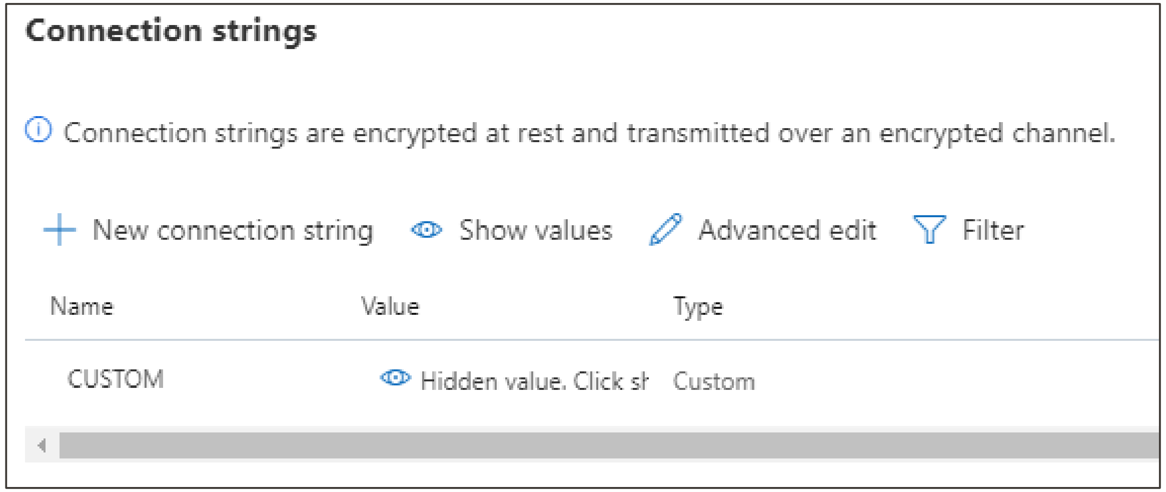


```
Parameters          :
                Name          Type                  Value
                =============== ========================= ==========
                location       String                centralus
                vmssName       String                testscale
                vmSku          String                Standard_B1s
                adminUsername    String                AZAdmin
                instanceCount   String                2
           [Truncated]
                publicIpAddressPerInstance  String              false
                upgradeMode      String                Manual
                adminPassword    String                IsThisCleartext?
```

Reader

PRIVILEGE ESCALATION - READER

- Reading App Services Configurations
  - Not enabled for default Reader access
    - Often granted to Developers with Reader access
  - Connection Strings for Azure SQL
  - Pivot into SQL DB
    - AzureSQL – Data Access Only
    - MSSQL on VM/Server – See PowerUpSQL



Connection strings

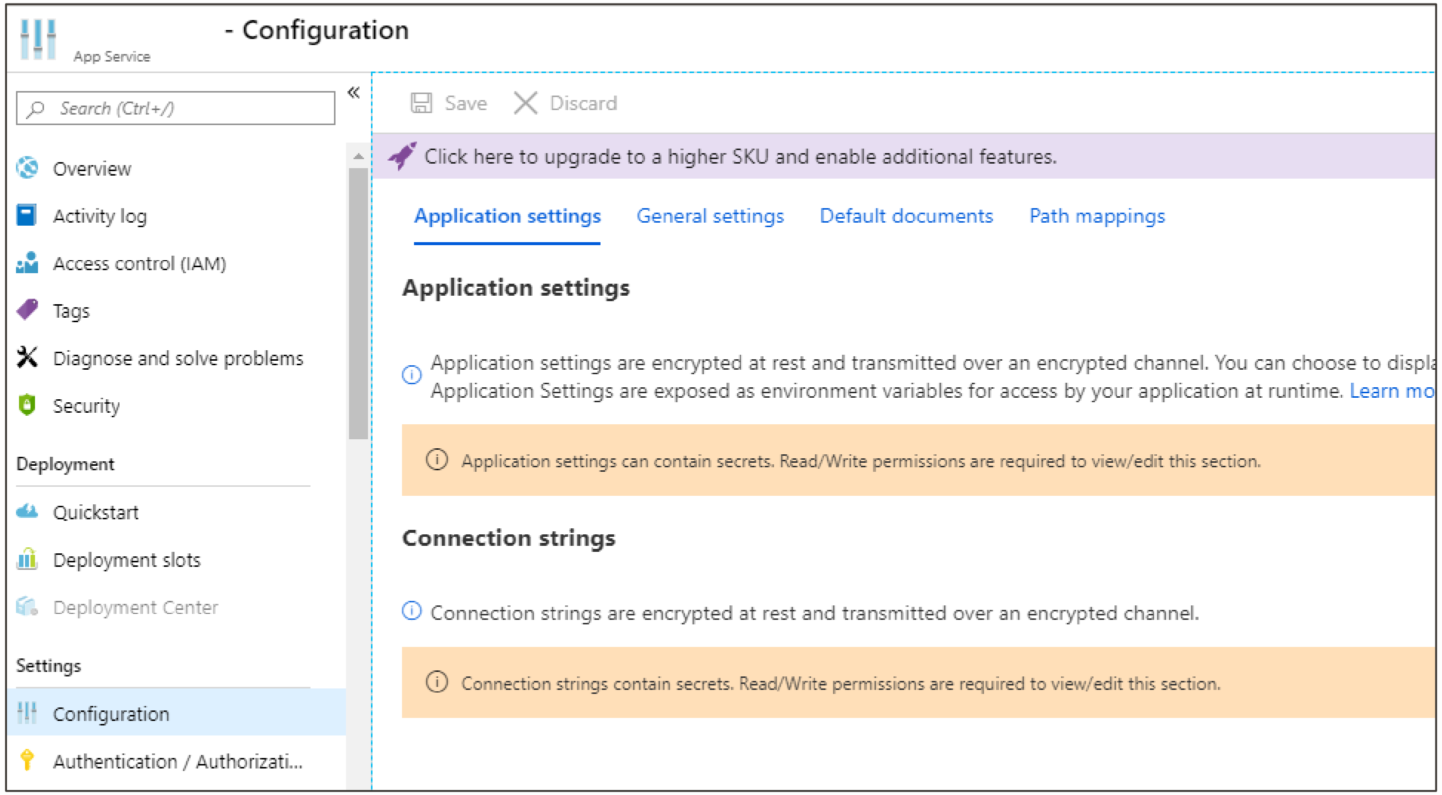
ⓘ Connection strings are encrypted at rest and transmitted over an encrypted channel.

Name	Value	Type
CUSTOM	Hidden value. Click sł	Custom

Reader

PRIVILEGE ESCALATION - READER

- Reading App Services Configurations
  - Credentials for Deploying Applications
    - Backdoor applications, access source code, etc.



- Configuration

App Service

Click here to upgrade to a higher SKU and enable additional features.

Application settings

Application settings are encrypted at rest and transmitted over an encrypted channel. You can choose to displa
Application Settings are exposed as environment variables for access by your application at runtime. Learn mo

Application settings can contain secrets. Read/Write permissions are required to view/edit this section.

Connection strings

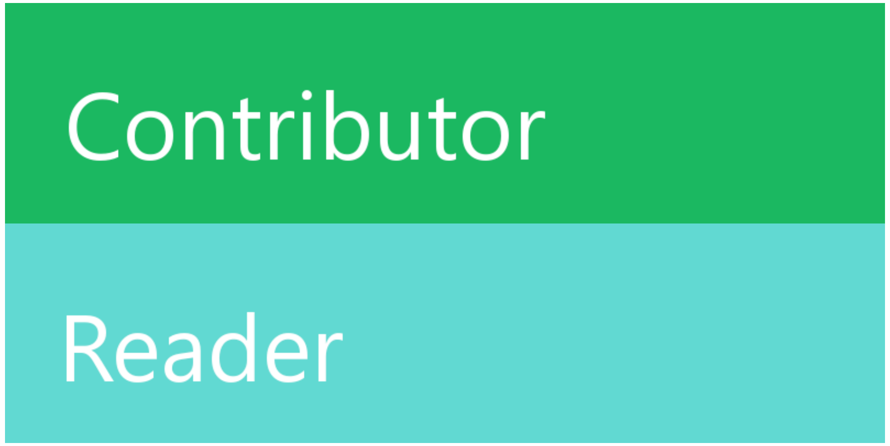
Connection strings are encrypted at rest and transmitted over an encrypted channel.

Connection strings contain secrets. Read/Write permissions are required to view/edit this section.

Reader

PRIVILEGE ESCALATION - READER

- Reader Level Example
  - Guessed external credentials
  - User has Subscription Reader rights
  - Deployment parameters expose local admin credential for domain joined virtual machine
  - RDP to VM exposed to available external network
  - Mimikatz Contributor account from Azure VM machine



PRIVILEGE ESCALATION - CONTRIBUTOR

Contributor Access

Contributor

PRIVILEGE ESCALATION - CONTRIBUTOR

- Your user has some level of contributor access
  - Subscription Level
    - Great!
  - Individual Resource Groups
    - Not bad
  - Single Resources/Services
    - We’ll see…

Contributor

PRIVILEGE ESCALATION - CONTRIBUTOR

- Contributor Level Access on Virtual Machines

- **NT Authority\SYSTEM command execution on VMs**

- Next Steps
  - Use PowerShell commands or the Portal to get data/shells/etc. from the VMs, pivot from there

- Related Blog:

https://blog.netspi.com/running-powershell-scripts-on-azure-vms/

Contributor

PRIVILEGE ESCALATION - CONTRIBUTOR

- Contributor Level Access on Storage Accounts
  - List out all of the Containers and Files
  - Look for config files, passwords, keys

- Next Steps
  - Copy off files
  - Backdoor office documents

Contributor

PRIVILEGE ESCALATION - CONTRIBUTOR

- Contributor Level Access on Virtual Disks
  - Ability to copy a disk off to another Azure VM
  - Read the disk
    - Hashes, files, etc.
    - See cloudcopy AWS attack (@_StaticFlow_)

https://medium.com/@_StaticFlow_/cloudcopy-stealing-hashes-from-domain-controllers-in-the-cloud-c55747f0913

https://github.com/Static-Flow/CloudCopy

Contributor

PRIVILEGE ESCALATION - CONTRIBUTOR

- Contributor Level Access to:
  - Key Vaults/App Services/Automation Accounts

- Get-AzurePasswords
  - Dump Key Vault Entries
  - App Services (See Reader Slides)
  - Automation Accounts
    - Frequently set up to run as Contributor Service accounts
    - Sometimes configured with higher level credentials
    - Cleartext credentials can be recovered for stored account “RunAs” creds
    - Automation Account certificate authentication “exportable” via runbooks

Contributor

PRIVILEGE ESCALATION - CONTRIBUTOR

- Contributor Level Access to Automation Accounts
- Runbooks = Funbooks
  - Accessing Key Vaults
    - New runbook to export all key vault entries
    - Automation account may have access that you don’t
  - Escalating Privileges
    - New runbook to operate as the privileged user
      - Privilege Escalation
        - Owner and/or Tenant Admin
        - Add additional owner or admin rights to your account

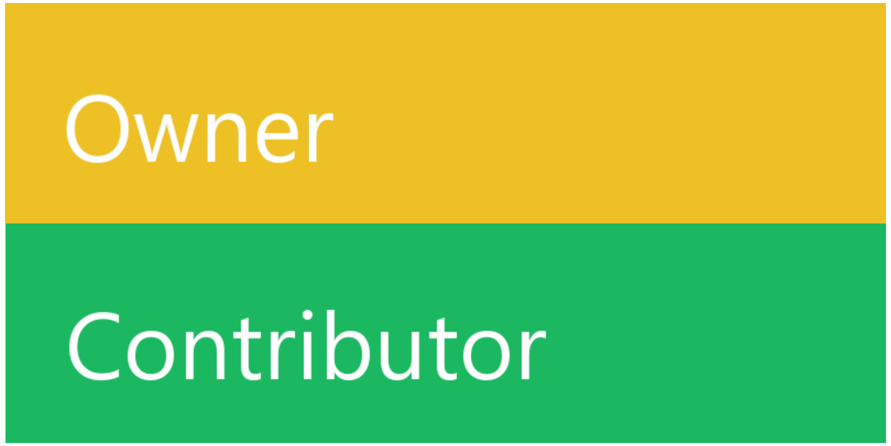
- Related Blog:

https://blog.netspi.com/azure-automation-accounts-key-stores/

Contributor

PRIVILEGE ESCALATION - CONTRIBUTOR

- Reader Level Example (Continued)
  - Guessed external credentials
  - User has Subscription Reader rights
  - Deployment parameters expose local admin credential for domain joined virtual machine
  - RDP to VM exposed to available (internal/external) network
  - Mimikatz Contributor account from Azure VM machine
  - Login to Azure with New Account
  - Contributor Access to Automation Accounts
  - Get-AzurePasswords used to dump Owner Account Credential from Automation Accounts stored credentials



PRIVILEGE ESCALATION - OWNER

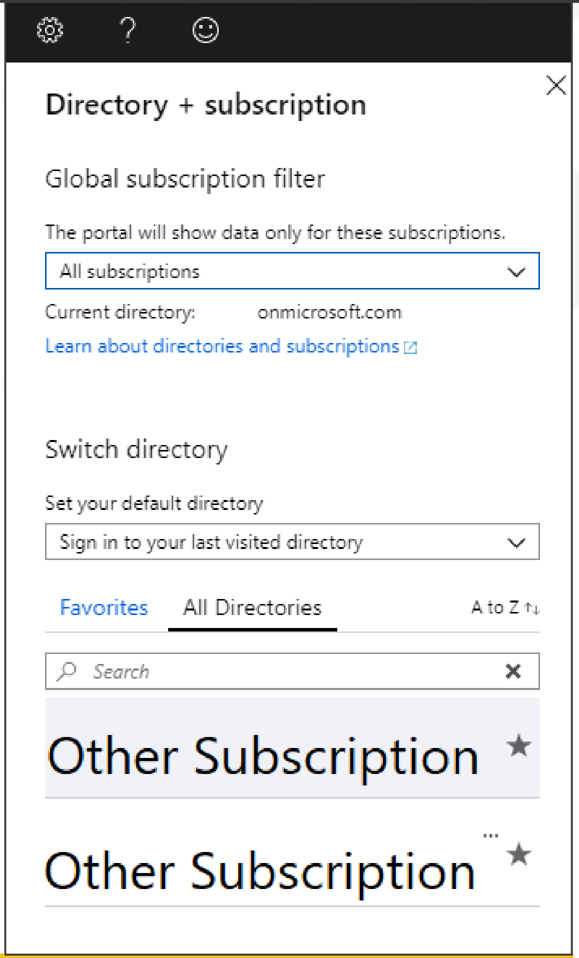
NETSPI

Owner Access

Owner

PRIVILEGE ESCALATION - OWNER

- Owner Level Access
  - Escalating up to Global Admin/Tenant Admin
  - Frequently Owner Accounts are configured with multiple subscriptions
    - Global admins are kept on their own island (Think Enterprise Admins)
  - Pivot to another subscription
    - Lather/Rinse/Repeat until you've accessed/"Owned" all subscriptions (effective Tenant Admin)
  - Listing available subscriptions
    - az account list --output table
  - Switching subscriptions
    - az account set --subscription "My Demos"



Directory + subscription

Global subscription filter

The portal will show data only for these subscriptions.

All subscriptions

Current directory: onmicrosoft.com

Learn about directories and subscriptions

Switch directory

Set your default directory

Sign in to your last visited directory

Owner

Tenant Admin and Persistence

Tenant Admin

PRIVILEGE ESCALATION – TENANT ADMIN

- Tenant Admin Access
  - You have global admin, now what?
  - ~~Burn it all down…~~
  - Pivot internally
    - Find your way to the internal network
    - Via Azure or other channels
  - Persist Access

Tenant Admin

PERSISTENCE

- Adding Azure AD accounts
  - Global Admins and User Admins are usually limited groups
    - Additions to these groups can be noisy
  - Slightly quieter…
    - Similar username to company (kfosaaen/karl.fosaaen)
    - Add as a Contributor or Owner for all (important) subscriptions
    - Mimic account attributes of other admins

List Subscriptions:

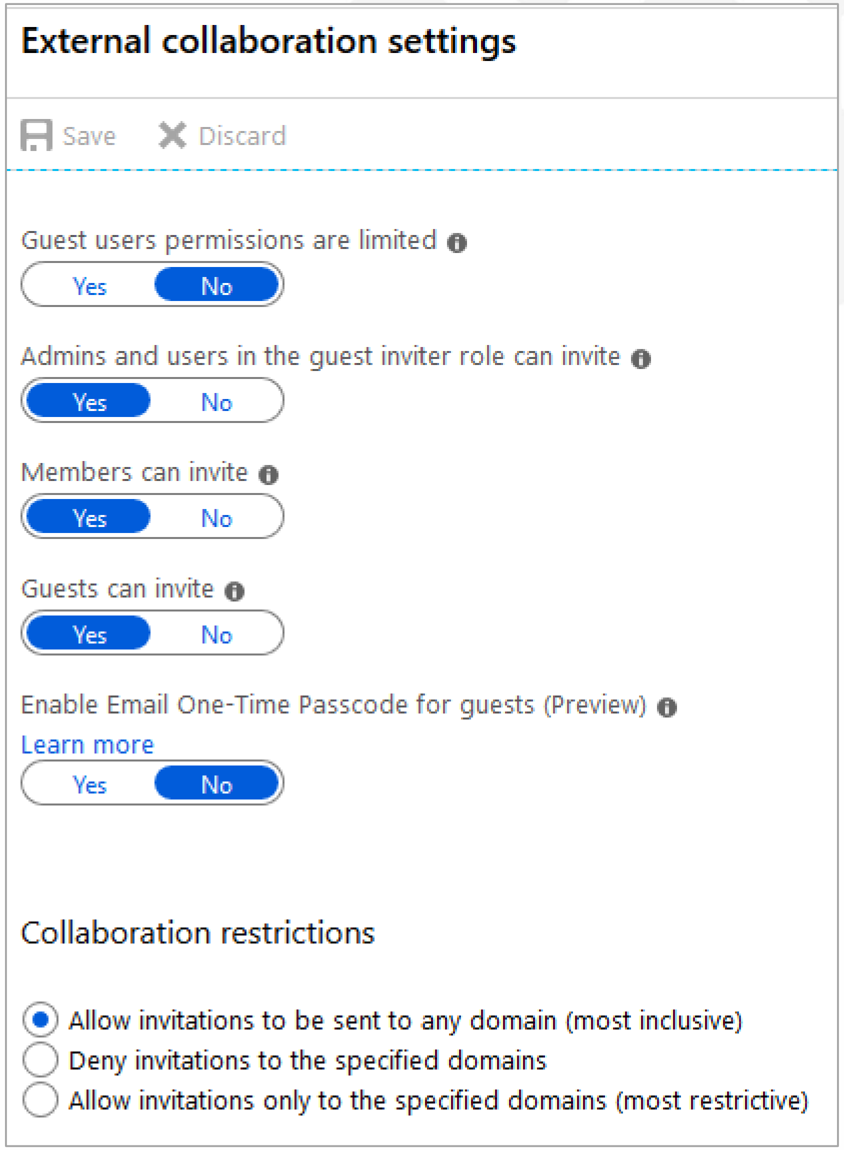
```
az account list | ConvertFrom-Json | ForEach-Object {$_.id}
```

Pipe those IDs into this command:

```
az role assignment create --role Owner --assignee USERNAME_HERE --scope /subscriptions/$id
```

PERSISTENCE

- Guest access to Tenant
  - Using a look-alike email domain (netspi.cloud)
  - Using vendor email domain (comcast.net)
    - ISP customer email could be perceived as legit vendor domain
  - Add appropriate IAM assignments as needed



External collaboration settings

Guest users permissions are limited
Yes [✓ No]

Admins and users in the guest inviter role can invite
[✓ Yes] No

Members can invite
[✓ Yes] No

Guests can invite
[✓ Yes] No

Enable Email One-Time Passcode for guests (Preview)
Learn more
Yes [✓ No]

Collaboration restrictions

● Allow invitations to be sent to any domain (most inclusive)
○ Deny invitations to the specified domains
○ Allow invitations only to the specified domains (most restrictive)

PERSISTENCE

- Add your own subscription
  - Limit access to everyone (minus Global Admins)
  - Not really practical
  - Additional costs incurred
  - Most likely going to work best for malicious attackers

I'LL MAKE MY OWN SUBSCRIPTION
WITH BLACKJACK AND CRYPTOMINERS
imgflip.com

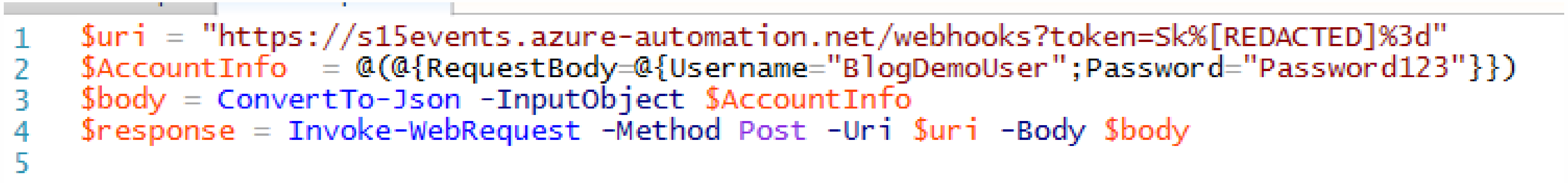
- Quieter Options…
  - Create SPN/Automation/Application with excessive privileges

PERSISTENCE

- Automation Account Backdoors
  - Use existing Automation Accounts (or Create New)
    - Add a runbook
    - Run with the rights for the account (Usually Contributor or more)
      - Add rights to the Automation Account, where needed
  - Job examples
    - Create a new AzureAD user
      - Add to Admins Group
        - Use as short term access
      - Automation account is long term access
    - Add existing user back to admins group
    - Run a specific payload on all/some of the VMs
    - Dump current Azure info out to public storage blob

PERSISTENCE

- Using Webhooks
  - Your backdoor has been set, set a hook to trigger when you need it
  - Trigger a run book with a web request
  - https://s13events.azure-automation.net/webhooks?token=q%2bREDACTEDJQ%3d



```
$uri = "https://s15events.azure-automation.net/webhooks?token=Sk%[REDACTED]%3d"
$AccountInfo  = @(@{RequestBody=@{Username="BlogDemoUser";Password="Password123"}})
$body = ConvertTo-Json -InputObject $AccountInfo
$response = Invoke-WebRequest -Method Post -Uri $uri -Body $body
```

- Related Blog:
  - To Be Released Next Week

PERSISTENCE

- Using Watchers
  - Watch for a specific event (RunBook Runs every x minutes)
    - Check if AzureAD user has been removed
  - Run another RunBook
    - Add Azure AD user back
  - Double Dead Man’s Switch
    - Two Automation accounts, they watch each other
    - One gets deleted, the other adds it back

https://docs.microsoft.com/en-us/azure/automation/automation-watchers-tutorial

PERSISTENCE

- Slightly “Loud” Options…
  - Adding a backdoor to VMs
    - C2 agents
    - Local admin account access
    - Might require opening FW rules (RDP, SSH, etc.)
  - Modify build templates to add accounts/software
    - Could be a major state change

Questions?

ADDITIONAL INFO

- MicroBurst GitHub - https://github.com/NetSPI/MicroBurst
- NetSPI Blog - https://blog.netspi.com
- MicroBurst Specific Blogs:
  - https://blog.netspi.com/get-azurepasswords/
  - https://blog.netspi.com/anonymously-enumerating-azure-file-resources/
  - https://blog.netspi.com/enumerating-azure-services/
  - https://blog.netspi.com/running-powershell-scripts-on-azure-vms/
- Twitter - @kfosaaen
- SlideShare - http://www.slideshare.net/kfosaaen

NETSPI

MINNEAPOLIS | NEW YORK | PORTLAND | DENVER | DALLAS

https://www.netspi.com

https://www.facebook.com/netspi

@NetSPI

https://www.slideshare.net/NetSPI