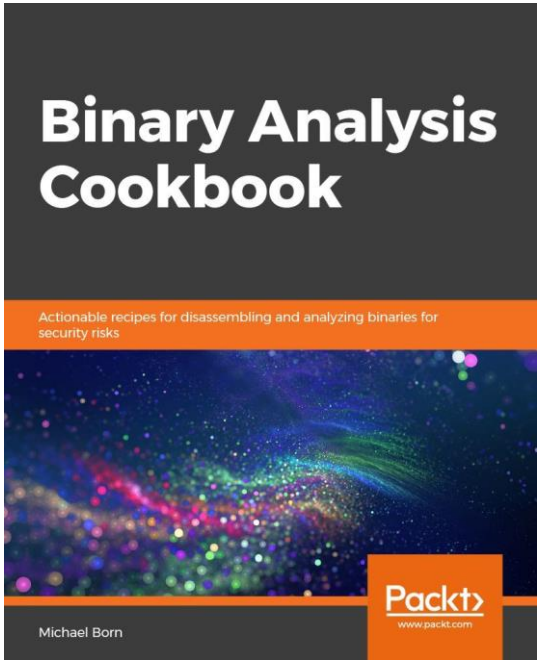
The Top 10 Tools for Cloud Penetration Testing

By Michael Born

About Me

- SecureSky, Inc.
  - Penetration Testing
  - Application Security
  - Internal Security Duties
  - Other Consulting Duties
- Previously
  - NTT Security
  - Lincoln Financial Group
  - Solutionary
  - …and more…
- Author – Binary Analysis Cookbook (Packt Publishing)
  - https://bit.ly/2VOvnlV



Focus of This Talk

- Why this talk?
  - In the News
  - The new perimeter
  - Shared responsibility
- Platforms
  - Microsoft Azure (Azure)
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)
- Miscellaneous tools

Focus of This Talk

- Why this talk?
  - In the News
  - The new perimeter
  - Shared responsibility
- Platforms
  - Microsoft Azure (Azure)
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)
- Miscellaneous tools

Why This Talk?

- Newsworthy attacks
  - Business Email Compromise (BEC)
  - Account takeover
  - Misconfigured services
  - Modern application gaps

Why This Talk?

- Newsworthy attacks
  - Business Email Compromise (BEC)
  - Account takeover
  - Misconfigured services
  - Modern application gaps

Why This Talk?

- Newsworthy attacks
  - Business Email Compromise (BEC)
  - Account takeover
  - Misconfigured services
  - Modern application gaps

Source: Security Magazine

Why This Talk?

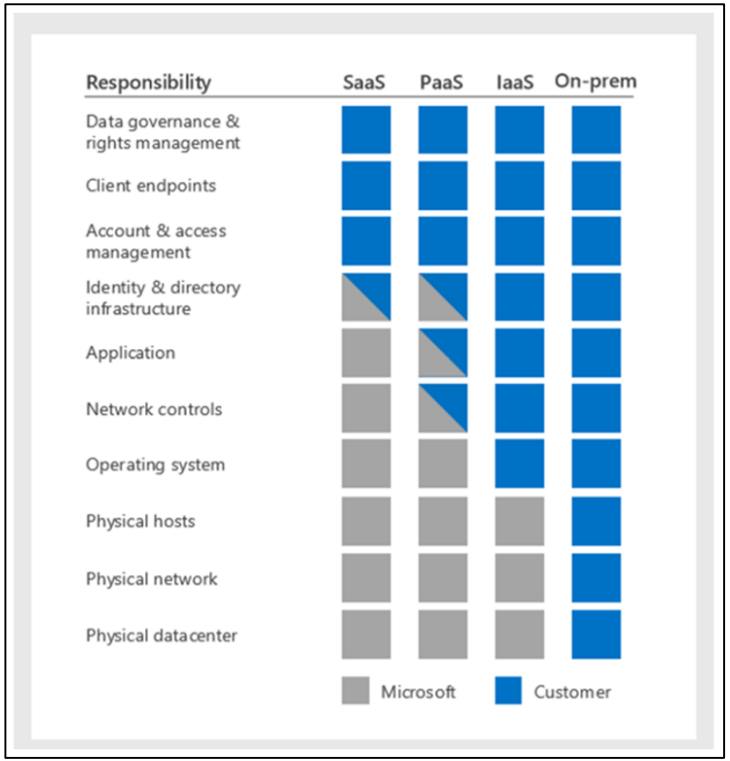
- The new perimeter
  - Identity (remember that last slide? BEC? Account Takeover?)
- Answer
  - Penetration testing needs are changing/have already changed

Why This Talk?

- The new perimeter
  - Identity (remember that last slide? BEC? Account Takeover?)
- Answer
  - Penetration testing needs are changing/have already changed

Why This Talk?

- The new perimeter
  - Identity (remember that last slide? BEC? Account Takeover?)
- Answer
  - Penetration testing needs are changing/have already changed

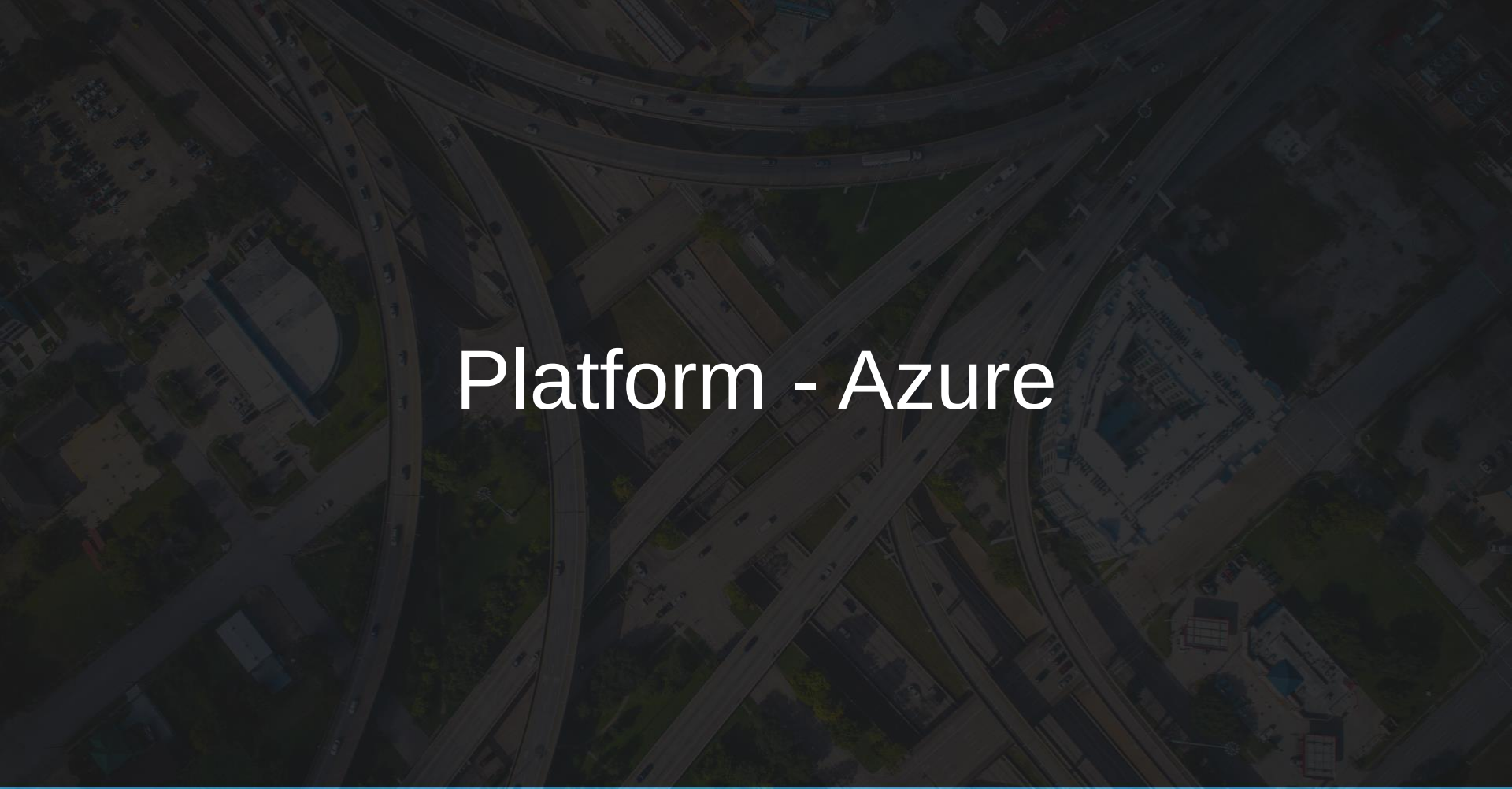


Why This Talk?

- The new perimeter
  - Identity (remember that last slide? BEC? Account Takeover?)
- Answer
  - Penetration testing needs are changing/have already changed

Why This Talk?

- The new perimeter
  - Identity (remember that last slide? BEC? Account Takeover?)
- Answer
  - Penetration testing needs are changing/have already changed

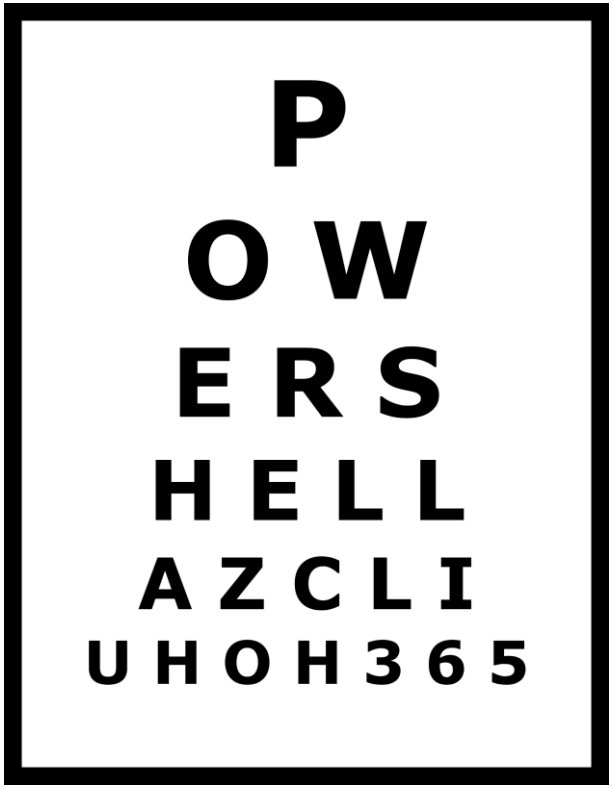

Platform - Azure

Platform - Azure

- Powershell
  - Az module
  - Msonline module
  - AzureAD module
  - Sharepoint Module
  - Exchange online module
- AZ Cli
- UhOh365

Platform - Azure

- Powershell
  - Az module
  - Msonline module
  - AzureAD module
  - Sharepoint Module
  - Exchange online module
- AZ Cli
- UhOh365

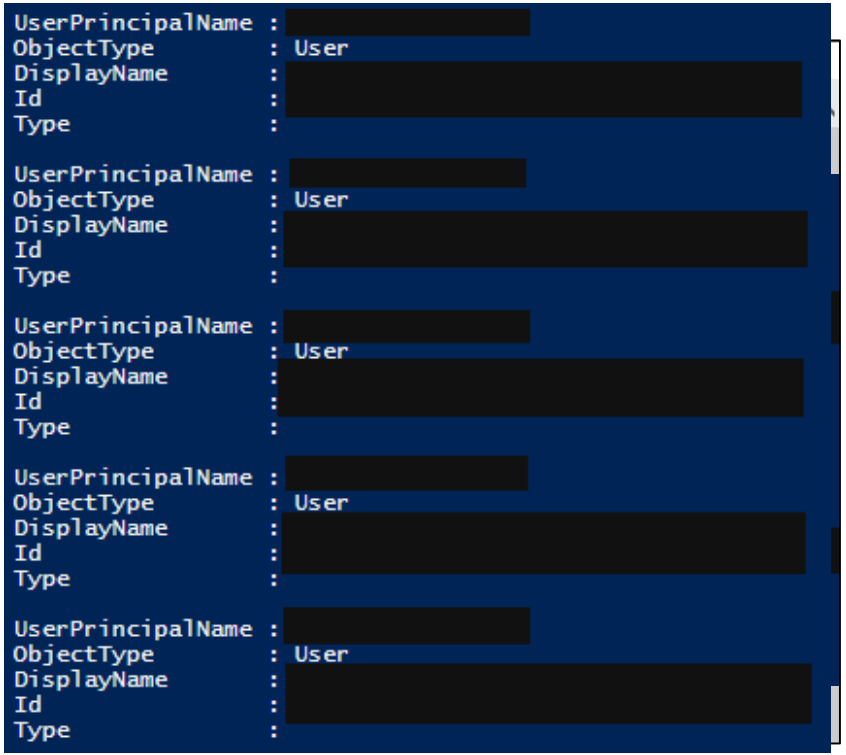


Platform - Azure

- UhOh365
  - User enumeration with AAD and O365
  - https://github.com/Raikia/UhOh365
- Why does this work?
  - Differing application responses
  - Microsoft doesn't consider this a vulnerability

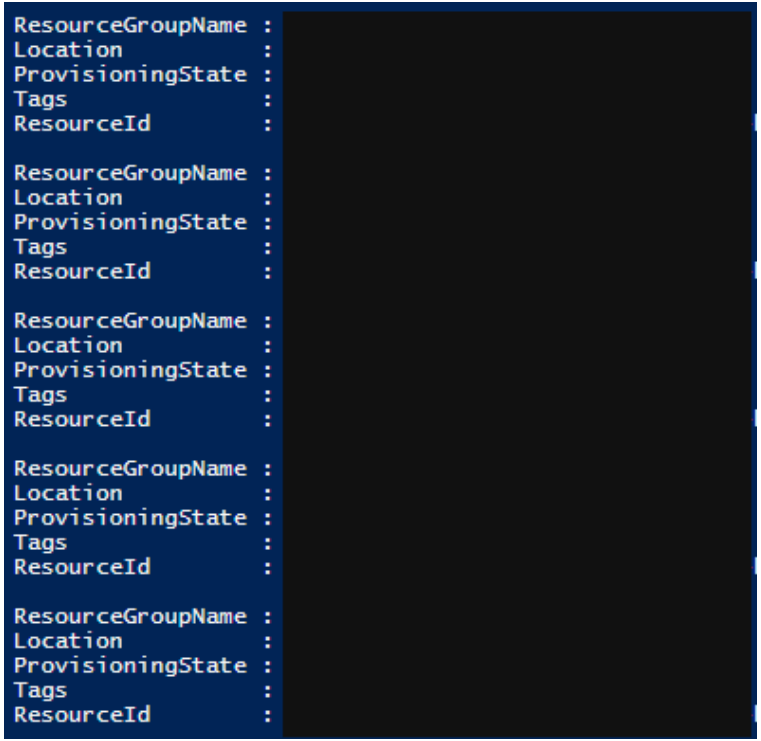
Platform - Azure

- PS - Authenticate
  - Connect-AzAccount
  - Connect-AzureAD
  - Connect-MsolService
- PS - User Enumeration
  - Get-AzADUser
  - Get-AzADGroup
  - Get-AzADGroupMember



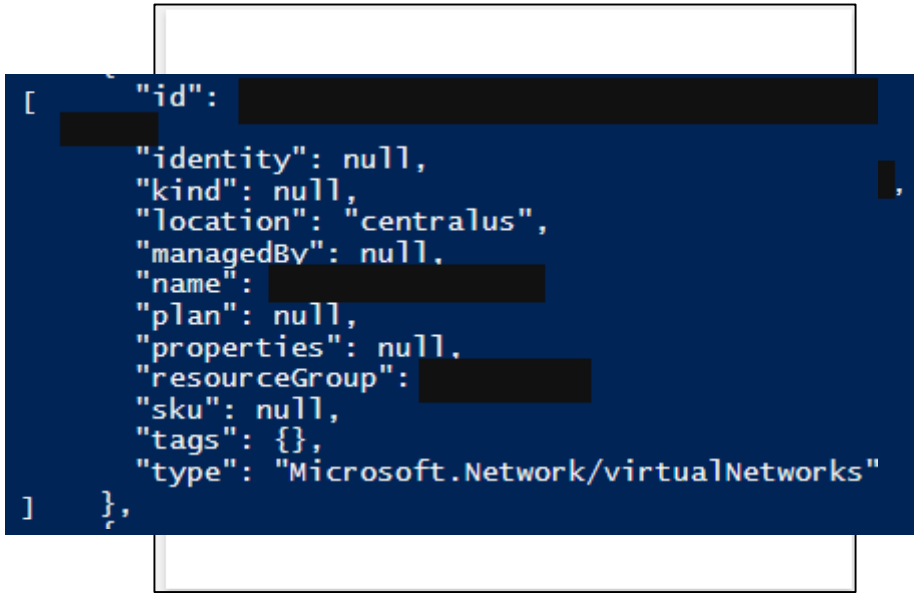
Platform - Azure

- PS - Tenant Information
  - Get-AzTenant
  - Get-AzSubscription
  - Get-AzResourceGroup
  - Get-AzResource
  - Get-AzureADTenantDetail
  - And So Much More…



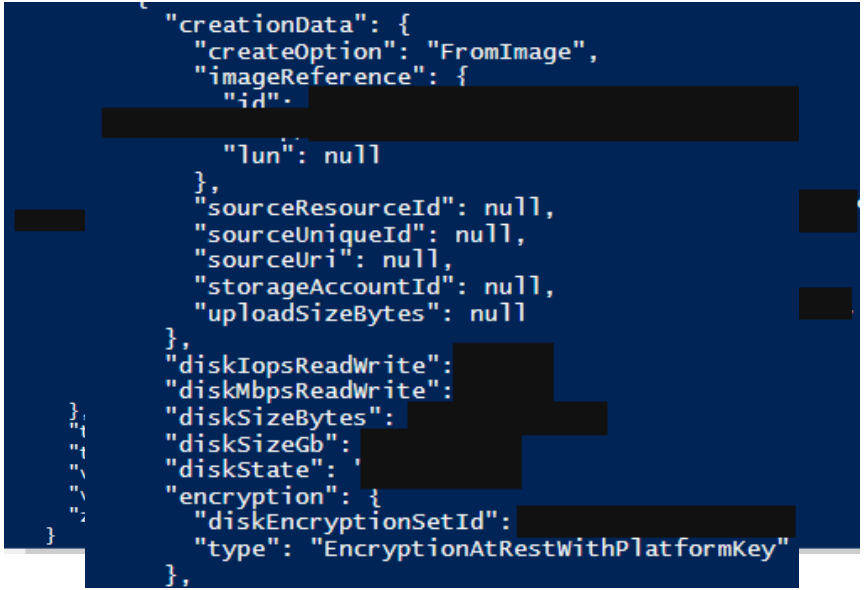
Platform - Azure

- Az Cli - Authenticate
  - az login
- Az Cli - Tenant Information
  - az resource
  - az account
  - az security

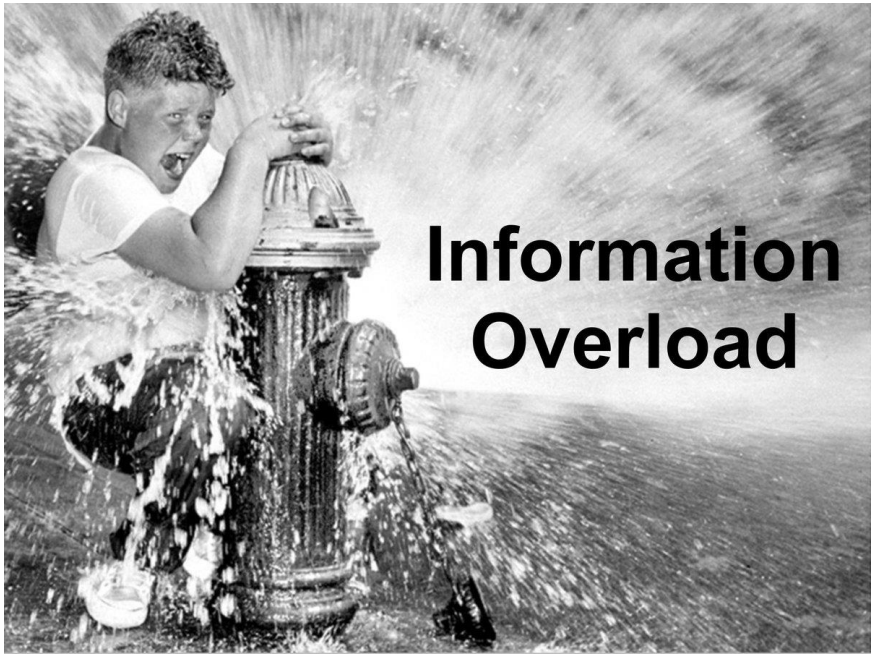


Platform - Azure

- Az Cli - Service Information
  - az vm
  - az disk
  - az image
  - az identity
  - az keyvault
  - az policy
  - az storage



Platform - Azure



Platform - AWS

Platform - Amazon Web Services (AWS)

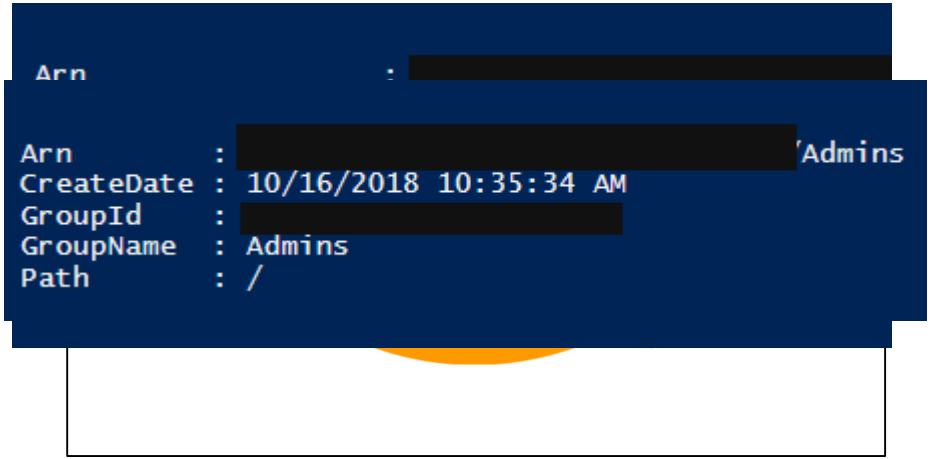
- AWS Tools for Windows
  - AWSPowerShell module
  - AWS SDK for .NET
- AWS Cli
- Pacu (Rhino Security Labs)

Platform - Amazon Web Services (AWS)

- AWS Tools for Windows
  - AWSPowerShell module
  - AWS SDK for .NET
- AWS Cli
- Pacu (Rhino Security Labs)

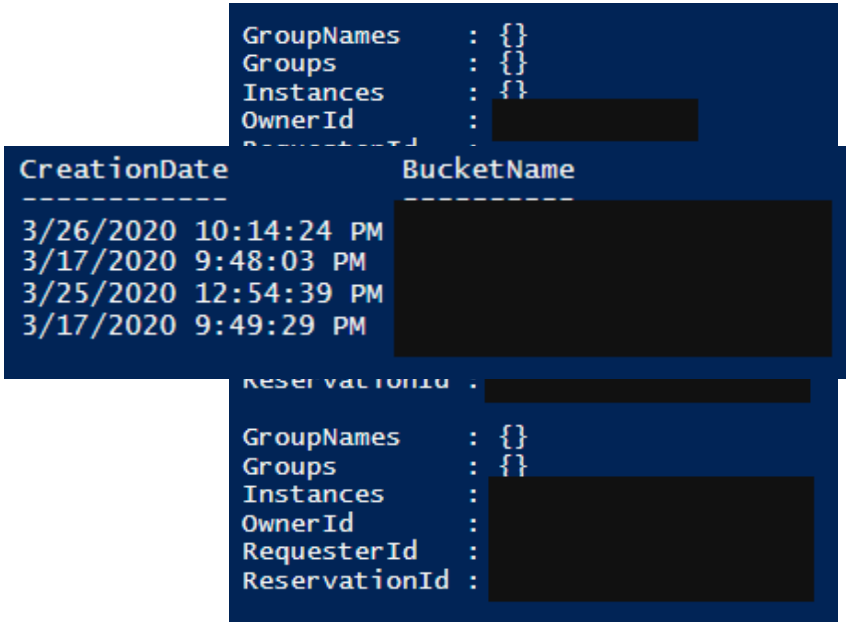
Platform - Amazon Web Services (AWS)

- AWS PS - Authentication
  - Set-AWSCredential
- AWS PS - IAM
  - Get-IAMUser
  - Get-IAMUserList
  - Get-IAMLoginProfile
  - Get-IAMGroupForUser



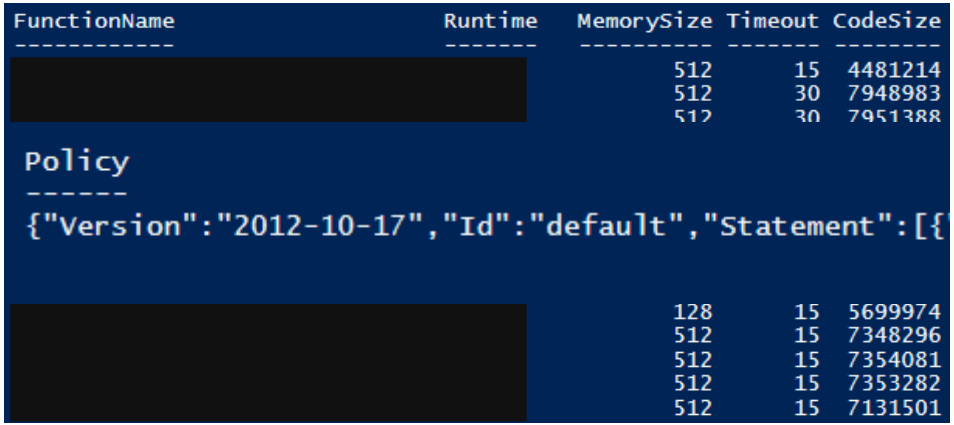
Platform - Amazon Web Services (AWS)

- AWS PS - EC2
  - Get-EC2Instance
  - Get-EC2InstanceMetadata
  - Get-EC2PasswordData
  - Get-EC2KeyPair
  - Get-EC2Address
- AWS PS - S3 Service
  - Get-S3Bucket
  - Get-S3ACL
  - Get-S3Object
  - Read-S3Object
  - Get-S3BucketEncryption



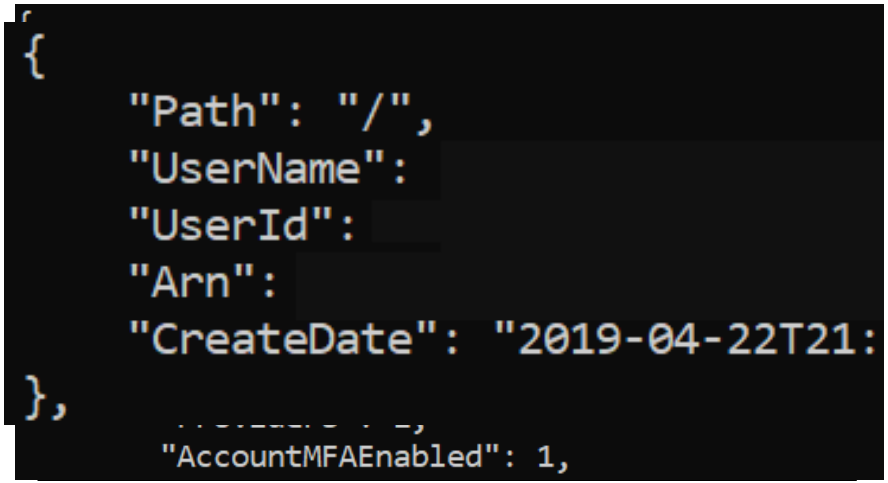
Platform - Amazon Web Services (AWS)

- AWS PS - Lambda Service
  - Get-LMFunctionList
  - Get-LMPolicy
  - Get-LMFunction



Platform - Amazon Web Services (AWS)

- AWS Cli - Authenticate
  - aws configure
- AWS Cli - IAM
  - aws iam get-account-summary
  - aws iam list-users
  - aws iam get-user
  - aws iam get-login-profile



Platform - Amazon Web Services (AWS)

- AWS Cli - EC2
  - aws ec2 get-password-data
  - aws ec2 describe-instances
  - aws ec2 describe-vpcs
- AWS Cli - S3
  - aws s3 <command> [<*args>]
    - cp, ls, mb, mv, presign, rb, rm, sync, website

Platform - Amazon Web Services (AWS)

- Pacu
  - Recon Modules
    - iam__enum_roles
    - s3__bucket_finder
    - iam__enum_users
    - iam__enum_permissions
  - Enumeration Modules
    - aws__enum_account
    - iam__get_credential_report
    - ec2__download_userdata\
    - ec2__enum

Platform - Amazon Web Services (AWS)

- Pacu
  - Privilege Escalation Module
    - iam__privesc_scan
  - Lateral Movement Modules
    - vpc__enum_lateral_movement
    - cloudtrail__csv_injection
  - Exploitation Modules
    - api_gateway__create_api_keys
    - ebs__explore_snapshots
    - Lightsail__download_ssh_keys

```
Pacu command info:
    list/ls                                 List all modules
    load_commands_file <file>               Load an existing file with list of commands to execute
    search [cat[egory]] <search term>       Search the list of available modules by name or category
    help                                    Display this page of information
    help <module name>                      Display information about a module
    whoami                                  Display information regarding to the active access keys
    data                                    Display all data that is stored in this session. Only fields
                                              with values will be displayed
    data <service>|proxy                    Display all data for a specified service or for PacuProxy
                                              in this session
    services                                Display a list of services that have collected data in the
                                              current session to use with the "data" command
    regions                                 Display a list of all valid AWS regions
    update_regions                          Run a script to update the regions database to the newest
                                              version
    set_regions <region> [<region>...]      Set the default regions for this session. These space-separated
                                              regions will be used for modules where regions are required,
                                              but not supplied by the user. The default set of regions is
                                              every supported region for the service. Supply "all" to this
                                              command to reset the region set to the default of all
                                              supported regions
    run/exec <module name>                  Execute a module
    set_keys                                Add a set of AWS keys to the session and set them as the
                                              default
    swap_keys                               Change the currently active AWS key to another key that has
                                              previously been set for this session
    import_keys <profile name>|--all        Import AWS keys from the AWS CLI credentials file (located
                                              at ~/.aws/credentials) to the current sessions database.
                                              Enter the name of a profile you would like to import or
                                              supply --all to import all the credentials in the file.
    exit/quit                               Exit Pacu
```

Platform - AWS


Platform - GCP

Platform - Google Cloud Platform (GCP)

- Cloud SDK
- Languages as tools
  - Java
  - Python
  - PHP
  - Ruby
  - .NET
  - NodeJS
  - Go

Platform - Google Cloud Platform (GCP)

- Cloud SDK
- Languages as tools
  - Java
  - Python
  - PHP
  - Ruby
  - .NET
  - NodeJS
  - Go

Platform - Google Cloud Platform (GCP)

- Cloud Security Scanner
  - Application Vuln Scan

Google Cloud

Platform - Google Cloud Platform (GCP)

- Cloud SDK
  - Environment Information
    - gcloud info
  - Identity and Security
    - gcloud iam (accounts + keys)
    - gcloud iap (policies)
    - gcloud resource-manager
    - gcloud secrets
    - gcloud access-context-manager
    - gcloud kms

Google Cloud

Platform - Google Cloud Platform (GCP)

- Cloud SDK
  - Security
    - gcloud asset (asset inventory)
  - Data
    - gcloud bigtable
    - gcloud datastore
    - gcloud firestore
    - gcloud sql
  - Compute (and apps)
    - gcloud app
    - gcloud compute
    - gcloud services (APIs & services)
    - gcloud endpoints (API services)
    - gcloud service-management

Google Cloud

Platform - Google Cloud Platform (GCP

Miscellaneous Tools

Miscellaneous Tools

- Modern Cloud Applications
  - BurpSuite Pro
  - OWASP Zap
  - NMAP
  - Browser Developer Tools
  - Angular Augury
  - SoapUI

Google Cloud

Miscellaneous Tools

- Password Spraying
  - MSOLSpray (https://github.com/dafthack/MSOLSpray)
- Breach Exposed Passwords
  - PWNDB (https://github.com/davidtavarez/pwndb)
  - Recon-NG (https://github.com/lanmaster53/recon-ng)
- O365 Abuse
  - Ruler (https://github.com/sensepost/ruler)

Google Cloud

Miscellaneous Tools

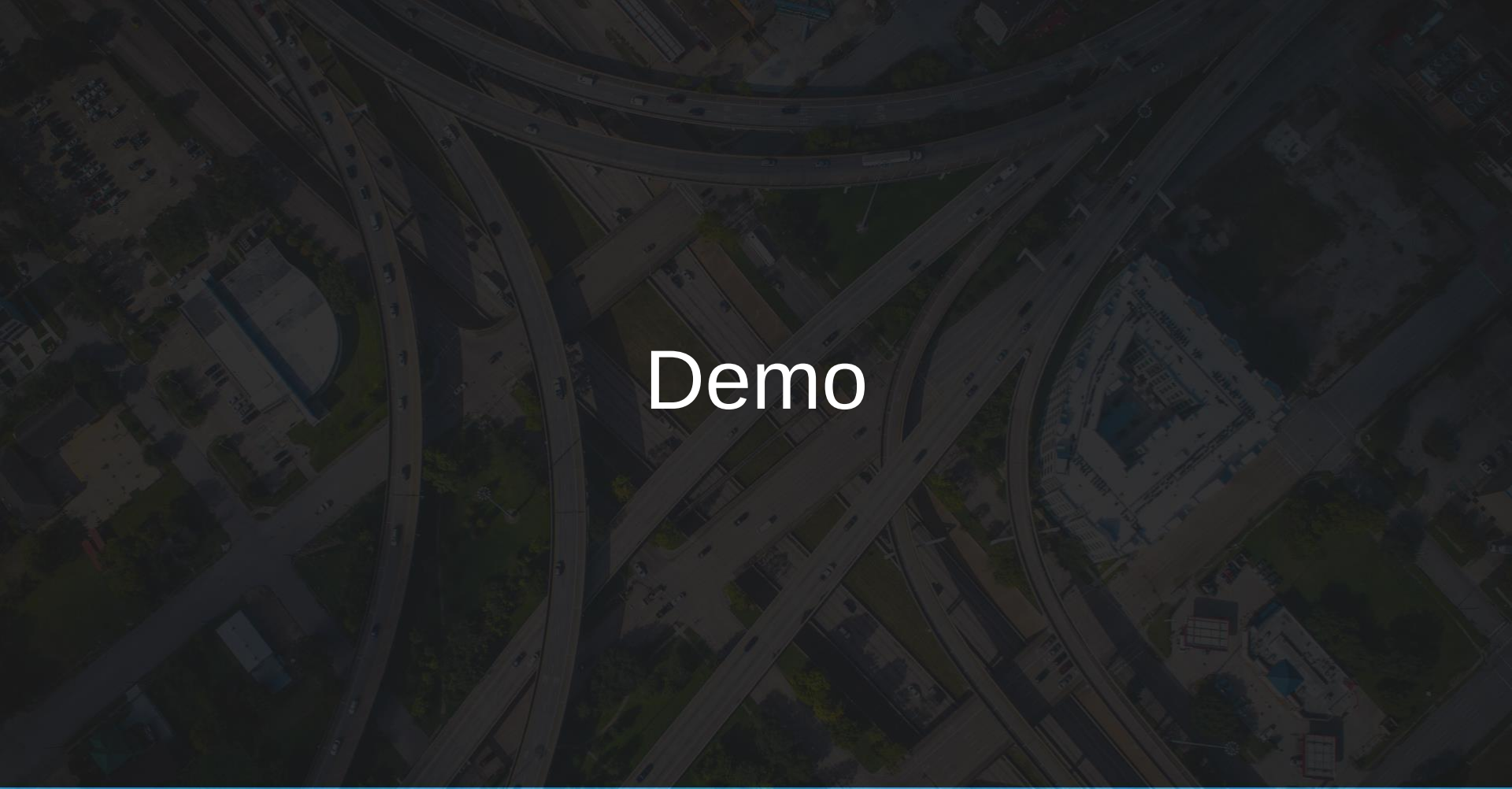
- AzureAD
  - PowerZure (https://bit.ly/2UBIaWh)
- Domain Information
  - DNS Dumpster
  - DNS Recon
  - WHOIS

Google Cloud

Miscellaneous Tools

- Common Tools
  - Platform API
  - Platform Web Console/Portal

Google Cloud


Demo

Thank You

Slides: https://github.com/blu3gl0w13/kernelcon-2020-preso