

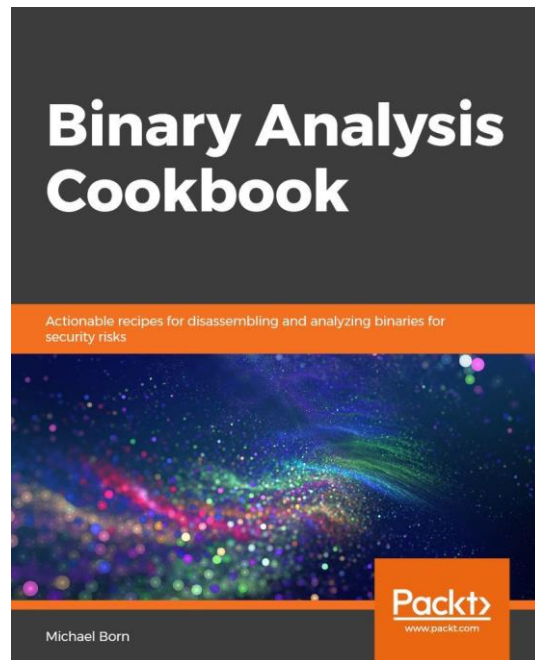


The Top 10 Tools for Cloud Penetration Testing

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/2VOvnIV>



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

Source: Security Magazine

CapitalOne

DOORDASH

FIRST AMERICAN
First American

at the Pool



State Farm

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

Responsibility	Self	Peer	Self	On-going
Data governance & rights management				
Cloud migration				
Account & access management				
Identity & directory infrastructure				
Application				
Network controls				
Operating system				
Physical security				
Physical network				
Physical infrastructure				

Legend: Self Peer

Why This Talk?

- The new perimeter
 - Identity (remember that last slide? BEC? Account Takeover?)

• Answer

- Penetration testing needs are changing/have already changed

Responsibility	Self	Peer	Self	On going
Data governance & rights management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cloud security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access & session management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Identity & directory administration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Network security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Operating system	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Physical security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Physical network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Physical perimeter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☐ Missing ☒ Covered

Why This Talk?

- The new perimeter
 - Identity (remember that last slide? BEC? Account Takeover?)

• Answer

• Penetration testing needs are changing/have already changed

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Shared	Shared	Customer	Customer
Application	Microsoft	Shared	Customer	Customer
Network controls	Microsoft	Shared	Customer	Customer
Operating system	Microsoft	Microsoft	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer
	Microsoft	Microsoft	Microsoft	Customer

Why This Talk?

- The new perimeter
 - Identity (remember that last slide? BEC? Account Takeover?)

• Answer

• Penetration testing needs are changing/have already changed

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Microsoft	Microsoft	Customer	Customer
Application	Microsoft	Microsoft	Customer	Customer
Network controls	Microsoft	Microsoft	Customer	Customer
Operating system	Microsoft	Microsoft	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer
	Microsoft	Microsoft	Customer	Customer

Why This Talk?

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

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Microsoft	Microsoft	Customer	Customer
Application	Microsoft	Microsoft	Customer	Customer
Network controls	Microsoft	Microsoft	Customer	Customer
Operating system	Microsoft	Microsoft	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer
	Microsoft	Microsoft	Customer	Customer



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



**P
O W
E R S
H E L L
A Z C L I
U H O H 3 6 5**

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

```
UserPrincipalName : [REDACTED]
ObjectType        : User
DisplayName       : [REDACTED]
Id               : [REDACTED]
Type             : [REDACTED]

UserPrincipalName : [REDACTED]
ObjectType        : User
DisplayName       : [REDACTED]
Id               : [REDACTED]
Type             : [REDACTED]

UserPrincipalName : [REDACTED]
ObjectType        : User
DisplayName       : [REDACTED]
Id               : [REDACTED]
Type             : [REDACTED]

UserPrincipalName : [REDACTED]
ObjectType        : User
DisplayName       : [REDACTED]
Id               : [REDACTED]
Type             : [REDACTED]

UserPrincipalName : [REDACTED]
ObjectType        : User
DisplayName       : [REDACTED]
Id               : [REDACTED]
Type             : [REDACTED]
```

Platform - Azure

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

```
ResourceGroupName :  
Location          :  
ProvisioningState :  
Tags              :  
ResourceId        :  
  
ResourceGroupName :  
Location          :  
ProvisioningState :  
Tags              :  
ResourceId        :  
  
ResourceGroupName :  
Location          :  
ProvisioningState :  
Tags              :  
ResourceId        :  
  
ResourceGroupName :  
Location          :  
ProvisioningState :  
Tags              :  
ResourceId        :  
  
ResourceGroupName :  
Location          :  
ProvisioningState :  
Tags              :  
ResourceId        :
```

Platform - Azure

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

```
[{"id": "[REDACTED]",  
  "identity": null,  
  "kind": null,  
  "location": "centralus",  
  "managedBy": null,  
  "name": "[REDACTED]",  
  "plan": null,  
  "properties": null,  
  "resourceGroup": "[REDACTED]",  
  "sku": null,  
  "tags": {},  
  "type": "Microsoft.Network/virtualNetworks"  
},  
]
```

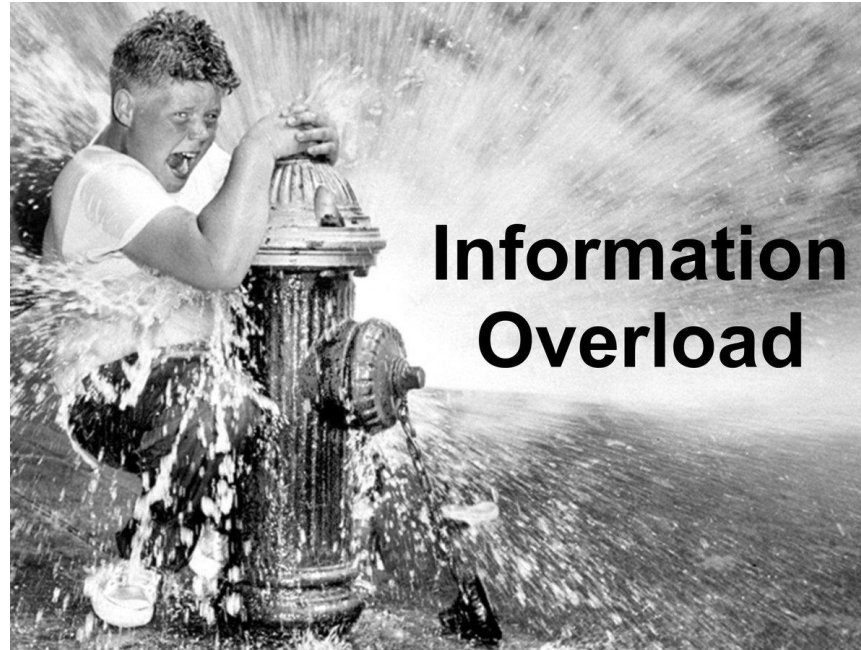
Platform - Azure

- Az Cli - Service Information

- az vm
- az disk
- az image
- az identity
- az keyvault
- az policy
- az storage

```
    "creationData": {  
      "createOption": "FromImage",  
      "imageReference": {  
        "id": "  
        "lun": null  
      },  
      "sourceResourceId": null,  
      "sourceUniqueId": null,  
      "sourceUri": null,  
      "storageAccountId": null,  
      "uploadSizeBytes": null  
    },  
    "diskIopsReadWrite":   
    "diskMbpsReadWrite":   
    "diskSizeBytes":   
    "diskSizeGb":   
    "diskState":   
    "encryption": {  
      "diskEncryptionSetId":   
      "type": "EncryptionAtRestWithPlatformKey"  
    },  
  },  
}
```

Platform - Azure





Platform - AWS

Platform - Amazon Web Services (AWS)

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



Platform - Amazon Web Services (AWS)

- AWS Tools for Windows
 - AWS PowerShell 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

```
Arn : [REDACTED]

Arn : [REDACTED] Admins
CreateDate : 10/16/2018 10:35:34 AM
GroupId : [REDACTED]
GroupName : Admins
Path : /
```

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

GroupNames : {}	
Groups : {}	
Instances : {}	
OwnerId : [REDACTED]	
RequesterId : [REDACTED]	
ReservationId : [REDACTED]	
CreationDate	
BucketName	

3/26/2020 10:14:24 PM	[REDACTED]
3/17/2020 9:48:03 PM	[REDACTED]
3/25/2020 12:54:39 PM	[REDACTED]
3/17/2020 9:49:29 PM	[REDACTED]
ReservationId : [REDACTED]	
GroupNames : {}	
Groups : {}	
Instances : [REDACTED]	
OwnerId : [REDACTED]	
RequesterId : [REDACTED]	
ReservationId : [REDACTED]	

Platform - Amazon Web Services (AWS)

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

FunctionName	Runtime	MemorySize	Timeout	CodeSize
		512	15	4481214
		512	30	7948983
		512	30	7951388
Policy				

{ "Version": "2012-10-17", "Id": "default", "Statement": [{				
		128	15	5699974
		512	15	7348296
		512	15	7354081
		512	15	7353282
		512	15	7131501

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

```
{  
  "Path": "/",  
  "UserName":  
  "UserId":  
  "Arn":  
  "CreateDate": "2019-04-22T21:  
},  
  "AccountMFAEnabled": 1,
```

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

```
{
  "Vpcs": [
    {
      "CidrBlock": "10.0.0.0/16",
      "DhcpOptionsId": "dopt-1",
      "State": "available",
      "VpcId": "vpc-1",
      "OwnerId": "i-1",
      "InstanceTenancy": "default",
      "CidrBlockAssociationSet": [
        {
          "AssociationId": "assoc-1",
          "CidrBlock": "10.0.0.0/16",
          "CidrBlockState": {
            "State": "associated"
          }
        }
      ]
    },
    {
      "IsDefault": true
    }
  ]
}
```


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

```
[ec2__enum] MODULE SUMMARY:

Session data:
aws_keys: [
]
id: 2
created: "2020
is_active: tru
name: "kernelc
boto_user_agen
key_alias: "mj
access_key_id:
secret_access_
session_region
"all"
]
s3: {
  "Buckets":
  {
    "h
    "C
  },
  {
  },
  {
  },
  {
  },
  {
  }
}

Regions:
ap-northeast-1
ap-northeast-2
ap-south-1
ap-southeast-1
ap-southeast-2
ca-central-1
eu-central-1
eu-north-1
eu-west-1
eu-west-2
eu-west-3
sa-east-1
us-east-1
us-east-2
us-west-1
us-west-2

39 total instance(s) found.
146 total security group(s) found.
5 total elastic IP address(es) found.
```

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 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

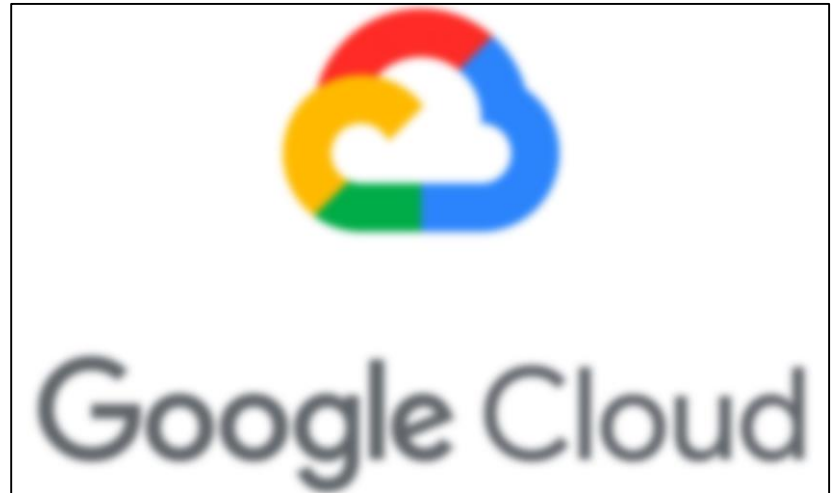




Platform - GCP

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/2UBlaWh>)
- 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-pres0>