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)
Cloud FTW!

What’s in it for me?
Staying clean while being mean
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
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?
Staying clean while being mean
Cause pissing off The Net is bad for business
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 could
Private cloud
Hybrid cloud

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

Albert Barron – https://www.linkedin.com/pulse/20140730172610-9679881-pizza-as-a-service
It’s not domain, but it’s still admin

Cloud assets are managed under an account or subscription

Getting access to that layer is often equivalent to DA

OH YOU
WANTED AN API?
CloudOS - Same ideas, different words

Server
Domain
Domain Admin
Pass the Hash
Private IPs
RDP / SSH

Services
Subscription
Subscription Admin
Credential Pivot
Public IPs
Management APIs

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?

Image: ©MITRE
SithCo’s app hosting

What are we looking at?
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
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)

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>outlook.com</td>
<td>116</td>
</tr>
<tr>
<td>pphosted.com</td>
<td>110</td>
</tr>
<tr>
<td>messagelabs.com</td>
<td>46</td>
</tr>
<tr>
<td>iphmx.com</td>
<td>34</td>
</tr>
<tr>
<td>ctmail.com</td>
<td>29</td>
</tr>
<tr>
<td>secureserver.net</td>
<td>25</td>
</tr>
<tr>
<td>cscdns.net</td>
<td>18</td>
</tr>
<tr>
<td>mimecast.com</td>
<td>18</td>
</tr>
<tr>
<td>google.com</td>
<td>15</td>
</tr>
<tr>
<td>m1bp.com</td>
<td>6</td>
</tr>
<tr>
<td>mb5p.com</td>
<td>6</td>
</tr>
<tr>
<td>googlemail.com</td>
<td>6</td>
</tr>
<tr>
<td>barracudanetworks.com</td>
<td>6</td>
</tr>
</tbody>
</table>
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>message labs.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.message labs.com</td>
<td>6</td>
</tr>
<tr>
<td>qualtrics.com</td>
<td>5</td>
</tr>
<tr>
<td>clears lid.e.com</td>
<td>5</td>
</tr>
<tr>
<td>click dimensions.com</td>
<td>5</td>
</tr>
<tr>
<td>constant contact.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.

DNS query for:

- adfs
- auth
- fs
- okta
- ping
- sso
<table>
<thead>
<tr>
<th>Web Server</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>Apache-Coyote/1.1</td>
</tr>
<tr>
<td>BigIP</td>
<td>Kestrel</td>
</tr>
<tr>
<td>JPM</td>
<td>Microsoft-HTTPAPI/2.0</td>
</tr>
<tr>
<td>Kestrel</td>
<td>Microsoft-IIS/7.5</td>
</tr>
<tr>
<td>Kestrel</td>
<td>Microsoft-IIS/7.5</td>
</tr>
<tr>
<td>Microsoft-IIS/7.5</td>
<td>Microsoft-IIS/6.0</td>
</tr>
<tr>
<td>Microsoft-IIS/7.5</td>
<td>Microsoft-IIS/7.5</td>
</tr>
<tr>
<td>Microsoft-IIS/8.0</td>
<td>Microsoft-IIS/8.5</td>
</tr>
<tr>
<td>Microsoft-IIS/8.5</td>
<td>Microsoft-HTTPAPI/2.0</td>
</tr>
<tr>
<td>nginx</td>
<td>Oracle-iPlanet-Web-Server/7.0</td>
</tr>
<tr>
<td>WebSEAL/7.0.0.8 (Build 160317)</td>
<td></td>
</tr>
</tbody>
</table>

**Pathfinding**

```
TiPMix=0.505320029568542; path=/; Domain=okta.
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
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.
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).
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>

<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.                                                                                           |
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 KRBGT 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 involves attempting authentication with a single password against all users before moving on to the next password.

Works against Cloud services: email, IM, etc.

Low & Slow: 1 to 2 per hour

Often works against VPN as well.
Password spraying tools

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

The authors have not evaluated these tools. Always test before use.
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?
Where Are API Keys? GitHub!

accessKeyId and secretAccessKey are leaking #9

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/jjingidy/5682149

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

```
var ApiBuilder = require('claudia-api-builder'),
    api = new ApiBuilder();

module.exports = api;

AWS.config.update({
    "accessKeyId": "AKIA_XXXXXXXXXXXXXXXX",
    "secretAccessKey": "XXXXXXXXXXXXXXXXXXXXXXXXX",
});
```

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?
The circle of access

What is the likelihood this cloud service needs to access resources from on-premises?
Happy fun exploit time

Pray to the demo gods, pray I say!
Demo stuff here

There should be a fun live demo here if everything goes right
Countermeasures and proper protection

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

Telling your client to close up shop and moving back into the basement is probably a non-starter.

Clouds do provide real business benefits and can improve security when done right.

How can the “cloud” be secured?
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: 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
Giving useful advice

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

Credential management is hard in a connected world – this is an massive opportunity for attackers
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!
Conclusion

Are we there yet?
References

Infiltrate 2017: Cloud Post Exploitation Techniques - Andrew Johnson & Sacha Faust
https://vimeo.com/214855977


Google Cloud Security: https://cloud.google.com/security/

MailSniper: https://github.com/dafthack/MailSniper

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