Hacking The Cloud(s)

B|Sides Vancouver 2018

Wesley Wineberg
Outline

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

All the Clouds

- Azure
- AWS
- GCP
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`
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
**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

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

- Server
- Domain
- Domain Admin
- Pass the Hash
- Private IPs
- RDP / SSH
- Services
- Subscription
- Subscription Admin
- Credential Pivot
- Public IPs
- Management APIs
Normal vs Cloud – AWS Translation

<table>
<thead>
<tr>
<th>Self Managed Server</th>
<th>EC2 Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Network</td>
<td>VPC</td>
</tr>
<tr>
<td>Firewall</td>
<td>Security Groups</td>
</tr>
<tr>
<td>Open Network Share</td>
<td>Open S3 Bucket</td>
</tr>
<tr>
<td>Event Logs, Syslog, etc</td>
<td>CloudWatch</td>
</tr>
<tr>
<td>Domain / LDAP Admin</td>
<td>AWS Root User</td>
</tr>
</tbody>
</table>
Normal vs Cloud – Azure Translation

- Self Managed Server
- Internal Network
- Firewall
- Open Network Share
- Event Logs, Syslog, etc
- Domain / LDAP Admin

- Virtual Machine
- Virtual Network
- NSG
- Open Storage Account
- Azure Diagnostics / Activity Logs
- 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
Enumerate - DNS

DNSDumpster (and others)
Enumerate - DNS
Shodan
Enumerate - DNS

Brute Force

```
root@suchlinux:~:/Desktop/subbrute# python subbrute.py -s merged-dedupe3.txt 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
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
```

Java SE Development Kit 9 Downloads

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.

The JDK includes tools useful for developing and testing programs written in the Java programming language and running on the Java platform.

See also:

- 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
- Java Magazine

**Java SE Development Kit 9.0.1 checksum**

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 now download this software.
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
  – Smeegescrape
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 be 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
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
Enumerate – Storage - GCP

• Storage on GCP is known as “Cloud Storage”

• Manually access:
  – https://content.googleapis.com/storage/v1/b/bucket/o?key=AIzaSyD-a91F8KgKYoC3cpgS-Al7hLQDbugrDcw

• Tools
  – None for enumeration?
  – CloudBerry Explorer, others?
Escalate

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

• Instead, you’re either going to want to find one of two things:
  1. Credentials for another service. Storage creds for example!
Escalate – Credential Types

• Different creds for different services on different cloud providers

• AWS Keypair:
  – Access Key ID: AKIAQPV2R2RKVOUKENCA
  – Secret Access Key: 7BQYjqsB58xaBZ/RabPH/bqTvUBkfpoK+1qq0aXh

• AWS HMAC’s:
  – AWSAccessKeyId=AKIAI0SFODNN7EXAMPLE&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%2FRHIX5Xcg0Mq2rqI3OltJEg2tYkboXr1P9ZUXDtkk%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 (PFX), 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..)
• 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.
Escalate – DNS tunneling

• Everyone knows about DNS tunneling, right?
• Apparently not, but someone did another nice writeup on it:
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
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
Case Study - Instagram

Step #2 – Shell
Case Study - Instagram

Step #2.5 – Still a shell
Case Study - Instagram

Step #3 – Config Files

```
config.txt - Notepad

{   "admin": {   "host": "https://instagram-packages.s3.amazonaws.com",   "user": "sensu-admin",   "group": "sensu-admin",   "host": "localhost",   "http_port": 80,   "http_port": 443,   "backend_port": 5000,   "repo": "https://github.com/sensu/sensu-admin.git",   "release": "v0.1.1",   "tarball": "https://github.com/sensu/sensu-admin.git",   "username": "sensuadmin",   "new": "sensuadmin",   "password": "********" },   "version": "0.13.1-1",   "rabbitmq": {   "host": "localhost",   "port": 5672,   "user": "sensu",   "password": "********" },   "redis": {   "host": "localhost",   "port": 6379 },   "api": {   "host": "localhost",   "port": 4567 },   "dashboard": {   "host": "localhost",   "port": 8080,   "user": "admin",   "password": "********" },   "sql": {   "host": "localhost",   "port": 3306,   "username": "sensu",   "password": "********" }
}
```

- Good
- Ok
- Uhh
Case Study - Instagram

Step #3.1 – Config Files

```yaml
"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-c3xlarge -s AIHAIIIOO888888888BC9R -s "wIfXoxYoI/y8888888888888888888888a34"",
  "interval": 60,
  "occurrences": 3,
  "category": "vxcode",
  "issue": "regression",
  "subscribers": [
    "sensu-backend"
  ],
  "handlers": [
    "alerts"
  ]
},
"mailer": {
  "mail_from": "sensu@instagram.com",
  "mail_to": [
    "i@fb.com"
  ],
  "smtp_address": "mail.thefacebook.com",
  "smtp_port": "587"
}
```
Case Study - Instagram

Step #4 - Storage
Case Study - Instagram

Step #5 – More keys
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?

Contact: wesley@exfiltrated.com
Slides: http://exfiltrated.com (eventually)
https://www.slideshare.net/GeraldSteere/cloud-basics-for-pen-testers-red-teamers-and-defenders