

What is the tool Ghostbuster? How can it help us when it relates to Web Application Testing Using Vulnhub?

Must Have Kali Linux Download. Use the Pen Testing Doc within the **RED TEAM**.

Step 1: Go to <https://www.vulnhub.com> Search Raven1

Step2: Sign into AWS console

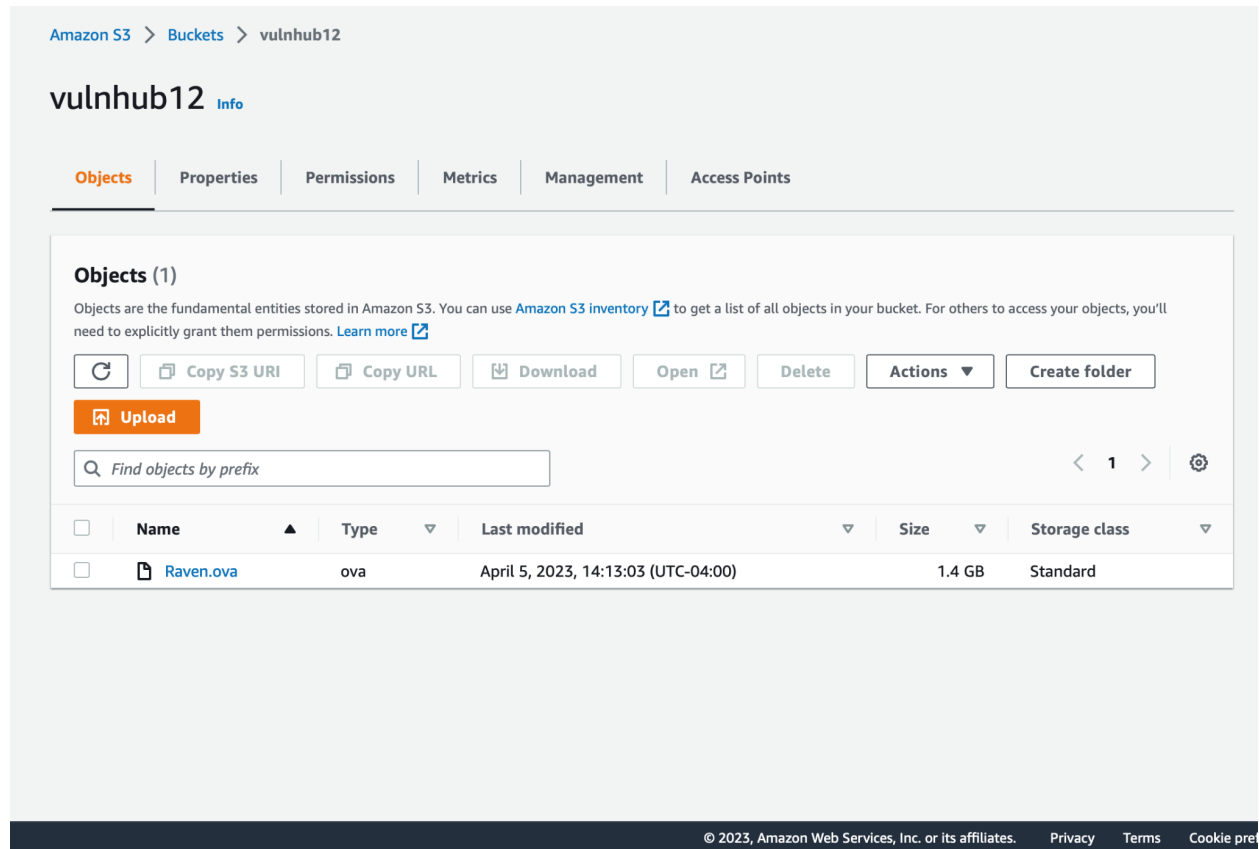
Step3: Create an S3 Bucket

The screenshot shows the Amazon S3 console interface. At the top, it says "Amazon S3 > Buckets". Below this is an "Account snapshot" section with a "View Storage Lens dashboard" button. The snapshot shows "Total storage" as 1.9 GB, "Object count" as 35, and "Average object size" as 54.7 MB. Below this is a "Buckets (2)" section with a search bar and buttons for "Copy ARN", "Empty", "Delete", and "Create bucket". A table lists the buckets:

	Name	AWS Region	Access	Creation date
<input type="radio"/>	<a href="#">static121</a>	US East (N. Virginia) us-east-1	Objects can be public	March 12, 2023, 12:38:26 (UTC-04:00)
<input type="radio"/>	<a href="#">vulnhub12</a>	US East (N. Virginia) us-east-1	Objects can be public	April 5, 2023, 12:24:15 (UTC-04:00)

At the bottom of the console, there is a footer with copyright information: "© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preference".

Step4: Upload the file you downloaded to your S3 bucket



**Step5:** Click [Here](#) for the steps and commands to upload your OVAFILES to your AWS cloudshell. <https://github.com/vick627/Turtorial/blob/main/Directions>

**Step6:** Go to your Ec2 Instance console click on create instance

**Step7:** Click on my AMI and your OVA File shall appear like in the screenshot below.

Name and tags
Info

Name

e.g. My Web Server

Add additional tags

Application and OS Images (Amazon Machine Image)
Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents
My AMIs
Quick Start

Owned by me
Shared with me

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

import-ami-0ed7a67f753905924
ami-053517aeb9aff9fa9
2023-04-07T20:25:16.000Z
Virtualization: hvm
ENA enabled: false
Root device type: ebs

Number of instances
Info

1

Software Image (AMI)
AWS-VMImport service: Linux - ...read more
ami-053517aeb9aff9fa9

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 20 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel
Launch instance
Review commands

**Step8: Click on Network Settings and make sure it's in a public subnet.**

**Step9: Click On Launch Instance.**

**Step10: SSH into your Kali linux with the following command `ssh -i <username>@ip` Here is an example below:**

```
visionary@Vision ~ % cd Downloads
visionary@Vision Downloads % ssh -i "Red_Team.pem" kali@ec2-18-234-45-187.compute-1.amazonaws.com
Linux kali 6.1.0-kali7-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.20-1kali1 (2023-03-22) x86_64

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

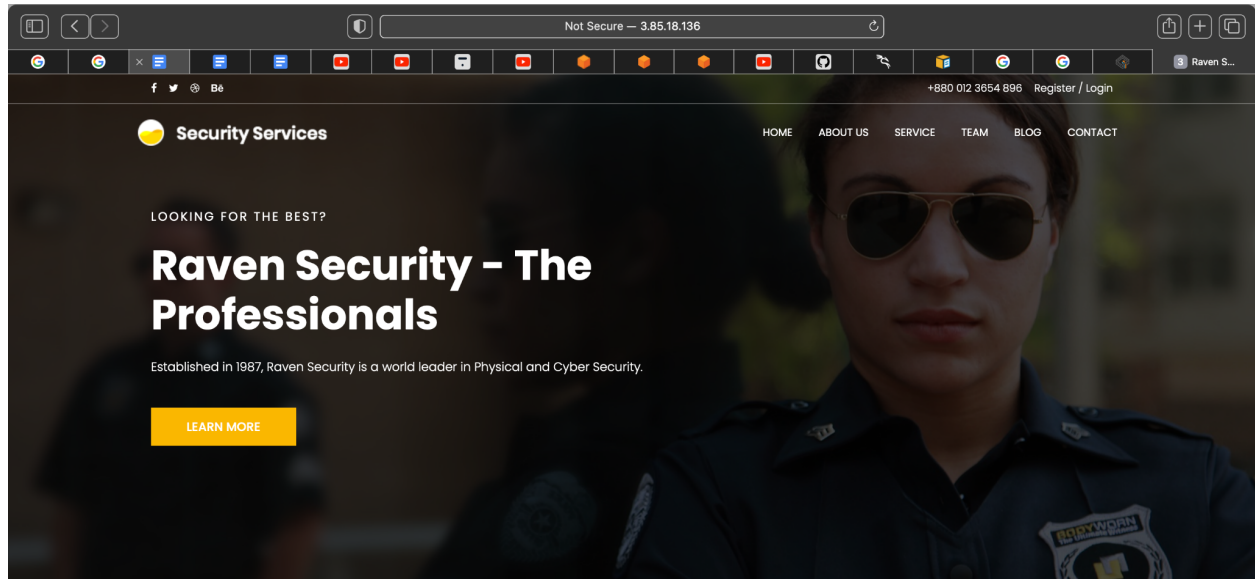
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr  9 19:13:20 2023 from 24.38.225.199
-(Message from Kali developers)

This is a cloud installation of Kali Linux. Learn more about
the specificities of the various cloud images:
→ https://www.kali.org/docs/troubleshooting/common-cloud-setup/

(Run: "touch ~/.hushlogin" to hide this message)
kali@kali:~$
```

**Step11:** Use this Link to get a default kali linux with all the necessary tools to perform a Web Application Test <https://www.kali.org/docs/general-use/metapackages/>

**Step12:** At this point you will want to start your vulnerable machine. With the IP address you should be able to reach a website. Look At Screenshot Below.



## Our Offered Services

Niche, Discreet, Professional

**Step 13: Ping the Ip address of the website from your Kali to ensure connectivity within the network.**

```
(kali㉿kali)-[~]  
$ ping 3.85.18.136  
PING 3.85.18.136 (3.85.18.136) 56(84) bytes of data.  
64 bytes from 3.85.18.136: icmp_seq=1 ttl=63 time=0.517 ms  
64 bytes from 3.85.18.136: icmp_seq=2 ttl=63 time=0.636 ms  
64 bytes from 3.85.18.136: icmp_seq=3 ttl=63 time=0.552 ms  
64 bytes from 3.85.18.136: icmp_seq=4 ttl=63 time=0.555 ms  
64 bytes from 3.85.18.136: icmp_seq=5 ttl=63 time=0.663 ms  
64 bytes from 3.85.18.136: icmp_seq=6 ttl=63 time=0.615 ms  
64 bytes from 3.85.18.136: icmp_seq=7 ttl=63 time=0.604 ms  
^C  
--- 3.85.18.136 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6143ms  
rtt min/avg/max/mdev = 0.517/0.591/0.663/0.048 ms  
  
(kali㉿kali)-[~]  
$ █
```

**Step14:** Install gobuster with the following command **sudo apt install gobuster**

**Step15:** Follow the steps in the github link to download seclists.

<https://github.com/danielmiessler/SecLists>

**Step 16:** With all the tools necessary you can now perform a scan of the website to see what ports are open. Look at the screenshot below.

```
(kali@kali)-[~]
└─$ sudo apt install gobuster
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gobuster is already the newest version (3.5.0-1).
(kali@kali)-[~]
└─$ gobuster dir --url http://3.85.18.136 --wordlist /usr/share/seclists/Discovery/Web-Content/big.txt -t20
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://3.85.18.136
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s
=====
2023/04/10 00:59:42 Starting gobuster in directory enumeration mode
=====
/.htaccess (Status: 403) [Size: 295]
/.htpasswd (Status: 403) [Size: 295]
/css (Status: 301) [Size: 308] [--> http://3.85.18.136/css/]
/fonts (Status: 301) [Size: 310] [--> http://3.85.18.136/fonts/]
/img (Status: 301) [Size: 308] [--> http://3.85.18.136/img/]
/js (Status: 301) [Size: 307] [--> http://3.85.18.136/js/]
/manual (Status: 301) [Size: 311] [--> http://3.85.18.136/manual/]
/server-status (Status: 403) [Size: 299]
/vendor (Status: 301) [Size: 311] [--> http://3.85.18.136/vendor/]
/wordpress (Status: 301) [Size: 314] [--> http://3.85.18.136/wordpress/]
Progress: 20476 / 20477 (100.00%)
=====
2023/04/10 00:59:45 Finished
=====
(kali@kali)-[~]
└─$
```