

ATTACK

DEFENSE

by PentesterAcademy

Name	APT Repo: Recon Basics
URL	https://www.attackdefense.com/challengedetails?cid=1068
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.

Q1.Which service is running on the target machine?

Answer: HTTP

Solution:

Check 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
15020: eth0@if15021: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
15023: eth1@if15024: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:fe:06:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.254.6.2/24 brd 192.254.6.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Launch Nmap scan on target

Command: nmap -p- -sV 192.254.6.3

```
root@attackdefense:~# nmap -p- -sV 192.254.6.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-10 08:55 IST
Nmap scan report for djhozv9e9v7gd8g42dz9lcepo.temp-network_a-254-6 (192.254.6.3)
Host is up (0.000029s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 02:42:C0:FE:06:03 (Unknown)

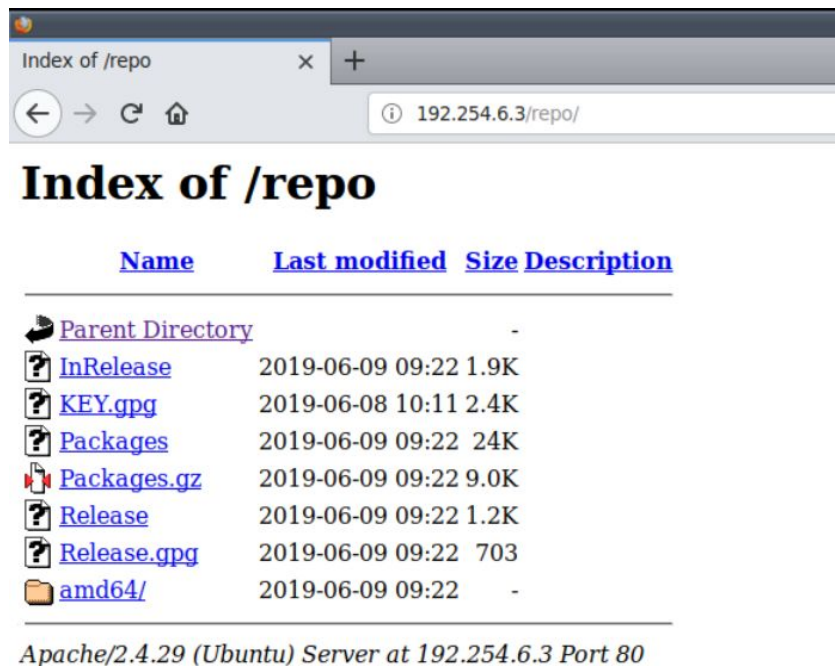
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 9.40 seconds
root@attackdefense:~#
```

Q2. What is the name of the directory in which all repository related files are kept?

Answer: repo

Open a web browser window and navigate to the IP address of the target machine.

URL: <http://192.254.6.3>



The screenshot shows a web browser window with the address bar displaying 192.254.6.3/repo/. The page title is "Index of /repo". Below the title is a table listing the contents of the directory. The table has four columns: Name, Last modified, Size, and Description. The entries are as follows:

Name	Last modified	Size	Description
Parent Directory	-	-	-
InRelease	2019-06-09 09:22	1.9K	
KEY.gpg	2019-06-08 10:11	2.4K	
Packages	2019-06-09 09:22	24K	
Packages.gz	2019-06-09 09:22	9.0K	
Release	2019-06-09 09:22	1.2K	
Release.gpg	2019-06-09 09:22	703	
amd64/	2019-06-09 09:22	-	

At the bottom of the page, it says "Apache/2.4.29 (Ubuntu) Server at 192.254.6.3 Port 80".





Q3. How many packages are present in the repository?

Answer: 19

Open a web browser window and navigate to the IP address of the target machine. And, manually count the packages.

URL: <http://192.254.6.3/repo/amd64/>



Name	Last modified	Size	Descri
 Parent Directory		-	
 auditd_2.8.2-1ubuntu1_amd64.deb	2019-06-09 09:22	189K	
 init-system-helpers_1.51_all.deb	2017-12-30 12:33	36K	
 libaudit1_2.8.2-1ubuntu1_amd64.deb	2018-02-08 00:23	38K	
 libauparse0_2.8.2-1ubuntu1_amd64.deb	2018-02-08 00:23	47K	
 libc6_2.27-3ubuntu1_amd64.deb	2018-04-17 03:18	2.7M	
 libestr0_0.1.10-2.1_amd64.deb	2017-11-01 21:38	7.4K	
 libfastjson4_0.99.8-2_amd64.deb	2018-01-14 23:18	20K	
 libsystemd0_237-3ubuntu10_amd64.deb	2018-04-21 11:59	199K	
 libuuid1_2.31.1-0.4ubuntu3_amd64.deb	2018-03-15 22:59	19K	
 libxtables-dev_1.6.1-2ubuntu2_amd64.deb	2017-11-12 02:58	11K	
 lsb-base_9.20170808ubuntu1_all.deb	2017-12-06 00:18	12K	
 mawk_1.3.3-17ubuntu3_amd64.deb	2018-04-04 23:38	80K	
 openssh-client_7.6p1-4_amd64.deb	2018-02-10 11:38	596K	
 openssh-server_7.6p1-4_amd64.deb	2018-02-10 11:38	325K	
 rsyslog_8.32.0-1ubuntu4_amd64.deb	2018-04-24 16:39	402K	
 ruby-all-dev_2.5.1_amd64.deb	2018-03-26 08:50	5.2K	
 ruby_2.5.1_amd64.deb	2018-03-26 08:50	5.6K	
 ufw_0.36-1_all.deb	2018-12-27 07:28	161K	

Q4. What command can be used to configure the attacker Kali machine to use this APT repository?

Command: `echo "deb http://192.254.6.3/repo/ /" > /etc/apt/sources.list.d/internal.list`

```
root@attackdefense:~#  
root@attackdefense:~# echo "deb http://192.254.6.3/repo/ /" > /etc/apt/sources.list.d/internal.list  
root@attackdefense:~#
```

Q5. What command can be used to add GPG key of the APT repository to the attacker Kali machine?

Command: `wget -q -O - http://192.254.6.3/repo/KEY.gpg | apt-key add -`

```
root@attackdefense:~#  
root@attackdefense:~# wget -q -O - http://192.254.6.3/repo/KEY.gpg | apt-key add -  
OK  
root@attackdefense:~#
```

Q6. There is a flag hidden in "auditd" package. Install the package and submit that flag.

Solution:

Step 1: Update the package list

Command: `apt update`

```
root@attackdefense:~# apt update  
Get:1 http://192.254.6.3/repo InRelease [1956 B]  
Get:2 http://192.254.6.3/repo Packages [9205 B]  
Fetched 11.2 kB in 0s (34.1 kB/s)  
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 2: 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 3: 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 193768 Jun  9 14:52 auditd_1%3a2.8.2-1ubuntu1_amd64.deb  
-rw-r--r-- 1 root root 48608 Feb  8 2018 libauparse0_1%3a2.8.2-1ubuntu1_amd64.deb  
-rw-r----- 1 root root      0 Jan 11 2018 lock  
drwx----- 1 _apt root 4096 Jun 10 11:10 partial  
root@attackdefense:~#
```

Step 4: Change to cache directory, extract the archive.

Commands:

```
cd /var/cache/apt/archives  
mkdir extracted  
dpkg-deb -R auditd_1%3a2.8.2-1ubuntu1_amd64.deb extracted
```

```
root@attackdefense:~# cd /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 5: Change to extracted directory and retrieve the flag.

Commands:

```
cd extracted  
find . -name *flag*  
cat sbin/flag.txt
```

```
root@attackdefense:/var/cache/apt/archives# cd extracted/  
root@attackdefense:/var/cache/apt/archives/extracted# find . -name *flag*  
./sbin/flag.txt  
root@attackdefense:/var/cache/apt/archives/extracted#  
root@attackdefense:/var/cache/apt/archives/extracted# cat sbin/flag.txt  
cb0893450787ebc2f621ffc323b7affb  
root@attackdefense:/var/cache/apt/archives/extracted#
```

Flag: cb0893450787ebc2f621ffc323b7affb

References:

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