**Challenge:** IronShade

**Platform:** TryHackMe

**Category:** Endpoint Forensics

**Difficulty:** Medium

**Tools Used:** bash

**Summary:** This challenge involved investigating a compromised Linux host, requiring you to identify malicious users, cronjobs, processes, services, and packages. I am very new to Linux forensics; therefore, this challenge was relatively difficult, however, with enough patience, you can easily complete this challenge.

**Scenario:** Based on the threat intel report received, an infamous hacking group, IronShade, has been observed targeting Linux servers across the region. Our team had set up a honeypot and exposed weak SSH and ports to get attacked by the APT group and understand their attack patterns.

You are provided with one of the compromised Linux servers. Your task as a Security Analyst is to perform a thorough compromise assessment on the Linux server and identify the attack footprints. Some threat reports indicate that one indicator of their attack is creating a backdoor account for persistence.

**What is the Machine ID of the machine we are investigating?**

On Linux, the machine ID can typically be found in the following location:

- `/etc/machine-id`

For context, the Machine ID is a unique identifier that is used to identify a specific machine. We can use cat to read this file:

- `cat /etc/machine-id`

```
ubuntu@cybertees:~$ cat /etc/machine-id
dc7c8ac5c09a4bbfaf3d09d399f10d96
```

Answer: dc7c8ac5c09a4bbfaf3d09d399f10d96

**What backdoor user account was created on the server?**

The /etc/passwd file stores essential information about user's accounts. If we cat this file and grep for home, we can see an account called "microservice":

```
ubuntu@cybertees:~$ cat /etc/passwd | grep "home" | cut -d ':' -f1
syslog
ubuntu
cups-pk-helper
mircoservice
```

If you filter for events related to this user in the auth logs, we can see that this user was created on the 5th of August at 22:05:33:


Answer: microservice

**What is the cronjob that was set up by the attacker for persistence?**

Cronjobs are scheduled tasks executed automatically at predefined intervals by the cron daemon. Users have their crontab file stored in the /var/spool/cron/crontabs directory, the main crontab file is at /etc/crontab, governing system-wide cronjobs. To list all users who have cronjobs, we can use the following command:

- `sudo ls -al /var/spool/cron/crontabs/`

```
ubuntu@cybertees:~$ sudo ls -al /var/spool/cron/crontabs/
total 16
drwx-wx--T 2 root   crontab 4096 Aug  6  2024 .
drwxr-xr-x 5 root   root    4096 Oct 26  2020 ..
-rw------- 1 root   crontab 1130 Aug  6  2024 root
-rw------- 1 ubuntu crontab 1225 Feb 27  2022 ubuntu
```

As you can see, root and ubuntu are the only users who have cronjobs. If you list the crontab for the root user, you can see an interesting cronjob:

- `sudo crontab -l -u root`

```
ubuntu@cybertees:~$ sudo crontab -l -u root
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

@reboot /home/mircoservice/printer_app
```

This cronjob means that the command will run once at every system boot (i.e., every time the system boots, printer_app is executed). If you run the file command against the printer_app file, you can see that it is an ELF file (executable file format):

```
ubuntu@cybertees:/home/mircoservice$ file printer_app
printer_app: ELF 64-bit LSB shared object, x86-64, versi
stripped
```

Answer: @reboot /home/mircoservice/printer_app

**Examine the running processes on the machine. Can you identify the suspicious-looking hidden process from the backdoor account?**

We can use the ps auxf command to list all running processes with full details. If you filter for /home, you can find processes running from user directories:

- `sudo ps auxf | grep "home"`

```
ubuntu@cybertees:~$ sudo ps auxf | grep "home"
root         575  0.0  0.0   2364   580 ?        Ss   04:39   0:00 /home/mircoservice/.tmp/.strokes
root         845  0.0  0.0   2496    72 ?        S    04:39   0:00 /home/mircoservice/printer_app
ubuntu       972  0.9  4.7 381136 188900 ?       S    04:39   0:17 /usr/bin/Xtigervnc :1 -desktop cyber
buntu/.vnc/passwd -rfbport 5901 -pn -localhost -SecurityTypes VncAuth
ubuntu      1062  0.0  0.1 378356  6192 ?        Sl   04:39   0:00 /usr/libexec/gvfsd-fuse /home/ubuntu
ubuntu      2949  0.0  0.0   3312   656 pts/2    S+   05:10   0:00      \_ grep --color=auto home
```

.strokes running from the .tmp directory is suspicious, especially as its associated with the backdoor account. Better yet, you can filter for all processes from the microservice user by entering the following command:

- `ps aux -u microservice`

```
ubuntu@cybertees:~$ ps aux -u mircoservice | grep strokes
root         575  0.0  0.0   2364   580 ?        Ss   04:39   0:00 /home/mircoservice/.tmp/.strokes
```

Answer: .strokes

**How many processes are found to be running from the backdoor account's directory?**

If you refer to the previous question, we can see that there are two processes running from the microservice directory:

```
root         575  0.0  0.0   2364   580 ?        Ss   04:39   0:00 /home/mircoservice/.tmp/.strokes
root         845  0.0  0.0   2496    72 ?        S    04:39   0:00 /home/mircoservice/printer_app
```

Answer: 2

**What is the name of the hidden file in memory from the root directory?**

If you run the ls -la command against the root directory, you can find the following hidden file:

```
ubuntu@cybertees:~$ sudo ls -la /
total 104
drwxr-xr-x  19 root root  4096 Jul 25 04:39 .
drwxr-xr-x  19 root root  4096 Jul 25 04:39 ..
-rw-r--r--   1 root root   191 Jul 25 04:39 .badr-info
-rwxr-xr-x   1 root root 17088 Jul  2  2024 .systmd
```

Answer: .systmd

**What suspicious services were installed on the server? Format is service a, service b in alphabetical order.**

Services refer to background processes or daemons that run continuously. Threat actors often abuse services to establish persistence. To list all services, we can execute the following command:

- `ls /etc/systemd/system`

```
ubuntu@cybertees:~$ ls /etc/systemd/system
backup.service                                  dbus-org.freedesktop.resolve1.service   multi-user.target.wants                 snap-core-16928.mount                                snap.lxd.daemon.unix.socket
backup.service.save                             dbus-org.freedesktop.timesync1.service  multipath-tools.service                 snap-core-17200.mount                                snapd.mounts.target.wants
badr.service                                    default.target.wants                    network-online.target.wants             snap-core18-2823.mount                               sockets.target.wants
bluetooth.target.wants                          display-manager.service                 oem-config.service.wants                snap-core18-2829.mount                               sshd-keygen@.service.d
cloud-final.service.wants                       display-manager.service.wants           open-vm-tools.service.requires          snap-core20-2105.mount                               sshd.service
cloud-init.target.wants                         emergency.target.wants                  paths.target.wants                      snap-core20-2318.mount                               strokes.service
dbus-fi.w1.wpa_supplicant1.service              final.target.wants                      printer.target.wants                    snap-lxd-24061.mount                                 sysinit.target.wants
dbus-org.bluez.service                          getty.target.wants                      rescue.target.wants                     snap-lxd-29619.mount                                 syslog.service
dbus-org.freedesktop.Avahi.service              graphical.target.wants                  sleep.target.wants                      snap.amazon-ssm-agent.amazon-ssm-agent.service       timers.target.wants
dbus-org.freedesktop.ModemManager1.service      iscsi.service                           'snap-amazon\x2dssm\x2dagent-7628.mount' snap.lxd.activate.service                           vmtoolsd.service
dbus-org.freedesktop.nm-dispatcher.service      mdmonitor.service.wants                 'snap-amazon\x2dssm\x2dagent-7993.mount' snap.lxd.daemon.service
```

```
ubuntu@cybertees:~$ cat /etc/systemd/system/backup.service
[Unit]
Description=updater

[Service]
ExecStartPre=/bin/sleep 5
ExecStart=/home/mircoservice/backup/sys_backup
Restart=always

[Install]
WantedBy=multi-user.target

ubuntu@cybertees:~$ cat /etc/systemd/system/strokes.service
[Unit]
Description=strokes

[Service]
ExecStart=/home/mircoservice/.tmp/.strokes
Restart=always

[Install]
WantedBy=multi-user.target
```

Answer: backup.service, strokes.service

**Examine the logs; when was the backdoor account created on this infected system?**

Recall how in the second question we discovered the backdoor user. If you filter the auth logs for events related to the microservice user, we can see when this user was created:

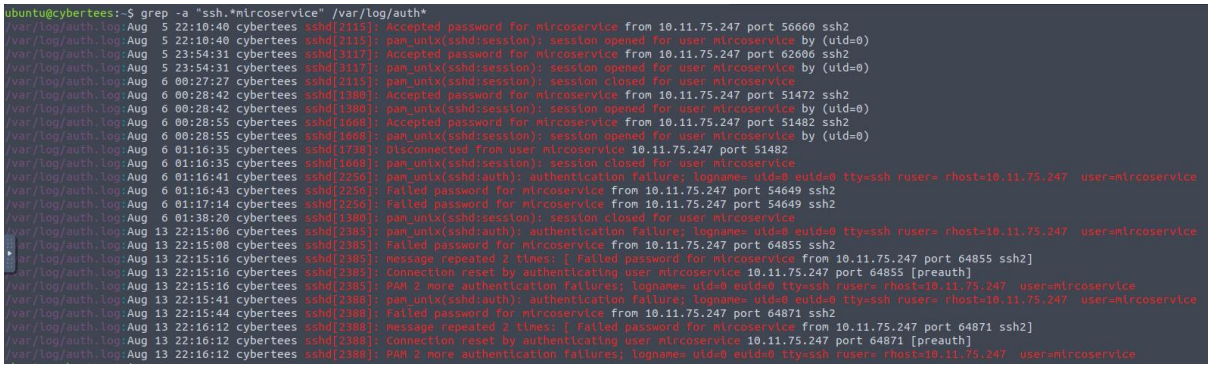
- `grep -a "mircoservice" /var/log/auth*`


Answer: Aug 5 22:05:33

**From which IP address were multiple SSH connections observed against the suspicious backdoor account?**

To find SSH authentication logs to the microservice user, we can filter the auth logs like as follows:

- `grep -a "ssh.*mircoservice" /var/log/auth*`



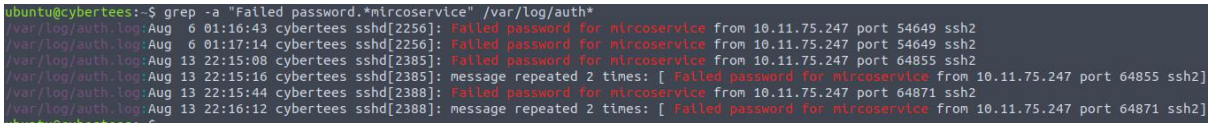

The IP associated with multiple SSH connections to the microservice user is 10.11.75.247.

Answer: 10.11.75.247

**How many failed SSH login attempts were observed on the backdoor account?**

In order to determine how many failed SSH authentication attempts were observed on the backdoor account, we can use the following command:

- `grep -a "Failed password.*mircoservice" /var/log/auth*`




As you can see, there are 8 failed authentication attempts (make sure to count the message repeated 2 times logs, i.e., 4+2+2).

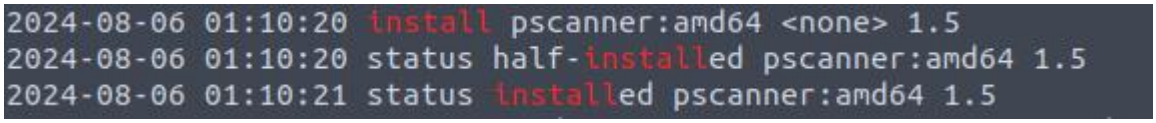
Answer: 8

**Which malicious package was installed on the host?**

To find the malicious package that was installed on the host, we can view the dpkg.log file using the following command:

- `grep "install" /var/log/dpkg.log`

After looking through the results, I came across the following package being installed:




Answer: pscanner

**What is the secret code found in the metadata of the suspicious package?**

To view the metadata of the malicious package, we can use the following command:

- `dpkg -s pscanner`

```
ubuntu@cybertees:~$ dpkg -s pscanner
Package: pscanner
Status: install ok installed
Priority: optional
Section: base
Maintainer: johnnyEng
Architecture: amd64
Version: 1.5
Description: Secret_code{_tRy_Hack_ME_}
```

Answer: {_tRy_Hack_ME_}