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

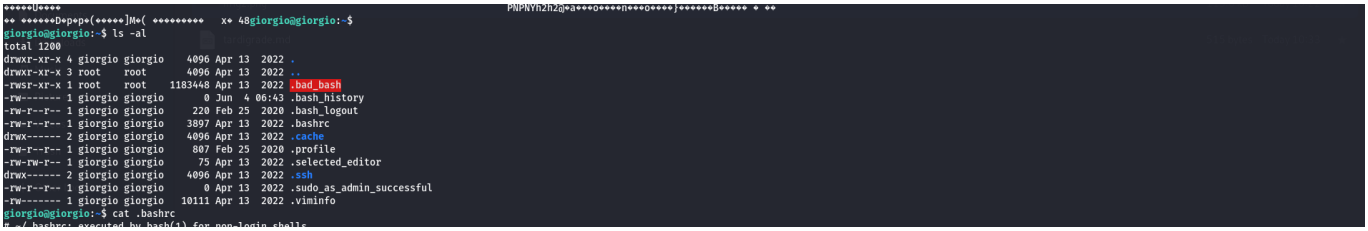
target = "10.10.220.55"

checking OS version

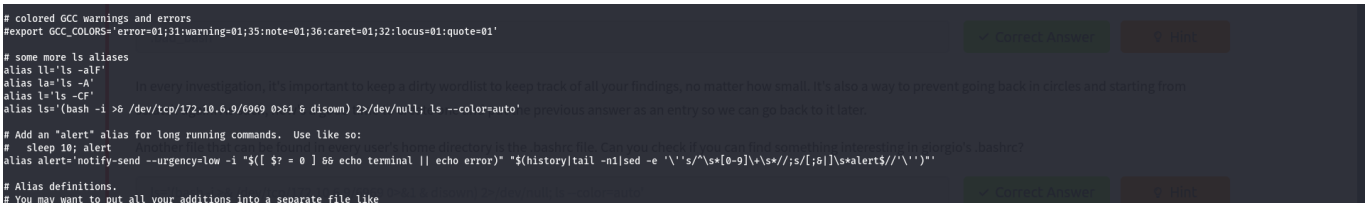
> cat /etc/os-release

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

There is a .bad_bash file.not usual



Lets check the content of .bashrc

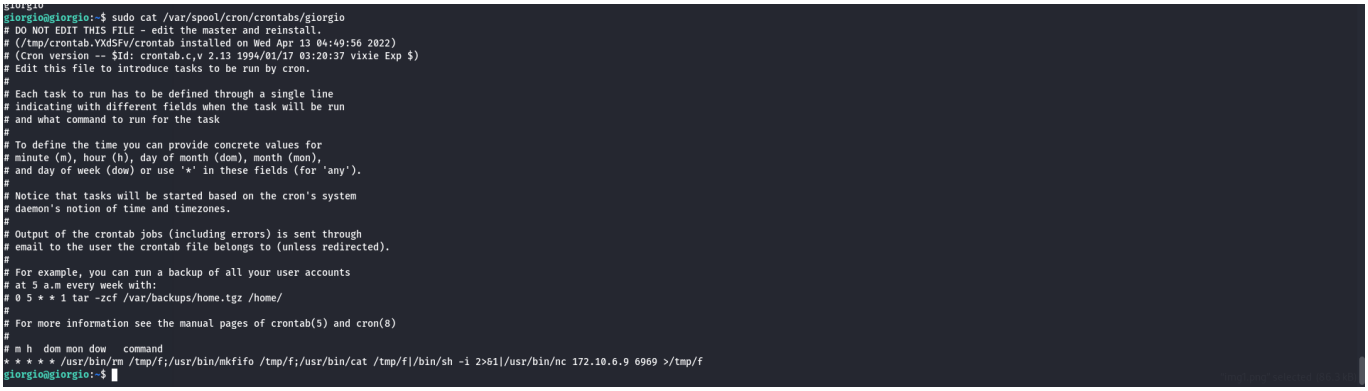


We no move to scheduled tasks, cronjobs

> /etc/crontab

Unfotunately, there is nothing at the system-level.
We need to check at the user level.

> /var/spool/cron/crontabs/giorgia



Lets look for any unusual users in the system

> /etc/passwd
>
> ```
> uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
> proxy:x:13:13: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
> irc: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-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
> systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
> systemd-timesync:x:102:104: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 user is running with permissions root which is not usual