

BIS Projekt 2024/25

Vypracoval: Bc. Adam Hos (xhosad00)

# Zmapování středozemně

Prvním úkolem je zmapování dané sítě. K uživatelskému stroji se dá připojit pomocí příkazu ssh. Užitím příkazu ip addr je možná zjistit následující připojení:

* eth0 10.89.1.212/24
* eth1 10.89.47.2/24

Neboli stroj je připojený do dvou sítí s těmito adresami.

Kvůli technické chybě nelze vypsat názvy zařízení sítích. Sítě mají následující složení:

**Port 22/tcp: ssh (Open)**

* 10.89.1.156
* 10.89.1.168
* 10.89.1.177
* 10.89.1.182
* 10.89.1.184
* 10.89.1.187
* 10.89.1.195
* 10.89.1.208
* 10.89.1.210
* 10.89.1.211
* 10.89.1.212 (de0bce1672d1 moje připojovací stanice)
* 10.89.1.213

**Port 80/tcp: http (Open)**

* 10.89.1.157 (The Iron Fortress – název z .html nástrojem curl)
* 10.89.1.159 (Mirkwood – název z .html nástrojem curl)

**Port 21/tcp: ftp (Open)**

* 10.89.1.158

Name servery: 10.89.47.1 a 10.89.1.1 (z ./LinEnum.sh)

## Zranitelnosti

# Nalezení tajemství

Připojovací stanici jsem ve složce /.hints následující popis pěti tajemství A-E:

## A

The secret A is hidden deep down in the shadow of the Iron Fortress. Although the gate used to be hard as a shell, nowadays it looks like it could easily crumble from a shock. A marking at the base of the gate shows the number: 2014-6271. It seems like the housekeeper of the Iron Fortress forgot to upgrade the defences of his house.

Jedná se o tajemství na serveru 10.89.1.157. Pomocí příkazu curl jsem si stáhl obsah http stránku. Z ní je možné vyčíst, že obsahuje odkaz na /cgi-bin/gate. S kombinací s tipem 2014-6271 lze odvodit, že jde o zranitelnost shell shock (CVE-2014-6271).

Pomocí curl jsem otestoval, že je skutečně možné využít shell shock. Vyzkoušel jsem příkazy jako ls a cat, ty ale nebyli úspěšné. Místo cat jsem zkusil:  
while read line; do echo \$line; done < „cesta k souboru/soubor“, který už fungoval. Zkoušel jsem ho na citlivé soubory a eventuálně jsem narazil na /etc/shadow, kde bylo tajemství A.

Příkaz na získání tajemství

curl http://10.89.1.157/cgi-bin/gate -H "User-Agent: () { :; }; echo Content-Type: text/plain; echo; while read line; do echo \$line; done < /etc/shadow"

## B

King of Edoras holds secret B hidden to everyone. He keeps the secret in his private space where only him can access it. Not even his very close elven friend - admin, who shares many secrets with the king - cannot access it. However, while the king keeps an eye on his secret, he may overlook access restrictions to some other important files. Find out how to control his friend - admin - and search some other interesting files to find out, how to bypass the king's guards. Perhaps, you should start gathering other information about his friend somewhere else.

## C

Secret C is easily retrieved from lousy workers at the elven kingdom. They barely check the outside of the incoming packages, let alone the insides. All they do is check the outsides and look on the lable, which describes the insides. Snuck a fake, possibly malicious package - a php script-like payload - through the input checkers and the secret is yours.

## D

The dark forest is a place of many webs and bugs, some of them hardly visible. Those who can not find their way should verify themselves to the forest and the way shall be pointed to them. Once you arrive to the right place, perhaps ask not only about items, but about the contents of the previous verification too. Some say the best way to approach this task is through union.

Jedná se o tajemství na serveru 10.89.1.159. Pomocí příkazu curl jsem si stáhl obsah http stránky. Je možné se odkázat na authentication.html, který obsahuje formu s jménem a heslem, a upload.html, který má formu pro uložení souboru.

## E

On thing is for sure - you are always welcome here in the house of Elrond. Your old friend said, that he has an interesting artefact. A chest with a damaged lid - to a common bystander, this chest looks like a junk. But Elrond is very persistent - he knows that the chest hides something.

V domácí složce uživatele jsem našel .ssh, v které jsem následně našel privátní ssh klíč a configuraci pro ssh připojení uživatele elrond využívající tento klíč. Chybělo ale nastavení HostName. Jelikož v době mého řešení už nebyli dostupné hostname jednotlivých serverů, zkusil jsem se připojit na servery podporující ssh.

Příkazem ssh -i ~/.ssh/id\_rsa elrond@10.89.1.156, jsem se připojil k servru. Zkusil jsem pomocí příkazu hostname zjistit jméno serveru, ale výsledek a873d388b394 nebyl moc nápomocný.

# Věci, co jsem udělal

* Přidání uživatele user do root skupiny

# Užitečné věci

* curl -I http://10.89.1.157