BIS

Bezpečnost informačních systémů

The FITfather

Ján Jakub Kubík (xkubik32)

8. augusta 2023

Obsah

1 Úvod

Cieľom projektu bolo získať vo vyhradenom čase čo najviac tajomstiev ukrytých na privátnych serveroch v sieti 147.229.8.53. K prístupu na danú sieť som dostal privátny kľúč pomocou ktorého som sa na danú IP adresu na port 2222 mohol cez SSH pripojiť. Kľúč prišiel v nesprávnom formáte a preto som musel zmeniť CRLF na LF. Potom mi to fungovalo. Tajomstvo je reťazec ľubovoľnej dĺžky, ktorý vždy obsahuje slovo "tajemství".

2 Tajomstvá

Podarilo sa mi odhaliť nasledujúcich 6 tajomstiev:

Kapitola 4	`Tajemstv_x_9d0ee8d48304b6efab1bfd60d10e661de4e5d13a0c12adce39d0ee8d`
Kapitola 5	`Tajemstvi_3_3f86d72b1ee288db25984ed5eeb3e4026d0d29fc9813cc50aab1bf`
Kapitola 6	`Tajemstvi_1_0a4fb503f7bbd8b66becb1b44df40f6be06fa99a6d71f4f2c1d706bbd589817f`
Kapitola 7	`tajemstvi_h_7155a291dcf4c45918b26de2571b13a0dffde1109a576863cddbd7b45d95508a`
Kapitola 9	`tajemstvi_w_8f29935c3ee89b9f32f5e91a8399043ffd6a40543c738a061012585dd911543e`
Kapitola 8	`tajemstvi_w_36f028580bb02cc8272a9a020f4200e346e276ae664e45ee80745574e2f5ab80`

Následujúce kapitoly popisujú postup pre odhalenie jednotlivých tajomstiev. Sú usporiadané podľa poradia ako som odhaľoval jednotlivé tajomstvá.

3 Analýza

Po pripojení na 147.229.8.53 som najskôr preskúmal vnútornú sieť. Pomocou príkazu `ifconfig` som zistil lokálnu adresu serveru (192.168.122.35) na ktorom som bol pripojený a sieťovú masku. Ďalej som sa pomocou príkazu `nmap -Pn 192.168.122.0/24` pokúsil zmapovať celú sieť. Získal som nasledujúce výsledky:

```
Nmap scan report for _gateway (192.168.122.1)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
MAC Address: 52:54:00:41:27:D1 (QEMU virtual NIC)

Nmap scan report for 192.168.122.3
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 52:54:00:53:08:85 (QEMU virtual NIC)

Nmap scan report for 192.168.122.90
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 52:54:00:41:02:A1 (QEMU virtual NIC)

Nmap scan report for 192.168.122.149
PORT     STATE SERVICE
22/tcp   open  ssh
5432/tcp open  postgresql
MAC Address: 52:54:00:2E:7A:F0 (QEMU virtual NIC)
```

```
Nmap scan report for server2 (192.168.122.235)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 52:54:00:3A:FB:88 (QEMU virtual NIC)

Nmap scan report for fedora (192.168.122.35)
PORT     STATE SERVICE
22/tcp   open  ssh
9090/tcp open  zeus-admin
```

Ďalej som preskúmal `$HOME` adresár pomocou `ls -R -A $HOME`. V priečinku `.ssh` som našiel privátny kľúč používateľa *pepa*. Ďalej som našiel adresáre s podozrivými súbormi. Konkrétne to boli `jsapp` (kapitola 6), `lib` (kapitola 5) a `app` (kapitola 4). Pomocou privátného kľúča som sa postupne pokúsil pripojiť na všetky dostupné servery. Úspešný som bol až so serverom 149 (`ssh -i  /.ssh/id_rsa.key pepa@192.168.122.149`, kapitola 9).

4 Tajomstvo myprog

V adresári myprog bola dostupná aplikácia `myprog`, ktorá po spustení vyžadovala heslo. Ako nápovedu obsahoval daný program text: `Uhiuhvk brxu dvvhpeohu vnloov wr rewdlq vhfuhw`. Zistil som, že je to Cézarová šifra a obsahovala nápovedu: `Refresh your assembler skills to obtain secret`. Tak som pomocou online disassembleru [1] dekompiloval aplikáciu. V assembler kódu aplikácie som vyčítal heslo `2ce2a20678`. Po zadaní hesla sa objavilo tajomstvo.

`Tajemstv_x_9d0ee8d48304b6efab1bfd60d10e661de4e5d13a0c12adce39d0ee8d`

5 Tajomstvo library

Adresár library obsahoval aplikáciu `secret_application` spolu s nápovedami uloženými v `foo.h` a `odposlech`. Aplikácia po spustení nevracala tajomstvo. Z foo.h som si uvedomil, že v secret_application sa pravdepodobne volá `secret_function`. Pomocou príkazu `nm secret_application` som si to potvrdil. Na základe nápovedy v odposlech som vytvoril novú dynamickú knižnicu s funkciou `secret_function`, ktorá vždy vracia 123 ako bolo v nápovede v `odposlech` súbore. Knižnicu som vytváral a linkoval k programu podľa tohoto návodu [2]. Po vytvorení a nalinkovaní knižnice k secret application som získal ďalšie tajomstvo.

`Tajemstvi_3_3f86d72b1ee288db25984ed5eeb3e4026d0d29fc9813cc50aab1bf`

6 Tajomstvo jsapp

Adresár jsapp obsoval súbor `app.html`. Bol to html kód spolu s obfuskovaným javascript kódom. Je to formulár, ktorý po zadaní správneho mena a hesla vypíše tajomstvo. Tajomstvo je javascriptový kód `"Tajemstvi_1_"+ sha3_256(username + password)`. Po deobfuskáci JS kódu pomocou online nástroja som zistil pomocou funckie `passw()` heslo 1f7413aa7. Username som nevedel nijako zistiť ale ako nápovedu som mal hash v JS aplikácii. Náhodou som pri prehladávani adresárov zistil pri prezeraní dostupných používateľov zvláštnych používateľov s menom user, a používatelov s menom test, kde je číslo. Tak som si napísal skript v Pythone, ktorý iteroval cez user od 0 až dokedy nenájde username hash z app.html. Bol som úspešný a username je `user3038`. Po zadaní mena user3038 a hesla 1f7413aa7 do formulára som získal tretie tajomstvo v poradí.

[1] https://onlinedisassembler.com/

[2] https://www.cprogramming.com/tutorial/shared-libraries-linux-gcc.html

`Tajemstvi_1_0a4fb503f7bbd8b66becb1b44df40f6be06fa99a6d71f4f2c1d706bbd589817f`

7 Tajomstvo prace

Prehľadávaním úplne všetkých adresárov som narazil na adresár `/prace` s podaresárom `/mail`, ktorý obsahoval súbor `korespondence`. V tomoto súbore som našiel ďalšie tajomstvo.

`tajemstvi_h_7155a291dcf4c45918b26de2571b13a0dffde1109a576863cddbd7b45d95508a`

V adresári prace som ďalej našiel privátny kľúč v súbore `idrsa.key`. Ďalej som našiel správu v súbore `.new_message` od uživateľa `joe`. Tak som sa skúsil pomocou tohoto kľúča s používateľským menom joe prihlásiť na všetky dostupné servery. Bol som úspešný so serverom `192.168.122.235`.

8 Tajomstvo joe server

Po tom ako som sa dostal na joe server (`192.168.122.235`) tak som dosť dlho nevedel nájisť nič od čoho by som sa mohol odpichnúť. Až po dlhej chvíle som si všimol, že hneď po prihlásení sa na server, sa mi objavuje podozrivý reťazec yfojrxynd|d8;k57=:=5gg57hh=7<7f>f575k9755j89;j7<;fj;;9j9:jj=5<9::<9j7k:fg=5. Pomocou nástroja [3] som zistil, že sa jedná o ASCII šiftovaciu šifru. Takto som získal ďalšie tajomstvo.

`tajemstvi_w_36f028580bb02cc8272a9a020f4200e346e276ae664e45ee80745574e2f5ab80`

9 Tajomstvo psql

Postgressql služba bola dostupná na serveri `192.168.122.149`. Tak som sa pomocou `pepa` používateľského mena a privátneho kľúča uloženého v `/.ssh.id_rsa.key` tam prihlásil. Po prihlásení ako používateľ pepa sa mi podarilo pomocou príkazu `su database_user` esklaovať práva. Pomocou `psql` som sa pripojil do databáze ako `database_user`. Vypísal som si podozrivú tabuľku `secret_advice`. Bola tam nápoveda `nejaka tajna data by mohl mit super uzivatel` a zašiforvaný text `|mfy%fgtzy%ifyfgxj%{jwxntsD`. Zašiforvaný text bola znovu ASCII šiftovaciu šifru a znamenala `what about databse version?` Z nápoved som sa rozhodol zistiť aký užívatelia sú dostupný na danom systéme z `/etc/passwd`. Našiel som tam používateľa `postgres`. Tak som vyskúšal ako prihlásený používateľ database_user zmeniť používateľa za postgres pomocou príkazu
`c posrgres` a bol som úspešný. Z `secret_table` som si vypísal posledné tajomstvo.

`tajemstvi_w_8f29935c3ee89b9f32f5e91a8399043ffd6a40543c738a061012585dd911543e`

10 Ďalšie tajomstvá

Keďže som sa nedostal na servre `192.168.122.3` a `192.168.122.90`, tak som si myslel že sú tam nejaké ďalšie tajomstvá. Navyše som našiel ďalšiu podozrivú stránku, ktorá bežala na `http://147.229.8.53/`. Bola tam podozrivá ikonka `favicon.ico`. Na internete som zistil, že je to hackersky symbol `The glinder`, tak som si myslel, že v danom obrázku je ukryté tajomstvo pomocou steganografie. Ďalej som sa pomocou `robots.txt` na tejto stránke dostal k `paigo` subdoméne, kde mali nejaký používatelia konverzáciu medzi sebou. Bol tam login formulár, za ktorým som predpokladal, že je ďalšie tajomstvo. So žiadným z týchto prípadov som nevedel pohnút a pár dní na to prišiel mail, že tajomstiev je celkovo 6. 6 tajomstiev som mal už získaných a tak som hľadanie ďalších tajomstviev ukončil.

[3] https://www.dcode.fr/cipher-identifier