Předmět: BIS – Bezpečnost informačních systémů
Autor: Jan Lorenc (xloren15)
Datum: 4. 12. 2022

Projekt – The FITfather

Zmapování sítě

Pomocí příkazu `ifconfig` jsem zjistil ip adresu výchozího serveru 192.168.122.35 a masku 255.255.255.0, díky čemuž jsem pak mohl příkazem `nmap -p- 192.168.122.0/24` nalézt všechny viditelné stanice s jejich aktivními porty:

192.168.122.1
22/tcp open ssh
53/tcp open domain

192.168.122.3
22/tcp open ssh

192.168.122.35
22/tcp open ssh
5355/tcp open llmnr
9090/tcp open zeus-admin

192.168.122.90
22/tcp open ssh

192.168.122.149
22/tcp open ssh
5355/tcp open llmnr
5432/tcp open postgresql

192.168.122.235
22/tcp open ssh

Tajemství 1

Toto tajemství se ukrývá v `jsapp/app.html` na výchozím serveru. Jedná se o formulář, který tajemství odhalil při správně zadaném jménu a heslu. Heslo bylo jednoduché získat, neboť funkce `checkpasswd` porovnávala zadaný input (`_0x1685cf`) s proměnnou `_0x5cf21a` obsahující heslo `7ad3286e4` v plain-textu. Toto bylo odhaleno při debugování. Pro snadnější práci byl původně dlouhý a těžko čitelný řádek upraven přes pretty print z devtools prohlížeče (případně by šlo použít deobfuskátor). Náročnější bylo získat login. Input byl hashován funkci `SHA1` a porovnáván s hashem v proměnné `user`. `SHA1` nelze dekryptovat a tak jsem se uchýlil ke slovníkovému útoku. Žádný z online nástrojů však daný hash neznal. Rozhodl jsem se zkusit štěstí s loginy xloren15 (kdyby to byl easter egg), pepa a joe (nalezenými uživateli viz další tajemství), ale bezúspěšně. Dále jsem se pokusil o bruteforce, nicméně kombinací je příliš a výpočet by trval několik dní, navíc zadání nás od tohoto odrazuje. Nezbylo mi než zkoušet typická uživatelská jména. Na webu [1] jsem nalezl 10 nejpoužívanějších uživatelských jmen. Žádné neprošlo, nicméně loginy mívají za sebou často číslo a kořeny jako admin, user nebo demo bývají poměrně časté a i na výchozím serveru v adresáři /home lze nalézt 4 uživatele user<6 cifer>. Postupně jsem pro každé běžné jméno z uvedeného webu zkusil přidat 1-6 ciferná čísla (takový silně omezený bruteforce) a měl jsem štěstí, neboť hash pro login `user8425` se shodoval.

Tajemství 3

Na výchozím serveru lze nalézt složku `library`. V souboru odposlech je vidět, že vrátí-li funkce `secret_function` hodnotu 123, pak se vypíše tajemství. Tato funkce je implementovaná sdílenou knihovnou `libfoo.so` a k dispozici je i hlavičkový soubor. Implementoval jsem tedy knihovnu v novém souboru `foo.c` s obsahem:

[1] The Top 10 Usernames and Passwords Hackers Try to Get into Remote Computers (lifehacker.com)

```
#include "foo.h"
void foo(void){return;}
int secret_function(int x){return 123;}
```

Knihovnu jsem zkompiloval a přepsal s ní původní knihovnu. Následně již `secret_function` vždy vracela 123 a program proto vždy vypisoval tajemství.

Tajemství H

Při prozkoumání výchozího serveru jsem si všiml adresáře `/prace`, což není běžný adresář z kořene, tak jsem zkusil příkazem `grep -Ril "tajemstvi" /prace`, jestli některý soubor uvnitř neobsahuje tajemství. Ukázalo se, že soubor `/prace/mail/korespondence` klíčové slovo obsahuje, a tak jsem si ho vatáhl pomocí příkazu `cat /prace/mail/korespondence | grep "tajemstvi"`. Výstupem byly 4 řádky obsahující dané slovo, 3 patrně na zmatení, nicméně jeden z nich byl pravé tajemství h.

Tajemství W - 1

Ve složce `.ssh` se nachází rsa klíč a z `.ssh/config` lze vyčíst, že patří uživateli pepa k serveru 192.168.122.149. K serveru jsem se přihlásil pomocí `ssh -i .ssh/id_rsa.key pepa@192.168.122.149`. Na serveru běží PostgreSQL a uxistuje tam další uživatel `database_user`, za kterého se lze vydávat bez nutnosti hesla příkazem `su database_user`. Dále jsem do postgre vstoupil příkazem `psql` a vylistoval si databáze pžíkazem `\l`. Jako první jsem si všiml databáze `secret_database`, nicméně ta je prázdná. Dále tam je databáze `database_user`, která uřivateli `database_user` patří, tak jsem ji prozkoumal. Z tabulky `secret_advice` příkazem `SELECT * FROM secret_advice;` lze zjistit, že super uživatel, tedy postgres, by něco mohl vědět. Připojil jsem se tedy do jeho databáze přes `\c postgres` a zde jsem nalezl `secret_table`, z níž jsem příkazem `SELECT * FROM secret_table;` získal tajemství. Jelikož jsem zde však nemusel nic „crackovat“ a uživatel `database_user` měl práva na všechny databáze, mám podezření, že někdo přede mnou po sobě neuklidil a ulehčil mi cestu k tomuto tajemství, za což děkuji.

Tajemství W - 2

V adresáři `/prace` na domovském serveru se nachází klíč `idrsa.key`. K čemu patří nebylo známo, nicméně autor zprávy ve skrytém souboru `.new_message` ve stejné složce s jmenuje joe. Jelikož jméno začíná malým j, šlo předpokládat jméno uživatele. Postupně jsem se tímto klíčem snažil přihlásit k všem ostatním serverům jako uživatel joe až mě to pustilo na server 192.168.122.235. Tedy příkaz byl `ssh -i /prace/idrsa.key joe@192.168.122.235`. Uvítala mě zašifrovaná motd (message of the day), kterou jsem pomocí ASCII Shift dekodéru dokázal rozluštit a při posuvu +5 lze nalézt již druhé talemství w.

Tajemství X

Na výchozím serveru se nachází program `myprog/myprog`, který po spuštění vyžaduje heslo. Bylo mi jasné, že při správně zadaném hesle mi to možná odhali tajemství. Jelikož je to samostatná binárka, tak tedy heslo musela skrývat uvnitř. Stáhl jem si reverse engineering nástroj Ghidra a program dekompiloval. V kódu bylo vidět, jak se v if stromu znak po znaku porovnává vstup s řetězcem `2402a141d3`. Po zadání tohoto hesla mi program odhalil tajemství.