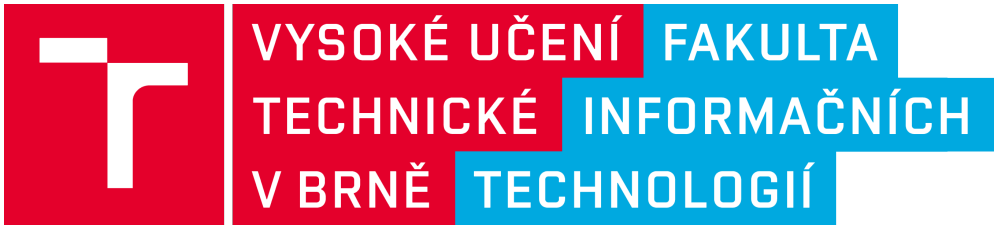

Bezpečnost informačních systémů

Projekt - The FITfather

Tereza Burianová (xburia28)

19. prosince 2022

Schéma vnitřní sítě

Pomocí příkazu *"ip addr"* a *"nmap"* jsem zjistila, že se tento server nachází na adrese 147.229.8.53 (maska 255.255.255.0) v síti s dalšími školními servery. Po připojení na server jsem analyzovala obsah ARP tabulky pomocí příkazu *"arp -a"* a našla jsem několik dalších souvisejících serverů. Na základě dalších indícií byly pro získání tajemství využity pouze dva z nich, zvýrazněny modrou barvou.

```
server2 (192.168.122.235) at 52:54:00:3a:fb:88 [ether] on enp1s0
? (192.168.122.3) at 52:54:00:53:08:85 [ether] on enp1s0
_gateway (192.168.122.1) at 52:54:00:41:27:d1 [ether] on enp1s0
? (192.168.122.150) at <incomplete> on enp1s0
? (192.168.122.148) at <incomplete> on enp1s0
? (192.168.122.149) at 52:54:00:2e:7a:f0 [ether] on enp1s0
? (192.168.122.90) at 52:54:00:41:02:a1 [ether] on enp1s0
```

Mezi některé ze zranitelností a slabin, nalezených při hledání tajemství, patří:

- použití již prolomeného šifrovacího algoritmu SHA1,
- odhalení správného hesla v textové podobě před jeho porovnáním s uživatelem zadaným heslem,
- uchovávání soukromých konverzací a odposlechů, obsahujících citlivé informace, v nezašifrované podobě,
- možnost jednoduše využít uživatele s vyššími právy pro přístup k PostgreSQL databázi,
- RSA klíče, IP adresy a uživatelská jména uloženy ve veřejných adresářích.

1. tajemství - myprog

Tajemstv_x_962cbf2a131fce89657e24802bbb12d917b47938d4cda5282962cbf2

Tajemství bylo získáno dekompilací binárního souboru *myprog*. Pro tyto účely jsem využila nástroj *ghidra*. Kód byl složen z několika zanořených smyček, které při vložení správného hesla vypsaly do terminálu dané tajemství. Analýzou těchto podmínek bylo možné správné heslo ve znění *"3d64c373a2"* získat.

2. tajemství - jsapp

Tajemstvi_1_6992b77cadea52add07dc8a2166356bdb9b2cf0373ba408571692db74e8b27b3

Ve zdrojovém kódu souboru *app.html* se v proměnné user nacházela hodnota zašifrovaná pomocí SHA1. Vzhledem k tomu, že tento šifrovací algoritmus byl již prolomen, jsem byla schopná pomocí veřejného slovníku (používaného webovou stránkou `https://md5decrypt.net/`) získat uživatelské jméno *"user11780"*. Po pečlivém prozkoumání JavaScript kódu sloužícího pro určení správnosti jména a hesla jsem zjistila, že ve funkci *function passw(_0x489f68)* se nachází nezašifrovaná podoba správného hesla sloužící pro porovnání s uživatelem zadaným heslem. Vypsáním funkcí vracené hodnoty přes *console.log()* jsem získala správné heslo *"f5f19e36a"*. Tato kombinace vypsala po zadání do webové stránky tajemství.

3. tajemství - secret_aplication

Tajemstvi_3_06fd2077848f01ac78fd98dd8d08f4199d677534059f181cd5d861

Ve složce *library* se nachází binární soubor *secret_aplication*, který ve své implementaci zřejmě využívá funkci *secret_function()*, deklarovanou v hlavičkovém souboru *foo.h*. Na základě souboru *odposlech* jsem zjistila, že by pro vrácení tajemství měla být splněna podmínka, že tato funkce vrací hodnotu *123*. Funkci jsem tedy implementovala tak, aby obsahovala pouze *"return 123;"* a přeložila následujícím příkazem pro její implementaci ve sdílené knihovně *libfoo.so*:

gcc -shared -o libfoo.so -fPIC foo.c

4. tajemství - korespondence

tajemstvi_h_7155a291dcf4c45918b26de2571b13a0dffde1109a576863cddbd7b45d95508a

Na serveru jsem našla složku s názvem *prace*, ve které se nacházela složka mail obsahující soubor *korespondence*. Po vyhledání klíčového slova "tajemství"jsem objevila jedno z tajemství schované na řádku 209 176.

5. tajemství - joe@fedora

tajemstvi_w_36f028580bb02cc8272a9a020f4200e346e276ae664e45ee80745574e2f5ab80

Ve složce práce se dále nacházel RSA klíč a soubor *.new_message*, který obsahuje správu, jejímž autorem je Joe. Pomocí příkazu *"arp -a"* jsem vypsala ARP tabulku a zkusila jsem se připojit na první ze serverů *server2 (192.168.122.235)* pomocí uživatelského jména *joe* a přiloženého RSA klíče. Po připojení na server jsem zjistila, že se jedná o server *joe@fedora*. Do terminálu byl vypsán MOTD s následujícím řetězcem:

$yfojrxy\{nd \mid d8; k57 =:= 5gg57hh = 7 < 7f > f575k9755j89; j7 <; fj; ; 9j9 : jj = 5 < 9 ::< 9j7k : fg = 5$

Všimla jsem si, že 1. a 7. písmeno je stejné, tedy y. Ve slově tajemství je 1. a 7. písmeno t. Při mapování slova tajemství na začátek tohoto řetězce jsem zjistila, že všechna písmena jsou v abecedě posunuta o 5. Vzhledem k tomu, že se v řetězci nachází i speciální znaky, vyvodila jsem, že posuny je třeba vykonávat v ASCII tabulce. Použila jsem tedy nástroj ASCII Shift Cipher (`https://www.dcode.fr/ascii-shift-cipher`), který při nastavení posunu na hodnotu 5 vrátil tajemství.

6. tajemství - PostgreSQL server

tajemstvi_w_8f29935c3ee89b9f32f5e91a8399043ffd6a40543c738a061012585dd911543e

V mé domovské složce se nachází složka *.ssh*, ve které je RSA klíč. V souboru *config* lze zjistit IP adresa serveru (*192.168.122.149*) a uživatelské jméno (*pepa*). Pomocí těchto informací se mi podařilo připojit na server *pepa@postgresqlserver*. Po připojení na server jsem zjistila, že uživatel *pepa* sice nemá potřebná práva, ale existuje také uživatel *database_user*. Pomocí příkazu *"su database_user"* se mi podařilo získat jeho práva. Ve složce tohoto uživatele jsem pak pomocí příkazu *"psql -U database_user"* spustila instanci PostgreSQL, přes $\backslash l$ jsem zobrazila dostupné databáze a ty jsem postupně prozkoumávala, zobrazovala seznam tabulek pomocí $\backslash dt$ a pak jejich obsah pomocí $\backslash d$. V databázi *postgres* se nachází tabulka *secret_table*, obsahující sloupec *secret*. Po zadání příkazu *"SELECT * FROM secret_table;"* jsem získala tajemství.