VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

PROJEKT – BIS
PROJECT – BIS

AUTOR PRÁCE **Bc. JAKUB SVOBODA – XSVOBO0Z**
AUTHOR

BRNO 2020/2001

Kapitola 1

The FITfather

1.1 Zmapování sítě

Po připojení na server *bis* provedu zmapování sítě pomocí příkazu `nmap -sP 192.168.122.48/24` nalezneme následující servery:

- Nmap scan report for 192.168.122.1
- Nmap scan report for s2 (192.168.122.5)
- Nmap scan report for s5 (192.168.122.36)
- Nmap scan report for xsvobo0z (192.168.122.48)
- Nmap scan report for s3 (192.168.122.55)
- Nmap scan report for s4 (192.168.122.211)
- Nmap scan report for s1 (192.168.122.234)

Dále pro každý z nalezených serverů provedeme podrobnější scan s přepínači `-sT`:

192.168.122.1
22/tcp open ssh
53/tcp open domain
5877/tcp filtered unknown
7019/tcp filtered doceri-ctl
9090/tcp filtered zeus-admin

s1 (192.168.122.234)
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
888/tcp open accessbuilder

s2 (192.168.122.5)
22/tcp open ssh

s3 (192.168.122.55)
22/tcp open ssh

s4 (192.168.122.211)
22/tcp open ssh
80/tcp open http
3306/tcp open mysql

s5 (192.168.122.36)
21/tcp open ftp
22/tcp open ssh
111/tcp open rpcbind

V domovském adresáři se nachází složka `.ssh`, po prohledání nacházím konfigurační soubor `.ssh/config`:

Host s1
Hostname 192.168.122.234
User server1

Host s2
Hostname 192.168.122.5
User server2

1.2 Tajemství A:

Připojuji se na s1 pomocí `ssh server1@192.168.122.234`. Zde se nachází skrytá složka `.secret`, ve které se nachází dva soubory: `cipher` a spustitelný soubor na generování tajemství z rozluštěné šifry. Soubor se šifrou obsahuje text:
BUMLNRSLESAEEINLBCLMTEAUHEAIPRRIOUUA

Tuto šifru rozluštím pomocí nástroje na luštění railfence šifer[1], vyšlý plaintext je:
BELARUSBURMACHILELEONEMAURITIUSNEPAL

Spustím tedy:
`./generate_secret_from_decrypted_cipher` "BELARUSBURMACHILELEONEMAURITIUSNEPAL"

Získávám tajemstvi A:
a_19-11-22-46-22_b1676e828ce2566ef0478483fc93e466209a89e083bc4e4680357b369075aa7e

1.3 Tajemství B:

Na s1 je opevřený port 80 se službou http. Protuneluji se přes ssh příkazem:
`ssh -D localhost:9999 student@bis.fit.vutbr.cz -p 65048 -i . id_ecdsa`

a přes firefox otevírám s1. Jedná se u webovou aplikaci, která spustí na s1 utilitu `host`. Aplikace je zřejmě naprogramována tak, že pouze vezme předaný řetězec, přiřadí je za řetězec "host " a spustí. Zadávám tedy:

[1] https://www.simonsingh.net/The_Black_Chamber/railfencecipher.html

" localhost & ls"

Z výstupu zjišťuji, že se zde nachází soubor secret.txt. Vytáhnu si jej pomocí `curl s1/secret.txt` a získávám tajemství B:
b_03-11-00-00-01_9dd89c68ee13703763a1c9ef48e660533ca749f5d622599d678aa9780e0bbd83

1.4 Tajemství C:

Připojuji se na s2 pomocí `ssh s2` a pomocí `find` hledám podezdřelé soubory. Po několik pokusech zkouším hledat:
`find / -regex ".*mail.*"2> /dev/null`

Všímám si, že se na severu vyskytuje pošta uživatele *joe* s cestou `/var/spool/mail/joe`. Nemám přístupová práva, ale zkouším:
`su - joe`

a úspěšně se připojuji. Nyní již mohu soubor číst a pomocí utility `grep` nacházím tajemství C:
c_29-10-14-00-01_ab1ab7f34c899c9a2eeaf2dc746f74ba363d5a845f2d0f6fc435d69c26426771

1.5 Tajemství D:

Na serveru s2 se v domovském adresáři nachází aplikace `.secret_app`. Spuštění mi npomáhá, ale další soubor – `.secret_app.swn` napovídá. Otevírám aplikaci v editoru vi a hledám řetězec s tajemstvím. Nacházím tajemství D:
d_03-11-00-00-01_5181feaaf9bc2cd1e41cc1e1edc834a8e38b93952bf7e5500df63e22fe7c18d5

1.6 Tajemství E:

Na server s2 je ve složce .ssh konfigurační soubor, odkud se dozvídám o uživateli joe ze server s3. Dále z SQL databáze ze serveru s4 (viz tajemství H – 1.9) víme o heslech uživatelů. Zkouším jedno po druhém, heslo *password1* nakonec vede k úspěšnému přihlášení. V domovském adresáři se pak nachází soubor *secret.txt* s tajemstvím E:
e_29-11-16-00-02_d925a69aac1615b754db0c2b58ee0bb6c6510fe88cb102278a479b5d255429cd

1.7 Tajemství F:

Na serveru s3 se v kořenovém adresáři nachází podezdřelá složka */database_backup*. V ní je soubor *2020_dump*, který byl vytvořený pomocí GDBM. Z něj je možné databázi obnovit příkazem
`gdbm_load /database_backup/2020_dump`

Tímto se obnoví databázový soubor *secret_db.gdbm*. Po vypsání jeho obsahu získávám tajemství F:
f_30-11-14-00-02_c9e54f1959d0e4f4aad812491f735c61cc89bee6c3b9495ab9e5f5703a148b36

1.8 Tajemství G:

Ze souboru *.ssh/config* ze serveru s2 známe username na server s4 a jsme schopni se na něj připojit. V domovském adresáři uživatele *server* se nachází složka s knihovnou *libgd*. Po přesunutí do tohoto adresáře pomocí příkazu *git log* vypisuji minulé commity, podezdřelá je zpráva posledního commitu:
commit 9d97783225a933883d5dca818e62e98f12b9aa4b (HEAD -> master)
Super secret commit message

Odtud vypisuji přesnější změny pomocí příkazu *git log -p*, ve výpisu se nachází tajemství G:
g_30-11-14-00-02_d925a69aac1615b754db0c2b58ee0bb6c6510fe88cb102278a479b5d255429cd

1.9 Tajemství H:

Na serveru s4 je oteřený port 80 s http a 3306 s mysql. Toto vybízí k útoku SQL injection. Připojuji se na stránku přes firefox a zjišťuji, že se jedná o o webovou aplikaci, která vypíše informace o zaměstnanci po zadání jeho jména a hesla. Vkládám do položky user `"or ""="` a do password také `"or ""="`. Dostávám seznam uživatelů, jejich hesel, telefoních čísel a adres:

Array ([name] => joe [password] => password [phone] => 369875254 [city] => Brno [street] => Pekarska) Array ([name] => lojza [password] => namornik [phone] => 787589636 [city] => Praha [street] => Videnska) Array ([name] => test [password] => password1 [phone] => 78885254 [city] => Trebic [street] => Komenskeho...

Poslední položka je tajemství H:
h_06-11-20-00-01_5181feaaf9bc2cd1e41cc1e1edc834a8e38b93952bf7e5500df63e22fe7c18d5

1.10 Tajemství I:

Na serveru s5 běží služba FTP na portu 21, na který se dá příhlásit jako anonymní uživatel s přihlašovacím jménem *anonymous* a s prázdným heslem. Zde se nachází pouze soubor *nosecret.txt*, tajemství bude jinde. Vytahuji si banner pomocí:
`nmap -sV --script=banner 192.168.122.36`

Zjišťuji, že se jedná o *vsFTPd 2.3.4*. Tato verze má známou bezpečnostní chybu. Připojuji se s uživatelským jménem *user:)* a s prázdným heslem. Vyskočí hláška *220 Opened port 51970, take a look ;)*. Připojuji se tedy pomocí:
`ftp 192.168.122.36 51970`

Získávám tajemství I:
i_28-10-18-00-02_0ffc96af83639729a9b2767b80375d00c62b84bf8c6d44132d858b7c46112787

1.11 Tajemství J:

Na severu s1 se nachází v domovském adresáři soubory soubory *paswd*, *shadow* a *gshadow*. Můžeme je jak číst, tak do nich zapisovat. Odtud se dozvídáme o uživateli *bis_user*. Dále na

serveru běží NIS server, který se stará o sdílení hesel mezi servery. Ze souboru */var/yp/Makefile* se dozvídáme o tom, že se data berou přímo z těchto souborů v domovském adresáři. Vygeneruji tedy vlastní hash hesla pomocí utility `mkpasswd` a přepisuji jím údaj v souboru *shadow*. Nyní již stačí znovu inicializovat žluté stránky pomocí `/usr/lib64/yp/ypinit -m`.

Nyní se již zkouším připojit na s5 jako uživatel *bis_user* s vlastním heslem. Přihlášení je úspěšné, ve složce *.secret* se nachází soubor *secret.txt*, který obsahuje tajemství J:
j_08-12-12-00-02_e32d33ff0d5b43daf1e2d0edd6c72ae80501d4dd1602a1e6f7c923363cb5c434