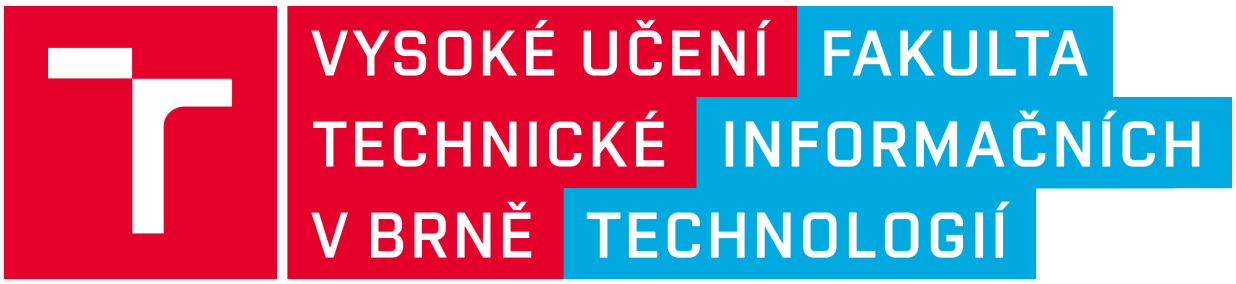
Fakulta informačních technologií
Vysoké učení technické v Brně



Bezpečnost informačních systémů

2019/2020

Tomáš Aubrecht (xaubre02)

23. listopadu 2019

1 Úvod

Projekt byl zadán formou příběhu vyprávějícím o nekalých činnostech probíhajících na fakultě, kde naším cílem bylo v dané síti nalézt všechna tajemství, která by zabránila těmto činnostem. K příběhu byla přiložena mapa Itálie, ve které bylo zakroužkované město Palermo, které představuje výchozí stanici dané sítě. Dále zde bylo zakřížkováno 10 měst, ze kterých lze odvodit, že cílem našeho snažení je získat 10 těchto tajemství. Síť, ve které jsme měli nalézt daná tajemství, se nachází na adrese *bis.fit.vutbr.cz*, která je dostupná pouze z vnitřní sítě VUT Brno. K zadání jsme dostali privátní klíč, pomocí kterého jsme získali přístup na výchozí stanici - Palermo.

2 Nalezená tajemství

Níže je uveden seznam jednotlivých tajemství a odpovídající kapitoly, které popisují jejich získání.

1. Tajemství A: A_17-11-14-54-01_5b047a3e23b4b19035e32afc5085fec2bd0cfda58e33555087c2e4e645ce
2. Tajemství B: B_21-11-19-54-01_2faf6e79720f73e9a0f573f323f2f7a472f75c81981fdbe7a95c6d76d5ef104c
3. Tajemství C: C_17-11-13-36-01_43a076c40b9fbdd74919e567af3d10a1e9e5d80f78e06a6009d49b6c7b2eba40
4. Tajemství D: D_17-11-15-55-01_ab51714cfa2b7ac650cd463f72d4e4feb5d6007ff0ab7ce49d411c4ac8bf6243
5. Tajemství E: E_17-11-15-14-01_06bf676bcd62fe064773218fab5473731ae99ff22672122222d0a0f838f1ba7d
6. Tajemství F: F_21-11-12-29-01_3c7f16ad9f880b1941e63ea3bea1b381b97230fd98aada7d58d53c029f2fde18
7. Tajemství G: G_17-11-14-07-01_6ab2d8a5a13420068e846f108065e8e5b019422711bf715fa4c302b68fb77e0e
8. Tajemství H: H_17-11-16-22-01_3373f46ffcf7c5832371e3614ed84b270e40b8207e6fde119f20d23c9fd80850
9. Tajemství I: I_21-11-14-48-01_dc6459c6b0efd621f9c4491fa9d7759794ecdf8b26c7b750d8de03d811181483
10. Tajemství J: J_20-11-22-03-01_9589c1e0c18e11c2f3a00f7e7a6e9896e08d87669fa78e4afc446218ca73f5d9

3 Analýza sítě

Po připojení na výchozí stanici jsem na ni nejprve hledal nějaká užitečná data. V domovském adresáři jsem nalezl soubor *known_hosts*, který obsahoval jeden záznam, ze kterého jsem se dozvěděl o serveru *192.168.122.220*. Poznamenal jsem si jej a pokračoval v hledání. Pomoci příkazu `ls / -laR` jsem se snažil najít další užitečná data, ale bohužel bez výsledku. Dalším krokem bylo zmapování sítě, ve které se daná stanice nachází. Pomocí příkazu `ip addr` jsem zjistil IP adresu své stanice a masku sítě, které jsem pak použil pro zmapování této sítě pomocí příkazu `nmap 192.168.122.193/24`. Výsledek tohoto příkazu obsahoval mnoho stanic, kde většina z nich byla přiřazena jiným studentům. Po odfiltrování těchto adres mi zůstaly následující stanice, na které se stojí podívat pod drobnohledem.

```
Nmap scan report for 192.168.122.1
Host is up (0.00019s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
```

```
111/tcp open rpcbind
2049/tcp open nfs
3306/tcp open mysql
MAC Address: 52:54:00:52:BE:C2 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.38
Host is up (0.00038s latency).
Not shown: 970 filtered ports, 27 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
MAC Address: 52:54:00:07:85:00 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.77
Host is up (0.00058s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
MAC Address: 52:54:00:D4:0D:75 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.83
Host is up (0.00073s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
MAC Address: 52:54:00:C2:A1:60 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.105
Host is up (0.00034s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
3306/tcp open mysql
MAC Address: 52:54:00:AD:2F:85 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.150
Host is up (0.00030s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
MAC Address: 52:54:00:71:10:A5 (QEMU Virtual NIC)
```

```
Nmap scan report for 192.168.122.155
Host is up (0.00031s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
MAC Address: 52:54:00:49:02:85 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.169
Host is up (0.00045s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
MAC Address: 52:54:00:5A:B6:76 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.206
Host is up (0.00035s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
MAC Address: 52:54:00:EC:02:F7 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.215
Host is up (0.00032s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
MAC Address: 52:54:00:49:52:E4 (QEMU Virtual NIC)

Stats: 0:00:16 elapsed; 246 hosts completed (73 up), 9 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.55 done; ETC: 16:38 (0:00:00 remaining)
Nmap scan report for 192.168.122.220
Host is up (0.0012s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
80/tcp open http
MAC Address: 52:54:00:27:58:18 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.227
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
```

```
111/tcp open rpcbind
MAC Address: 52:54:00:8E:17:1B (QEMU Virtual NIC)
```

Z otevřených portů na těchto stanicích jsem zjistil, že na některých z nich běží webový server. Vytvořil jsem si tedy SSH tunel a nakonfiguroval proxy v prohlížeči Firefox, aby se mi snadněji hledalo na těchto webech. Mezi vyfiltrovanými stanicemi se náchazel i server, o kterém jsem se dozvěděl ze souboru *known_ host* zmíněném výše. V následujících kapitolách je popsán postup, jakým jsem postupně odhalil veškerá tajemství.

4 Tajemství C

Můj prvotní postup obnášel prozkoumání webových serverů, kde jsem zjistil, že na serveru *192.168.122.169* mám přistup k jeho adresářové struktuře. Po bližším prozkoumání obsahu jsem v souboru */etc/raddb/sql.conf* nalezl své první tajemství.

5 Tajemství G

Z otevřených portů na serveru *192.168.122.38* jsem zjistil, že zde běží FTP server. Nevěděl jsem však ani uživatelské jméno, ani heslo, ale server vracel informaci o jeho verzi. Věděl jsem, ze některá starší verze FTP měla slabinu, proto jsem začal hledat informaci o tom, zdali to není právě tato verze. A také že byla. Slabina spočívala v tom, že uživatelské jméno pro přihlášení muselo obsahovat podřetězec `":)"`. Pak již stačilo zadat náhodné heslo a tímto jsem získal přístup a zároveň své druhé tajemství.

6 Tajemství A

Na webovém serveru *192.168.122.220* byl zobrazen výpis z databáze, který jsem mohl filtrovat podle určitých kritérií. První co mě napadlo byl útok *SQL–injection*. Po nastudování tohoto útoku jsem zjistil, že na daném serveru není možné použít zřetězení více dotazů, ale pouze jeden. Tím pádem jsem použil klíčové slovo UNION pro výpis dodatečných informací. Níže je uveden seznam použitých řetězců pro provedení útoku *SQL–injection*.

1. `"UNION SELECT table_name AS name, ""AS email, ""AS address, ""AS id FROM information_schema.tables WHERE table_name LIKE "`
2. `"UNION SELECT column_name AS name, ""AS email, ""AS address, ""as id FROM information_schema.columns WHERE table_name LIKE "auth`
3. `"UNION SELECT login AS name, passwd AS email, ""AS address, ""as id FROM auth WHERE login LIKE "`

První řetězec byl použit pro výpis všech tabulek v dané databázi, kde tabulka auth zaujala mou pozornost nejvíce. Druhým řetězcem jsem si tedy vypsal všechny její sloupce. Dozvěděl jsem se, že obsahuje sloupce *login* a *passwd*, jejichž obsah jsem si nechal vypsat pomocí třetího řetězce. Zde jsem nalezl tajemství A.

7 Tajemství E

Na webovém serveru na adrese *192.168.122.220* byl formulář pro přihlášení. Zkoušel jsem se přihlásit pomocí uživatelských účtů a hesel získaných z databáze v předchozí kapitole, avšak bez úspěchu. Potom jsem ale zjistil, že daná stránka využívá cookies, kde jednou z nich byla cookie *LOGGED_IN=False*. Změnil jsem tedy její hodnotu na *True*, obnovil jsem stránku a tím jsem získal další tajemství.

8 Tajemství D

Nyní jsem využil znalosti o možnosti SSH připojení na server *192.168.122.220*, o které jsem se dozvěděl ze souboru *known_hosts* na výchozí stanici. Po připojení mě server uvítal jako pana Smithe a požadoval heslo. Po 3 neúspěšných pokusech o přihlášení jsem byl odpojen, znovu jsem se tedy připojil na tento server, nyní však jako uživatel *smith* pomocí příkazu `ssh smith@192.168.122.220` a takhle jsem se dostal na danou stanici bez nutnosti zadávat heslo. Po prozkoumání domovského adresáře jsem nalezl script pro zachycení telnet komunikace a jeho výstup v podobě dvou soborů *agg* a *agg2*. Ty jsem si pomocí *scp* stáhl k sobě a otevřel je ve Wiresharku. Po bližším prozkoumání jsem nalezl uživatelské jméno *ada* a heslo *nachystejteuzenace*. To jsem použil pro připojení na tu stejnou stanici, o které jsem věděl, že obsahuje domovský adresář pro uživatele *ada*, kde se v tomto adresáři nacházel soubor obsahující tajemství D.

9 Tajemství H

Když jsem byl na serveru *192.168.122.220* přihlášený jako uživatel *ada*, rekurzivně jsem si vypsal obsah všech adresářů na dané stanici, ke kterým jsem měl přístup. Výsledků bylo mnoho, proto bylo potřeba jej vyfiltrovat. Použil jsem tedy příkaz `ls / -laR | grep secret`, který mi značně zúžil výběr. Následně jsem kontroloval jednotlivé výsledky, až jsem narazil na spustitelný soubor *show_secret*. Ten jsem tedy spustil a získal tak další tajemství.

10 Tajemství J

Na serveru *192.168.122.77* byl otevřen port pro SSH, zkoušel jsem se tedy na tento server připojit. Vyzkoušel jsem všechna uživatelská jména a hesla, se kterými jsem doposud přišel do styku, avšak ani jedno nebylo to spravné. Po nějaké době zkoušení jsem se úspěšně připojil jako uživatel *root* s heslem *root* a v domovském adresáři byl soubor obsahující další tajemství.

11 Tajemství F

Obdobně jako u předchozího tajemství i na serveru *192.168.122.227* byl otevřen port pro SSH. Po připojení mě server upozornil, že se mám přihlásit jako *teacher*. Neváhal jsem a hned jsem se zkusil připojit s tímto loginem. Vyžadovalo to heslo a první co mě napadlo bylo, jestli to není opět stejné jako login. A také že bylo. Po získání přístupu jsem zde však nic zajímavého nenalezl. Jediné co by se dalo využít byla služba *dig*, která zde byla nainstalovaná. Tu jsem však k ničemu nepoužil. Důležitou informací při připojení bylo, že je zde zakázaný root login, takže jsem začal hledat možnosti, jak jinak získat root práva. Po nějaké době hledání jsem narazil na sudo zranitelnost. Vyzkoušel jsem ji pomocí příkazu `sudo -u#-1` a také že jsem získal root práva. Nyní už stačilo opět pomocí příkazu `ls / -laR | grep secret` nalézt tajemství, které bylo v souboru */root/secret.txt*.

12 Tajemství I

Při prvotní návštěvě webového serveru na adrese *192.168.122.105* jsem nic nezjistil. Server mě pouze informoval o přesměrování na */www*, které však vedlo na chybu. A právě tato chyba byla klíčová. Jedná se totiž o způsob výpisu chyby(Tracy), jaký používá framework *Nette*, jehož adresářová struktura obsahuje také složku */app* pro backend aplikace. A právě zde jsem nalezl tajemství I.

13 Tajemství B

Při hledání posledního tajemství jsem již nevěděl, kde hledat nebo co vyzkoušet. Znovu jsem si chtěl zmapovat danou síť, ale zjistil jsem, že příkaz *nmap* nezobrazuje všechny porty bez explicitního uvedení. Proto jsem si nyní zmapoval danou síť podruhé s přepínačem *-p-* a objevil jsem otevřený port *42424* na adrese *192.168.122.169*. Po vyzkoušení různých služeb jsem zjistil, že na daném portu běží FTP. Pro přihlášení jsem začal opět se všemi známými uživatelskými jmény a hesly, ale opět bez úspěchu. Připojit se dalo jako anonymní uživatel, tedy s loginem *anonymous* a libovolným heslem. Po vypsání obsahu serveru jsem nalezl soubor *secret.txt*, jehož obsah obsahoval poslední tajemství, tajemství B.