VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÝCH TECHNOLÓGIÍ
FACULTY OF INFORMATION TECHNOLOGY

THE FITFATHER
PROJEKT DO PREDMETU BIS

AUTOR PRÁCE — **MAROŠ ORSÁK**
AUTHOR

BRNO 2020

Obsah

Kapitola 1

Hľadanie tajomstiev

1.1 Príprava na dobrodružstvo

Začiatok mojho dobrodružstva začalo pri prihlasení sa na server *bis.vutbr.cz* pomocou klúča *id_ecdsa*. Prvým problém bolo však, že klúč pomocou ktorého som sa chcel prihlásiť obsahoval windows znaky a bolo nutné ho prekonvertovať na linux/mac podobu. Nato som použil tool doc2unix čo mi daný problém vyriešilo. Dobrodružstvo, teda mohlo začať a tým som sa prvykrát úspešne prihlásil na spomenutý server.

1.2 Neúspechy za podkladmi

Po prihlasení na server som si hovoril kde by som mohol nájsť informácie, ktoré by mi pomohli niečo nájsť. Prvé čo som skúsil bolo vylistovanie všetkých procesov pomocou príkazu *ps aux* to mi však ne-napovedalo nič. Následne som skúsil aplikovať príkaz *find secret* kde bohužiaľ som nemal taktiež úspech. Prvý záblesk, ktorý sa javil ako prvé tajomstvo, ktoré som našiel pomocou príkazu *find* bol súbor */etc/shadow*. Čo sa znovu smárnilo moje činy boli práva, ktoré mi nedovolili daný súbor prečítať. V tomto bode to bolo pre mňa dosť ťažké ale potom ma napadla zaujimavá myšlienka, kde som pomocou nástroja *nmap* vedel zistiť aké služby bežia na daných súboroch.

1.3 Svitanie na dobré časy

Moja hlavná procedúra ako som už zmienil na začiatku bola pre-scanovať celú sieť. K tomu mi pomohol príkaz *ip a*, kde som si pomocou neho získal korešpodujúcu adresu a začal skanovať celú sieť *192.168.122.1-255*. Výsledkom bolo prehľad všetkých serverov so spolu bežiacimi službami, kde už som vlastne mohol čerpať z tohoto a tým pádom som bol veľmi spokojný, že sa takto moja cesta vyvíja.

```
Nmap scan report for 192.168.122.1
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
```

```
Nmap scan report for s2 (192.168.122.5)
Host is up (0.0019s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for s5 (192.168.122.36)
Host is up (0.0021s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap scan report for s3 (192.168.122.55)
Host is up (0.0021s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for xorsak02 (192.168.122.72)
Host is up (0.0023s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for s1 (192.168.122.234)
Host is up (0.00095s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
888/tcp open  accessbuilder
```

Následne som však potreboval podrobnejšie informácie a skúsil som skanovať všetky porty na daných serveroch:

```
# S1 server
nmap -p- 192.168.122.234
Not shown: 65530 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
887/tcp open  iclcnet_svinfo
888/tcp open  accessbuilder

# S2 server
```

```
nmap -p- 192.168.122.5
Not shown: 65534 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

# S3 server
nmap -p- 192.168.122.55
Not shown: 65534 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

# S4 server
nmap -p- 192.168.122.211
Not shown: 65532 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

# S5 server
nmap -p- 192.168.122.36
Not shown: 65531 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
111/tcp open  rpcbind
613/tcp open  hmmp-op
```

1.4 Úsvit

1.5 Prvý úspech (Tajomstvo I)

Týmto bola moja cesta zahájená a ja som si ako prvý server vybral *s5* na adrese *192.168.122.36* kde som videl, že tam je aktívna služba ftp a tak som sa skúsil pripojiť cez telnet na špecifický port s príkazom *telnet 192.168.122.36 21*. Hneď nato som bol vyzvaný ku zadaniu ku zadaniu uživateľského mena ktorým suffixom bol *:)*. Potom sa mi zobrazil otvorený port na ktorý som sa ihneď prihlásil cez telnet session *telnet 192.168.122.36 52650* a tým získal moje prvé tajomstvo I! Úžasný pocit :)

```
Tajemstvi:i_24-11-10-00-02_f3c2dee1c50266691181220c30
7031620092516273b475e3beb9057d756736a6
```

Následne som rozmýšlal nad ďaľšou variantou a snažim som sa cez suffix tajomstva dekódovať cez dekóder base64 (*echo "f3c2dee1c50266691181220c307031620092516273b475 e3beb9057d756736a6 base64 -d)* čo mi však nič dobrého ne-prinieslo.

1.6 Druhý úspech (Tajomstvo A)

Potom som si však uvedomil, že by som mohol pozrieť zložku .ssh na mojom login uzle a teda bola to doslova zlatá baňa. Pomocou *cat .ssh/config* som si vylistoval všetky konfigurácie pomocou ktorých sa budem moct dostať na špecifické servery. V tomto prípade to boli *s1* a *s2*. Zvolil som teda s1 a následne som prehľadal celý filesystem pomocou príkazu *find — grep secret*. Výsledok tejto operácie bol veľmi príjemný a doležitý výstup vypadal takto:

```
/home/server1/.secret
/home/server1/.secret/cipher
/home/server1/.secret/generate_secret_from_decrypted_cipher
```

Prešiel som teda do súboru */home/server1/.secret* a tam spustil script *.generate_secret_from_decrypted_cipher*, ktorý mi dodal ďalšie tajomstvo. Radoval som sa veľmi skoro keď som si to potom znovu kontroloval prišiel som na to, že je nutné *cipher* rozšifrovať. Musím povedať, že som sa nechal nachytať, že by to bolo až tak jednoduché. Čo bolo zároveň takžé bolo aký klúč použiť na rozšifrovanie. Uvedomil som si, že kedysi som používal automatické nástroj, ktoré robia analýzu a skúšajú rozne klúče na daný reťazec. Urobil som teda to že som zadal do google code breaking cipher tools, kde na mňa vyskočila stránka *https://www.boxentriq.com/*. Vybral som si Columnar Transposition Cipher Tool kde som dodal retazec ktorý bol v cipher súbore. Výsledkom bol text *slovakialithuanianorwayirelandpolandfinland* s klúčom *abcde*. Následne som tento text použil ako parameter skriptu a výsledok nadmerne uspokojúci!!!

```
Tajemstvi: a_24-11-14-47-58_cd8ec165169defab8531a0e51663c39d3901341b787e9b05bb3f5e33d87
```

1.7 Tretí úspech (Tajomstvo D)

Spočiatku sa veľmi nedarilo a rozmýšla som, že napíšem jednu sekciu o neúspechoch. Napokon som sa rozhodol, že tu predsa budem písať tie najpodstanejšie výztržky. Potom ako som nemohol nájsť žiadne ďalšie tajomstvo na server *s1* presunul som sa na *s2*, kde ma čakala binárka *secret_app*. Začal som rozmýšlať čo s ňou možem urobiť a teda som ju spúštaľ a snažil sa dávať rozne vstupy. Zároveň som skúsil rozne parametre, ktoré by mohli nejako uškodiť. Následne som si povedal, čo ak vložím rovnaký reťazec čím ma privítala aplikácia. Nič však pre mňa nebolo pozitívne. Nakopon som si uvedomil, že by som mohol začal analyzovať ten binárny kód. Zadal som teda do google ako analyzovať binárny kód a zároveň som si vyhľadal najznámejšie nástroje. Ponúkali sa napríklad hexdump, strings a podobne. Skúsil som teda nástroj hexdump kde som pomocou príkazu *'hexdump -C secret_app — grep Tajem'* získal:

```
00002010  00 00 00 00 00 00 00 00  54 61 6a
65 6d 73 74 76  |........Tajemstv|}
```

Týmto som jedine zistil, že dané tajomstvo je uložené v binárke. Nebolo to však postačujúce. Mal som 2 nápady buď urobiť nejaký parser a vytvoriť postupnosť znakov z *........Tajemstv* a urobiť konkatenáciu a následne grep alebo by som použil ďalší nájstroj. Rozhodol som sa pre druhú alternatívu a to preto už spomínaný nástroj *strings*. Podľa návodu som zistil, že daný nástroj podporuje vyhľadávanie reťazcov ktoré majú vačší počet znakov ako mi zadáme. Toto bolo pre mňa veľmi super zistenie a preto som použil *strings -n 50 secret_app* tak som našiel dané Tajomstvo D. Znova Hurá!!

```
Tajemstvi:d_24-11-12-00-02_e79cb5dbfa0e0fc21ba0ab7768c5fd14f752acfc9cdb520f2c9685322a1f
```

1.8 Štvrtí úspech (Tajomstvo B)

Po pár neúspechoch som si znovu povedal, že skúsim server číslo 1 a kedže pomocou nmap nástroja bolo jasne vidieť, že tam beží služba http určite to bude mať niečo spoločné s prevolávaním REST API. Začal som teda GET metódou čo mi vrátilo stránku a ja som tým zistil, že to prakticky vykonáva DNS prekladové operácie.

```
<html>
<body>
<h1>
Check host IP
</h1>
<h2>
Simple web app, executing host utility
</h2>
<form action="" method="post">
<label> Host: </label>
<input type="text" id="url" name="url"/>
<input type="submit"/>
</form>
```

Podľa vrátenej kostry som zistil, že to po mne chce ako parameter do metodý POST url. Čo bolo avšak zaujimavé skúsil som sa pozrieť do zložky */var/www/html*, kde by teoreticky mal apache zložku. Avšak nemal som dostatočné práva sa tam dostať. V tom momente som dostal geniálnu myšlieku a takú, že čo ak podhodím hocijakú url cez parameter ale zároveň presmerujem výstup a dám na vstup vylistovanie daného adresára, kde sa apache nachádza. Skúsil som to pomocou príkazu *curl –data 'url= something |ls -all |cat secret.txt' localhost* a výsledkom bolo ďalšie tajomstvo do mojej zbierky!

```
Tajemstvi:b_24-11-18-00-01_08b08b84a43e6caee57a463111df091a6aa78dde5162149490cd5c6e921c
```

1.9 Piaty úspech (Tajomstvo H)

Keďže som mal na konte 2 tajomstvá zo serveru s1 a 1 zo s2 a 1 zo s5, povedal som si, že dobrým adeptom budem server číslo 4. Kedže na tomto severy bežia http a mySQL služby bolo nutné sa koncentrovať na práve tieto. Mojou prvotnou intuíciou bolo vytvoriť nejako SQL Injection. Ako som tak pozoroval daný sever tak som skúsil jednoducho prevolať REST API s GET metódou ako som to urobil v predošlom serveru. Príkaz, pomocou ktorého som zistil danú view *curl localhost* aplikácie:

```
<html>
<body>
<h1>
Check user information
</h1>
<h2>
```

```
Simple web app, showing user information
</h2>
<form action="" method="post">
<label> Username: </label>
        <input type="text" id="name" name="name"/>
<label> Password: </label>
        <input type="text" id="password" name="password"/>
        <input type="submit"/>
</form>
 </body>
</html>
```

Skúšal rôznu formu, že som posielal parametrov vkladal selekty. Nič nepomáhalo. Zároveň som si vylistoval pomocou *find |username* zložku so všetkými uživateľskými menami. Obdobne aj s heslami kde však som zistil, že mi moc nepomohli a nejde to.

```
cat /usr/share/nmap/nselib/data/passwords.lst
cat /usr/share/nmap/nselib/data/usernames.lst
```

Nakoniec som dostal nápad, že by som mohol použiť už nejaký SQL injection tool, ktorý funguje a pustiť to oproti tomu formuláru, ktorý má ako parametre *username* a *password*. A teda som si vy-googlil 'sql injection tool' a hneď prvé vyhľadávanie bol nástroj zvaný *sqlmap*. Neváhal som a hneď som si o ňom niečo naštudoval. O chvíľu neskor som si repozitár sqlmap nástroja naklonoval na s4 kde som následne pustil ich hlavný script s parametrom *–wizard*. Potom som už len vyklikal potrebné časti ako napríklad silu útoku a podobne kde som zvolil ten najsilnejší. Po pár minutách bol výsledok veľmi uspokojivý. Na konci logu som dostal tabuľku user v ktorej som mohol vidieť tajomstvo H a znovu sa mohol o čo viac radovať!

```
Database: web
Table: user
[4 entries]
+---------+--------+-----------+------------+--------------------------+
| city    | name   | phone     | street     | password                 |
+---------+--------+-----------+------------+--------------------------+
| Brno    | joe    | 369875254 | Pekarska   | password                 |
| Praha   | lojza  | 787589636 | Videnska   | namornik                 |
| Trebic  | test   | 78885254  | Komenskeho | password1                |
| <blank> | SECRET | <blank>   | <blank>    | Tajemstvi:h_24-.......   |
+---------+--------+-----------+------------+--------------------------+

Tajemstvi:h_24-11-20-00-01_5181feaaf9bc2cd1e41cc1e1edc834a8e38b93952bf7e5500df63e22fe7c
```

1.10 Šiesty úspech (Tajomstvo C)

Ďalším a pre mňa štastným bolo tajomstvo na servery s2. Opať som sa pozrel do zložky .ssh/config, ktorú som si vylistoval a bol tam joe. Skúsil som vyhladať meno joe v celom filesystéme a tam mi vyskočilo veľa najdených častí včetne */var/spool/....* Skúšal som sa dostať do súboru */var/spool/mail/joe* avšak beznádejne. Nemal som práva. Rozmýšlal som

či by som náhodou nemohol sa pripojiť na nejakú službu pop3 alebo imap kde by som si dané maily mohol prečítať. Žial, podľa reportu, ktorý som získal analýzou a skanovaním daného serveru to nebolo možné. Nakoniec som si ale však uvedomil. Čo ak uživateľ menom joe dané práva má a ja nie. Hneď som vy-googlil ako si prepnúť uživateľa na linuxe a pomocou príkazu *su joe* som bol prihlasený pod uživateľom joe. Teraz iba stačilo prejsť do súboru */var/spool/mail/joe* a pomocou less alebo more commandu si vyhladať reťazec, ktorý začínal na 'Tajemstvi'. Presne takto aj bolo a ja som našiel ďalšie tajomstvo do mojej bohatej zbierky!!

```
Tajemstvi:c_24-11-22-00-01_ab644a10f6764172815fcbdae754007baf11c383aeda3eb2cd9feeabf372
```

1.11 Úpadok

Po dlhom skúšaní roznych expeerimentov som bol na pokraji zrútnia. Jedinú dobrú informáciu ktorú som mal bola, že na s3 sa dostanem jedine nejakým bruteforce útokom. Vyhladal som si teda nástroje pre bruteforce attack a jeden z nich bol metasploit, ktorý sme však mali zakázaný. Na druhú stranu tam bola aj alternatíva, ktorú som použil. Jednalo sas o hydru, ktorú som si stiahol pridal si tam list uživateľov a list hesiel, ktoré som našiel v *cat /usr/share/nmap/nselib/data/passwords.lst*. Keď som chcel ale pustiť hydru nedarilo sa. Boli tam určité závislosti, ktoré som ale nemohol stiahnuť kvoli tomu, že tam nebol balíčkový manazer apt-get :(. Poslednou alternatívou, bol nástroj 'Nmap Scripting Engine'. Pustil som teda daný nmap s pridaným parametrom aby sa jednalo o bruteforce útok nad všetkými heslami a všetkými uživatľmi, ktorými som našiel *cat /usr/share/nmap/nselib/data/usernames.lst*. Toto však bola rana do srdca keď som videl, že ani tento nástroj to nevie vyriešiť.

```
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 15m00s exceeded.
Nmap scan report for s3 (192.168.122.55)
Host is up (0.00089s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 2434 guesses in 901 seconds, average tps: 2.8

Nmap done: 1 IP address (1 host up) scanned in 900.97 seconds
```

1.12 Siedmy úspech (Tajomstvo E)

Po výdatnom spánku som sa opať pustil do roboty a hneď ma osvietilo. Predsa na jedným z tých serveroch som sa prihlasoval na server s3 pod uživateľom joe. Hneď akonáhle som si uvedomil túto informáciu tak som pustil moj nmap s scriptom *nmap s3 -p 22 –script ssh-brute –script-args userdb=users.txt,passdb=passwords.txt*, kde som pozmenil súbor users.txt a dal tam iba uživateľa joe. Hneď potom som to pustil a po necelých 12 sekundách som mal výsledok. Skvelý pocit!!!

```
Nmap scan report for s3 (192.168.122.55)
Host is up (0.00076s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     joe:password1 - Valid credentials
|_  Statistics: Performed 28 guesses in 11 seconds, average tps: 2.5

Nmap done: 1 IP address (1 host up) scanned in 11.74 seconds
```

Prihlásil som sa teda pod uživatľom joe na s3 server, kde som našiel súbor secrets.txt a tam bolo uložené tajomstvo E. Zaslúžené!

```
Tajemstvi:e_25-11-08-00-02_e3a0d1a9f1cb3f7f3e1756d58809d1701c2a41d672b6c718f9040affd4a9
```

1.13 Ôsmy úspech (Tajomstvo F)

Dalším úlovkom do mojej zbierky bolo tajomstvo F. Akonáhle som sa poobezeral po servery s3 videl som súbor *.viminfo*, v ktorom boli informácie ohľadom nejaké secretu.

```
# File marks:
'0  1  0  ~/secret_db.gdbm
|4,48,1,0,1606332790,"~/secret_db.gdbm"
'1  95  0  ~/.viminfo
|4,49,95,0,1606332785,"~/.viminfo"
'2  1  0  /usr/share/cracklib/cracklib.magic
|4,50,1,0,1606301634,"/usr/share/cracklib/cracklib.magic"
'3  1  0  /usr/share/cracklib/cracklib-small.hwm
|4,51,1,0,1606301611,"/usr/share/cracklib/cracklib-small.hwm"
'4  1  0  /usr/share/cracklib/pw_dict.pwi
|4,52,1,0,1606301598,"/usr/share/cracklib/pw_dict.pwi"
'5  930  0  /usr/share/cracklib/pw_dict.pwd
|4,53,930,0,1606301575,"/usr/share/cracklib/pw_dict.pwd"
'6  1  0  /usr/share/cracklib/pw_dict.hwm
|4,54,1,0,1606301462,"/usr/share/cracklib/pw_dict.hwm"
'7  562  0  /usr/share/cracklib/cracklib-small.pwd
|4,55,562,0,1606301440,"/usr/share/cracklib/cracklib-small.pwd"
'8  1  12961  ~/secret_db.gdbm
|4,56,1,12961,1606295987,"~/secret_db.gdbm"
'9  1  0  ~/secret
|4,57,1,0,1606295974,"~/secret"
```

Hľadal som teda po celom servery. Začal som od roota a hneď v ten moment som tam videl zložku *database_backup* v ktorej sa nachádzal súbor *2020_dump*. Prezrel som čo obsahuje a veľmi mi prišiel povedomý reťazec:

```
VGFqZW1zdHZpOmZfMjUtMTEtMjAtMTEtMTRfNzkzZmQyMjdmY2RjMjExMDI0YjVhZjJiYmRhNWIy
ZmQ5OTJjZjMyYTYxZTIwYTVhYjFjMjUwNjJmOWFkMDAwZg==
```

Vďaka mojej práci, kde používame Kubernetes technológiu som si hneď uvedomil, že toto možno bude enkódovaný řetazec v formáte base64. Skúsil som teda príkaz na dekódovanie, ktorý mi následne ukázal Tajomstvo F!!!.

```
echo "VGFqZW1zdHZpOmZfMjUtMTEtMjAtMTEtMTRfNzkzZmQyMjdmY2RjMjExMDI0YjVhZjJiYmRhNWIy
ZmQ5OTJjZjMyYTYxZTIwYTVhYjFjMjUwNjJmOWFkMDAwZg==" | base64 --decode

Tajemstvi:f_25-11-20-11-14_793fd227fcdc211024b5af2bbda5b2fd992cf32a61e20a5ab1c25062f9ad
```

1.14 Deviaty úspech (Tajomstvo G)

Čo sa týka tajomstva G, tak pri tomto musím povedať veľké šťastie. V mojej práci už som vždy naučený na každé repo dávať *git status* úplne implicitne. Tento príkaz mi dal neskutočnú informáciu a to že daný repozitár bol pozmenený. Hneď na to som vykonal príkaz *git log*, kde som zistil, že niekto lokálne commitol zmeny:

```
commit 5be2ed93ff6d01f514baed9b4f9d6f2d5415f503 (HEAD -> master)
Author: root <you@example.com>
Date:   Wed Nov 25 20:10:11 2020 +0100
Super secret commit message
...
```

Najskor som si myslel, že sa jedná o nejakú šifru v rámci commit hash *5be2ed93ff6d01f514baed9b4f9d6f2* a skúšal som to nejakými sposobmi dekódovať ale ničím to nešlo. Potom som si ale spomenul na moj menej používaný príkaz. Ale vďaka prvému projektu z AVS som použil *git diff*, ktorý mi ukázal všetky zmeny. Zo začiatku som nič nevidel ale napokon som ho našiel. Tajomstvo G!!! Hurá!

```
set(CPACK_RESOURCE_FILE_LICENSE "${CMAKE_SOURCE_DIR}/COPYING")
-
-set(CPACK_SOURCE_GENERATOR TGZ)
-set(CPACK_SOURCE_IGNORE_FILES
-"~$"
-"\\\\.swp$"
-"\\\\.gitignore$"
-"^${PROJECT_SOURCE_DIR}/debian/"
-"^${PROJECT_SOURCE_DIR}/old/"
-"^${PROJECT_SOURCE_DIR}/bld/"
-)
-install(FILES ${top_level_DOCFILES} DESTINATION ${DOC_DIR})
-INCLUDE(CPack)
-Tajemstvi:g_25-11-20-11-14_3969abb3b1af8d787134d5c574732ebae5182954a1ef7b76a5600bccb0b

Tajemstvi:g_25-11-20-11-14_3969abb3b1af8d787134d5c574732ebae5182954a1ef7b76a5600bccb0bc
```

1.15 Desiaty vydretý úspech (Tajomstvo J)

Ako hovorí pán prof. Vojnár: "Letem svetem...". Presne tak som sa cítil pri hladaní posledného tajomstva. Strávil som priňom najvac času a z ničím som nemohol prísť. Skúšal

som bruteforce taktiku na server s5, všelijaké exploity no nič nezaberalo. Nevedel som čo by mohlo byť klúčom ku získaniu tajomstva. Po 3 nájdených som znovu myslel, že príde ďaľšia dlhšia kríza. Potom prišla slabšia svetlejšia chvíľka, kde som si uvedomil, že na s5 je služba rpc bežiaca na porte 111. Naštudoval som si toho veľa a následne som zistil, kde sa možu nachádzať konfiguračné súbory. Spomenul som si, že napríklad na servery s1 boli v domovskej zložke súbory ako *passwd* a *shadow*. Dočítal sosm sa ďalej, že konfiguračné súbory sa väčšinou nachádzajú v */var/yp*, kde som uvidel súbory ako *passwd.byname* a podobne. Naśledne som vykonal príkaz *ypservers*, čo mi dalo na výstup *bis-server*. Hneď nato som si povedal, že skúsim sa prihlásiť na s5 ako uživateľ *bis-server*. Bohužial bez úspechu. Zároveň som si všimol *Makefile* súbor, ktorom boli premenné ako *PASSWD* alebo *SHADOW*, ktoré ukazovali na domovské súbory passwd a shadow. Potom som intuitivne skúsil zbuildiť *Makefile*. Vygenerovalo to nejaké pre mňa neznáme súbory. Potom som v dokumentácií dočítal pár častí o súboroch. Pozeral som sa na */etc/rc.conf*, */var/yp/securenets* a mnoho dalších ale nič nepomáhalo. Skúšal sosm hladať viacero častí po internete no bez žiadného úspechu. Už som nemal silu a celú noc som rozmýšlal čo budem mocť použiť. Toto tajomstvo bolo úprimne najväčšou hádankou zo všetkých. Nechcel som tu písať všetko čo som skúšal, pretože by táto dokumentácia nadobudla obrovské rozmery. Nakoniec po asi 6 hodínách, kde už som prezrel všetky manuály a pozrel videá som skúsil jednu zaujimavú vec. Všimol som si, že v súbore *shadow* je u *bis_user* je nejaký hash. Tento hash som poznal podľa toho, že sa v práci stretnem s takým zápisom. 6 značil použitie algoritmu SHA-512 a za dalším $ nasledovala postupnosť zahashošovaných znakov. Uvedomil som si, čo ak je ten hash heslo ku serveru s5? Čo som teda spravil je, že som pomocou *mkpasswd -m sha-512* vytvoril svoj hash daného hesla čo som špecifikoval. V mojom prípade sa jednalo o hash:

```
$6$ZX6YJU4stJpd9ono$.UBwW11Fcg85g2an7oG4uFXAvzAvuyRncWEZyQEo20pnV6sYSlxoPQHwYIwZM0rOD8B
```

A potom som skúsil sa prihlásiť ako *ssh s5*. Čo bola banálna chyba a hneď som si uvedomil, že je nutné sa prihlásiť pomocou uživateľa ako *ssh bis_user@s5* čo znovu ale nefungovalo. Už som nevedel čo ďalej. Nakoniec som si spomenul, že v jednej dokumentácií bolo nutné inicializovať NIS mapy. Tak som teda skúsil vykonať príkaz *ypinit* čo však vyústilo v neúspech pretože ne-našlo danú binárku. Potom som však skúsil vyhladať binárku cez celý filesystem pomocou *find / |grep ypinit* kde som uvidel v cestu */usr/lib64/yp/*. Hneď som sa tam premiestnil a uvidel binárku *ypinit*. Už som myslel, že som veľmi blízko. Potom som spustil danú binárku *ypinit* s parametrom -m a následne som skúsil sa prihlásiť cez *ssh bis_user@s5* spolu so zadaným heslo a wualha. Bol som na servery!!! Ten pocit bol neopísateľný. Každopádne domovská zložka bola prázdna a ja ako skúsený linuxák som si hneď listol aj skryté pomocou *ls -all* čo skončilo ako úspech, kde som videl skrytý súbor *.secret.txt*. Tam som našiel tajomstvo J!

```
Tajemstvi:j_26-11-08-00-01_aa1a5c126400cd6a042fb96e37d7f8313fc552eb0b9381f78d1a85178ed5
```