Fakulta informačních technologií
Vysoké učení technické v Brně

# BIS

## Bezpečnost informačních systémů

### Tajomstvo BIS

Adrián Tóth (xtotha01)

20. novembra 2018

# Obsah

# 1 Úvod

Cieľom projektu bolo uskutočniť APT útok na zadaný server. Výsledok útoku spočíval v odhalení všetkých tajomstiev ktoré boli poukrývané na rôznych miestach. Nasledujúce kapitoly popisujú proces hľadania jednotlivých tajomstiev po pripojení pomocou privátneho kľúča na *bis.fit.vutbr.cz*.

# 2 Tajomstvá

| | |
|---|---|
| Kapitola 4 | `C_17-11-19-41-01_47533bc4b523ba4f7d0ebef3d25fe654f5ec126bc6a161394b027f4355ed6f64` |
| Kapitola 6 | `E_17-11-20-44-01_6454d0f7031b689cccb1bedf8de6f6c0b904eeaa810d7aef98bab5cba308fafe` |
| Kapitola 7 | `F_18-11-22-13-01_2d04f2e14d44efadf60e1921b8902d2648c65dfe364dbc0cb23da17d4008cf62` |
| Kapitola 5 | `I_17-11-20-14-01_adb2020a691f94c4a2b0f3ea1b16c21936567ee6b07f5a3308959c47a1b19abe` |

# 3 Analýza

Po pripojení na *bis.fit.vutbr.cz* som si najskôr prezrel `$HOME` pomocou „`ls -R -A $HOME`“. Odhalil som v priečinku `.Trash` privátny kľúč používateľa *itcrowd*. Následne na to, som si zistil IP adresu zariadenia pomocou „`ip addr`“. IP adresa zariadenia: `192.168.122.6`, maska siete: `255.255.255.0`. Zanalyzoval som si sieť v ktorej sa nachádza toto zariadenie pomocou „`nmap 192.168.122.6/24 -Pn`“. Vo výstupe som spozoroval *ptest*, tak na základe tohto, som spustil príkaz „`nmap 192.168.122.6/24 -Pn grep -A 6 "ptest"`“. Získal som nasledujúci výsledok:

```
Nmap scan report for ptest1.bis.mil (192.168.122.143)
Host is up (0.00072s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap scan report for ptest2.bis.mil (192.168.122.27)
Host is up (0.00049s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap scan report for ptest3.bis.mil (192.168.122.22)
Host is up (0.00062s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap scan report for ptest4.bis.mil (192.168.122.210)
Host is up (0.0016s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
6667/tcp open  irc
```

Z týchto poznatkov som zvážil, že by som sa pomocou odhaleného kľúča vedel pripojiť na jeden z hore uvedených zariadení. Popis pripojenia pomocou tohto privátneho kľuča pokračuje v kapitole 4.

# 4 Tajomstvo *C*

S využitím privátneho kľúča v priečinku `$HOME/.Trash/itcrowd.key` pre používateľa *itcrowd* nachadzájúceho sa na *bis.fit.vutbr.cz* som sa pripojil na zariadenie `ptest3` pomocou príkazu „`ssh -i .Trash/itcrowd.key -l itcrowd ptest3`“.

Po úspešnom pripojení som si znovu preskúmal `$HOME` pomocou „`ls -R -A $HOME`“ ale nič som nenašiel. Keďže na *ptest3* je otvorený port *http*, tak som vykonal „`cd /var/www/html && ls -R -A .`“. Spozoroval som súbor `/var/www/html/secret.txt` ktorého obsah som si následne chcel vypísať pomocou „`cat secret.txt`“. Výpis nebol možný z dôvodu nedostatočných práv, t.j. *cat: /var/www/html/secret.txt: Permission denied*. Port *http* bol ale otvorený, tak som skúsil zda sa ten súbor neviem stiahnuť pomocou „`curl http://ptest3/secret.txt`“.

```
                                Ziskali jste tajemstvi
C_17-11-19-41-01_47533bc4b523ba4f7d0ebef3d25fe654f5ec126bc6a161394b027f4355ed6f64
```

# 5 Tajomstvo *I*

Tajomstvo *I* som získal pokračovaním v analýze priečinka `/var/www/html` po odhalení tajomstva *C* ktoré je popísané v kapitole 4. Pri vypísaní obsahu súbora `/var/www/html/robots.txt` pomocou „`cat /var/www/html/robots.txt`“ som získal tajomstvo *I*.

```
                                Ziskali jste tajemstvi
I_17-11-20-14-01_adb2020a691f94c4a2b0f3ea1b16c21936567ee6b07f5a3308959c47a1b19abe
```

# 6 Tajomstvo *E*

Pri pripojení na zariadenie `ptest3` pomocou príkazu „`ssh -i .Trash/itcrowd.key -l itcrowd ptest3`“ sa zobrazila uvítacia správa ktorá obsahova *Riddle of the day*:

```
====== Riddle of the day ======
|>Qefkdp xob klq xitxvp texq qebv pbbj; qeb cfopq xmmbxoxkzb abzbfsbp jxkv;
qeb fkqbiifdbkzblc x cbt mbozbfsbp texq exp ybbk zxobcriiv efaabk.<|
|>Ql zixfj vlro mofwb ork zljjxka: ofaaib bppbkqfxifqfbp<|
================================
```

Zistil som, že sa jedná o Caesarovau šifru s pousnutím o 23. Dekódovaná správa vyzerala následovne:

```
====== Riddle of the day ======
|>Things are not always what they seem the first appearance deceives many;
the intelligence of a few perceives what has been carefully hidden.<|
|>To claim your prize run command: riddle essentialities<|
================================
```

Po vykonaní príkazu „`riddle essentialities`“ som získal tajomstvo *E*.

```
                                Ziskali jste tajemstvi
E_17-11-20-44-01_6454d0f7031b689cccb1bedf8de6f6c0b904eeaa810d7aef98bab5cba308fafe
```

# 7 Tajomstvo *F*

Všimol som si po analýze siete ktorá je popísaná v kapitole 3, že na *ptest4* beží `irc` na porte `6667`. Spustil som si IRC client pomocou „`irssi`“ a následne som sa napojil na *ptest4* pomocou „`/connect ptest4`“. Vypísal som si zoznam kanálov (channels) pomocou „`/list`“.

```
20:20 -!- Channel Users  Name
20:20 -!- #bis 1
20:20 -!- &SERVER 0 Server Messages
20:20 -!- #anonbox 0 Post all your ideas, complaints and everyday issues.
20:20 -!- #itcrowd 0 All IT issues to be discussed here.
20:20 -!- #meetings 0 In this channel you can find transcripts of the meetings.
20:20 -!- #finances 0 Channel for accountants and all monetary operations.
20:20 -!- #internal 1 Internal affairs.
20:20 -!- #general 0 Feel free discuss various topics in here.
20:20 -!- End of LIST
```

Všimol som si že na kanále `#bis` sa nachádza 1 user (používateľ). Pripojil som sa na kanál `#bis` a vypísal som si mená na tomto kanály pomocou „`/names`“.

```
20:26 [Users #bis]
20:26 [@Willie] [ student]
20:26 -!- Irssi: #bis: Total of 2 nicks [1 ops, 0 halfops, 0 voices, 1 normal]
```

Zistil som že `@Willie` je bot z github.com/mikeywaites/willie a má reagovať na určité príkazy začínajúce s bodkou. Zadal som príkaz „`.commands`“ na ktorý mi bot reagoval:

```
20:49 <@Willie> student: I am sending you a private message of all my commands!
```

Otvoril som si privátny chat s botom kde mi `@Willie` poslal všetky príkazy:

```
20:49 <Willie> Commands I recognise: CUKOO, action, addtrace, addtraceback, agreed,
announce, ask, at, ban, bitcoin, blocks, btc, c, calc, ch, chairs, choice, choose,
commands, comment, comments, countdown, cukoo, cur, currency, d, ddg, define, deop,
devoice, dice, dict, distance, duck, endmeeting, ety, exchange, findbug, findissue,
g, getchanneltimeformat, getchanneltz, getctf, getctz, getsafeforwork, getsfw,

20:49 <Willie> gettf, gettimeformat, gettimezone, gettz, gify, gtfy, help, imdb,
in, info, ip, iplookup, isup, join, kb, kick, kickban, length, link, listactions,
lmgify, lmgtfy, load, makebug, makeissue, mangle, mangle2, mass, me, mode, movie,
msg, op, part, py, quiet, quit, radio, rand, redditor, reload, roll, rss, safety,
save, search, seen, set, setchanneltimeformat, setchanneltz, setctf, setctz,

20:49 <Willie> setlocation, setsafeforwork, setsfw, settf, settimeformat,
settimezone, settz, setwoeid, showmask, spell, spellcheck, startmeeting, subject,
suggest, t, tell, temp, time, title, tld, tmask, topic, tr, translate, u, unban,
unquiet, update, uptime, version, voice, w, wa, wea, weather, weight, wik, wiki,
wolfram, wt, xkcd.

20:49 <Willie> For help, do 'Willie: help example' where example is the name of
the command you want help for.
```

Ukončil som privátny chat pomocou príkazu „`/q`“ aby som sa vrátil naspať do kanála `#bis`. Napísal som príkaz „`.CUKOO`“ na ktorý mi ale bot nereagoval, vyskúšal som „`.help CUKOO`“ na čo reagoval:

```
20:56 <@Willie> student: I might spoil you a secret.
```

Znovu som si otvoril privátny chat s botom kde som vyskúšal „`.CUKOO`“ na čo bot reagoval správou:

```
21:13 <Willie> Ziskali jste tajemstvi
F_18-11-22-13-01_2d04f2e14d44efadf60e1921b8902d2648c65dfe364dbc0cb23da17d4008cf62

21:13 <Willie> Ziskali jste tajemstvi
F_18-11-22-13-01_2d04f2e14d44efadf60e1921b8902d2648c65dfe364dbc0cb23da17d4008cf62
```

V správe som získal tajomstvo $F$.

```
Ziskali jste tajemstvi
F_18-11-22-13-01_2d04f2e14d44efadf60e1921b8902d2648c65dfe364dbc0cb23da17d4008cf62
```