Vysoké učení technické v Brně
Fakulta informačních technologií

Mystery of BIS

Dokumentácia k projektu

Dávid Bolvanský 20. novembra 2018

Zmapovanie siete

Po prihlásení na BIS server som zistil aktuálne sieťové nastavenie pomocou príkazu `ifconfig`. Následne som túto sieť zmapoval pomocou nástroja `nmap` a odhalil štyri servery („ostrovy“), na ktorých sú umiestnené tajomstvá použitím príkazu `nmap -sP 192.168.122.29/24 | grep "ptest"`.

```
Nmap scan report for ptest3.bis.mil (192.168.122.22)
Nmap scan report for ptest2.bis.mil (192.168.122.27)
Nmap scan report for ptest1.bis.mil (192.168.122.143)
Nmap scan report for ptest4.bis.mil (192.168.122.210)
```

Pomocou nástroja `nmap` som taktiež zistil, aké služby na dotyčných serveroch bežia:

```
Nmap scan report for ptest1 (192.168.122.143)

PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh

Nmap scan report for ptest2 (192.168.122.27)

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
3306/tcp open mysql

Nmap scan report for ptest3 (192.168.122.22)

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind

Nmap scan report for ptest4 (192.168.122.210)

PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
6667/tcp open irc
```

Tajomstvo A

Na BIS serveri som preskúmal zaujímave súbory a našiel pár dokumentov (pdf, doc) a v koši (`.Trash`) kľúč `itcrowd.key`. Obsah dokumentov som preskúmal a v `tc48-2008-024-Rev4.pdf` som našiel URI - `jbarber@ptest1.bis.mil`. Pomocou SSH som sa teda pokúsil o pripojenie ako `jbarber` na server `ptest1`. Server požadoval heslo. Na internete som si našiel zoznam najčastejších hesiel a vyskúšal som ich, až pokým nenastal úspech a pripojil som sa na server `ptest1` s heslom *welcome*. Po prieskume súborov na tom serveri som v `/etc/shadow` našiel tajomstvo A.

Tajomstvo B

Keď som prechádzal súbory na serveri `ptest3`, preskúmal som aj priečinok `.ssh` a našiel som v nom súbor `config`, z ktorého obsahu vyplývalo, že ako užívateľ `webmaster` sa môžem pripojiť na server `ptest2`. To som aj urobil pomocou `ssh webmaster@ptest2` a úspešne som sa pripojil na tento server. Nasledoval klasický prieskum servera. Dostal som do `/var/www/html/`, kde ma zaujal súbor `internal-memo.php`, ktorý som preskúmal. Našiel som zaujímavú časť kódu, ktorá žiaľ bola v nedostupnej vetve kódu:

```
echo $GLOBALS['INTERNAL_MSG'];
```

Zdá sa, že text v `INTERNAL_MSG` bude obsahovať niečo interné/tajné a mojím cieľom je sa k tomu nejakým spôsobom dostať. Skúmal som ďalej a v súbore `index.php` som našiel ďalšiu zaujímavú časť kódu:

```
if (isset($_GET['debug_variable'])) {
    var_dump(${$_GET['debug_variable']});
};
```

Využil som tento ladiací (*debug*) kód, ktorý sa dostal aj do produkčného (*release*) kódu na získanie ďalšieho tajomstva. Kód slúži na výpis (*dump*) premennej, ktorá je určená obsahom `debug_variable`. Vďaku tomuto ladiacemu kódu som sa teda vedel ľahko dostať k obsahu `INTERNAL_MSG`. Do terminálu som zadal príkaz `curl http://ptest2/index.php?debug_variable=INTERNAL_MSG` a získal som tajomstvo B.

Tajomstvo C

Ako som už zmienil pri tajomstve A, na BIS serveri som našiel kľúč `itcrowd.key`, s ktorým som skúsil pripojiť na nejaký zo štyroch serverov. S týmto kľúčom

a užívateľským menom `itcrowd` som sa úspešne pripojil na server `ptest3`. Preskúmal som na tom serveri rôzne priečinky a našiel som zaujímave veci vo `/var/www/html/`. Našiel som tu súbor `secret.txt`, ktorý síce nešiel otvoriť pomocou nástroja `cat`, no pomocou príkazu `curl http://ptest3/secret.txt` som odhalil tajomstvo C.

Tajomstvo D

Zo zmapovania siete som vedel, že na serveri `ptest4` beží DNS server (port 53). Skúšal som sa pýtať práve tohto servera nejaké DNS dotazy. Pomocou `dig @ptest4.bis.mil ptest4.bis.mil SOA` som zistil autoritatívny server - `bis.mil`. O tomto serveri som chcel zistiť ďalšie informácie, tak som si vypísal všetky DNS záznamy pre tento server pomocou `dig @ptest4.bis.mil bis.mil ANY`. V TXT zázname som našiel tajomstvo D.

Tajomstvo E

Po prihlásení na server `ptest3` ma uvítala správa, ktorá nedávala moc zmysel. Napadlo ma, že by to mohlo o Ceasarovu šifru s posunutím, ktoré však už s prvého pohľadu nemohlo byť 3. Pomocou online stránky na internete som dekódoval túto správu a zistil som jej obsah a že sa jedná o posun o 23 znakov. Časť správy obsahovala nasledovný text: *To claim your prize run command: riddle rope*. Zadal som teda príkaz `riddle rope` do terminálu a získal som tajomstvo E.

Tajomstvo F

Zo zmapovania siete som vedel, že na serveri `ptest4` beží IRC server. Na BIS serveri sa nachádzal IRC klient `irssi`, ktorý som spustil a pomocou príkazu `\connect ptest4` som sa naň pripojil. Následne som si pomocou príkazu `\list` zobrazil všetky IRC kanály. Pripojil som sa kanál s zaujímavým menom - `#bis`.

Spoločnosť mi tu robil IRC bot `Willie`. IRC boti reagujú na príkazy a následne vykonávajú nejakú činnosť, preto ma zaujímalo, čo tento bot vie. Pomocou príkazu `.commands` som zistil zoznam príkazov, na ktoré bot reaguje. Medzi príkazmi bol aj jeden, ktorý sa odlišoval na prvý pohľad od ostatných - príkaz `.CUKOO`. V chate s botom Willie som tento príkaz zadal a bot mi odhalil tajomstvo F.

Tajomstvo G

Zo zmapovania siete som vedel, že na serveri `ptest1` beží FTP server. Pripojil som sa naň pomocou príkazu `ftp ptest1` z BIS servera. Zistil som, že na serveri beží `vsFTPd` vo verzii 2.3.4, na ktorú je možné použiť smajlíkový útok. Ako

užívateľské meno som zadal reťazec zakončený smajlíkom (napr. `x:)`), heslo som nezadal žiadne. Následne sa mi otvoril port, na ktorý keď som sa pripojil, získal som tajomstvo G.

Tajomstvo H

Tajomstvo H nebolo ďaleko od tajomstva A, na tom istom serveri (`ptest1`) som preskúmal domovský priečinok užívateľa `jbarber`. V priečinku `Mail` som si otvoril súbor `Trash` a našiel som tu tajomstvo H.

Tajomstvo I

Po ďalšom hľadaní som hneď vedľa tajomstva C našiel v súbore `robots.txt` aj tajomstvo I.

Tajomstvo J

Vedľa tajomstva B, konkrétne v priečinku `/var/www/html/libs/`, som našiel súbor `constants.php`, ktorý obsahoval prístupové údaje k databáze:

```
define('DB_HOST_USERNAME', 'arcturus');
define('DB_HOST_PASSWORD', '16431879196842');
define('DB_DATABASE', 'arcturus');
```

S týmito údajmi som sa dostal do databáze pomocou príkazu `mysql -u arcturus -p16431879196842` a následne `use arcturus;`. Pomocou príkazu `show tables;` som si následne zobrazil všetky tabuľky. V tabuľkách `pages` a `tagline` som nič zaujímavé nenašiel, no v tabuľke `contracts` som našiel tajomstvo J.