VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií

Bezpečnost informačních systémů

Mystery of BIS 14

June 11, 2019

Autor: Jan Pawlus, xpawlu00@stud.fit.vutbr.cz

1 Realizace

1.1 Zmapování

Po připojení na server `bis.fit.vutbr.cz` se dá příkazem `arp -a` zjistit zhruba topologie sítě. Je vidět, že v síti jsou servery `ptest1`, `ptest2`, `ptest3` a `ptest4`. Když jsem projekt začal řešit, nenacházel se ale na tomto serveru nástroj `nmap`, kterým bych zjistil, co na jakém serveru běží za služby na jakých portech. Ve složce `Mail` je soubor `Trash`, který ukazuje na potenciální tajemství na stanici `anna@ptest2.local`. Ve složce `.ssh` jsem nalezl `ssh` klíč pro připojení na server `ptest1`.

1.2 ptest1

Zde jsem se jako vždy pokusil získat přístup `root`, což se mi povedlo příkazem `sudo -s`. V kořenové složce jsem příkazem `ls -R` zjistil, že ve složce `root` se nachází dvě tajemství - *A* a *B*.

Díky `root` přístupu jsem na server `ptest1` nainstaloval programy `nmap` a `tcpdump`. Pomocí `nmap` jsem zjistil, že na serveru `ptest2` je otevřený port pro `http`, stejně jako na `ptest3`. Na `ptest4` jsem našel otevřený `ftp` port.

1.3 ptest2

`HTTP` službu jsem si přesměroval k sobě příkazem
`ssh -L 8180:ptest2:80 student@bis.fit.vutbr.cz -p 65125 -N -i id_ecdsa` a zjistil jsem, že web využívá `cookies` k uložení `session ID`. Začal jsem tedy programem `tcpdump` odposlouchávat port 80 a našel přicházející `HTTP` požadavky, kde jsem našel i `session ID`. Příkazem `curl --cookie` jsem nastavil `session ID` (přesnou odchycenou hodnotu jsem si bohužel nezaznamenal) a prohlížečem `elinks` vstoupil na web, kde potvrdil prázdné jméno a heslo a získal tajemství *E*.

Následně jsem se pokoušel najít heslo pro stanici `anna@ptest2.local`, bohužel neúspěšně, načež jsem vyzkoušel `dictionary attack` programem `hydra` (databázi hesel jsem stáhl zde: https://wiki.skullsecurity.org/Passwords) a získal heslo `princess`, kde v adresáři `anna` získal tajemství *C*.

Poté jsem hledal cokoliv společného se slovem `robocop` příkazem `ls -R` a našel stejně pojmenovaný binární soubor, a příkazem `cat robocop` získal tajemství *D*.

1.4 ptest3

Na serveru `ptest3.local` jsem našel webovou službu, kterou jsem si příkazem
`ssh -L 8180:ptest3:80 student@bis.fit.vutbr.cz -p 65125 -N -i id_ecdsa` přesměroval k sobě do prohlížeče. Zjistil jsem, že při špatném filtrování se vypisuje `SQL` chyba, zkoušel jsem tedy zmapovat databázi, což se mi povedlo, pokud jsem do pole `name` (zjistil jsem totiž z vypsané `SQL` chyby, že se v databázi vyhledává jako `WHERE name LIKE %obsah_pole%`) zadal `abcd" UNION SELECT table_name, column_name, 1, 1 FROM information_schema.columns WHERE 1 LIKE "`.

Z toho jsem zjistil, že v databázi existuje tabulka `auth` se sloupci `login`, `id` a `passwd`. Po zadání `abcd" UNION SELECT id, login, passwd, 1 FROM auth WHERE 1 LIKE "` mi databáze díky *SQL injection* prozradila tajemství *F* jako heslo administrátora.

1.5 ptest4

K `FTP` službě běžící na `ptest4` jsem se dostal příkazem `ftp`. Jako autentizaci jsem zkusil klasické anonymní přihlášení (login `anonymous`, heslo jakékoliv), což zafungovalo a já získal obrázek `definitely-not-a-secret.gif`, který obsahoval tajemství G.

2 Závěr

Děkuji za zábavný a zajímavý projekt.