Vysoké učení technické v Brně
Fakulta informačních technologií

Bezpečnost informačních systémů

1. projekt – dokumentace

26. listopad 2017

Ján Jusko

1 Úvod

Tento dokument popisuje riešenie prvého projektu v predmete BIS. Jeho cieľom bolo získať čo najviac tajných reťazcov (secrets) nachádzajúcich sa v poskytnutej vnútornej sieti. Ako východiskový bod mi bol pridelený prístup na server *bis.fit.vutbr.cz* prostredníctvom privátneho kľúča a *ssh* portu.

2 Mapovanie serverov

Prvým krokom bolo zmapovanie serverov v sieti a následne získanie informácií o bežiacich službách na servroch. K tejto úlohe som použil nástroj *nmap* a *arp*. Po vyfiltrovaní klientskych staníc študentov sú objavené servery a služby nasledovné:

- **ptest1** (192.168.122.243)
  - ssh (22)
  - rcpcbind (111)
  - nfs (2049)
- **ptest2** (192.168.122.204)
  - ssh (22)
  - http (80)
  - rcpcbind (111)
- **ptest3** (192.168.122.160)
  - ssh (22)
  - http (80)
  - rcpcbind (111)
  - ssl/https (443)
  - mysql (3306)
- **ptest4** (192.168.122.10)
  - ftp-data (20)
  - ftp (21)
  - nfs (2049)

3 Tajomstvá

Po serveroch *ptest1* - *ptest4* je rozmiestnených 7 tajomstiev A-G.

3.1 Tajomstvo A

- **Umiestnenie:** ptest1

Na server *ptest1* som sa pripojil na ssh port pomocou súkromného kľúča ktorý som našiel na východiskovom serveri *bis* v skrytej zložke *.ssh*. Tajomstvo A sa tam nachádza v súbore *secret.txt* ktorý patrí užívateľovi *eis*.

3.2 Tajomstvo B

- **Umiestnenie:** ptest1

Rovnako ako tajomstvo A, aj tajomstvo B sa nachádza na serveri ptest1. Tentokrát v súbore *secret2.txt* nachádzajúcom sa v priečinku užívatela not-rootkit.

3.3 Tajomstvo C

- **Umiestnenie:** ptest2

Na server *ptest2* som sa pripojil na ssh port pomocou prihlasovacieho mena anna ktoré som našiel v e-mailovej komunikácii na východiskovom serveri *bis*. Na prelomenie hesla stačil jednoduchý slovníkový útok. Hneď v domovskom adresári anna sa nachádza súbor *secret.txt* ktorý obsahuje tajomstvo C.

3.4 Tajomstvo D

- **Umiestnenie:** ptest2

Na serveri ptest2 som hľadal ďalej. V spomenutej e-mailovej komunikácii sa spomína istý program pre mechanickú ruku – *robocop*. Po prehľadaní servera som v adresári */bin* našiel binárny súbor *robocop* ktorý som prehľadal pomocou nástroja grep s nastavením *–binary-files=text* a našiel v ňom tajomstvo D.

3.5 Tajomstvo E

- **Umiestnenie:** ptest2

Na serveri ptest2 beží na HTTP porte webový portál eis. Hneď na úvodnej stránke je prihlasovací formulár. Usúdil som, že skôr či neskôr niekto bude pracovať v portále a preto som začal odchytávať komunikáciu pomocou nástroja *tcpdump*. Takto sa mi podarilo ukoristiť tajomstvo E.

3.6 Tajomstvo F

- **Umiestnenie:** ptest3

Na bežiacej službe HTTP, port 80 (prístup pomocou nástroja elinks) sa zobrazí list užívateľov s rôznymi textovými poliami pre filtrovanie alebo vkladanie nových užívateľov. Okrem klasických mien a e-mailov, boli v tabuľke aj SQL dotazy čo ma naviedlo vyskúšať **SQL Injection**. Po odoslaní nezmyselného vstupu so špeciálnymi znakmi sa dokonca zobrazí chybová hláška s kompletným SQL query reťazcom. Query musí vracať vždy 4 stĺpce. Najprv som zistil z information.schema aké tabuľky a stĺpce sa nachádzajú v databáze a to vstupom '%" AND 1=1 UNION SELECT table name, column name, 1, 1 FROM information schema.columns WHERE "%"="' Po chvíli hľadania som v tabuľke *auth* našiel tajomstvo F.

3.7 Tajomstvo G

- **Umiestnenie:** ptest4

Pri skenovaní serveru ptest4 som objavil otvorený port. Zistil som že na ňom beží služba FTP v anonymous režime. Na pripojenie stačilo zadať uživateľské meno anonymous bez hesla. Tam som objavil tajomstvo G.