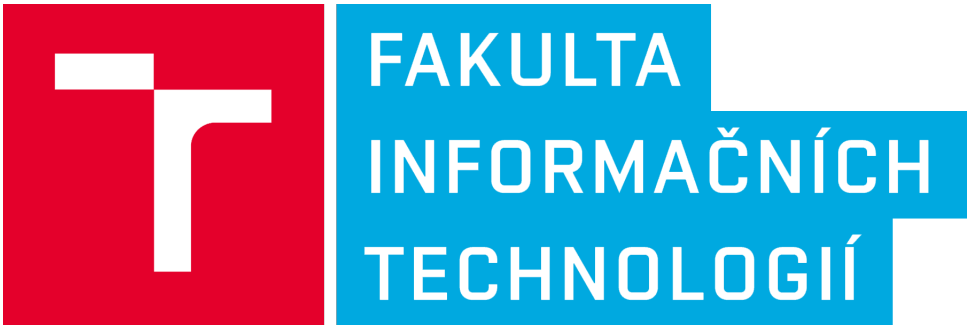

Dokumenácia k projektu 1 v predmete BIS

Matej Marušák, November 2017

1 Zmapovanie

K zmapovaniu bola použitá utilita nmap, cez celý rozsah portov. Výsledky sú zobrazené v tabuľke 1. Tučne sú označené porty, ktoré boli neskôr aj využité.

Názov	IP adresa	Otvorené porty	Tajmostvá
ptest1	192.168.122.160	**22**, 111, 2049 (nfs)	A,B
ptest2	192.168.122.204	**22**, **80**, 111	C,D,E
ptest3	192.168.122.243	22, **80**, 111, 443, 3306 (mysql)	F
ptest4	192.168.122.10	**20**, 21 (ftp)	G

Tabuľka 1: Zmapovanie serverov

2 Popis získaných tajomstiev

Udalosti popísané v nasledujúcom texte nie sú v chronologickom poradí.

Pripájam sa kľúčom na server z emailu. Obzerám sa okolo a nič zaujímave nevidím. V `/.ssh/config` sa dozvedám o servery ptest1, tak sa na neho priamo cez ssh pripájam (A podľa mapky aj tak viem, že na štartovacom servery nič nie je). Zisťujem kto som, kde sa nachádzam a pri tom narazím aj na fakt, že som vo `wheel` skupine (príkaz `groups`). Z `/etc/passwd` zisťujem, že sa tu nachádzajú dvaja zaujímavý užívatelia a to `not-rootkit` a `eis`. Chcem sa pozrieť do ich domovského adresára, ale ako užívateľ `centos` tam nemám prístup, tak sa prepínam na roota za pomoci `sudo su`. Získavam tak tajomstvá **A** a **B**, pričom obe boli úplne jasné.

Pokúšam sa dostať na ptest2 - ssh vyžaduje heslo, tak skúšam web. Tam sa taktiež vyžaduje meno a heslo. Predpokladám, že užívateľ bude `anna`, nakoľko som sa o nej dozvedel z mailu ešte na prvom servery. Skúšam pár očividných hesiel, neúspešne. Púšťam na to slovníkový útok za pomoci slovníka `/usr/share/dict/words` (napísal som si jednoduchý python skript). Avšak neúspešne. Skúšam preto slovníkovú útok aj na ssh, tento krát už úspešne a dozvedám sa, že heslo je `princess`. Hneď pri príchode ma čaká tajomostvo **C**. Očakávam, že by

na tomto servery mohol existovať zaujímavý spustiteľný súbor a tak na možné cesty (získané z $PATH púštam príkaz `ls | xargs -L1 rpm -qf | grep owned`. Rýchlo nachádzam súbor `robocoup` ale jeho spustením neviem nič získať. V nádeji, že je to v interpertovanom jazyku si otváram zdrojový kód. Je kompilovaný, ale tajomstvo **D** sa nechádza v priamej podobe. Pre neúspech na webovej stránke sa idem pozrieť na zdrojové kódy v `/var/www/html/index.html`, kde sa dozvedám aké heslo očakáva užívateľ `admin`. Pripájam sa teda ešte raz na webové rozhranie, zadávam meno a heslo a získavam tajomstvo **E**.

Pripájam sa na webové rozhranie serveru ptest3. Viem že tam sa nachádza aj databáza tak ihneď idem skúsať `SQL injection`. Po prvom dotaze sa ihneď dozvedám, že je možné takýto útok previesť a aj ako vyzerá základy dotaz. Posielam preto dotaz v tvare `“union select “table_name“as name, ““as email, ““as address, 0 as id from information_schema.tables where name like “`. Dozvedám sa dostupné tabuľky, postupne si prehľadávam všetky relatívne zaujímave tabuľky, až v tabuľke `auth` nachádzam tajomstvo **F**.

Pre získanie posledného tajomstva sa pripájam za pomoci ftp na ptest4. Nakoľko nemám žiadne prihlasovacie údaje, tak využívam anonymné prihlásenie (meno: anonymous, heslo: anon@test.com). Vylistujem si obsah adresára, následne si vylistujem obsah aj podadresára a v tom na nachádza súbor `definitely-not-a-secret.git`. Sťahujem si ho a ked si ho otvorím ako text, tak nachádzam tajomstvo **G**.

Tým pádom som našiel všetkých 7 tajomstiev a moja práca je tu hotová.