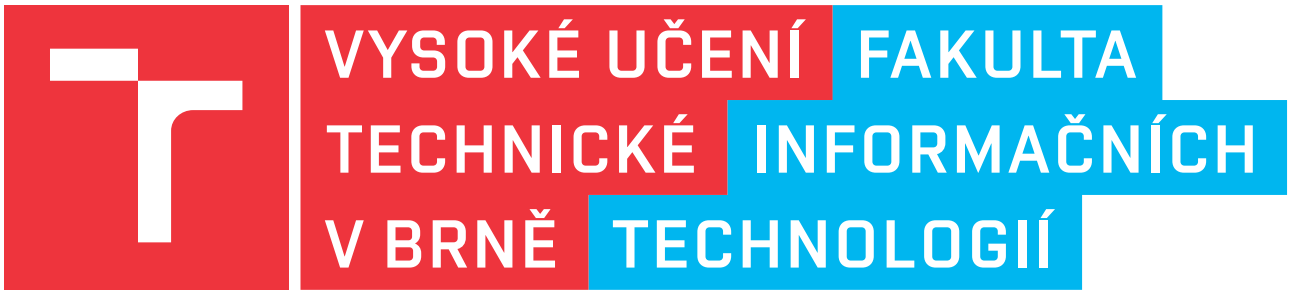

Dokumentace k projektu č. 1

Bezpečnost informačních systémů

Nikola Valešová (xvales02)

18. listopadu 2017

1 Zmapování sítě

Pro zmapování sítě byl využit nástroj `nmap`. Čtyřmi ostrovy, na kterých se nalézají tajemství, a porty, na kterých naslouchají, jsou:

- ptest1.local (192.168.122.243)

PORT	STATE	SERVICE
22/tcp	open	ssh
111/tcp	open	rpcbind
2049/tcp	open	nfs

- ptest2.local (192.168.122.204)

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

- ptest3.local (192.168.122.160)

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind
443/tcp	open	https
3306/tcp	open	mysql

- ptest4.local (192.168.122.10)

PORT	STATE	SERVICE
20/tcp	closed	ftp-data
21/tcp	open	ftp

2 Cesta k tajemstvím

2.1 Tajemství A

Na výchozím serveru se v domovském adresáři nachází složka .ssh a v ní soubor config. Z něj získáme informace o uživateli appsrv, zkouším tedy příkaz ssh appsrv a úspěšně se připojuji. Jdu do kořenového adresáře a zadávám příkaz „sudo find . -regex ".*secret.*"2>/dev/null“ a v adresáři ./var/local/eis v souboru secret.txt nacházím tajemství A.

Získáno: 28. 10. 2017 v 18:49
A:28:10:18:49:02:8339b2f77af190be976c91f08aaa309608bab98f0751f21c686d1b235a94266b

2.2 Tajemství B

Nedaleko tajemství A se nachází i tajemství B, v adresáři ./var/local/not-rootkit v souboru secret2.txt.

Získáno: 28. 10. 2017 v 19:54
B:28:10:19:54:01:3eca19d6e510538299cfae9e399397c3670873badd1d76b081dd40809afa78df

2.3 Tajemství C

Z e-mailu v domovském adresáři na serveru ptest1 se dozvídáme o osobě s loginem „anna“. Po provedení slovníkového útoku na port 22 na server ptest2 zjistíme, že zde takový uživatel opravdu existuje a má heslo „princess“. Stačí se tedy připojit pomocí ssh -l anna ptest2.local a zadat zjištěné heslo. V domovském adresáři na serveru ptest2 se nachází soubor secret.txt, který obsahuje tajemství C.

Získáno: 17. 11. 2017 v 23:35

C:17:11:23:35:01:16ac77d63f3abb03fafdb3b30052b3c69801f4687d1293dc0127b8417b427fe8

2.4 Tajemství D

Ve zmíněném e-mailu se mluví o programu robocop, i tato informace nám je užitečná, jelikož v některých dalších souborech v domovském adresáři na serveru ptest2 nás odkazují na soubor v adresáři /usr/bin/robocop a skutečně, po zobrazení jeho obsahu získávám tajemství D.

Získáno: 18. 11. 2017 v 10:56

D:18:11:10:56:02:9ad2c9b7e40e229d85d166c84034f00c3465a5496569bc61a4dd4cd3e86d958e

2.5 Tajemství E

Po několika minutách pátrání objevuji ve složce /var/www/html v souboru action_page.php přihlašovací údaje – login admin a heslo „8}Yg3,9ro¿&jR{“. Zkouším tedy příkaz elinks http://ptest2.local, zadávám zjištěné přihlašovací údaje a po úspěšném přihlášení se mi zobrazí také tajemství E.

Získáno: 18. 11. 2017 v 11:11

E:18:11:11:11:01:2abccdc6e12509f2cdf7f55a4aa404bb00b52ce38a37a1d9cc7959ff67b88ec1

2.6 Tajemství F

Na server ptest3 se lze připojit pomocí příkazu elinks ptest3.local. Zobrazí se nám databáze, což vybízí k útoku pomocí SQL injection. Po zadání znaku ”nám databáze vypíše, že zadaný příkaz není validní a celý příkaz, tedy ideální návod na to, jak stávající příkaz doplnit o libovolný svůj požadavek pomocí operace UNION. Zadávám tedy nejprve

None”UNION SELECT table_schema, table_schema, table_name, column_name FROM information_schema.columns WHERE table_schema != ’mysql’ AND table_schema != ’information_schema’;#

pro zjištění názvů tabulek v databázi a jejich schémat. Poté zjišťuji obsah tabulky auth zadáním

None”UNION SELECT id, login, passwd, login FROM auth;#,

mezi hesly nacházím mimo jiné i tajemství F.

Získáno: 2. 11. 2017 v 11:06

F:02:11:11:06:01:b25b5440af76e70e89505d4805388d60496a22e19a454542fd166285bd201af6

2.7 Tajemství G

FTP spojení na server ptest4 vybízí ke vzdálenému připojení přes daný protokol. Po chvilce pátrání na internetu objevuji údajně časté a typické přihlašovací jméno, anonymous. Zkouším tedy příkaz ftp -A 192.168.122.10, zadávám zmíněné přihlašovací jméno, prázdné heslo a jsem úspěšně připojena. Při procházení vzdáleného adresáře objevuji soubor definitely-not-a-secret.gif v podsložce pub. Pomocí

příkazu get se mi jej podaří stáhnout na server ptest1 a poté si jej přetahuji do svého počítače. Po otevření tohoto souboru v textovém editoru se zobrazí poslední ze skrytých tajemství, tajemství G.

Získáno: 5. 11. 2017 v 21:38

G:05:11:21:38:01:c615108e5a36f46a1d65bbde3ec7a7f47b373446cb8a043394c82edb36672746