# Dokumentácia k projektu do predmetu Bezpečnosť informačných systémov: Mystery of BIS

Autor: Filip Gulán (*xgulan00*)

## 1 Úvod

Úlohou tohoto projektu bolo vo vyčlenenom čase získať čo najviac tajomstiev ukrytých na privátnych serveroch vo vnútornej sieti BIS.

## 2 Zmapovanie siete

Po prihlásení na server BIS, som si získal Ip adresu stanice a následne siete (***ifconfig).*** Potom som pomocou programu ***nmap*** zmapoval túto sieť. Keďže som si všimol záznamov ***ptest***, tak som použil program ***grep,*** iba pre zobrazenie týchto záznamov (***nmap 192.168.122.0/24 -Pn | grep "ptest"***). Následne som zistil, aké služby bežia na týchto serveroch, znovu pomocou **nmap**:

Nmap scan report for **ptest4 (192.168.122.10)**
Host is up (0.00071s latency).
rDNS record for 192.168.122.10: ptest4.local
Not shown: 998 filtered ports
PORT STATE SERVICE
**20/tcp closed ftp-data**
**21/tcp open ftp**

Nmap scan report for **ptest3.local (192.168.122.160)**
Host is up (0.0035s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
**22/tcp open ssh**
**80/tcp open http**
**111/tcp open rpcbind**
**443/tcp open https**
**3306/tcp open mysql**

Nmap scan report for **ptest2.local (192.168.122.204)**
Host is up (0.0029s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
**22/tcp open ssh**
**80/tcp open http**
**111/tcp open rpcbind**

Nmap scan report for **ptest1.local (192.168.122.243)**

Host is up (0.0036s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
**22/tcp open ssh**
**111/tcp open rpcbind**

## 3 Tajomstvo A

V zložke ***.ssh***, v konfiguračnom súbore ***config*** som našiel alias ***appsrv (ptest1)***. Pripojil som sa na tento ssh server (***ssh appsrv***). Zistil som, že tam je nejaký program ***eis***, ktorý môže byť dôležitý. Vyhľadal som si tento program (***which eis***), spustil som ho, a keďže spustením som nezaznamenal nič neobvyklé, tak som si dal vypísať obsah tohoto súboru (***cat eis***). Zistil som, že tento program pravdepodobne spúšťa ďalší skript (***/var/local/eis/bootstrap.sh***). Pozrel som sa teda do tejto zložky (***sudo ls /var/local/eis***) a videl, že okrem súboru ***bootstrap.sh, invoices.db*** obsahuje ešte aj ***secret.txt***.

## 4 Tajomstvo B

Keďže sa tajomstvo sa volá ***secret.txt***, tak som si skúsil vypísať všetky zložky a súbory s týmto kľúčovým slovom v koreňovom adresári (***sudo ls /* | grep "secret"***) serveru ptest1. Príkaz mi zobrazil secret1 a secret2. Potom som vyhľadal umiestnenie týchto tajomstiev (***sudo find -name secret2***). Našiel som secret1 a secret2 zložku. Ako som zistil, tak secret1 je už vlastnené tajomstvo A, ale v secret2 je nové tajomstvo B.

## 5 Tajomstvo C

Z mailu ***Trash*** na servery BIS som zistil, že na ***ptest2*** by sa mohol nachádzať užívateľ ***anna***. Skúsil som sa prihlásiť na ssh ako ***anna*** a zistil som, že užívateľ naozaj existuje. Skúsil som teda bruteforce metódou pomocou programu ***ncrack*** zistiť heslo. Využil som zoznam 500 najhorších hesiel, ktorý je dostupný z https://github.com/danielmiessler/SecLists/blob/master/Passwords/500-worst-passwords.txt . Program našiel heslo ***princess*** a po vstupe na server sa v domovskom adresári nachádzalo tajomstvo C.

## 6 Tajomstvo D

V maile ***Trash*** na servery BIS sa spomínal program ***robocop***. Skúsil som teda na **ptest2** spustiť program ***robocop*** a zistil som, že program existuje. Program som našiel (***which robocop***) v ***/usr/bin*** a zobrazil jeho obsah (***cat robocop***). Rovnako ako program eis, tak aj program ***robocop*** obsahoval tajomstvo.

## 7 Tajomstvo E

Išiel som pomocou ssh na ***ptest2*** a keďže som vedel, že podľa nmap programu tu musí byť niekde ***web server***, tak som išiel do zložky ***/var/www/html*** , kde som našiel ***action_page.php***. V tomto php skripte som našiel v zdrojovom kóde užívateľské meno ***admin*** a heslo ***.8}Yg3,9ro>&jR{*** . Toto

meno a heslo som využil vo formulári na http://ptest2 (***elinks http://ptest2***), kde mi po úspešnom prihlásení bolo zobrazené tajomstvo E.

## 8 Tajomstvo F

Keďže na ***ptest3*** beží ***http server*** spolu s ***mysql***, tak sa k tomtuto serveru pripojil (***elinks http://ptest3***). Zistil som, že sa tam nachádza akýsi zoznam zamestnancov firmy. Na tejto stránke je vyhľadávací ***input***, do ktorého som skúsil zadať časť SQL (***"; --***) a tým som zistil, že znaky z ***inputu*** sa pri dotazovaní na databázu neescapujú a aký presný dotaz sa vykonáva. Zadal som teda zložitejší dotaz, aby som zistil, aké všetky tabuľky a stĺpce sa v databázi nachádzajú (***test" or 1=1 union select column_name as name, table_name as email, 3, 4 from information_schema.columns; --*** ). Videl som, že sa tam nachádza tabuľka ***auth***. Tabuľku som si nechal teda vypísať (***test" or 1=1 union select id, login as name, passwd as email, 4 from auth; --*** ). Nakoniec som videl, že užívateľ ***admin*** má ako heslo tajomstvo.

## 9 Tajomstvo G

Po zistení, že na ***ptest4*** beží FTP server, som sa pripojil ***ssh ptest1,*** kde mám root práva a nainštaloval som program ***ftp***. Pomocou ***ftp*** som sa pripojil na ptest4 ***ftp 192.168.122.10*** ako ***anonymný (anonymous)*** užívateľ bez hesla, použil som príkaz ***passive*** a následne ***ls***. Zistil som, že na FTP je zložka ***pub***. Išiel som do tejto zložky (***cd pub***) a stiahol súbor definitely-not-a-secret.gif (***get definitely-not-a-secret.gif***). Po otvorení súboru (***cat***) som videl, že sa v ňom nachádza tajomstvo G.

## 10 Záver

Úlohou tohoto projektu bolo vyhľadávať ukryté tajomstvá vo vnútornej sieti BIS . Podarilo sa mi získať 7 z 7 tajomstiev.