VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií


Bezpečnost informačních systémů

# Mystery of BIS 14

November 26, 2017

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

# 1 Příběh Black Cats

Musím jednat rychle... Ale nejprve musím vymyslet, jak se odtud dostat na další ostrov na mapě, která ukazuje tři ostrovy: *Zamanův ostrov*, *Sušenku*, *Databáze* a obchodní cestu. Jenže Černovousova posádka číhá všude kolem, i u mé lodi. Nepozorovaně se protáhnu postranními uličkami a dostávám se až k opačnému břehu, kde čeká opuštěná plachetnice, na které nacházím potrhaný dopis nějaké Anně z ostrova Sušenka, kde nějaký blázen píše o své dřevěné noze. Nechápu, nastupuji a zvedám kotvy...

## 1.1 Zamanův ostrov

Doplul jsem až na Zamanův ostrov pojmenovaný podle místního starého zlého opilého krále. Mezi piráty se traduje, že ve svém paláci ukrývá velmi vzácné a magické lahve s alkoholem, které dokáží člověka teleportovat. Poloha na mapě by tomu také odpovídala... Musím vymyslet lest, jak se tam dostat. A náhle mě to napadlo - stačí se zbavit jeho ochranky, která se nechá vyprovokovat každou narážkou na jejich pána. Zaplatím tedy několika místním, aby vyšli do ulic a posměšně poukazovali na královu neschopnost. Ochranka je tedy pryč, a starý opilec už určitě leží někde doma v lihu. Jednoduše tedy proklouznu do jeho paláce a bez obtíží v jeho truhle nacházím dvě magické lahve s alkoholem s nálepkou Absinth.

## 1.2 Sušenka

Utíkám po náročném dni do místní putiky. Objednávám tři korbely a slyším, jak si dva obchodníci snažíc se nenápadně povídají o něčem na první pohled důležitém. Vytahuji své magické naslouchátko, které jsem našel v pokladu před pár lety. Co mé uši neslyší - na malém ostrůvku Sušenka jeden z nich pod kokosovou palmu zakopal cenný poklad! Poloha na mapě také zhruba odpovídá, dopíjím rychlostí blesku svůj lahodný mok a vydávám se pro poklad. Kopu pod kokosovou palmou a nacházím starý pirátský klobouk, jehož nositel získá nepochopitelné přesvědčovací schopnosti.

## 1.3 Databáze

Po předchozí dobré zkušenosti s putikou se vracím a objednávám s radostí další korbel. Všichni na pohled významní boháči jsou už pryč. Přisednu k místním štamgastům a čekám, zda se nedozvím něco zajímavého. Jeden z nich vykládá o tom, že si byl dnes na ostrově Databáze vyřizovat změnu jména, aby se ukryl před lichváři, kterým dluží peníze. Stěžoval si, že pracovník na úřadě vypadal, že si už dávno vypil mozek. V tom mě to napadlo - nemohl by se další poklad ukrývat právě na takovém úřadě? Poloha na mapě by odpovídala...

Vyrážím tedy na tento ostrov, kde žije jeden známý boháč, kterému se říká Admin, protože má díky svému bohatství vliv na všechny okolo. Přicházím na úřad a spatřuji člověka, co odpovídá popisu... Přijdu k němu a opravdu - vůbec neví, kde je sever. Nakukám mu nesmysly a přesvědčuji ho, že jsem Admin, a on mě zmateně vpouští do přísně tajné místnosti Admina, kde je uschována kouzelná róba, která nositele ochrání před útoky ostatních.

## 1.4 Transportní lodě

Vracím se zpět do své putiky, která mi přinesla už tolik štěstí. Přisedám k dalším štamgastům, kteří si vykládají o tom, že zítra vyplouvají lodě převážející cenné poklady do cizích království. Otvírám mapu a vidím, že poloha přístavu odpovídá potenciálnímu pokladu... Vydávám se tedy pro další poklad. Přicházím zrovna, když se náklad přenáší na lodě. Jeden z pracovníků vypadá hodně naštvaně a neustále nadává. Ptám se, co ho trápí. Stěžuje si, že už ho nebaví tahat se s těžkými náklady, když si za otrockou dřinu sotva dovolí dva korbely v putice. V duchu se opět ujistím o tom, že poctivou prací se nikdy živit nebudu, a to mu také řeknu. Nebožák upustí náklad a odchází se slovy, že tohle zapotřebí nemá a že bude také krást. Zmocňuji se upuštěného nákladu a co nenajdu - velmi cenný kompas, který vždy ukáže tam, kam chci plout.

## 1.5 Poslední dech

Společensky znaven se vracím do putiky, kde už jsou všichni tak namol, že se nic dalšího nedozvídám. Vzpomenu si na dopis zanechaný na mé plachetnici o Anně a ostrově Sušenka. Vím, že už nemám moc času, tak se tam vydávám znova s vidinou, že mi opět štěstí cvrnkne do nosu.

Na ostrově nacházím panství, kam se ale nemohu dostat, jelikož ochranka po mně chce nějaké tajné heslo. Z nedostatku dalšího alkoholu si jen povzdychnu: *Potřebuji další rum...* Ochranka na mě nechápavě zírá a vpouští mě dál. Koho by napadlo, že *rum* je tajné heslo pro vstup... Jako uvítání mi přistane do ruky podivná flaška rumu dodávající údajně sílu v boji. Uvědomím si, že je to další tajemství, které jsem měl najít.

Nakonec nacházím dům Anny, který je ale opuštěný. Vidím jen pohozenou dřevěnou nohu a vzpomínám na dopis. Prohlížím si ji, a znenadání se promění na bájný zapomenutý meč, který je silnější, než všechny ostatní.

V tom se otevřou dveře a já spatřuji podruhé Černovouse. Jenže teď se něco změnilo. Našel jsem všechny věci potřebné k tomu, abych jej porazil...

# 2 Verze pro suchozemské psy

## 2.1 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`.

## 2.2 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.

## 2.3 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*.

## 2.4 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.

### 2.5 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*.

## 3 Závěr

Děkuji za zábavný a zajímavý projekt.