Projekt v predmete BIS

Dokumentácia

Adam Švenk (xsvenk00) **26.12.2021**

Úvod

V emaili som dostal privátny kľúč, s ktorým som sa pomocou SSH pripojil na vzdialený server na porte, ktorý mi taktiež prišiel emailom.

Pomocou príkazu `ip addr` som zistil IP adresu, ktorú predstavovala `192.168.10.194` s maskou podsiete `255.255.255.0`. V ďalšom kroku som si programom `nmap` a príkazom `sudo nmap -sn 192.168.10.194/24` vykonal ping scan všetkých aktívnych alebo zaujímavých hostiteľských staníc. Po vyfiltrovaní hostiteľských staníc, ktorých hostname bol vo formáte `xlogin00`, som dostal zoznam hostiteľských staníc s prislúchajúcimi IP adresami:

```
Nmap scan report for bda-boz.fit.vutbr.cz (192.168.10.1)
Nmap scan report for a6 (192.168.10.14)
Nmap scan report for antonin (192.168.10.44)
Nmap scan report for a3 (192.168.10.82)
Nmap scan report for a1 (192.168.10.100)
Nmap scan report for a5 (192.168.10.116)
Nmap scan report for a2 (192.168.10.119)
Nmap scan report for a4 (192.168.10.138)
Nmap scan report for sv6 (192.168.10.145)
Nmap scan report for sv1 (192.168.10.150)
Nmap scan report for sv2 (192.168.10.166)
Nmap scan report for sv3 (192.168.10.170)
Nmap scan report for sv4 (192.168.10.199)
```

Tajomstvá

Následne som si ešte pomocou príkazu `ls -a` zobrazil zoznam všetkých súborov a adresárov. Zaujal ma skrytý adresár `.ssh`, ktorého obsah som si taktiež zobrazil. V súbori `config` som našiel konfiguračné údaje, pomocou ktorých som objavil užívateľské meno a kľúč, pomocou ktorého sa s príkazom `ssh -i SV2 Trust@192.168.10.166` pripojil na stanicu `SV2`. Po pripojení na stanicu ma privítala uvítacia správa, vďaka ktorej som vedel, že som na dobrej ceste. Pomocou príkazu `find / -group Trust` som si zobrazil všetky súbory, ktoré upravoval používateľ `Trust`. Na konci celého výpisu ma zaujal adresár `/trash/`, ktorý by mohol obsahovať zaujímavé informácie. V uvedenom adresári som objavil súbor `crack_me.zip`. Nájdený `.ZIP` archív som si preniesol na lokálne zariadenie a pokúsil sa ho "odarchivovať" pomocou programu `unzip`. Zistil som však, že archív vyžaduje heslo. Podarilo sa mi zistiť, že v archíve sa nachádza súbor `geheimnis.txt`. Nakoľko som nemal žiadne informácie o tom, čo by mohlo predstavovať dané heslo, rozhodol som sa pokúsiť prelomiť daný archív pomocou metódy brute-force. Na tento účel som použil program `yazc`, dostupný pre linuxovú distribúciu Ubuntu. Z dôvodu, že som netušil, aké znaky môže obsahovať heslo a aká môže byť jeho dĺžka, som použil program s metódou brute-force a všetkými dostupnými znakmi. Maximálnu dĺžku som obmedzil na 10 znakov. Po pár sekundách som dostal heslo - `" / $"`, vďaka čomu sa sa dostal k súboru `geheimnis.txt`. Ten obsahoval tajomstvo:

"Tajemstvi E_25-12-16-45-02_0a20b617b9cf85373fa76b1c0d52d825afc07dcdba27f5aa3c4f47584f077a31"

Okrem tajomstva sa v ňom nachádzal aj ďalší text - "Fredek, next time please don't forget your default SSH credentials for the SV1 (192.168.10.150) server". Ešte raz som si pozrel archív `crack_me.zip` na stanici `SV2`, a zistil som, že bol vytvorený používateľom `iperesini`. Zobrazil som si pomocou príkazu `find / -group iperesini` všetky súbory, ktoré boli upravené používateľom `iperesini`, a na konci výpisu som našiel súbor s názvom `was_es_ist` v adresári `/mnt/root/`. Podľa prekladača som zistil, že výraz "was es ist" pochádza z nemeckého jazyka a v preklade namená "what is it". Nakoľko som z prechádzajúceho získaného tajomstva vedel, že jeho počet znakov je 91 a zašifrovaný reťazec má počet znakov 122, s najväčšou pravdepodobnosťou sa nebude jednať o jednoduchú substitučnú šifru. Napadlo ma, či nemôže byť náhodou tajomstvo zakódované pomocou schémy base64. Skúsil tom dekódovať reťazec zo súboru `was_es_ist`, no nedostal som žiadny rozumný výsledok. Pre istotu som však skúsil zakódovať pomocou schémy base64 už získané tajomstvo a zistil som, že takto zakódované tajomstvo má 122 znakov. Vďaka tomu som došiel k domnienke, že nájdený reťazec môže byť zakódovaný pomocou base64, avšak jednotlivé znaky nie sú v správnom poradí. Už na prechádzajúcom tajomstve som prišiel na to, že obsah tajomstva sa v periodických intervaloch mení. Vedel som, že napríklad slovo "Tajemstvi" sa bude nachádzať v každom zašifrovanom reťazci s predpokladom, že je v rovnakej podobe. Taktiež aj údaj dátumovej pečiatky bude v prípade jedného dňa rovnaký, no hodinová pečiatka bude rozdielna. Niekoľkokrát som si teda zobrazil obsah súboru `was_es_ist` a spozoroval som, že moje predpoklady sú pravdivé, a teda, že sa v jednotlivých reťazcoch vyskytujú časti, ktoré sú v jednotlivých periódach rovnaké, a aj také, ktoré sú rozdielne. Zistil som, že identických, neopakujúcich sa reťazcov je presne 7. Neskôr, keď som mal viacero tajomstiev, som si dve vybral, zakódoval som ich pomocou schémy base64 a zistil som, že prvých 14 znakov je identických. Spojil som si uvedenú znalosť o počte periodicky identických reťazcov a prišiel som na to, že prvé písmená identických reťazcov za sebou odpovedajú prvej polovici 14 znakového reťazca. Z toho som prišiel na to, že s najväčšou pravdepodobnosť sa jedná o šifru, ktorá postupne vyberá znaky z identických slov a ukladá ich za sebou. Následne som zistil, že k takto vytvoreným reťazcom je potrebné doplniť znaky z meniacich sa reťazcov a správne ich usporiadať. Priradil som teda za každú identickú, neopakujúcu sa časť, takú časť, ktorý sa periodicky menila. Postupne som odoberal prvé písmenká z takto vytvorených 7 "zásobníkov" písmenok a pohyboval sa v nich tak, že keď som prišiel na posledný, tak som zmenil smer, a vrátil sa na počiatočný, a rovnako som sa otočil na počiatočnom. Takto vytvorený reťazec som následne dekódoval pomocou schémy base64 a dostal som ďalšie tajomstvo:

"Tajemstvi F_26-12-16-15-01_bd2dfe3e4bad342203f34a70d4be68e33804489828cd7b5123ba8b0d436206d1"

Pomocou programu `nmap` som vykonal sken otvorených portov na stanici číslo `192.168.10.170`. Zistil som, že na stanici `192.168.10.170` sú otvorené porty `22 (ssh)`, `80 (http)` a `3306 (mysql)`. S programom `curl` a príkazom `curl http://192.168.10.170` som sa dostal k webovej stránke, ktorá vyžadovala zadanie použíateľského mena (Login) a hesla (Password). Domnieval som sa, že vďaka otvorenému portu `3306` a službe `mysql` môžem použiť jednoduchý SQL Injection. Použil som teda reťazec `"" or ""=""` ako používateľské meno a heslo, žiaľ, neúspešné. Skúsil som následne zameniť znaky `""" za "'"`, čiže `"' or ''='"`, vďaka čomu som dostal odpoveď a ďalšie tajomstvo:

"Tajemstvi B_25-12-18-15-01_51bd076f6de6f3956eecefda383d99a638238e4c4c4be01df11cc8603f50152f"

Na uvedenej webovej stránke sa na vrchu nachádzala poznámka s textom: "Admin, please care for absconditum directory". Pomocou prekladu som zistil, že slovo

"absconditum" je z latinského jazyka a po anglicky znamená "hidden". Skúsil som teda vykonať príkaz `curl http://192.168.10.170/hidden/`. Dostal som odpoveď - webovú stránku, ktorá okrem iného obsahu taktiež obsahovala odkaz na súbor `secret.php`. Predpokladal som teda, že sa daný súbor nachádza v adresári `hidden`. Skúsil som teda vykonať príkaz `curl http://192.168.10.170/hidden/secret.php`, vďaka čomu som dostal odpoveď a ďalšie tajomstvo:

"Tajemstvi C_25-12-18-15-01_88bdf2ec1614b2732e2421207706f9df94db00e8e56f408ff3210539c31135a6"

Taktiež ma zaujal aj text na spodnej strane webovej stránky - "Please for admin log in, follow this link". Rozhodol som sa teda sledovať uvedený odkaz `admin.html` a dostal som sa k ďalšej webovej stránke, po ktorej analýze som zistil, že sa na stránke nachádza odkaz na súbor, ktorý obsahuje zdrojový kód programu v jazyku Java Script. Tento zdrojový kód som následne taktiež analyzoval a zisitl som, že sa s najväčšou pravdepodobnosťou jedná o skript, ktorý vráti požadované tajomstvo. Dôležitý prvok predstavovala funkcia `checkCode`. Predpokladal som, že požadovaný prístupový kód bude s najväčšou pravdepodobnosťou tvorený numerickými znakmi, takže som si napísal jednoduchú funkciu, ktorá metódou brute-force testovala funkciu, aby vrátila `true`. Vďaka tejto funkcii sa mi podarilo nájsť požadovaný prístupový kód. S pomocou funkcie `sha256`, ktorej zdrojový kód bol taktiež dostupný na cieľovej stanici, sa mi podarilo získať tajomstvo:

"Tajemstvi A_26-12-12-45-01_895996010255c2d171d37d5a343ba22997953b927f4deae1ff8d35d6cc2c106b"

Pomocou programu `nmap` a príkazu `sudo nmap 192.168.10.199` som zistil, že sa na stanici nachádza otvorený port `21 (ftp)`. Skúsil som teda pomocou programu `curl` a príkazu `curl ftp://192.168.10.199` získať čo najviac informácii. Zistil som, že sa na stanici nachádza adresár `pub`. Pokúsil som sa teda pomocou príkazu `curl ftp://192.168.10.199/pub/` získať jeho obsah. Z odpovede som sa dozvedel, že sa v danom adresári nachádzajú štyri súbory: `data.txt`, `image1.jpg`, `image2.jpg` a `secret.asc`. Obsah adresáru som si presunul na lokálne zariadenie, kde som so súbormi pracoval. Súbor `data.txt` mi nebol nápomocný a v súbore `secret.asc` sa nachádzala zašifrovaná PGP správa. Zaujali ma však jednotlivé obrázky, ktoré na prvý pohľad vyzerajú identicky. Napadlo mi, že v jednotlivých obrázkoch môžu byť pomocou steganografie zašifrované zaujímavé informácie. Rozhodol som sa použiť viacero online nástrojov, ktoré poskytujú steganografické dekódovanie. Pomocou online nástroja `Stegosaurus` sa mi podarilo dekódovať z obrázku `image1.jpg` ďalšie tajomstvo:

"Tajemstvi J_25-12-19-15-01_42c5b84b01fb7c6ddeabffad4493ec72248856c79a197f0b610897a3a8fe9dff"

Z nápovedy, ktorá sa nachádzala v Tajomstve E, som zistil, že používateľské meno, pomocou ktorého sa môžem pripojiť na stanicu `SV1 (192.168.10.150)`, je `Fredek`. Najprv som pomocou príkazu `sudo nmap 192.168.10.150` zistil, že sa na cieľovej stanici nachádzajú otvorené porty `22 (ssh)` a `2049 (nfs)`. Predpokladal som, že na cieľovej stanici beží NFS server. Najprv som však potreboval zistiť cestu k adresáru, ku ktorému je možné sa pomocou NFS pripojiť. Z manuálu programu `nmap` som zistil, že integruje skript, ktorý umožňuje spustenie útoku typu brute-force s cieľom uhádnuť prihlasovacie SSH heslo. Upravil som súbor knižnice `unpwdb`, ktorá obsahuje najčastejšie vyskytujúce sa uživateľské mená a heslá, konkrétne súbor `passwords.lst` tak, že obsahoval iba jediné používateľské meno - `Fredek`. Následne som vykonal príkaz `nmap 192.168.10.150 -p 22 -Pn --script ssh-brute`, pomocou ktorého som dostal

prihlasovacie heslo - `iloveyou`. S týmto heslom sa mi pomocou programu `SSH` úspešne podarilo pripojiť na cieľovú stanicu. Následne som zo súboru `/etc/exports` zistil, že adresár, ktorý chcem pripojiť pomocou NFS je `/home/shared_dir`. Na to, aby som si mohol pripojiť vzdialený adresár pomocou služby NFS, som si doinštaloval pomocou programu `rpm` požadované balíčky a ich príslušné závislosti. Následne sa mi úspešne podarilo pripojiť vzdialený NFS adresár. Pri pokuse o zmenu aktuálneho adresáru do pripojeného NFS adresáru mi tento pokus bol zamietnutý s textom `Permission denied`. Tento problém som vyriešil príkazom `sudo su`. Následne sa mi úspešne podarilo zobraziť obrah NFS adresára. Ako prvý upútal moju pozornosť súbor `secret`, ktorý obsahoval ďalšie tajomstvo:

"Tajemstvi H_25-12-22-45-01_7dc92e343f80959c7de6009345d3aafcc3d7c8dc867a09b793241d24ee959752"

Okrem toho sa v adresári nachádzal súbor "private.key", ktorý obsahoval PGP súkromný kľúč. Na konci tohoto súboru sa nachádzal text "passphrase is "123". Spomenul som si, že na stanici "192.168.10.199" som našiel zašifrovanú PGP správu. Pomocou dekóderu a dostupnej zašifrovanej správy, súkromného kľúča a znalosti prístupovej správy som dekódoval PGP správu a získal ďalšie tajomstvo:

"Tajemstvi G_25-12-19-15-01_abb737b8d111b9d6502891e316105aa439a7d210e96690554cfdc6e1471fb11d"

Už z prechádzajúcich tajomstiev som si všimol, že prvá časť tajomstva s najväčšou pravdepodobnosťou predstavuje dátum. Pomocou príkazu `ls -l` som si zobrazil okrem iného aj dátum poslednej úpravy súborov v pripojenom NFS adresári a zistil som, že dátum úpravy súboru `secret` je výrazne odlišný od dátumu ostatných súborov. Všimol som si však, že okrem tohoto súboru má odlišný dátum úpravy od väčšiny aj súbor `112302.jpg`. Pomocou online nástroja som zistil, že tento súbor obsahuje metadáta vo formáte EXIF. Tieto metadáta som si zobrazil a našiel som reťazec `Ahqltzacp P_25-12-23-15-01_k10k32i1lj80ijjj78i7h926mih14281526157lk4868l03jm h035231m7i812k1`, ktorého formát a počet znakov odpovedá prechádzajúcim nájdeným tajomstvám. Predpokladal som, že reťazec `Ahqltzacp` odpovedá po dekódovaní reťazcu `Tajemstvi`. Nakoľko počet znakov zašifrovaného reťazca a tajomstva bol identický, rozhodol som sa vyskúšať Cézarovu šifru, nakoľko sa jedná o jednoduchú a intuitívnu šifru. Nepoznal som však počet posunutí, takže som musel vyskúšať všetky. Pri 7. posunutí som po dekódovaní dostal slovo `Tajemstvi`, vďaka čomu som následne mohol dekódovať celý reťazec a dostal som tajomstvo:

"Tajemstvi I_25-12-23-15-01_d10d32b1ec80bccc78b7a926fba14281526157ed4868e03cfa035231f7b812d1"

Ďalej som vďaka programu `nmap` a príkazu `sudo nmap 192.168.10.145` zistil, že aj na stanici s uvedenou IP adresou sa nachádzajú otvorené porty `22 (ssh)` a `5000 (upnp)`, pričom najmä port `5000` môže byť zaujímavý. Po obsiahlej analýze som dospel k tomu, že sa na cieľovej stanici nachádza obraz pre program `docker`. Tento obraz som si následne uložil na svoju stanicu. Obraz som spustil, no nenašiel som na ňom nič zaujímavé. Následne som pomocou príkazu `docker inspect` pokúsil o získanie čo dodatočných informácii o danom obraze. Zaujal ma riadok `rm -rf /tmp/secret.txt`, ktorý hovorí o tom, že v danom obraze pravdepodobne existuje súbor `/tmp/secret.txt`. Pokúsil som sa obraz spustiť a nájsť daný súbor, žiaľ, neúspešne. Predpokladal som, že sa uvedený príkaz `rm -rf /tmp/secret.txt` vykoná hneď po spustení obrazu, a teda sa súbor `/tmp/secret.txt` odstráni. Napadlo mi, či by nebolo možné upraviť daný obraz tak, aby sa nevykonal príkaz `rm -rf /tmp/secret.txt`. Toto sa mi žiaľ vykonať nepodarilo.

Prišiel som však s alternatívnym riešením, ktoré predstavovalo možnosť pripojiť sa k súborovému systému daného obrazu, a vyhľadať v ňom požadovaný súbor. Presunul som sa do adresára `/var/lib/docker`, v ktorom som spustil príkaz `find . -name secret.txt`, pomocou ktorého som sa dostal k tajomstvu:

"Tajemstvi D_26-12-10-15-01_abb737b8d111b9d6502891e316105aa439a7d210e96690554cfdc6e1471fb11d"