

Bezpečnost informačních systémů (BIS)

dokumentace k semestrálnímu projektu

David Hudák (xhudak03)

26. listopadu 2023

1 Úvodní přístup do systému

Po zadání příkazů ze zadání pro přístup do systému:

```
• ssh -i klic.txt -p 65097 bis.fit.vutbr.cz .
```

jsem se dostal na server, kde téměř nic nebylo. Po kratším průzkumu různých složek došlo ke zjištění, že nemám na nic pořádně práva, a to ani na zmapování sítě. Nefungoval ani pokus `grep -r "Tajemstvi" \.`. Naštěstí se mi podařilo najít zvláštní soubor `config` v podsložce domácí složky `home`. Všiml jsem si, že se tam nachází číslo jakéhosi serveru `192.168.122.60` a jméno `jimmy`. V téže složce bylo též něco, co připomínalo klíč, se kterým jsme se připojil k původní síti, tak jsem zkusil `ssh -i id_ecdsa jimmy@192.168.122.60` a překvapivě to fungovalo. Byl jsem konečně někde, kde to aspoň trochu vypadalo.

2 Hledání tajemství

V této sekci popíšu svůj postup v získávání tajemství. Tajemství nemusí být seřazena postupně od A po Z, nýbrž jsou seřazena tak, jak jsem na ně postupně přicházel.

2.1 Tajemství A

Opět jsem zkusil nejzoufalejší pokus vůbec `grep -r "Tajemstvi" \.`. Toto shořelo na tom, že ve složce `proc` existuje opravdu mnoho souborů (zjevně odkazující na spuštěné procesy), a tak jsem k tomu přistoupil systematictěji a začal hledat po složkách. Když už jsem prošel asi 20 různých složek, úsilí se vyplatilo a já našel své první tajemství:

```
• Tajemstvi_A_ec9a103caa5f7a2266a0d6579c8b8b40e56119a950952e1cdef4b5a8f2c78015
```

Nachází se v souboru `/trash/.3789_2023_09_07.invoice`.

2.2 Připojení na Boba

V domovském adresáři jsem narazil na zajímavý soubor `.bash_history`, který mi po příkazu `cat` vyhodil nejspíše posloupnost posledních volaných příkazů, tak jsem z něj začal čerpat informace. Vykopíroval jsem si soubor k sobě a někdo se nejspíš snažil připojit na nějakého `bbbooba` (`ssh bbbooba@192.168.122.1`) a používal poměrně žertovné heslo `Mega-SuperHeslo123NikdoHoNezjistí`. Této informace jsem se pokusil využít a zkoušel jsem taky. Původní zadání, žel, nefungovalo. Tak jsem se koukal dál a vyzkoušel pár dalších kombinací. O pár řádků dole ve zmíněné historii jsem si všiml, že někdo použil poněkud méně „prsaté“ `ssh bob@192.168.122.216`, což následně se zmíněným heslem fungovalo. Připojil jsem se na další server! Ještěže někdo nepoužívá příkaz `history -c`.

2.3 Tajemství C

Když jsem byl na Bobovi, tak jsem vyzkoušel opět velmi kreativní

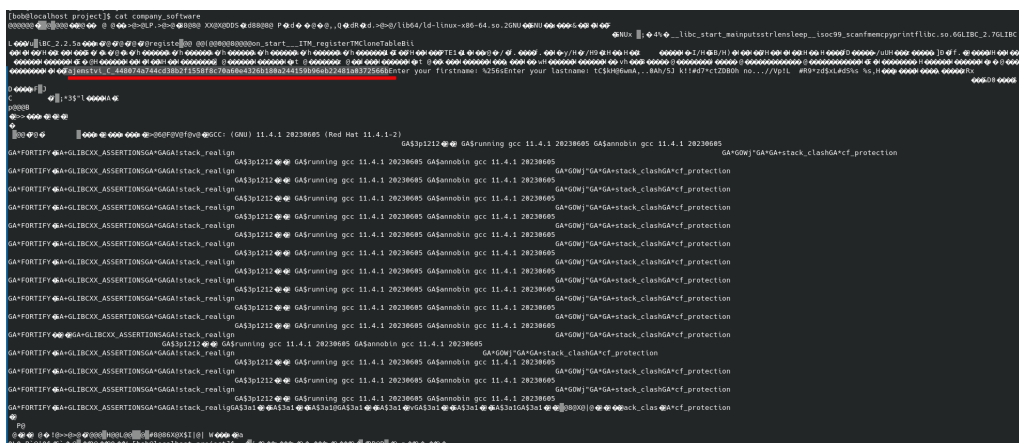
- `[bob@localhost ~]$ grep -r "Tajemstvi" .`

což mi vypsallo poněkud zvláštní odpověď:

- Binární soubor `./project/company_software` odpovídá

To mě na chvíli zmátlo a ignoroval jsem to. Nakonec jsem soubor vytiskl s pomocí příkazu `cat`, což na mě vyplivlo kupu znaků, přemýšlel jsem, kterou šifrovací metodu tam asi použili. Šifrovací metoda nakonec byla spíš testem zraku, protože až po chvíli jsem si všiml velmi potutelně ukrytého tajemství (viz obrázek 1):

- `Tajemstvi_C_448074a744cd38b2f1558f8c70a60e4326b180a244159b96eb22481a0372566b`



Obrázek 1: Ukázka vizuálně dobře skrytého tajemství

2.4 Zjištění struktury sítě

Na základě příkazu `ifconfig` jsem zjistil, že síťová maska je 255.255.255.0 (24-bitová maska), což znamená, tudíž lokální zařízení budou od 192.168.122.0 až 192.168.122.254 (255 je broadcastová adresa). S pomocí příkazu `nmap` jsem tak proskenoval síť s pomocí příkazu `nmap 192.168.122.0-254`. Výsledek jsem si s pomocí `scp` poslal na Merlina, z Merlina pak přes FileZilla k sobě. Soubor s výsledkem jsem prozkoumal.

Po první analýze mě překvapilo, když jsem zahlédl login svého kamaráda z FITu a následně i spoustu dalších loginů. Jestli tomu rozumím správně, pak se jedná o studentské servery v síti, na kterých předpokládám, že budou maximálně jejich tajemství. Vyzkoušel jsem se tedy připojit na svůj login. Nelze. Tak nic. Zajímavé nejspíš budou ty, které žádné označení nemají. Soubor s výsledky jsem tak promazal od serverů, které mají nějaký login a nechal si jen ty bez nich.

2.5 Tajemství H

Na základě výpisu naslouchajících zařízení v síti jsem zjistil, že na adrese 192.168.122.134 je spuštěna služba `http`, tak jsem zkusil použít příkaz `curl`. Ten mi vypsal nějaký `html` soubor, ve kterém bylo zajímavé, že se na něm nachází dva odkazy. Vyzkoušel jsem první z nich, opět s pomocí stejného příkazu:

- `192.168.122.134/user.php?id=0`

Vypsáno bylo něco jako defaultní profil. Tak jsem zkusil použít další id, pak jsem zkusil dát řetězec admin apod. Nic moc nefungovalo, ale došlo mi, že se nejspíš jedná o nějaký SQL dotaz, který bude potřeba injectnout. Zkoušel jsem tak různé formáty, kde jsem například místo `id=0` dal `id=True`. Zkusil jsem tak více prozkoumat, co se na daném serveru nachází a ve složce Nakonec jsem došel metodou pokus omyl k formátu `id=1+or+1`, který mi získal další tajemství, H.

2.6 Tajemství G

Na tajemství G jsem narazil náhodou poté, co jsem zkoušel na daném serveru použít přístup k adresáři admin (fungoval). Zkoušel jsem tak různá klíčová slova jako „tajemství“, „skryte“ apod. Nakonec vyšlo slovo secret a zobrazil se mi ukradený článek z Wikipedie o závodu gumových kačenek. A taky další tajemství, tajemství G, bylo na světě.

2.7 Tajemství F

V seznamu serverů získaných s pomocí nmapu se nachází i server 192.168.122.249, který má spuštěnou službu git na portu 9418. Zkusil jsem tedy použít git clone na tento server, ale to nefungovalo. Inspiroval jsem se tedy z tajemství G a vyzkoušel získat složku secret. To už fungovalo. Přesto jsem původně nenalezl žádné tajemství. Tak jsem zkusil zkompileovat a párkrát spustit main.c, ale to nebylo k ničemu. Následně jsem s pomocí ls -a vyzkoušel, jestli se nestáhl nějaký skrytý soubor. Kromě .git se nestáhl nic navíc. Zkusil jsem tak tuto složku prozkoumat, ale krom souborů s příponou pck a idx jsem nic nenašel. Nakonec jsem se pokusil zjistit, jestli třeba někdo nenechal heslo v předchozí verzi repozitáře, a proto jsem párkrát poskočil do minulosti s pomocí:

- `git checkout HEAD^`

To fungovalo. V main.c se objevilo vícero zajímavých věcí, ale především pak tajemství F.

2.8 Hinty z tajemství F

- Jméno psa: buster, misbebeslosamocontodomicorazon
- Pin k debetní kartě: 4242
- Podezřelé číslo v bufferu: 45197
- Alternativní heslo k bobovi: iloveyou
- FTP heslo bylo třeba změnit: „commonly used password“ nebylo „safe password“
- Bylo potřeba opravit uploadování obrázků: Johnovi se povedlo uploadnout php skript.
- V TODO listu bylo ještě za úkol smazat stará data z PCAP listu.

2.9 Tajemství D

Pro zjištění tajemství bylo potřeba se nabourat na ftp server na adrese 192.168.122.164. Zde jsem nevolil nějakou chytrou strategii, prostě jsem tipoval nejprve login. Začal jsem postupně: john, John, bob, Bob, jimmy a admin. Admin se chytl. Z předchozího tajemství jsem věděl, že někdo pes se jmenoval buster, tak jsem to vyzkoušel. Fungovalo to. Ještěže používám taky takové heslo... Cože? Prokousal jsem se nejprve do složky ftp a stáhl si obrázky 2 kačenek, 1 pečené kachny s nudlemi a soubor secret.txt. Obsah souboru txt byl následující:

- Dktowcdfs_N_k9m21695o7opnkpn2mmn8opo67706
o82p09n9196nk297117mkoo0k6l8nn218n5

První část textu je zjevně Tajemství X_, tak jsem se pustil do dešifrování na papíru. To mi moc nešlo, tak jsem použil řešení <https://cryptii.com/pipes/vigenere-cipher> a zkoušel různě natipovat klíče tak, aby to vycházelo na to Tajemství. Nakonec jsem zjistil, že to není ani Vigenerova šifra, ale jen vylepšená varianta Caesarovy, kde se posouvá o písmeno k (posun o 10).

Vyšlo mi, že se jedná o tajemství D, a tak moje cesta zase pokročila. Velmi oceňuji vtip v posloupnosti dvou gumových kačenek a jedné pečené.

2.10 Tajemství J

Z další analýzy dostupných serverů jsem si všiml, že existuje server: 192.168.122.21, který na portu 2049 má službu nfs, která slouží pro sdílené složky. Zkusil jsem tak zadat příkaz pro namountování mé složky s jejich pomocí příkazu `nfs` z login uzlu, ale ten je zjevně blokován. Tak jsem se pokusil přes jimmyho. Ten ale nemá nainstalované nfs. Tak jsem po poměrně dlouhém samostudiu přišel na dlouhý příkaz:

- `ssh -i /home/student/.ssh/id_ecdsa`
– `-L 2049:192.168.122.21:2049 jimmy@192.168.122.60 -N`

který v jednom z terminálů vytvoří tunel mezi login uzlem a nfs uzlem. Následně jsem ve druhém terminálu zadal:

- `sudo mount -t nfs localhost: /mnt/nfs_share`

který by měl namountovat právě sdílenou složku z kořenového adresáře nfs serveru. To fungovalo a získal jsem cenná data ve formě adresáře se spoustou souborů. Tyto soubory jsem si postupně pracně přenesl přes scp k sobě lokálně. Nejprve jsem na každý soubor vyzkoušel nástroj zvaný stegdetect. Nic. Následně jsem zkusil projít soubory `public.key` a `private.key`. V těch jsem pouze našel text „John Seanah (My very SECRET key for my important SECRET stuff)“, což se možná někdy bude hodit. Nakonec jsem vyzkoušel pár nástrojů na steganografii (převážně online), například <https://www.aperisolve.com/>, což taky nepomohlo. Nakonec jsem narazil na nástroj `strings`, který převádí obrázky na řetězce. Přesněji jsem aplikoval:

- `strings *|grep "Taje"`

Poměrně nečekaně, tajemství J bylo na světě.

2.11 Tajemství I

Tajemství I mi dalo asi nejvíce zabrat. U serveru s Gitem byla nápověda, že se Johnovi povedlo uploadovat php skript přes login na http serveru. To mi moc nedávalo smysl, tak jsem nejdřív zkusil zaslat php skript, který jenom dělá `echo 10;`, což ale nefungovalo, protože to nebyl obrázek. Pak jsem zkusil zastat různé normální obrázky. Pak jsem pojmenoval obrázek `echo 10;.jpeg` a podobně. Stále nic. Nakonec jsem pojmenoval obrázek příponou `.php` a tajemství I bylo po explozi serveru na světě.

Formát, jakým jsem se dotazoval:

- `curl -X POST -F "image_file=@duck-3.php"`
– `192.168.122.134/upload/upload_file.php`

2.12 Tajemství B

Na Bobovi se nachází soubor `mail.exported.txt`. S tím jsem se již dříve docela trápil, protože mi nefungovalo kopírování přes `scp` na Merlina (nejspíš nedostatek práv). Jediné, co jsem uměl, bylo `ctrl+c` a `ctrl+v`, které ale na binární soubor funguje poněkud blbě (některé znaky jsou prostě nezobrazitelné). Po nějaké době jsem přišel na to, že nejjednodušší bude převést soubor do `base64`, který je na serveru nainstalován, překopírovat ho s `ctrl+c` a vykopírovat ho k sobě (takto se, pokud je mi dobře známo, pořád kódují maily). Pak byl úkol dvě, a to použít vhodný dešifrovací algoritmus. Pak jsem si vzpomněl, že jsem kdysi narazil na nfs serveru na soubor `private.key`, který přímo říkal, že má tajný klíč k nějakému tajemství.

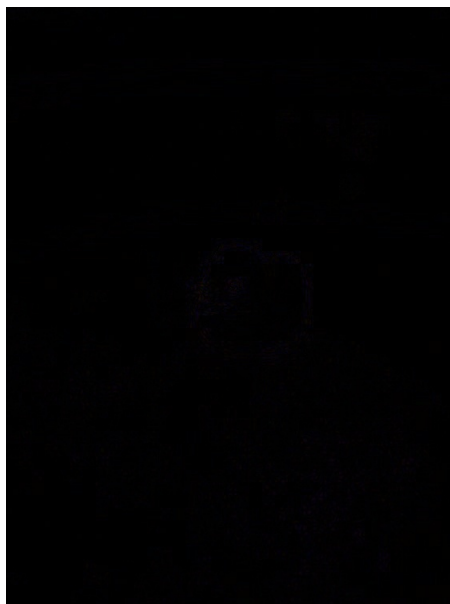
Po nějakém hledání, čím by to mohlo být zašifrováno, jsem došel k PGP (Pretty Good Privacy), které se používalo například při šifrování zpráv na dark webu. Tak jsem použil implementaci PGP u sebe doma (`gpg`). Postupně jsem zadal, nejprve pro import klíče, následně pro dešifrování, následující příkazy:

- `gpg --import private.key`
- `gpg --decrypt mail_kopie.txt`

Tajemství B bylo na světě.

2.13 Tajemství E

Na tajemství E jsem narazil až jako úplně poslední na základě nástroje <https://www.aperisolve.com>, který při použití metody Outguess na `duck-1.jpg`¹ našel poslední tajemství. Ta spočívá v principu hledání tajné zprávy na základě zakódování na místech nejméně významných bitů (LSB). Takto zašifrovaný soubor je následně ještě zkontrolován na základě DCT (diskrétní cosinové transformace).



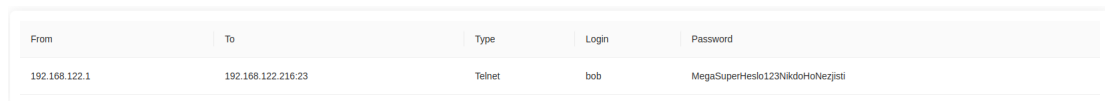
Obrázek 2: Porovnání dvou kačenek

Jako hint k tomuto tajemství sloužilo porovnání obrázků kačenky 1 a kačenky 2 na úrovni pixelů, viz obrázek 2. To možná nemusí být v dokumentaci vidět, každopádně při zazoomování lze

¹Soubory s kačenkami se nacházely na FTP serveru, stejně jako tajemství G.

spatřit, že se na mnohých místech lehce liší (barva není čistě černá). Kdo je fajnšmekr, ten mohl ještě porovnat dva obrázky s pomocí hashů a zjistil, že jsou jiné, tj. alespoň jeden obrázek musel být modifikován. Na druhou stranu, tímto porovnáním se dalo dobře ukázat, že se dva obrázky liší jenom velmi málo, tj. musela zde proběhnout úprava pouze na nejméně významných bitech.

3 Doplnění k řešení



From	To	Type	Login	Password
192.168.122.1	192.168.122.216:23	Telnet	bob	MegaSuperHeslo123NikdoHoNezjistí

Obrázek 3: Screenshot z aplikace pro analýzu pcapů.

Vzhledem k tomu, že přihlašovací údaje na boba jsem našel v historii příkazové řádky po nějakém studentovi, rozhodl jsem se dohledat i „legitimní“ způsob řešení. Ten na základě nápovědy z Git serveru nebyl moc obtížný, bylo potřeba pouze někde najít nějaký pcap soubor. To se mi poměrně rychle i skutečně podařilo najít v adresáři `/log` na jimmym pod názvem `old_traffic.pcapng`. K jeho analýze jsem pak použil nástroj <https://apackets.com/>, který mi vypsál nabídku toho, co v daném pcapu našel. Pod službou telnet našel i zajímavé Credentials (přihlašovací údaje), viz obrázek 3.

4 Seznam nalezených tajemství

- Tajemstvi_A_ec9a103caa5f7a2266a0d6579c8b8b40e56119a950952e1cdef4b5a8f2c78015
- Tajemstvi_B_373c593a4c00bf401e1bcf4fa2ba16e98ba5af8ec1f54c63f19f092ec6958972
- Tajemstvi_C_448074a744cd38b2f1558f8c70a60e4326b180a244159b96eb22481a0372566b
- Tajemstvi_D_a9c21695e7efdafd2ccd8efe67706e82f09d9196da297117caee0a6b8dd218d5
- Tajemstvi_E_cb474912685a598d9325bd4d4e3b88015e006582297cb0aa6802cb001302980c
- Tajemstvi_F_fbe448154dd4d0b39772f077b4a4722be704193127c52902778ceebb27d763ee
- Tajemstvi_G_06f92e877f98d74c5de355cec290dd6c4bdbca3bdc12d5cda1ca33f6768afad6
- Tajemstvi_H_7a3e2b0e8db3288d7410ec4836af6ac65525ce897870bf0f8c4dc64909ae311c
- Tajemstvi_I_fa393edd4085614eeb16c825d0af37afe21efce8dc07f6dc77cae5d222b3171c
- Tajemstvi_J_58ee6793ed16f63e073bb8242c26e58c8439e461cfd65fa8054dfffb2b26a369f

5 Závěr

Úspěšně se povedlo najít všech 10 tajemství.