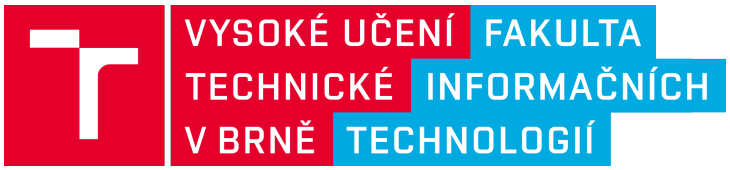

Bezpečnost informačních systémů (BIS)

Projekt – The FITfather

Jan Krejčí (xkrejc70)

19. prosince 2023

1 Schéma vnitřní sítě

Na serveru *bis.fit.vutbr.cz* byla příkazem `ip route | grep "src"| awk '{print $1}' | head -n 1` získána IP adresa výchozí brány: **192.168.122.0/24**. Příkazem `nmap -p- 192.168.122.0/24` byly skenovány porty na všech zařízeních v celé lokální síti. Celkem bylo nalezeno 11 (nestudentských) IP adres, na kterých byly pomocí příkazu `sudo nmap -sS -sV IP_address` nalezeny následující služby *(ip_ adresa: tcp_ port služba)*:

- 192.168.122.21: 22 ssh, 111 rpcbind, 2049 nfs
- 192.168.122.27: 22 ssh, 111 rpcbind
- 192.168.122.38: 22 ssh, 111 rpcbind
- 192.168.122.43: 22 ssh, 111 rpcbind
- 192.168.122.60: 22 ssh, 111 rpcbind
- 192.168.122.84: 22 ssh, 111 rpcbind
- 192.168.122.131: 22 ssh, 111 rpcbind
- 192.168.122.134: 22 ssh, 80 Apache http 2.4.6 ((CentOS) PHP/5.4.16)
- 192.168.122.164: 21 vsftpd 3.0.2, 22 ssh
- 192.168.122.216: 22 ssh, 111 rpcbind
- 192.168.122.249: 22 ssh, 9418 git

2 Postup nalezení tajemství

V této sekci jsou popsány jednotlivé servery, jejich běžící služby včetně jejich zranitelností a postup úspěšných i neúspěšných pokusů ve snaze nalezení tajemství.

2.1 192.168.122.21 – NFS

Na serveru 192.168.122.21 běží služba nfs. Příkazy `showmount -e 192.168.122.21` a `nmap -sV 192.168.122.21 --script=nfs-ls` bylo zjištěno, že */shared* je exportovaný adresář a je přístupný počítačům v podsíti 192.168.122.*. Takže typická slabina nfs (přidání veřejného klíče do seznamu autorizovaných klíčů ve složce .ssh, což by umožnilo připojení prostřednictvím SSH k serveru) se zde využít nedala.

Později stejný příkaz `nmap -sV 192.168.122.21 --script=nfs-ls` spuštěn na S3 odhalil, že nfs exportuje i několik obrázků a veřejný klíč, které mají povelení čtení. Na S3 však nešlo provádět mountování z důvodu neznámého root přístupu. Na login uzlu tak byl vytvořen SSH tunel na server S3 příkazem `ssh -L 2049:192.168.122.21:2049 -N -f -l jimmy -i  /.ssh/id_ecdsa 192.168.122.60`. Po vytvoření SSH tunelu byl proveden příkaz pro mountování `sudo mount -t nfs -o port=2049 127.0.0.1: /dir/`. Mountování se povedlo a v adresáři *dir/shared* se kromě obrázků nacházel i privátní a veřejný klíč k tajemství uživatele Johna Seanah. Nad obrázky byl spuštěn příkaz `grep -H -i "tajemstvi".shared*.jpg`, který našel shodu u obrázku *pexels-pixabay-417273.jpg*. Pomocí nástroje ExifTool bylo v jeho komentáři nalezeno **tajemství J**.

2.1.1 Neúspěšné pokusy

- Nalezený privátní klíč byl vyzkoušen při připojování na ssh ostatních serverů.
- Pomocí steganografických nástrojů byly prozkoumány i zbylé obrázky.

2.2 192.168.122.60 – S3

Při prohledávání studentského uzlu byl ve složce `/home/student/.ssh` nalezen soubor *config*, ve kterém byly přihlašovací údaje k tomuto serveru. Příkazem `ssh S3` se podařilo připojit. Při procházení adresářů bylo ve složce */trash* nalezeno **tajemství A**.

Dále byl nalezen soubor */log/old_ traffic.pcap*, který obsahoval poměrně rozsáhlou komunikaci. Při analýze v programu Wireshark byla nalezena relace přihlašování uživatele bob na server 192.168.122.216, který, jak bylo zjištěno dříve, jako jediný ze serverů, na kterých běží služba ssh, umožňoval zadání přihlašovacích údajů. Přihlášení uživatelem bob bylo úspěšné. K tomuhle souboru také vedla nápověda *'4) clean the old pcap traffic files'*.

2.2.1 Neúspěšné pokusy

- V */trash* složce se nachází obrázek i217642.jpeg, na němž byla provedana analýza, ale žádný z použitých nástrojů nic neodhalil.
- Ze studentského uzlu byl opět vytvořen ssh tunel a byl použit příkaz tcpdump pro odchytávání paketů na rozhraní ens3.
- Byl spuštěn příkaz `find . -type f -exec grep -q "Tajemstvi"  -print`, bez pozitivního výsledku.

2.3 Server 192.168.122.134 – HTTP

Na tomto serveru je služba http, na které běží jedoduché webové stránky s informacemi o uživatelých společnosti a nahráváním obrázků.

Informace o uživatelích je možné získat pomocí dotazu `curl http://192.168.122.134/user.php?id=X`, kde X je ID uživatele. ID je možné uhádnout nebo pokud aplikace využívá databázi nabízí se vyzkoušení SQL injection. První varianta přinesla informace o dalších třech uživatelích s ID 1, 2, 3. Druhá varianta vedla k zisku tajemství, a to přidáním podmínky, která je vždy pravdivá a vypíše tak všechny uživatele z databáze. Zbytek dotazu je ignorován zakomentováním: `curl http://192.168.122.134/user.php?id=0+OR+1+=+1--`. Tento dotaz vypsal dle očekávání všechny uživatele včetně admina, který obsahoval **tajemství H**.

Při jednom z pokusů uhádnout podstránky webu (*/secret*) se podařilo získat **tajemství G**. Bylo tak využito nedostatečného bezpečnostního opatření serveru, které by zabránilo neoprávněnému přístupu k "neveřejným"částem webu.

2.3.1 Neúspěšné pokusy

- Prohlížečem elinks v části */upload* bylo vyzkoušeno nahrát různé typy souborů, ale žádné jiné soubory než obrázky se nahrát nepodařilo. Vyzkoušeny byly jednotlivé tipy ze stránky File Upload od Hacktricks[1] jako například změna Content-Type, úvodní "magic bytes"či použití njrůznějších koncovek. Po získání nápovědy z git serveru *'2) fix image upload - John managed to upload php script???'* byly znovu důkladně vyzkoušeny php injections, ale bez úspěchu.
- Pokusy o uhodnutí dalších podstránek s běžným názvem jako (*/public, /log, /info, /api, /login* atd.) Byla objevena podstránka */images* a */icons*, obsahující mnoho souborů, ale žádná nápověda zde nalezena nebyla.
- Ve zdrojovém kódu domovské stránky získané příkazem `curl http://192.168.122.134/` byla nalezena sekce pro přihlášení admina. Je možné, že se přihlašovací údaje ověřují v databázi, byly vyzkoušeny běžné SQL injection obdobné tomu, které vedlo k zisku tajemství H, ale bez úspěchu.
- Jméno Jimmy Kim a popis 'I like dogs' v uživatelských datech mohou odkazovat na video[2] od Jimmy Kimmel Live, kde žena vyzradila heslo "Jameson2009", tedy jméno jejího psa a datum dokončení školy. Jméno psa *"misbebeslosamocontodomicorazon"* bylo později nalezeno na git serveru.

  Pokusy o přihlášení v admin sekci s různými kombinacemi těchto možných přihlašovacích údajů však nevedly k úspěchu. Byly vyzkoušeny také nejčastější slovníkové přihlašovací údaje.

[1] `https://book.hacktricks.xyz/pentesting-web/file-upload`
[2] `https://www.youtube.com/watch?v=opRMrEfAIiI&ab_channel=JimmyKimmelLive`

2.4 Server 192.168.122.164 – FTP

Na git serveru byla získána nápověda *'1) change my FTP password.. apparently "commonly used password"doesnt mean "safe password"*. Bylo vyzkoušeno, že heslo je dovoleno zadat pro uživatele admin a root. Nakonec fungovala kombinace *admin* a hesla *buster*, které bylo nalezeno v jednom z commitů na git serveru v proměnné *name_ of_ my_ dog*. Pomocí příkazu wget byla celá složka stažena na studentský uzel. Obrázky duck-1 a duck-2 obsahovaly zašifrované tajemství. To bylo dešifrované asi nejznámější a nejjednodušší Ceasarovou šifrou. Tím, že bylo známo, jak má výsledek vypadat nebylo dešifrování složité. Klíč délky 10 odhalil **tajemství D**. Obrázky obsahovaly také další hesla, která byla již dříve nalezena na git serveru.

2.4.1 Neúspěšné pokusy

- Příkazem nmap byla zjištěna verze vsftpd 3.0.2. Její zranitelnost[3] se však využít nepodařila.
- Příkazem `nmap -p 21 192.168.122.164 --script ftp-anon` bylo zjištěno, že anonymní přihlášení na tomto serveru povoleno není.
- Příkazem `nmap -p 21 -sS --script tftp-enum,ftp-vsftpd-backdoor 192.168.122.164` žádné další zranitelnosti zjistěny nebyly.
- Dále pokusy o připojení mimo kořenový adresář FTP serveru.
- Pokus o uhádnutí souboru `curl ftp://192.168.122.164/filename`.
- Stahování všech souborů pomocí `wget -m ftp://192.168.122.164`.

2.5 192.168.122.216 – BOB

V souboru ze záznamu síťové komunikace na serveru S3 byly nalezeny přihlašovací údaje k tomutu serveru. Na serveru byl příkazem `find . -type f -exec grep -q "Tajemstvi"{} \; -print` nalezen binární soubor *company_ software* ve složce */home/bob/project/*, který obsahoval **Tajemství C**.

V domovském adresáři boba se nacházel GPG šifrovaný soubor *mail.txt*. Soubor byl následujícími příkazy dešifrován pomocí privátního klíče Johna nalezeného na nfs serveru: `gpg --import private.key` a `gpg --output dec_mail.txt --decrypt mail.exported.txt`. Dešifrovaný soubor obsahoval **tajemství B**.

2.6 192.168.122.249 – GIT

Příkaz `git ls-remote git://192.168.122.249:9418/secret` zobrazil informace o referencích ve vzdáleném git repozitáři dostupném na adrese 192.168.122.249:9418. Zobrazila se hlavička a master větev repositáře *secret*. Příkazem `git clone git://192.168.122.249:9418/secret/` byl repositář naklnován na studentský uzel. Při procházení commitů bylo v komentáři souboru *main.c* nalezeno **tajemství F**. Dále bylo nalezeno přihlašovací jméno a heslo boba

V dalším commitu byly v souboru *TODO* nalezeny další nápovědy:

- 1) change my FTP password.. apparently "commonly used password"doesnt mean "safe password"
- 2) fix image upload - John managed to upload php script???
- 3) done
- 4) clean the old pcap traffic files

3 Závěr

Celkem bylo získáno 8 z 10 tajemství, jsou uvedena v přiloženém textovém souboru secrets.txt.

[3] `https://vuldb.com/?id.68991`