BIS projekt – dokumentace

19. prosince 2023

Ondřej Ondryáš
xondry02@stud.fit.vut.cz

I. Průzkum vstupního uzlu

Prvním krokem bylo prozkoumání prostředí uzlu, ke kterému jsme dostali přístup. Identifikoval jsem účet přihlášeného uživatele (student), hostname (xondry02), IPv4 adresu (192.168.122.175/24), operační systém (CentOS 7.4.1708). Stanice měla přiřazenu pouze link-local IPv6 adresu, IPv6 jsem tedy dále neuvažoval. Zjistil jsem, že účet student má povolení k použití příkazu `sudo su`, a může se tedy přepnout na účet superuživatele.

V domovském adresáři účtu student se nacházela konfigurace SSH klienta, která obsahovala předdefinovanou položku *S3*:

```
Host S3
  HostName 192.168.122.60
  User jimmy
  IdentityFile ~/.ssh/id_ecdsa
```

Uvedený soukromý klíč zde existoval také a byl pro přístup na stanici použitelný. Průzkum stanice S3 je popsán dále.

V souboru *authorized_keys* vstupního uzlu se nacházel záznam pouze pro klíč, který jsme k přístup dostali.

V domovském adresáři účtu root se žádný zajímavý obsah nenacházel. V jeho konfiguraci SSH je uveden veřejný klíč použitelný pro přístup, předpokládám, že zde šlo o „servisní“ položku.

Podle obsahu souboru */etc/passwd* jsou na stanici různé další servisní účty, potenciálně zajímavé jsou *ftp*, *rpc* a *rpcuser*, *nfsnobody*, *postfix*, které ukazují na přítomnost jistých služeb. Výchozí účet *centos* neobsahoval žádná zajímavá data.

II. Průzkum sítě

Dalším krokem byla instalace nástroje *nmap* pro průzkum sítě.[1] Oskenoval jsem služby v celé podsíti 192.168.122.0/24, ve které se stanice nacházela, a to pomocí klasického TCP SYN skenu, navíc s aktivovanou detekcí verzí a OS:

```
nmap -sV -O 192.168.122.164
```

Výstupem byl seznam stanic a nalezených služeb, který však obsahoval mnoho stanic ostatních studentů. Ty bylo možné odlišit podle přítomnosti hostname začínajícího na x: `grep -P 'report for (?!x)' -A 12 nmap_sv`. Následující stanice byly identifikovány jako potenciálně zajímavé, uvedeny jsou také objevené služby. U stanic s dostupnou službou SSH byl proveden test připojení na účet *root*, který ukázal, zda má stanice povolenou autentizaci heslem – tyto stanice jsou označeny symbolem †.

- .1 otevřeny porty 22 (ssh†), 53 (dnsmasq-2.85)
- .21 otevřeny porty 22 (ssh), 111 (rpc)
- .27 otevřeny porty 22 (ssh), 111 (rpc)
- .38 otevřeny porty 22 (ssh), 111 (rpc)
- .43 otevřeny porty 22 (ssh), 111 (rpc)
- .60 otevřeny porty 22 (ssh), 111 (rpc); stanice S3 (viz sekci I)
- .84 otevřeny porty 22 (ssh), 111 (rpc)
- .131 otevřeny porty 22 (ssh), 111 (rpc)
- .134 otevřeny porty 22 (ssh), 80 (Apache **http**d 2.4.6)
- .164 otevřeny porty 22 (ssh), 21 (Vs**ftp**d 3.0.2)
- .216 otevřeny porty 22 (ssh†), 111 (rpc)
- .249 otevřeny porty 22 (ssh), 9418 (služba git protocol)

U všech stanic s otevřeným RPC portem byly zjištěny dostupné RPC programy pomocí `rpcinfo` (pro kontrolu také `nmap -sSUC -p111`. Na stanici .21 byla nalezena služba NFS (související RPC programy: status, mountd, nfs, nfs_acl, nlockmgr). Ostatní stanice neobsahovaly žádné běžící služby (kromě portmapper, ta souvisí s fungováním RPC).

Potenciálně zajímavé nalezené služby tedy jsou:

1) NFS (192.168.122.21)
2) HTTP (192.168.122.134)
3) FTP (192.168.122.164)
4) Git (192.168.122.249)

V použitém nastavení *nmap* testuje pouze 1 000 běžných portů. Později jsem pro známé nestudentské stanice spouštěl nástroj také nad celým prostorem čísel portů (parametr `-p-`). Objevil však pouze porty různých už objevených RPC služeb. Dále jsem spustil sken IP protokolů (parametr `-sO`) nad větším blokem adres (192.168.112.0/20), žádné další stanice nebyly nalezeny.

III. Průzkum stanice S3

Po připojení na stanici S3 jsem v domovském adresáři nalezl několik souborů, mezi nimi obrázek, *mail.export.txt*, *mail.txt* s různým zašifrovaným obsahem a prázdný soubor *main.db*. Předpokládal jsem, že šlo o soubory sem zkopírované jinými studenty, nicméně zašifrované e-mailové zprávy jsem považoval za možné umístění tajemství. V domovském adresáři se nacházela také složka *.gnupg*, což naznačovalo, že zprávy budou zašifrovány pomocí GPG, nicméně na této stanici nebyly přítomny příslušné klíče. Na stanici nebyly přítomné žádné SSH klíče pro přístup na jiné stanice.

Stanice naslouchala na TCP portu 22 (ssh) na všech rozhraních; a na portech 25 (SMTP) a 1001 na loopback adrese

[1] Podobně důležitou byla také instalace editoru *nano*, protože na *vim* nemám ~~nervy~~ ~~schopnosti~~ čas.

127.0.0.1. Také naslouchala na všech rozhraních na UDP portech 68 (DHCP klient), 111 (RPC), 676, 14513, 46482 a na loopback adrese na portu 323.

Vypsání kořenového adresáře souborového systému poukázalo na odlišně nastavená práva pro složky */log*, */tmp* a */trash*. V adresáři */trash* se nacházely tečkou prefixované soubory „invoice“, v jednom z nich (*.3789_2023_09_07.invoice*) bylo nalezeno **tajemství A**. Dále se zde nacházel obrázek *I217642.jpeg*. Tento jsem analyzoval pomocí nástroje pro steganografickou analýzu obrázků *AperiSolve*[2] a pomocí rychlého nástroje pro testování klíčované steganografie *stegseek*[3] s použitím několika obsáhlých seznamů nejčastějších hesel[4]. V obrázku žádná další tajná informace nebyla nalezena.

V adresáři */log* byl nalezen soubor *old_traffic.pcapng*, který byl čitelný pro všechny. V tomto PCAP souboru zachycujícím síťovou komunikaci byly odhaleny mj. TCP toky komunikace protokolů SSHv2 a telnet. Protože protokol telnet není šifrovaný, bylo možné pomocí disektoru nástroje *Wireshark* obsah této komunikace přečíst. Ukázalo se, že obsahovala záznam přihlašování ke stanici .216 s přístupovými údaji:

- login: `bob`
- heslo: `MegaSuperHeslo123NikdoHoNezjisti`

Další zajímavé soubory nebyly na stanici S3 odhaleny.

IV. Průzkum stanice .216

Odhalené přístupové údaje byly použitelné pro přístup na stanici .216 pomocí SSH. V domovském adresáři se zde nacházel opět soubor *mail.export.txt* a dále potenciálně zajímavý adresář *project*, jež obsahoval binární spustitelný soubor *company_software*. Tento soubor jsem otevřel v disassembleru *IDA*[5]. V úvodu funkce main jsem pak objevil instrukci:

```
mov [rbp+src], offset aTajemstviCCefd
```

Symbol `aTajemstviCCefd` pak ukazoval na adresu v segmentu *.rodata*, na které bylo uloženo **tajemství C**.

Při prvním připojení na tuto stanici nebylo možné ani zde pomocí `gpg -d` dešifrovat e-mailovou zprávu v domovském adresáři, a předpokládal jsem tedy, že příslušný klíč bude přítomen jinde (viz sekci V). Při pozdějším pokusu však jiný student tyto klíče naimportoval do GPG klíčenky na této stanici a e-mail bylo možné dešifrovat přímo na této stanici. Ukázalo se, že obsahuje **tajemství B**.

Další zajímavé soubory ani potenciální zranitelnosti nebyly na této stanici nalezeny.

V. NFS server

Přímo na vstupním uzlu bylo možné spustit příkaz `showmount -e 192.168.122.21`, který vypsal adresáře dostupné k připojení na NFS serveru dříve odhaleném na stanici .21. Server nabízel jediný adresář */shared*. Tento bylo možné **bez autentizace** připojit ze vstupního uzlu:

```
sudo mount -t nfs -o vers=3 \
192.168.122.21:/shared nfs
```

Připojený adresář obsahoval řadu JPEG obrázků a dva binární soubory: *private.key* a *public.key*. Pomocí `gpg --show-key` jsem potvrdil hypotézu, že jde o pár GPG klíčů:

```
pub   rsa4096 2023-10-02 [SC]
      92DCFE2D3F118EF6AC28C5949F90F3887C1
      568D6
uid   John Seanah (My very SECRET key for
      my important SECRET stuff)
sub   rsa4096 2023-10-02 [E]
```

Po úspěšném importu pomocí `gpg --import` bylo možné dešifrovat zprávu nalezenou na stanici .216 obsahující **tajemství B**.

Protože obrázků zde bylo větší množství, před využíváním steganografických nástrojů jsem se pokusil prostým voláním nástroje *grep* zjistit, zda se tajemství nenachází v nějakém z nich přímo jako sekvence bajtů:

```
$ grep Taje *
grep: pexels-pixabay-417273.jpg: binary
file matches
```

Nahlédnutí na obsah uvedeného souboru v hexadecimálním editoru ukázalo, že se jako souvislý řetězec znaků uvnitř souboru nachází **tajemství J**.

VI. Git server

Git protokol je jedním z možných způsobů přístupu ke Git serverům. Speciální Git služba naslouchá na portu 9418. Při použití tohoto protokolu není k dispozici **žádná autentizace** nebo kryptografie, jediný způsob zabezpečení spočívá v tom, že v repozitáři musí být přítomen speciální soubor označující, že má být tento repozitář nabízen [1].

Protokol neumožňuje získat seznam repozitářů, které nabízí, název repozitáře tedy musí uživatel znát dopředu. Žádnou přímou nápovědu k možným názvům jsem dosud nezískal, inspirován kapitalizací slova *secret* v popisu klíčů nalezených na NFS serveru jsem ze vstupního uzlu vyzkoušel, zda neexistuje takto pojmenovaný repozitář na Git serveru:

```
git clone git://192.168.122.249/secret.git
```

Repozitář existoval a byl naklonován na mou stanici.

V repozitáři byl přítomen soubor se zdrojovým kódem *main.c*. Program samotný měl charakter nonsensu, nicméně obsahoval některé potenciálně zajímavé konstanty[6]:

```
const char *name_of_my_dog =
  "misbebeslosamocontodomicorazon";
const char *my_debit_card_pin = "4242";
```

[2] https://www.aperisolve.com/

[3] https://github.com/RickdeJager/stegseek

[4] https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials

[5] https://hex-rays.com/ida-free/

[6] El próximo tiempo, sería muy insidioso incluir un secreto verdadero en una cadena de caracteres en otra idioma…

Užitečnějším se však ukázalo procházení historie commitů v repozitáři. V jednom z nich se nacházel soubor *TODO* s nápovědami:

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

Zároveň se ve stejném commitu nacházela změna konstanty `name_of_my_dog` z předchozí hodnoty **buster** na hodnotu uvedenou výše.
V jednom z commitů (ff7ef987) byly dočasně přidány další konstanty a řádek s komentářem, ve kterém bylo uvedeno **tajemství F**:

```
const char *login = "bob";
  // REMOVE BEFORE COMMIT
const char *password = "iloveyou";
  // Tajemstvi_F_...
```

VII. FTP server

FTP server na stanici .164 byl podle nálezu nástroje *nmap* ve verzi 3.0.2, pro kterou nebyly v seznamu CVE evidovány žádné zranitelnosti. Pomocí skriptu ftp-anon nástroje *nmap* jsem ověřil, že server neumožňuje anonymní přístup. Bylo tedy nutné zjistit jméno a heslo.

Vsftpd ve výchozím nastavení využívá pro autentizaci systémové uživatele. Toto chování jsem ověřil tak, že jsem po připojení zaslal příkaz `USER root`, na který server reagoval výzvou k zadání příkazu `PASS`; zatímco při uvedení náhodné kombinace znaků jako uživatelského jména server přímo reagoval zprávou 530 Denied. Tímto způsobem by bylo možné hledat uživatele v systému.

Tipováním běžných jmen jsem odhalil, že v systému patrně existuje také uživatel *admin*. Vzhledem k nápovědě 1) z git repozitáře jsem se rozhodl vyzkoušet řetězce, které jsem v repozitáři objevil: 4242, misbebes…, bob, iloveyou, buster. Ukázalo se, že kombinace jména admin a hesla buster byla platná a dostal jsem přístup na FTP server.

Na serveru byly přítomné tři obrázky kachen a soubor *secret.txt*. V textovém souboru byl řetězec ve tvaru podobném již nalezeným tajemstvím: „Dktowcdfs_N_…“, bylo však zjevné použití nějaké jednoduché šifry. Napadlo mě, že by mohlo jít o Vigenèrovu šifru, první část řetězece jsem tedy vložil do příslušněh nástroje aplikace dCode[7] a použil jsem možnost dekódování se znalostí původního slova „Tajemstvi“. Výsledkem bylo nalezení klíče „KKKK“, což značí, že jde dokonce o jednodušší Caesarovu šifru s posunem A→K. Takto bylo objeveno celé **tajemství D**.

V obrázcích jsem se pokusil najít tajemství nástrojem *grep* podobně jako v sekci V, zde však patřičný řetězec nalezen nebyl. Proto jsem opět použil nástroj *AperiSolve*, který obrázek vkládá do několika různých steganografických dešifrovacích nástrojů. V obrázku *duck-1.jpg* nalezl užitečná data nástroj Outguess[8]. Daty zakomponovanými v obrázku bylo přímo **tajemství E**. V ostatních dvou obrázcích žádný z nástrojů nenašel užitečná data.

VIII. HTTP server

HTTP server na stanici .134 poskytuje pouze nešifrovaný přenos bez TLS na portu 80. V Apache httpd ve verzi 2.4.6 podle seznamu CVE nebyly nalezeny zranitelnosti, které by zde bylo možné využít. Předpokládal jsem proto, že zde budou možné útoky vést především přes nedostatečně zabezpečenou webovou aplikaci.

Z hlavní stránky byly odkazovány dvě stránky: jedna vedla na výpis uživatele, druhá na nahrávání obrázků. Stránka s výpisem uživatelů využívala URL parametr *id*, podle kterého vypisovala detaily vybraného uživatele. Bylo pravděpodobné, že hodnotou parametru se přímo klíčují dotazy do databáze – enumerací zde byly objeveny účty uživatelů Default, John Seanah, Bob Wazi a Jimmy Kim. Enumerací dalších hodnot jsem další uživatele neobjevil, nicméně nechtěl jsem zde využívat bruteforce útok nad stavovým prostorem neznámé velikosti. Pokusil jsem se však provést klasický útok typu **SQL injection** použitím hodnoty parametru `1 OR 1=1 --`. Po zaslání tohoto požadavku byli vypsáni všichni uživatelé, navíc byl uveden záznam „Admin“, u kterého bylo vypsáno **tajemství H**.

Apache server ve výchozím nastavení zpřístupňuje adresář */icons/* s různými předdefinovanými ikonami. Navigace na stránku 192.168.122.134/icons/ ukázala, že je na serveru zapnuto vypisování adresářů. Pokusil jsem se o přístup na různé typické cesta, např. */scripts/*, */js/*, */content/*, */images/*. Poslední z nich na serveru existovala a obsahovala jediný soubor *image.php*.

Tento PHP skript poskytl výpis vestavěné funkce `phpinfo()`, která poskytuje **citlivé informace** o konfiguraci serveru[9]. Zaujala mě přítomnost nestandardních znaků na začátku vykreslené stránky, která poukazovala na přítomnost neznámých bajtů. Náhled na soubor hexadecimálním editorem ukázal, že soubor začíná sekvencí FF D8 FF E0, kterou už jsem předtím zaznamenal při analýze JPEG obrázků. Skutečně, sekvence FF D8 je značka začátku obrázku, další dva bajty určují druh obsahu [2]. Předpokládal jsem, že tento soubor souvisí se stránkou pro nahrávání obrázků a s nápovědou 2) z git repozitáře (viz sekci VI). Soubor jsem stáhl a nahrál na příslušné stránce. Výsledkem byla odpověď serveru s **tajemstvím I**.

Po delším experimentování s hledáním dalších cest na serveru jsem vyzkoušel podobně triviální dotaz jako na Git serveru: cestu */secret*. Na této **neautentizované** adrese bylo uvedeno **tajemství G**.

[7] https://www.dcode.fr/vigenere-cipher

[8] https://github.com/resurrecting-open-source-projects/outguess

[9] https://www.php.net/manual/en/function.phpinfo.php

REFERENCE

[1] S. Chacon and B. Straub, *Pro Git*. Apress, 2023, ch. The Protocols, accessed: 2023-12-19. [Online]. Available: https://github.com/progit/progit2/releases/download/2.1.412/progit.pdf

[2] "Information Technology – Digital Compression and Coding of Continuous-Tone Still Images – Requirements and Guidelines," International Telecommunication Union, ITU-T Recommendation T.81, 09 1992. [Online]. Available: https://www.w3.org/Graphics/JPEG/itu-t81.pdf