Vysoké učení technické v Brně
Fakulta informačních technologií

Bezpečnost informačních systémů
Projekt – The FITfather

Dominik Harmim (xharmi00)
xharmi00@stud.fit.vutbr.cz
26. listopadu 2019

1 Úvod

Cílem tohoto projektu je získat co nejvíce tajemství ukrytých na privátních serverech ve vnitřní síti **`bis.fit.vutbr.cz`**. Následující kapitoly popisují zmapování vnitřní sítě a postup získání jednotlivých tajemství.

2 Zmapování sítě

Po přihlášení na server **`bis.fit.vutbr.cz`** bylo příkazem **`ifconfig`** zjištěno, že se počítač nachází v síti 192.168.122.0/24. Příkazem **`nmap -p- 192.168.122.0/24`** byly nalezeny následující počíteče a jejich otevřené porty:

- 192.168.122.38
  - 21/tcp ftp
  - 22/tcp ssh
  - 80/tcp http
- 192.168.122.42
  - 22/tcp ssh
  - 111/tcp rpcbind
- 192.168.122.77
  - 22/tcp ssh
  - 111/tcp rpcbind
- 192.168.122.83
  - 22/tcp ssh
  - 111/tcp rpcbind
- 192.168.122.105
  - 22/tcp ssh
  - 80/tcp http
  - 111/tcp rpcbind
  - 3306/tcp mysql
- 192.168.122.150
  - 22/tcp ssh
  - 111/tcp rpcbind
- 192.168.122.155
  - 22/tcp ssh
  - 111/tcp rpcbind
- 192.168.122.169
  - 22/tcp ssh
  - 80/tcp http
  - 111/tcp rpcbind
  - 42424/tcp unknown
- 192.168.122.206
  - 22/tcp ssh
  - 111/tcp rpcbind
- 192.168.122.215
  - 22/tcp ssh
  - 111/tcp rpcbind
- 192.168.122.220
  - 22/tcp ssh
  - 23/tcp telnet
  - 80/tcp http
- 192.168.122.227
  - 22/tcp ssh
  - 111/tcp rpcbind

3 Získání tajemství

Tato kapitola popisuje postup získání jednotlivých tajemství.

3.1 Tajemství A

Na počítači 192.168.122.38 běží HTTP server na portu 80. Při přístupu přes prohlížeč **elinks** příkazem **elinks http://192.168.122.38/** bylo zjištěno, že na serveru běží webová aplikace pro zadávání a vyhledávání zaměstnanců určité firmy, která pravděpodobně používá nějakou SQL databázi. Je možné zkusit *SQL injection* vložením řetězce **"foo foo;** do vyhledávacího pole. Zobrazí se SQL chybové hlášení, ze kterého lze zjistit, že se jedná o SQL server MariaDB a provádí se dotaz **SELECT id, name, email, address FROM contact WHERE name LIKE "%"foo foo;%**. Je možné tohoto využít pomocí příkazu **UNION** a do uvedených databázových sloupců, které se zobrazují v aplikaci, je možné vytáhnout požadovaná data. Zadáním **"UNION SELECT 42, `table_name`, 'foo', 'foo' FROM `information_schema`.`tables` WHERE `table_type` = 'BASE TABLE';#** do vyhledávacího pole je získán seznam všech definovaných databázových tabulek. V tabulce s názvem **auth** by mohly být uložené nějaké přihlašovací údaje. Názvy sloupců této tabulky lze získat zadáním **"UNION SELECT 42, `column_name`, 'foo', 'foo' FROM `information_schema`.`columns` WHERE `table_name` = 'auth';#** do vyhledávacího pole. Bylo zjištěno, že tato tabulka obsahuje sloupce **id**, **login** a **passwd**. Vypsání sloupců **login** a **passwd** je možné zadáním **"UNION SELECT 42, `login`, `passwd`, 'foo' FROM `auth`;#** do vyhledávacího pole. V poli **passwd** u sloupce, kde má pole **login** hodnotu **admin**, se nachází tajemství **A**.

3.2 Tajemství B

Na serveru 192.168.122.169 běží na portu 42424 neznámá služba. Pokusem o připojení na tento port přes protokol FTP bylo zjištěno, že na tomto portu běží FTP server. Po připojení příkazem **ftp 192.168.122.169 42424** byly vyžadovány přihlašovací údaje. Bylo vyzkoušeno, že je možné se autentizovat jako anonymní uživatel s přihlašovacím jménem **anonymous** a s prázdným heslem. Na FTP serveru se nachází soubor **/secret.txt**. Po jeho stažení příkazem **get /secret.txt** a vypsání příkazem **cat ~/secret.txt** bylo získáno tajemství **B**.

3.3 Tajemství C

Na počítači 192.168.122.169 běží HTTP server na portu 80. Při přístupu přes prohlížeč **elinks** příkazem **elinks http://192.168.122.169/** bylo zjištěno, že lze prohledávat dostupné adresáře. Pří přístupu k souboru **http://192.168.122.169/etc/raddb/sql.conf** bylo získáno tajemství **C**.

3.4 Tajemství D

Na počítači 192.168.122.220 běží SSH server na portu 22. Při pokusu o připojení na tento server přes protokol SSH příkazem **ssh 192.168.122.220** byl vypsán řetězec **Hello, smith!** a byly vyžadovány přihlašovací údaje. Při přihlášení jako uživatel s přihlašovacím jménem **smith** příkazem **ssh smith@192.168.122.220** už nebylo heslo vyžadováno. Příkazem **tcpdump -i ens3 -w out.pcap** byl vygenerován záznam síťové komunikace na rozhraní s názvem **ens3**, který byl zjištěn příkazem **ifconfig**. Síťová komunikace byla zaznamenávána pouze po určitou dobu, poté byl zaznamenaný výstup uložen do souboru. Tento soubor byl následně analyzován v programu Wireshark. Protože na tomto serveru běží služba TELNET na portu 23, tak byla analýza zaměřená na pakety právě protokolu TELNET. Při zobrazení TCP toku těchto paketů bylo vidět, že se zasílá přihlašovací jméno **ada** a heslo **nachystejteuzenace** v čisté podobě. Při přihlášení na server 192.168.122.220 přes protokol TELNET příkazem **telnet 192.168.122.220** s přihlašovacím jménem **ada** a heslem **nachystejteuzenace** byl na tomto serveru nalezen soubor **~/secret.txt**. Po je ho vypsání příkazem **cat ~/secret.txt** bylo nalezeno tajemství **D**.

3.5 Tajemství E

Na počítači 192.168.122.220 běží HTTP server na portu 80. Při přístupu přes prohlížeč **elinks** příkazem **elinks http://192.168.122.220/** byl zobrazen přihlašovací formulář, kde bylo vyžadováno jméno a heslo. Příkazem **curl -v http://192.168.122.220/** bylo zjištěno, že pro kontrolu přihlášení se používá cookie s názvem **LOGGED_IN**, které je nastaveno na hodnotu **False**. Byl proveden HTTP dotaz na tento server s nastavením tohoto cookie na hodnotu **True** příkazem **curl --cookie 'LOGGED_IN=True' http://192.168.122.220/**. Tímto bylo získáno tajemství **E**.

3.6 Tajemství F

Na počítači 192.168.122.227 běží SSH sever na portu 22. Při pokusu o připojení na tento server přes protokol SSH příkazem **ssh 192.168.122.227** byla zobrazena hláška, která říká, že je možné přihlásit se jako uživatel **teacher** a byly vyžadovány přístupové údaje. Bylo zjištěno, že je možné se přihlásit jako uživatel **teacher** s heslem **teacher** příkazem **ssh teacher@192.168.122.227**. Bylo zjištěno, že na tomto serveru je možné využít zranitelnosti příkazu **sudo**, kde při zadání příkazu s prefixem **sudo -u#-1** není vyžadováno heslo správce, ale heslo aktuálně přihlášeného uživatele. Proto bylo vyzkoušeno na celém serveru vyhledat soubory, které ve svém názvu obsahují podřetězec **secret** příkazem **sudo -u#-1 find / -name *secret***. Byl nalezen soubor **/root/secret.txt**. Vypsáním tohoto souboru příkazem **sudo -u#-1 cat /root/secret.txt** bylo získáno tajemství **F**.

3.7 Tajemství G

Na serveru 192.168.122.38 běží FTP server na portu 21. Při pokusu o připojení na tento server přes protokol FTP příkazem **`ftp 192.168.122.38`** byly vyžadovány přístupové údaje. Tímto bylo také zjištěno, že se jedná o FTP server verze **`vsFTPd 2.3.4`**, který obsahuje takovou zranitelnost, že při přihlášení s uživatelským jménem, které obsahuje podřetězec **`:)`**, lze zadat prázdné heslo. Při pokusu o přihlášení stejným příkazem, se zadáním uživatelského jména **`foo:)`** a prázdného hesla, se pouze zobrazí, že je otevřen port 53244. Při přihlášení na tento server přes protokol FTP na port 53244 příkazem **`ftp 192.168.122.38 53244`** bylo získáno tajemství **G**.

3.8 Tajemství H

Na serveru 192.168.122.220 (připojení viz tajemství D, kapitola 3.4) byly vyhledávány v dostupných adresářích soubory, které ve svém názvu obsahují podřetězec **`secret`**. Příkazem **`ls /usr/bin/ | grep secret`** byl nalezen spustitelný soubor **`/usr/bin/show-secret`**. Spuštěním tohoto souboru příkazem **`/usr/bin/show-secret`** bylo získáno tajemství **H**.

3.9 Tajemství I

Na počítači 192.168.122.105 běží HTTP server na portu 80. Při přístupu přes prohlížeč **`elinks`** příkazem **`elinks http://192.168.122.105/`** bylo zjištěno, že na serveru existuje adresář **`www`**. Při následném přístupu do tohoto adresáře příkazem **`elinks http://192.168.122.105/www/`** se zobrazuje chybová hláška s kódem 500. Jedná se o klasické chybové hlášení *PHP frameworku Nette*. Zdrojové kódy aplikací napsaných v tomto frameworku jsou typicky uloženy o úroveň výše v adresáři **`app`**. Proto byl vyzkoušen přístup do tohoto adresáře příkazem **`elinks http://192.168.122.105/app/`**.
Zde je možné procházet adresářovou strukturu. Prohledáváním jednotlivých souborů bylo v souboru **`http://192.168.122.105/app/config/local.neon`** jako heslo k databázi nalezeno tajemství **I**.

3.10 Tajemství J

Na počítači 192.168.122.77 běží SSH server na portu 22. Při pokusu o připojení na tento server přes protokol SSH příkazem **`ssh 192.168.122.77`** byly vyžadovány přístupové údaje. Bylo vyzkoušeno, že je možné přihlásit se jako uživatel **`root`** s heslem **`root`** příkazem **`ssh root@192.168.122.77`**. Na tomto serveru byl nalezen soubor **`~/secret.txt`**. Jeho vypsáním příkazem **`cat ~/secret.txt`** bylo získáno tajemství **J**.

4 Závěr

Všech 10 tajemství (A-F) bylo úspěšně nalezeno, jak je popsáno v kapitolách výše.