Vysoké učení technické v Brně
Fakulta informačních technologií

BIS

CTF projekt

10. prosince 2023 Adam Zvara (xzvara01)

Táto dokumentácia je spísaná vo forme krokov, ktoré som realizoval na to, aby som našiel tajomstvá v rámci projektu (teda poradie tajomstiev nie je nutne chronologické).

Zmapovanie siete

Keďže na prihlasovacom uzli máme prístup ku užívateľovi root, môžeme si tam nainštalovať nmap na zmapovanie internej siete (som si vedomý toho, že nmap sa nachádza na iných serveroch v sieti ale pracoval som na prihlasovacom uzli aby som nerobil bordel pre ostatných študentov).

V prvom rade musíme získať ip adresu login uzlu pomocou príkazu `ip address`. Vidíme, že sa nachádzame v lokálnej sieti `192.168.122.X` Príkazom `nmap 192.168.122.0-255` môžeme zistiť, aké služby sa nachádzajú na ostatných serveroch v tejto sieti (vypísané sú len tie uzly, ktoré neprislúchajú študentom):

IP adresa	Služby
192.168.122.21	22 / ssh
	111 / rpcbind
	2049 / **nfs**
192.168.122.134	22 / ssh
	80 / **http**
192.168.122.164	21 / **ftp**
	22 / ssh
192.168.122.249	22 / ssh
	9418 / **git**

Zároveň som si všimol, že existujú niektoré servery, na ktorých beží ssh a rpcbind ale neprislúchajú žiadnym študentom (pomenovania serverov *jimmy* a *bob* vyplývajú z ďalších častí textu):

IP adresa	Užívateľ
192.168.122.27	(???)
192.168.122.38	(???)
192.168.122.43	(???)
192.168.122.60	(jimmy)
192.168.122.84	(???)
192.168.122.131	(???)
192.168.122.216	(bob)

Zároveň som si všimol, že v súbore `.ssh/config` sa nachádza konfigurácia na pripojenie na server 192.168.122.60 ako užívateľ jimmy, na ktorý som sa následne pripojil.

192.168.122.60 - jimmy

Po pripojení na tento server bolo pomerne náročné sa v ňom zorientovať, keďže študenti po sebe zanechávali veľké množstvo súborov. Mojím cieľom bolo nájsť pôvodne nahrané súbory, ktoré boli zamýšľaným riešením tohto projektu. K tomu mi pomohol výpis poslednej aktualizácie súborov (pretože dôležité súbory boli automaticky nahrávané každých 5 minút užívateľom root). Pri výpise koreňového adresára `ls -la /` som si všimol 2 adresáre, ktoré nie sú úplne bežné pre unixové systémy.

/trash

Po vypísaní obsahu priečinka `/trash` som si všimol, že obsahuje 4 skryté súbory `*.invoice`. Pri výpise obsahu súboru `.3789_2023_09_07.invoice` som našiel prvé **tajomstvo A**.

/logs

Tento priečinok obsahoval zachytenú komunikáciu vo forme *pcap* súboru. Tento súbor som si stiahol a preskúmal pomocou programu wireshark, kde som objavil že v zachytenej komunikácií sa pokúša užívateľ bob prihlásiť na server pomocou protokolu telnet, z ktorého sme schopní zistiť jeho heslo: *MegaSuperHeslo123NikdoHoNezjisti*.

192.168.122.216 - bob

Po prihlásení sa na tento server môžeme vidieť jeden priečinok `project/` a niekoľko mailových súborov (zašifrovaných pomocou GPG - jeden z nich je periodicky aktualizovaný užívateľom root, takže asi bude podstatný neskôr).

project/

V tomto priečinku som našiel binárny súbor, z ktorého som si vypísal textové reťazce pomocou príkazu `strings company_software`, z čoho som našiel **tajomstvo C**.

192.168.122.134 - http

Prvé tajomstvo na tomto serveri som našiel pomerne náhodou, keď som si prezeral priečinok `.elinks/` kde som narazil na súbor `globhist` v ktorom som si všimol valídnu odpoveď serveru na požiadavok `/secret/`, v ktorom som našiel **tajomstvo G**. Ďalej som si všimol, že stránka obsahuje 3 ďalšie časti: `/user.php`, `/upload/index.php` a `/admin/index.html`.

/user.php

Tento skript vypisuje informácie o užívateľskom účte, ktorý je indexovaný identifikačným číslom predávaným prostredníctvom GET parametru. Predpokladal som, že užívatelia sú uložení v databáze a taktiež som si domyslel štruktúru query (príklad: `SELECT * FROM users WHERE id = $ID`). Využil som SQL injection na výpis všetkých užívateľských účtov (`curl 192.168.122.134/user.php?id=1'+OR+1'`), čím som získal **tajomstvo H**.

/upload/index.php

Táto stránka volá skript `upload_file.php` s priloženým súborom vo forme multipart/form-data. Z git serveru (predbieham) som sa dozvedel, že existuje chyba, kedy užívateľ môže nahrať na server php súbor. Najprv som však skúsil nahrať platný obrázok, aby som zistil, ako server zareaguje:
`curl 192.168.122.134/upload/upload_file.php -F "image_file=@/home/student/image.jpg"`, pri ktorom server odpovedal hláškou *File uploaded. Nothing happened.* Následne som skúsil premenovať tento súbor na *image.php* a získal som **tajomstvo I**.

192.168.122.249 - git

Nmap odhalil server, na ktorom beží služba git. Cieľom teda bolo uhádnuť meno repozitára uloženého na tomto serveri. Po niekoľkých pokusoch som zistil, že je možné si naklonovať repozitár s názvom `secret`: `git clone git://192.168.122.249/secret/`. Po zobrazení histórie commitov (`git log`) v tomto repozitári a zobrazení zmien v hlavnom súbore `main.c` (`git show COMMIT_ID`) som našiel v jednom z commitov **tajomstvo F**. Zároveň som odhalil aj niekoľko nápovied, ktoré mi pomohli v ďalších častiach tohto projektu:

1. *FTP ... "commonly used password"doesnt mean "safe password"* - odhadol som, že heslo na ftp server bude niektoré z podozrivo pomenovaných premenných v súbore main.c (napríklad: `name_of_my_dog = buster, my_debit_card_pin = 4242` ...). Tieto potenciálne heslá som si uložil do súboru `passwords`:

buster
4242
commonly used password
safe password
misbebeslosamocontodomicorazon
iloveyou

192.168.122.164 - ftp

Po nainštalovaní ftp klienta na login server som sa skúšal prihlásiť na ftp server. Všimol som si, že pre určité prihlasovacie mená server rovno odmietne prihlásenie ale pre určité (admin, root, nobody) vyžaduje heslo. S pomocou nápovedy z git serveru som teda použil nmap na zistenie prihlasovacích údajov na ftp server: `nmap -script ftp-brute -script-args userdb=usernames,passdb=passwords -p 21 192.168.122.164` pomocou čoho som odhalil prihlasovacie údaje `admin:buster`. Po vypísaní súborov som našiel jeden súbor s názvom `secret.txt` a 3 obrázky.

secret.txt

Po vypísaní obsahu tohto súboru som si všimol, že je v podobnom formáte ako všetky ostatné tajomstvá. Samotné tajomstvo ale bolo zakódované Caesarovou šifrou, ku ktorej som odhalil posunutie +16 (na základe toho že viem, že začiatok tajomstva je stále v tvare *Tajemstvi_*) a získal som **tajomstvo D**.

duck-*.jpg

Na FTP serveri sa nachádzali 3 obrázky. Skúšal som rôzne nástroje na steganografiu v obrázkoch a narazil som na stránku aperisolve , na ktorú som nahral všetky obrázky. V sekcii nástroja `Outguess` som si pri prvom obrázku všimol, že bol vygenerovaný nejaký výstup a tak som našiel **tajomstvo E**.

192.168.122.21 - nfs

Posledný zo serverov, ktoré som navštívil, bol server ktorý disponoval službou nfs. Príkazom `showmount -e 192.168.122.21` som odhalil, že si môžem k sebe namountovať zdieľaný priečinok `/shared`. Pri snahe o jednoduché mountovanie tohto adresára na login uzol (`sudo mount -t nfs 192.168.122.21:/shared ./mnt/`) som však narazil na problém, pretože som nebol schopný priečinok namontovať (permissions denied). Skúsil som teda vytvoriť ssh tunnel na iný server, ku ktorému som mal prístup (`ssh -fN -L 2080:192.168.122.21:2049 jimmy@192.168.122.60`). Takto sa mi podarilo priečinok namountovať pomocou príkazu `sudo mount -t nfs 127.0.0.1:/shared ./mnt/ -o port=2080`. Po pripojení zdieľaného priečinku som si vypísal jeho obsah a zistil som, že obsahuje niekoľko súborov a dvojicu privátny a verejný kľúč.

*.jpg

Keďže je týchto obrázkov veľa tak som predpokladal, že v nich nebude tajomstvo sofistikovane schované a jednoducho som si vypísal reťazce zo všetkých obrázkov (`strings *.jpg | grep Tajemstvi`) a našiel som **tajomstvo J**.

(private|public).key

Predpokladal som, že sa jedná o privátny kľúč na dešifrovanie emailovej komunikácie nájdenej na serveri bob. Stiahol som si teda tieto súbory na login server, kde som si pridal nájdený privátny kľúč pomocou príkazu `gpg -import private.key` a následne dešifroval správu pomocou príkazu `gpg -d mail.exported.txt`, čím som získal **tajomstvo B**.