1. projekt do předmětu BIS

Sára Škutová, xskuto00

13. prosince 2018

1 Zmapování vnitřní sítě

Pomocí příkazu `$ ifconfig` jsem zjistila rozsah ip adres, které se nachází v dané sítí. Následně pomocí `$ nmap 192.168.122.1-254` jsem provedla skenování sítě, čímž jsem zjistila, že mezi studentskými servery se nacházejí následují servery s tajemstvím:

Nmap scan report for ptest3.bis.mil (192.168.122.22)

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind

Nmap scan report for ptest2.bis.mil (192.168.122.27)

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
3306/tcp	open	mysql

Nmap scan report for ptest1.bis.mil (192.168.122.143)

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh

Nmap scan report for ptest4.bis.mil (192.168.122.210)

PORT	STATE	SERVICE
22/tcp	open	ssh
53/tcp	open	domain
6667/tcp	open	irc

Při pozdějším skenování jsem zjistila, že port 111 mají nově otevřeno také ptest1 a ptest2.

2 Klientská stanice

Při prohledávání souborů klientské stanice jsem se dozvěděla, že stanice zná server ptest3.bis.mil. Dále jsem také ve složce **Documents** nalezla různá pdf, příčemž jedno z nich (**tc48-2008-024-Rev4.pdf**) obsahovalo na konci kontaktní informace: **jbarber@ptest1.bis.mil**. Zábavné je, že daný login jsem objevila již dříve, na ptest2 v souboru **.php_history**, asi jsem někoho nechtíc odposlechla při práci, když jsem ovšem později chtěla ověřit zda tam skutečně tyto údaje jsou, tak už je soubor neobsahoval. Následně jsem ve složce **.Trash** objevila soubor s klíčem **itcrowd.key**. Tento klíč jsem přejmenovala na **id_rsa** a přesunula ho do adresáře **.ssh**. Následně jsem se připojila na server ptest3.bis.mil:

```
$ ssh itcrowd@ptest3.bis.mil
```

3 ptest3.bis.mil

Hned v úvodu jsem si všimla, že se zde nachází text *Riddle of the day*, tento text vypadá jako zašifrovaný, tak mě napadlo použít jednu z nejjednodušších šifer – substituční Caesarovu šifru. Jelikož vidím, že celý zbytek textu je v angličtině, a také vidím, že se v zařifrovaném textu nachází osamocené písmenko x, tak mě napádá zda se x nemapuje na a a následně je celá abeceda posunutá vůči jejích rozdílu:

Abeceda:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Posunutá:	x y z a b c d e f g h i j k l m n o p q r s t u v w

Po dešifrování mi hádanka říká, že mám sputit příkaz `$riddle penguinery`, čímž jsem získala **tajemství E**.

Dále při prozkoumávání souborů na ptest3 zjišťuji, že na ptest2.bis.mil se nachází uživatel **webmaster** (zjištěno ve složce **.ssh** v souboru **config**).

Z mapování vnitřní sítě jsem věděla, že se zde nachází také i webový server. Při proukoumávání zdrojových kódů jsem ve složce **/var/www/html** nalezla 2 zajímavé soubory **robots.txt** a **secret.txt**. Z výpisu robots.txt jsem nakonec získala **tajemství I**.

Operace vypsání souboru secret.txt mi ale byla odmítnutá. Při zkoušení různých přístupů ke stránkám ze souboru **.elinks/globhist** jsem nakonec pomocí následujicícho příkazu získala **tajemství C**

```
$curl localhost/secret.txt
```

4 ptest2.bis.mil

Na server ptest2 se lze přihlásit pouze z ptest3 a to pomocí dříve zjištěného uživatelského jména webmaster:

```
$ ssh webmaster@ptest2.bis.mil
```

Při prozkoumávání souborů v domovském adresáší na ptest2 jsem si v adresáři **.elinks** a v souborech **globhist** a **gotohist** všimla, že se stránky z místního webového serveru spouštějí s různými debug proměnnými. Při dalším zkoumání jsem skutečně ve **/var/www/html/index.php** nalezla, že se na začátku provádí příkaz výpisu hodnoty proměnné specifikované pomocí *debug_variable*. Při zkoušení různých proměnných, které jsem nalezla v souboru globhist se mi pak pomocí proměnné *INTERNAL_MSG* podařilo získat **tajemství B**.

```
$curl ptest2/index.php?debug_variable=INTERNAL_MSG
```

Dále jsem při proukoumávání webového serveru narazila na přihlašovácí údaje k místní mysql databázi (**/var/www/html/libs/constants.php**).

DRUH	HODNOTA
Login	arcturus
Heslo	16431879196842
Databáze	arcturus

Následně pomocí příkazu `$ mysql -u arcturus -h localhost -p arcturus` a zadání požadovaného hesla jsem se připojila na lokální databázi, kde jsem z tabulky contracts (`select * from contracts;`) získala **tajemství J**.

5 ptest1.bis.mil

Na ptest1 se nachází FTP server po kontrole o jakou verzi se jedná (`nmap -A ptest1.bis.mil`), jsem zjistila, že se jedná o vsftpd 2.3.4. Tahle verze ftp je známá tím, že se pomocí řetezce *:)* vloženého do prostřed nebo na konec loginu (může být jakýkoliv) můžeme dostat na ftp server aniž bychom vůbec museli zadávat heslo. Po připojení na ftp pomocí `$ ftp ptest1`, zadání loginu ve tvaru *log:)in* a odentrování hesla jsem získala přístup na ftp server, kde mi bylo zděleno, že se mám podívat na nově ovetřený port *56572*. Po připojení na daný port na ptest1 (`$ nc ptest1 56572 -v`) se mi zobrazilo **tajemství G**.

Následně jsem se přihlásila na server pomocí již dříve zjištěného loginu jbarber, jako heslo jsem zkoušela postupně nejčastější používáná hesla až jsem došla k heslu: **welcome**.

```
$ ssh jbarber@ptest1.bis.mil
```

Při již klasickém prohledávání adresářů a vypisování souborů jsem pak v souboru **Mail/Trash** nalezla **tajemství H**.

Další tajemství jsem získala spíše náhodou. Když jsem si nechala vypsat soubor **.viminfo**, tak moji pozornost upoutal poslední řádek, na kterém psalo **/var/db/Makefile**. Ze zvědavosti jsem si ho nechala vypsat a vyčetla jsem, že se tam píše o nějaké *shadow* skupině, a že Makefile na začátku načítá různé **/etc/** soubory. Po prozkoumání jednotlivých souboru jsem pak v **/etc/shadow** nalezla **tajemství A**.

6 ptest4.bis.mil

Z klientské stanice a pomocí programu `irssi` jsem se připojila na irc službu co běží na ptest4. Po prozkoumání jsem zjislila, že se zde nachází chatovací bot jménem Willie a to v místnostech #**bis** a #**internal**. Po připojení do #bis a prozkoumání jaké Willie podporuje příkazy (příkaz `.commands`), jsem se Willieho zeptala co dělá první příkaz na jeho listině: `Willie: help CUKOO`. Po tom co mi napsal, že mi může vyzradit tajemnství jsem neváhala, zadala příkaz `.CUKOO` a získala **tajemství F**.

Dále se na ptest4 vyskytuje také DNS server. Při jeho prozkoumávání z klientské stanice pomocí nástroje `$ dig @ptest4 ptest4.bis.mil` jsem jsem si všimla, že autoritativním DNS serverem k serveru ptest4 je server **bis.mil**. Při dotazu `dig @ptest4 bis.mil ANY` jsem pak v záznamu TXT nalezla **tajemství D**.