Kapupásztázás és általános ping

Ismerkedjünk meg a betörők által használt két leggyakoribb hálózatvizsgáló eljárással.

A nagyobb hálózatok rendszergazdái általában azt állítják, hogy az ő hálózatukon már volt betörési kísérlet. Mivel a betörő-programokból egyre több van, ráadásul mind népszerűbbek, már nem csak a nagyobb hálózatokat fenyegeti veszély. A hálózatvizsgáló programok önmagukban nem veszélyesek ugyan, mégis figyelnünk kell rájuk, hiszen ezek használata egyértelműen betörési kísérletet jelez. Ahogy a mondás is tartja, jobb félni, mint megijedni.

Kapupásztázás

A hálózat vizsgálatának legnépszerűbb módja a kapupásztázás (port scan). Ez egy olyan eljárás, aminek segítségével a betolakodó felderítheti a kiszemelt számítógépen futó szolgáltatásokat. Ezen adatok birtokában a támadó megkísérelheti felhasználni a futó szolgáltatások egyikének-másikának ismert hiányosságait. Például ha a betolakodó azt látja, hogy a 143-as kapu (az IMAP kapuja) nyitva van, akkor kideríti, hogy az IMAP melyik változata fut a számítógépen. Ha ez a változat sebezhető, akkor képes rendszergazdai jogosultságot szerezni egy akna segítségével (ezek olyan programok, amelyekkel ismert biztonsági hibákat, réseket lehet kihasználni). A kapupásztázás tulajdonképpen nagyon egyszerű dolog. Csupán kapcsolódni kell a kiszemelt gép kapuira, és megfigyelni, hogy melyik válaszol és melyik nem. Egy egyszerűbb kapuvizsgáló programot egy jó programozó Javában vagy Perlben 15 perc alatt elkészít. Azonban ezt a fajta kapuvizsgálatot a kiszemelt számítógép operációs rendszere is könnyen észreveszi. Az *1. listán* lévő naplófájlban (a /var/log/messages egy részlete) egy kapuvizsgáló program nyomai láthatók. Látható, hogy a kapcsolódások különböző szolgáltatásokhoz kevesebb, mint három másodperc alatt történtek. Mivel ez könnyen felismerhető, a behatolók manapság már nem is használják a kapuvizsgálatnak ezt a fajtáját. A kapupásztázás másik, rejtettebb változata a „félnyitott” SYN-pásztázás. Itt is a kapuhoz kapcsolódik a program, de még a kapcsolat teljes felépítése előtt megszakítja a kapcsolatot (innen a „félnyitott” elnevezés). Mivel a teljes kapcsolat soha nem jön létre, az operációs rendszer nem is naplózza ezeket kísérleteket. A működési elv biztosan jobban érthető, ha egy kicsit elmélyedünk a TCP/IP protokoll belső működésében. A rendes TCP/IP-kapcsolatban, a két eszköz összekapcsolódásához egy háromlépéses üdvözlésre (three-way handshake) van szükség. A félnyitott SYN-pásztázásnál a program csak arra kíváncsi, hogy működik-e az adott kapu, ezért a harmadik lépés előtt megszakítja a kapcsolatot.

Ismerkedjünk meg napjaink legnépszerűbb és legerősebb hálózatvizsgáló programjával, melynek neve Nmap (Network Mapper). Az Nmap képes a kapupásztázás mindkét említett típusára, sőt, képes más típusú vizsgálatra is, de erre majd később visszatérünk.

A *2. listán* láthatjuk, hogy milyen jelentést készít. Felmerül a kérdés, hogy ha a kapupásztázást rejtve végzik, akkor vajon hogyan lehet felderíteni. A jó hír az, hogy a legtöbb kapupásztázást felderíthetjük az erre a célra készült eszközökkel. A Solar Designer kifejlesztette a scanlogd nevű programot, mely démonként a háttérből figyeli a hálózati csatoló kapuit. Ha a scanlogd kapupásztázást érzékel, ezt jelzi a rendszernaplóban. A *3. listán* látható, hogy miként jelez a scanlogd egy felderített kapupásztázást. Természetesen más olyan eszközök, illetve programok is léteznek, amelyekkel a pásztázás ugyanilyen eredményesen felderíthető. Most nem ezekkel foglalkozunk, de az érdeklődők a fejezet végén található Kapcsolódó címek között tallózva számos hasznos címet találnak. Ajánlom még a tcplogd programot, mely egy remekül beállítható, TCP-kapupásztázást felderítő alkalmazás: meghatározható a naplózni kívánt csomagok típusa az elárasztás (flooding) megelőzésére, valamint a megbízható helyek és kiszolgálók is beállíthatók.

Általános ping

Az általános pingek (ping sweeps) a hálózatvizsgálók másik típusát képviselik. A behatoló ICMP ECHO csomagokat küld a hálózat számítógépeinek (általában meghatározott IP-címtartományban), és figyeli, hogy melyik válaszol. (A ping eredetileg hangutánzó szó.) Így állapítja meg, hogy melyik gép működik, és melyik nem. Ez kicsit olyan, mint ha hajnali háromkor kopogtatnánk a szomszédok ajtaján, és azt figyelnénk, hogy ki alszik, és ki nem (ezzel a módszerrel azért csak csínján bánjunk!). Ha a betolakodó megtudja, hogy melyik számítógép üzemel, arra fog összpontosítani, és munkához lát. Az fping egy olyan program, amely kitűnően használható általános pingeléshez. A program a kapott IP-címeknek küldözget pingcsomagokat. A hagyományos pinggel szemben az fping csak egy csomagot küld az első címre, majd azonnal a következő címet veszi, így forgatja körbe a kapott listát. A *4. listán* egy olyan egyszerű Perl parancsfájlt láthatunk, amely C osztályú IP-címeket hoz létre (a példánkban 192.168.0.1-től 192.168.0.20-ig). Az *5. listán* megfigyelhetjük, hogy a Perl parancsfájl miként működik együtt az fpinggel a meghatározott IP-címtartományban üzemelő számítógépek felderítésében. A -a kapcsolóval csak a válaszoló gépeket jeleníthetjük meg (enélkül az fping az elérhetetlen gépeket is megjeleníti).

Mind a kapupásztázást, mind az általános pinget fel lehet deríteni egyedi eszközök használatával. Az ippl egy olyan IP-protokollnaplózó alkalmazás, amely rögzíti a TCP-, az UDP- és az ICMP-csomagokat. Hasonlóan a scanlogdhez, a háttérben csücsül, és onnan figyeli a csomagokat. A *6. listán* látható, hogy az ippl miként jelzi az elkapott pingcsomagokat. Óvatosnak kell lennünk az ippl használatával,

1. lista A kapupásztázás nyomai a naplóban

```
Jul 18 02:42:25 target sshd[2370]: log: Connection from 192.168.0.1 port 2107
Jul 18 02:42:25 target sshd[2370]: fatal: Did not receive ident string.
Jul 18 02:42:25 target wu.ftpd[2369]: connect from root@attacker
Jul 18 02:42:25 target in.telnetd[2368]: connect from root@attacker
Jul 18 02:42:26 target imapd[2366]: connect from root@attacker
Jul 18 02:42:26 target in.pop3d[2367]: connect from root@attacker
Jul 18 02:42:26 target ftpd[2369]: FTP session closed
Jul 18 02:42:26 target telnetd[2368]: ttloop: read: Broken pipe
Jul 18 02:42:28 target in.fingerd[2365]: connect from root@attacker
```

2. lista Az Nmap eredménye

```
root@attacker# nmap -sS -O target.example.com

Starting nmap V. 2.53 by fyodor@insecure.org/
(http://www.insecure.org/nmap/)
Interesting ports on target.example.com
(192.168.0.2):
(The 1507 ports scanned but not shown below
are
in state: closed)
Port    State   Service
21/tcp open    ftp
22/tcp open    ssh
23/tcp open    telnet
25/tcp open    smtp
37/tcp open    time
79/tcp open    finger
110/tcpopen    pop-3
111/tcpopen    sunrpc
113/tcpopen    auth
143/tcpopen    imap2
515/tcpopen    printer
901/tcpopen    samba-swat
2049/tcp       open    nfs
6000/tcp       open    X11
7100/tcp       open    font-service

TCP Sequence Prediction:
       Class=random positive increments
       Difficulty=2135704 (Good luck!)
Remote operating system guess:
Linux 2.1.122 - 2.2.14

Nmap run completed - 1 IP address
(1 host up) scanned in 3 seconds
```

3. lista A scanlogd segítségével felderített kapupásztázás

```
Jul 18 02:56:22 target scanlogd: 192.168.0.1
to 192.168.0.2 ports 38681, 18, 1127, 1486, 966,
1493, 682, 401, 211, ..., f??pauxy, TOS 00 \
       @02:56:21
```

mert ha egy nagy forgalmú hálózaton használjuk, az ippl naplófálj (amit általában a `/var/log/ippl/` elérési úton találhatunk meg) nagyon gyorsan megtelhet.
Van néhány más lehetőség is az ippl-ben, sajnos ezekbe még nem tudtam belemélyedni. Valami azonban felkeltette az érdeklődésemet, és ez nem más, mint a pingd. Ez olyan felhasználó oldali démon, amely kiszolgálószinten kezeli az ICMP-forgalmat. Nagyon hasznos a pingdben, hogy együttműködik a TCP-burkolókkal, így a hozzáférést szabályozó állományban (/etc/hosts.allow és /etc/hosts.deny) jól beállítható, hogy ki pingelheti a gépet és ki nem.

Egyéb hálózatvizsgáló eljárások

A kapupásztázás és az általános ping csak kettő a hálózatvizsgáló eljárások közül. A jelenlegi módszerek száma jelentős, amellett folyamatos fejlesztés alatt állnak, ez pedig azt jelenti, hogy a rendszergazdák egyre érdekesebb kísérletekkel találkozhatnak a jövőben. A rengeteg egyéb típusú kísérlet közül egy párat ismer még az Nmap, ilyen például a csalétek pásztázás (Decoy Scan). Ennél a pásztázásnál a gép különböző IP-címekről kap kérelmet, így nem tudja megállapítani, hogy melyik gépről is indult ki a támadás. Ennek fő oka a rendszergazda megzavarása. A csalétek pásztázás (Decoy Scan) mellett, az Nmap képes megállapítani a kiszemelt számítógép operációs rendszerének típusát és annak változatát is. Ez a „TCP/IP-verem ujjlenyomat” (TCP/IP stack fingerprinting) nevű eljárás segítségével lehetséges. Ahogy azt a *2. listán* is láthattuk, az Nmap felismerte, hogy a célszámítógép a Linux 2.1.122–2.2.14 közötti változatát futtatta (a valóságban a 2.2.12-es változat futott a gépen). Írásom elkészítésekor az Nmap 2.53-as 465 különböző operációs rendszert (különböző változatokkal), útválasztót és egyéb eszközt képes felismerni és azonosítani.

4. lista Egy egyszerű Perl parancsfájl

```
#! /usr/bin/perl
$networkid = "192.168.0";
$begin = 1;
$end = 20;
for ($hostid = $begin; $hostid <= $end;
$hostid++) {
     print "$networkid.$hostid\n";
}
```

5. lista Az fpinggel futtatott általános ping

```
root@attacker# perl gen.pl | fping -a
192.168.0.17
192.168.0.15
192.168.0.12
192.168.0.10
192.168.0.1
```

6. lista Az ippl segítségével felderített pingkérelem

```
Jul 19 04:19:37 ICMP message type echo \
       request from
attacker.example.com [192.168.0.1] \
       (192.168.0.1->192.168.0.2)
```

Állandó figyelem

Remélem, hogy ez a kis írás hasznos lesz a két leggyakoribb hálózatvizsgáló eljárás működésének és felderítési módjainak megértéséhez. A megfelelő biztonságot természetesen folyamatosan szeretnénk fenntartani. A hálózatvizsgáló programokból egyre több lesz, újabb és újabb biztonsági lyukakat fedeznek fel, és gyakorlatilag naponta szerepelnek a hírekben, úgyhogy érdemes naprakész adatok birtokában lenni. Ezért ajánlatos feliratkozni egy biztonsági témájú levelezőlistára (például BUGTRAQ), vagy a hasonló témájú hírcsoportokat és weblapokat sűrűn látogatni.

Nmap: ➲ http://www.insecure.org/nmap
fping: ➲ http://www.stanford.edu/~schemers/docs/fping/

Lawrence Teo (lawrenceteo@usa.net) jelenleg a behatolási módszerek felderítéséről folytat kutatásokat a tudományos fokozat megszerzéséhez Ausztráliában, a Monash egyetemen. Amikor nem unixos gépekkel vacakol, egy jó japán éttermet keresve kóborol Melbourne utcáin.