Analysis of the Scan of the Month #18

Peter Turczak

September 20, 2001

General Analysis:

After successfully exploiting the statd and spawning a shell, the attacker issues a "cd /; uname -a; id;" which returns a few information which may be useful for further exploitation, such as operating system , kernelversion and the real and effective uid/gid of the shell that was spawned out of statd.

The next step was to fetch the rootkit (filename "lk.tgz") from the server "ftp.home.ro" with username "soane". After the transfer was completed, the ftp client was idle, until the server closed the idle connection. As a following step the ftp client was left and the attacker unpacked the rootkit "tar -zxvf lk.tgz". This rootkit gives some messages in romanian, which may be a hint to the origin of the attackers..

1. What modifications did they make to the break in process to both automate and make the process faster?

   The packet which exploited the vulnerability of statd is similar to the one created by ron1n's "statdx" [see IDS422]. They used a program similar to luckyroot[1], which is based upon "statdx" that automatically exploited the statd vulnerability and installs a rootkit. But again the commands executed have changed a little (see above).

   By doing this the attackers were able to infiltrate a machine nearly completely automatically. Only the fact, that there was a long idle time after the ftp download makes me think that the last part (downloading/installing the rootkit), was maybe done manually. But unfortunately i can't prove that.

2. What nationality are the badguys, and how were you able to determine this?

   Well, the ip which the exploit and the commands came from was a Korean one, but the server from which the rootkit was downloaded was a romanian one, the messages of the rootkit where also mostly romanian. The commands typed sound quite constructed, this may be because the attacker used a block oriented utility like "netcat" for the attack, or this was an at least partially automated one, which is the most probable to me.

   My idea is, that the attackers used a Korean machine for the attack. Maybe this system was already compromised by them and only used to hide their real origin.

[1] For a detailed discussion of luckyroot see: http://project.honeynet.org/scans/scan13/som/som19.txt

3. What nationality are the badguys, and how were you able to determine this?

   According to the server from which the rootkit was downloaded and the language of the rootkit i am almost certain that the badguys came from Romania.

4. What do the answers to questions #1 and #2 tell us about the tactics the badguys are using?

   The blackhat community seems to use compromised machines for hiding their traces. So we cannot continue to consider the attacking ip as the machine of the real attacker.

5. What did you learn from this challenge?

   As i already said, the most important fact is that the machine attacking maybe is not the real origin of the attack. Furthermore it is important to keep the versions uptodate and have a tripwire like system running, in order to prevent an undiscovered attack.

6. How long did this challenge take you?

   I needed two hours for writing a script to extract all the TCP sessions. One more hour was needed for answering the questions.‘