



Inside the Hacker's Head

The first suspicious activity is a generic information request such as: What is your name? And where are you from? The question is sent to one of the computers (xxx.xx.x.xxx). In this case the attacking computers (xx.xxx.xx.xx) just want to know which version of the domain system software is running on the computer. The attacker now has a target.

Using an automated tool, I can scan the ip addresses one at a time and I WILL have a target...

With the target, the attacker now sends a “buffer overflow” attack to the computer. The idea is to send a command to the computer that is so long that the computer now becomes confused. The attacker can then trick the computer into executing a command tacked onto the end of the buffer overflow.

Once again, with the automated tools (easily obtained from the web) I'll get a command prompt. From there, I can do whatever I want.

Once the command is in place, the attacker then double-checks some details, asking the name of the system that he/she's on, the current directory, and current id. Then he/she immediately adds user accounts to the machine so next time he/she will be able to log on as if he/she is a rightful user.

I AM IN. I will get to the root directory and have it tell me what it's called. Then I'll add several accounts (users/log on).

Now inside, the hacker can decide to install other software on the “honey pot” and multiple utilities and tools in the case the tools are recognized or disabled. With this, the hacker can connect to another system via ftp and download a tool kit to another target computer within the network.

My next step is to connect to an anonymous computer via the internet where I stored utilities software and downloaded it into the target system. If someone cancels the user accounts I've added, I will still have 100% access to the target system.

Typically, the backdoor telnet program is then installed. It allows telnet users with a specific setting to gain entry into the computer regardless of user name and password.

With the utility, I can telnet into the target accounts –I then cut and paste to make sure all of the commands that I want to use give me the full functionality I want to have.

To get rid of the activities, the hacker then pastes a long string of commands at a prompt designated to remove most of the files that would leave any trace of his/her visits.

With the above commands, I will erase any trace of my visit. Log files, timestamps, etc.

The hacker then uses ftp to a different computer to transfer the infamous “TRINOO program” into the “honey pot.” This is one of the programs that turn computers into zombies, ready to be used in a massive internet attack.

I wait for a month and “voila:” TRINOO is downloaded. Then I will turn all the target computers into zombies....I now have the key to the castle.