How a Hacker Can Attack in your network

A paper by Dr. Ajay Data , CEO, Data Infosys Limited

What is Denial-of-Service (DoS) Attacks

• Ping of death – Sends an invalid fragment, which starts before the end of packet, but extends past the end of the packet.

• Syn Flood – Sends TCP SYN packet (which starts connections) very rapidly, leaving the attacked machine waiting to complete a huge number of connections, and causing it to run out of resources and start dropping legitimate connections. A new defense against this is "SYN cookies." Each side of a connection has its own sequence number. In response to a SYN, the attacked machine creates a special sequence number that is a "cookie" of the connection, then "forgets" everything it knows about the connection. It can then recreate the forgotten information about the connection when the next
packets come in from a legitimate connection.

• Loop – Sends a forged SYN packet with identical source/destination address/port so that the system goes into an infinite loop trying to complete the TCP connection. System Configuration Holes Weaknesses in enterprise system configuration can be classified as follows:

To execute a Denial-of-Service (DOS) attack, a hacker uses Trojans to take control over a potentially unlimited number of zombie computers, which then take aim at a single target and flood it with traffic in an attempt to overwhelm the server.

• Default configurations – Most systems are shipped to customers with default, easy-to-use configurations. Unfortunately, "easy-to-use" can mean "easy-to-break-into" as well. Almost any UNIX or WinNT machine shipped can be exploited rather easily.

• Empty/Default root passwords – A surprising number of machines are configured with empty or default root/administrator passwords. One of the first things an intruder will do on a network is to scan all machines for empty passwords.

• Hole creation – Virtually all programs can be configured to run in a non-secure mode which can leave unnecessary holes on the system. Additionally, sometimes administrators will inadvertently open a hole on a machine. Most administration guides will suggest that administrators turn off everything that doesn't absolutely need to run on a machine in order to avoid accidental holes. Unfortunately this is easier said than done, since many administrators aren't familiar with disabling many common services. Exploiting Software Issues Software bugs can be exploited in the server daemons, the client applications, the operating system, and the network stack. Software bugs can be classified in the following manner:

• Buffer Overflows – Almost all the security holes you read about in the press are due to this problem. A typical example is a programmer who will set aside a specific number of characters to hold a login username. Hackers will look for these types of vulnerabilities, often sending longer strings than specified, including code that will be executed by the server. Hackers find these bugs in several ways. First, the source code for a lot of services is available on the net. Hackers routinely look through this code searching for programs that have buffer limitations. Hackers will also examine every place the program accepts input and try to overflow it with random data. If the program crashes, there is a good chance that carefully constructed input will allow the hacker to break into the system.

• Unexpected Combinations – Programs usually are constructed using many layers of code, including the underlying operating system as the bottom-most layer. Intruders can often send input that is meaningless to one layer, but meaningful to another when constructed properly.

• Unhandled Input – Most programs are written to handle valid input. Most programmers do not consider what happens when somebody enters input that doesn't match the specification. Exploiting the Human Factor Education of e-mail users by organizations regarding how hackers seek to exploit them has improved to the point that a large majority of e-mail users now have at least a rudimentary understanding of fundamental security. The basic message regarding not opening certain malicious attachment types, particularly .exe files, from unknown senders is widely known.

This means the hackers are being forced to redouble their efforts in order to counteract the education that e-mail users are receiving. Examples of hackers using sophisticated means to get users to open e-mail attachments include the following:

• Double Extension – The Netsky, lovegate, and Klez viruses took advantage of this vulnerability. Malicious files are given double extension such as “filename.txt.exe” to trick the user into running the executable. NetSky actually would place 100 spaces between the extensions so the victim would not see the second extension. NetSky would also put the DOS command “COM” at the end of a string that appeared to be a Web address ending in .COM.

• Password-Protected Zip File – Virus writers encrypt the virus in a password protected zip and send the file to users with the password in the message body. Since the encrypted file skips virus scanning, the end user gets what they think is legitimate e-mail. Unfortunately, in most cases this message has a look of urgency and the unsuspecting user will many times go the extra mile to open the malicious attachment.

• Plain Trickery – Hackers harvest e-mail addresses from “directory” servers and spoofing the “from” field with names the victim would recognize so they open the e-mail and attachments, and by trying to trick the victim into accessing a Web site. Common tactics include sending e-mails with headings with “re:” or “Re: re: re:” included to make the victim believe it is a chain e-mail. Another common header tactic is including technical terms that make the victim believe that e-mail system error was encountered; MyDoom used this tactic effectively. The Bagle worm would use icons of text file, folders, and Excel files for executables in hopes a user would not check the filename closely. The Sober.D worm tried to fool the user into believing that it was a patch delivered from Microsoft for the MyDoom worm. Again, this message contained a malicious attachment which preyed upon the user’s belief that the message was sent by a legitimate source.

Self-Propagation: The New Mission of Hacker Attacks

Hackers are becoming increasingly sophisticated and are no longer content with simply gaining access to networks to cause mischief and disrupt service. Whereas hackers first spread viruses through individual networks simply because they could, we now are seeing more and more attacks that involve the use of Trojans designed to spread a virus to as many computers as possible, with the intent of taking control of these machines for “hackers” purposes.

Trojans

Trojans enter the victim’s computer undetected, usually disguised as a legitimate e-mail attachment. Once the Trojan is opened by the unsuspecting recipient, the attacker is granted unrestricted access to the data stored on the computer. Trojans can either be hidden programs running on a computer, or hidden within a legitimate program, meaning a program that the user trusts will have functions they are not aware of. Black Orifice, Netbus, Bugbear are some of the most popular types of Trojans used by hackers

Spreading Viruses via Trojans

Hybrid attacks that combine the use of Trojans and traditional viruses have become increasingly popular. An example of this is the notorious Nimba virus that used multiple methods to spread itself and managed to get past anti-virus software by using a behavior not typically associated with viruses. Nimda exploited a flaw in the MIME header and managed to infect 8.3 million computers worldwide. The increased sophistication of attacks is evidenced by viruses containing their own SMTP engines (MyDoom, Bagle.G,
NetSky). By using its own SMTP engine, a virus can avoid the use of MAPI, which allows it to isolate itself from any e-mail client configuration issues and integrated virus scanner(s) that may be present.

About Xgen Plus

Xgen Plus is the Worlds Most Advanced Email Server Software providing innovative solutions to stop inbound e-mail threats such as spam, viruses, intrusions, spy ware, phishing, and protects against outbound policy and compliance violations. Xgen Plus uniquely communicates in a secured matter with other Xgen Plus server which means the more number of servers uses Xgen the more number of domains will get protected automatically.

Xgen Plus got the place on the Cover on Linux Magazine in Oct. 2005 issue and successfully running in 8 ISPs and 2000 domains all over world. Visit www.xgen.in for details.