Network Security

Author: Punit Ganshani
Email Address: punit@ganshani.com
Downloaded from http://www.ganshani.com
Published In: DeveloperIQ, December 2003, Asia

Abstract

Network Security is a matter of utmost importance to everyone. One entire life is based on presumption that our information is secure, and our actions are confidential – this is hardly the case. Securing your own machine is the first rule of privacy and protection but understanding and securing your network is just as important, especially in this world of cyber crime when a hacker can have complete access to your machine without physical access.

This paper presents the ways a hacker gets the root on your machine. It might appear that understanding network security from a hackers perspective is an upside down way of doing it – but understanding how attacks are made, is a needed in order to create protection against it. After all a thief only knows how to catch another one.

Collecting Information of Victim's Machine

Every system has some identification name, which is unique in that network. If we consider the Internet as a network then the system has a unique *Internet Protocol address* or *IP address* while in Ethernet the system may have different names as given by the administrator. This name can be also referred to by its IP address, which is local in nature.

An IP address is a 32 bit address or number normally written in decimal number system however it can be expressed in binary, hexadecimal or octal systems. The 32-bit address is divided into 4 decimal numbers (of 8 bits each). Assume these 4 decimals to be variables of format A.B.C.D

IP Address	Netmask	Class	Information		
0.0.0.0 to	255.0.0.0	I	First	8	bits represent NetID
126.255.255.255			Last	24	bits represent HostID
128.0.0.0 to	255.255.0.0	II	First	16	bits represent NetID
191.255.255.255			Last	16	bits represent HostID
192.0.0.0 to	255.255.255.0	III	First	24	bits represent NetID
223.255.255.255			Last	8	bits represent HostID
224.0.0.0 to	255.255.255.255	IV	First	32	bits represent
239.255.255.255					multicast GroupID

Now a typical IP address is 206.32.13.55. Here A is 206, B is 32, C is 13 and D is 55. The IP address changes every time you connect to Internet while in case of Cable connection or Ethernet it remains the same forever.
The IP address 206.32.13.55 belongs to Class III, which says that 206.32 is NetID and 13.55 is HostID.

Ways to get IP Address

1. YOUR OWN IP ADDRESS

    i. DOS has inbuilt command netstat
    ii. The Command netstat –n gives following information
        1. Local Address (Your IP Address)
        2. Visiting Site IP Address
        3. Protocol
            a. TCP in case of Internet
            b. Localhost in case of Ethernet

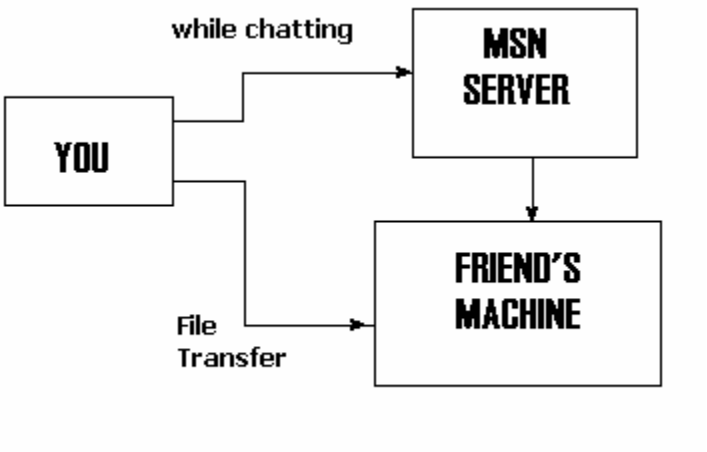
```
Ms DOS Prompt
C:\WINDOWS\Desktop>netstat /?
Displays protocol statistics and current TCP/IP network connections.
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
 -a         Displays all connections and listening ports.
 -e         Displays Ethernet statistics. This may be combined with the -s option
 -n         Displays addresses and port numbers in numerical form.
 -p proto   Shows connections for the protocol specified by proto; proto
            may be TCP or UDP.  If used with the -s option to display
            per-protocol statistics, proto may be TCP, UDP, or IP.
 -r         Displays the routing table.
 -s         Displays per-protocol statistics.  By default, statistics are
            shown for TCP, UDP and IP; the -p option may be used to specify
            a subset of the default.
 interval   Redisplays selected statistics, pausing interval seconds
            between each display.  Press CTRL+C to stop redisplaying
            statistics.  If omitted, netstat will print the current
            configuration information once.
```

2. VICTIMS IP ADDRESS

   i. MSN Messenger File Transfer

   While you transfer any file to your friend through MSN Messenger you are directly connected to his machine, which is not the case while chatting. This fact is evident from the figure shown below.

   In such case, you can again use netstat –n to get the Foreign IP address or your friend's machine.



ii. Through Your Website

A person visiting your website unknowingly can leave back his machine's IP address. However this method can't be so useful as IP address is dynamic each time when you connect to Internet.

iii. Through Email Headers

While sending emails, you unknowingly send your IP address to the receiver. This IP address can be seen in Email Headers.

Return-Path: <BhPat4@aol.com>
Delivered-To: p_b_ganshani@rediffmail.com
Received: (qmail 13334 invoked from network); **20 Aug 2002 13:23:20 *-0000***
Received: from unknown (HELO imo-m04.mx.aol.com) (**64.12.136.7**)
by mailserver with **SMTP**; 20 Aug 2002 13:23:20 -0000
Received: from BhPat4@aol.com
by **imo-m04.mx.aol.com** (mail_out_v33.5.) id j.1a7.711d7fc (4418)
for <p_b_ganshani@rediffmail.com>; Tue, 20 Aug 2002 09:21:34 -0400 (EDT)
Message-ID: <***1a7.711d7fc.2a939c5d@aol.com***>
Date: Tue, 20 Aug 2002 09:21:33 EDT
Subject: PgWorld
To: p_b_ganshani@rediffmail.com

The above text is direct copy of the header of a received email. The IP address of sender, the date, the server, the method to send the email (SMTP) are all available without any effort.

Information from IP Address

Geographical Information Using IP Address

Using IP Address following information can be obtained:

- Continent, Country
- City, ISP's name
- Phone Number, Home Address
- Full Name of Victim.

Let me take my IP address: 203.98.12.34

Each ISP is given some Network IP address say 203.98.12 and 34 is the your particular Identity at some time. Thus all people using a particular ISP will have their IP addresses in a particular range. However as IP addresses are dynamic, ISP maintain the record of phone number and allotted IP address to their users.

How:

Method 1

To get the geographical address of a machine, we can use the traceroute facility of DOS.

tracert IP or *Hostname*

C:\WINDOWS\Desktop>tracert *203.98.12.34*
Tracing route to 203.98.12.34 over a maximum of 30 hops

1 mail.myisp.com (232.65.55.22) 2 ms 1 ms 1ms
2 we21.backbone.com 5 ms 5 ms 1ms
3 mtnl.net.in (203.194.56.00) 105 ms 67 ms 22 ms
Trace complete.

It indicates that on IP address 203.98.12.34 (my IP address) the information is sent using ISP *myisp* through *backbone.com* to the site *mtnl.net.in* which is Mumbai's ISP. Thus we can get the complete information.

Method 2

Through Internet Sites we can get the information by simply writing the IP address in the text box.

http://cello.cs.uiuc.edu/cgi-bin/slamm/ip2ll/ or
www.visualroute.com

These sites just don't tell you the victim's visiting site but also their Operating System, the internet settings and many more information.

IP Spoofing

Spoofing is the creation of TCP/IP packets using somebody else's IP address. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source.

A common misconception is that "IP spoofing" can be used to hide your IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection.

However, IP spoofing is an integral part of many network attacks that do not need to see responses (blind spoofing).

The Mechanism

- You send a packet to the VICTIM from your FAKE IP Address.
- VICTIM acknowledges you by sending a packet back to your FAKE IP Address.
- You have to assume that VICTIM might have sent you the packet on FAKE IP Address
- So after some time, you again shoot a packet to the VICTIM to tell him that you received its Acknowledgment packet.

This continues on assumptions.

How is IP Spoofing Done

IP Spoofing is very risky however a proper proxy server can suite you as IP Spoofing media. You have to find a TRUSTED site that can very well act as server. However this server **should never respond** to the received acknowledged packet from VICTIM.

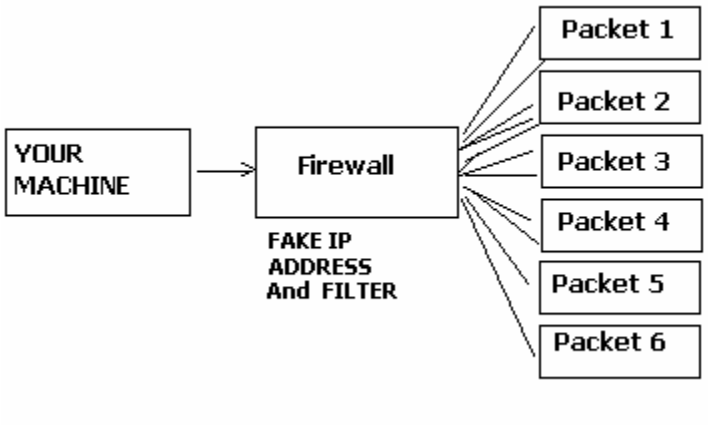
Ways to get a TRUSTED system:

- By digging the maximum information of the VICTIM and its network.
  This is done by IP address and using various Internet sites as mentioned earlier.

- Brute Force System:
  A brute force system is applied on the network to check the reliability of the network to be treated as a TRUSTED system.

Thus to ensure this, the TRUSTED system should be blocked which is done by using up all the memory of the TRUSTED system so that it doesn't respond to Synchronized Acknowledged packets sent by the VICTIM. Thus once the TRUSTED system gets

blocked, then we can be assured of being freed of problems during IP Spoofing mentioned above.



IP Spoofing can also be implemented by using a FIREWALL system. A firewall system acts as a FILTER. It acts as a barrier to the unwanted packets coming to our machine. But a good firewall is one that can monitor both packets leaving the machine and those coming to the same.

While sending the packets, a good firewall deletes or stops those packets that don't go to desired part of the network.

Unspoofing

The amount and frequency of denial of service attacks are escalating. It is becoming harder to track down the source who initiates them due to trace-evasion techniques. A raw interface to the networking stack allows anyone to send spoofed packets to a target host, eliminating the ability of its administrator to determine the origin of the attack. In today's world of e-commerce and globalization, the devastating attacks and the inability to determine their source can be devastating. It gives small companies a bad name, and destroys the good reputations of larger companies.

The ability to track down the source that uses spoofing techniques will certainly increase the chance to catch those attacking, and will force people to think of more intricate ways to attack servers on the net. This paper describes a few ways to track down these sort of attacks up to the last link in the chain (the attacker himself), or at least his ISP.

Usually, when a denial of service attack is initiated against a target host, it is something like:

./attack target.com

In order to send the spoofed packets to **target.com**, the attacker's NameServer has to resolve its domain name to an IP address, and only then can it inject the malicious

packets. In theory, the NameServers for **target.com** will receive packets originating from the true source host of the attack or their NameServer. If we keep a log of these DNS queries, we could later *cross-reference logs* of the attack and the queries, look for equal or very small differences in the timestamps, and in most cases, we will have a certain match.

We must also be careful in what we do log; too much data can be just as useless as not enough logging. If we just log all external hosts attempting to resolve an internal host, this should cut down the amount of possibilities considerably.

Tracing the attacker

Assuming the attacker uses his ISPs NameServers, we can tell his ISP from our logs, contact them, and have them do the cross-referencing. In fact, once we have a source host, we can contact its owners, and have them look at logs and do the cross-referencing for the respective times of the attack.

In short: The host we have in our logs is either the attacker himself doing the DNS query, or a NameServer he used to perform the query. In either case, assuming proper logging is in place, we have the true source of the attack.

Attacks

There are several types of attacks a hacker tries to get the root on the machine. Some of them are discussed here:

Land Attack

An Attacker is trying to slow down your machine.

Attacker has sent a frame to the system with the same source and destination IP address being that of the system. This requires the IP address to be spoofed.

Because this is theoretically impossible, the Windows stack doesn't handle the condition correctly. While the system doesn't crash, each packet received causes a temporary slow-down. This is caused by the system trying to resolve an infinite series of connections to itself.

Defense

Fixes are available for most operating systems - consult your operating system vendor for more information, or look at the CERT and Microsoft Advisories on this subject.

Teardrop Attack

Denial of Service attempt

Dangerous IP fragment overlap generated by teardrop program. Your operating system may become unstable or crash. Fixes are available for most operating systems - consult your operating system vendor for more information, or look at the CERT and Microsoft Advisories on this subject.

The source address is likely to be spoofed. This means that the sender of the frame is probably not using his ***actual source address***, and is pretending to be someone else. Unfortunately, there is no easy way to determine who is actually sending spoofed frames.

Ping of Death Attack

This indicated an attempt to crash your system.

A TCP/IP packet with a theoretical length greater than 65536-bytes has been sent to the machine. This attack was popular around July of 1997, but since then most systems have been patched to prevent this bug.

TCP/IP supports a feature called "fragmentation", where a single IP-packet can be broken down into smaller segments. This is needed because the typical Internet connection (dial-up, Ethernet, cable-modem, etc.) only supports packets of around a couple thousand bytes, but IP supports packets up to 64-kbytes. Thus, when sending a single packet that is too large for a link, it is broken up into smaller packet fragments.

A quirk of IP is that while a single packet cannot exceed 65536-bytes, the fragments themselves can add up to more than that. The "**Ping of Death**" technique does just that. Since this is a condition thought impossible, operating systems crash when they receive this data.

Ping of death can actually be run from older versions of Windows. At a command line, simply type:

ping -l 65550 VICTIM

A further bug in Windows is that it not only crashes when it receives the invalid data, but it can accidentally also generate it. *Newer versions of Windows prevent you from sending these packets.*

Spoofing

Ping-of-Death packets are easily spoofed, so you cannot rely upon the IP address of the sender.

Aliases

There are lots of variants to this attack: jolt, sPING, ICMP bug, IceNewk, Ping o' Death

IP Source Route

Intruder is using "source routing" in order to break into the system.

The "source routing" feature of TCP/IP allows the sender of network traffic to force the traffic to be routed through a certain point on the network. This is useful because it allows intruders to force packets to travel in unexpected directions.

For example, many organizations and home users use private addresses like 192.168.x.x. These addresses are not normally reachable on the Internet, yet intruders can still reach them by source routing through a machine that supports source routing.

False Positives

Some network management utilities employ source routing in order to map the network. You can set "trust" levels on the intrusion detection system in order to mask these events from those platforms.

Defense

Most systems allow source routing to be disabled.

TCP SYN flood Attack

Denial of service overload attempt.

The SYN flood attack sends TCP connections requests faster than the system can process them. This causes the memory to fill up, forcing the new connections to be ignored. The effect of this is to make it appear as if the system is either very slow, or not available at all.

False Positives

This detection triggers whenever a large number of SYN packets are seen in a short period of time. There are cases where it will trigger incorrectly. For example, if a busy web-site becomes unavailable for a few minutes, then is brought back online, this event triggers because of the "pent up" connections waiting for the system to become available. If this report occurs frequently on your network, and your network appears to be operating correctly, you should adjust the value of the **tcp.maxsyn** parameter in the configuration file to reflect the characteristics of your network.

Spoofing

In SYN floods, the source IP address is almost always spoofed. Therefore, the source IP address cannot be used to track the intruder.

Defense

Many *firewalls* come with SYN flood protection features.

Many *open source* UNIX systems (Linux, xBSD, etc.) have patches available that can be used to minimize the impact of SYN floods.

WinNT can be reconfigured to minimize the impact of SYN floods.

DNS Spoofing

Two responses were received when looking up a computer name. This might indicate an attempt to redirect the system from a well-known website to a hostile website.

When visiting websites, such as **http://www.punitganshani.com/**, the system must first resolve the name into an IP address using DNS. This is similar to how you must lookup someone's name in the phone book in order to dial their telephone number.

There exists a hacker technique whereby they can sometimes force a duplicate reply to the DNS lookup. Using the phone book analogy, it is similar to calling 411/information for somebody's number and getting back two replies. Imagine a hacker breaking into the phone system such that the first number you heard was to the hacker. The hacker who broke into the telephone system might use this technique to redirect people buying with credit cards to his own phone number, then pretend to be the real vendor, then steal the credit card numbers. In much the same way, hackers use this DNS spoof in order to redirect people to their own website.

False Positives

This symptom is caused when two different copies of a DNS response have been received. However, we are finding that home users are seeing such behavior from ISPs. Some ISPs attempt to re-direct users through their own caching servers. Therefore, this "spoof" symptom doesn't actually indicate a hostile attack.

Removing the Traces from the Root

All work is not a game of fun unless the hacker retains the traces of attack. Here comes **Network Security**.

Each and every move is traced in by the remote system from the time you log in. And when it comes to system using Unix it becomes even tough. Unix keeps the track of messages you send till you log out. And the remote system keeps the track of all the information received. It becomes easy to trace the attacker.

syslog Daemon

The syslog daemon is used to log all types of activities may it be kernel messages, system messages, commands, logins & log outs. The syslog is located at: **\usr\sbin\syslogd** This syslog is helped by a configuration file named *syslog.conf*. It tells the syslog which activities it has to trace.

So either you can remove the lines like

Log all kernel messages to the consol
Log anything (except mail) of level info or higher

Or you can delete the log files created. The paths and the Information of the same is as given below

Information	Location
Log Mail Messages	/var/maillog
News and Mail Errors	/var/spoolers
TCP Wrappers Log File	/var/secure
Logs everything,except mails	/var/messages
Logs all Logins and Logout	/var/adm/wtmp
Similar to above	/var/adm/utmp
Last Login information	/var/adm/lastlogin

By default, all log files are stored in /var/log directory. However the administrator can easily change the directory from *syslog.conf* So it is advisable to always take the root.

Trojans

Once the attacker gets the root he can install a Trojan or a key logger that really harm the system. Trojan binds itself to a port and enables it even when the computer is switched off.

Working of Trojans

- Trojan runs on server & a part of it runs on client.
- Trojan is normally sent through ICQ or messenger service
- Trojan installs itself manually to get physical access of the machine
- It is normally put into a single .EXE file that is executed the most.
- Trojan installs itself on particular port on the target system and listens for connections.

Detection of Trojans

- Detect the Trojan by using **netstat –n** when no connections are established. If it says that port is listening then a Trojan is installed
- Trojans secretly send mails through SMTP port or 25 Port. So mails going through these ports should be monitored.
- Using various tools like Lockdown 2000, Prcview
- A Virus detection method

Trojan Cum Virus Detection Method

Windows gives you the best platform to do various operations but this little master also allows viruses to load themselves. All viruses normally put their initialization string or the call in one of these registry branch
HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER
Keys:

Run
RunOnce
RunOnceEX
Runservices
RunservicesOnce

These keys may contain the call to anti-virus software, or modem driver but to anything else is dangerous. Delete the key value not the key which contains something ambiguous.

References

- Unofficial Guide to Ethical Hacking, Ankit Fadia
- The Hacker, BPB Publications

Online References

- neworder.box.sk
- www.securityfocus.com
- www.winguides.com