*Available online a*t www.scientiaresearchlibrary.com

**Scientia Research Library**

**Journal of Engineering And Technology Research,**
**2013, 1 (1):22-41**

(*http://www.scientiaresearchlibrary.com/arhcive.php*)

# Remote System Accessing and Network Security Using Efficient Experimental Techniques

**Er. Asim Ahmad[1], Er. Avadhesh Kumar Maurya[2],Prof. (Dr.) Vishwa Nath Maurya[2]**

*Department of Mathematics, School of Science & Technology,*
*University of Fiji, Saweni/Suva, Fiji Islands*
*Department of Electronics & Communication Engineering,*
*Lucknow Institute of Technology, G.B. Technical University, India*
*Department of Information Technology,*
*Lucknow Institute of Technology, G.B. Technical University, India*

## ABSTARCT

*Present paper demonstrates a novel approach for remote system accessing and network security techniques. This paper contains five sections and organized as follows. Section 1 describes an overview of frequently occurring network attacks and discusses related earlier research works carried out so far, also presents the experimental results. Section 2 describes some basic concepts of Internet Protocol (IP) address, special cases of IP addresses, conversion of a DNS IP address into a normal IP address, and ruling for Internet Protocol address. Section 3 discusses remote system accessing through various experimental techniques such as instant messaging software, through websites, HTTP and scripting methods, email headers, internet relay chat (IRC), and netstat. In addition to that, the present paper also includes a brief discussion on various counter-measures that can be taken to prevent a system whether desktop or any system in a network to be get accessed from outside the network (to which it belongs) without the knowledge of administrator. In section 4, two experimental techniques for hiding IP addresses have been proposed. Finally, the outcomes of our current study have been summarized in our conclusive observations in section 5. We remark here that some experimental techniques explored herein for remote system accessing and network security are much more efficient in the detection of network intrusions, compared with network based techniques; therefore, the proposed experimental techniques are useful particularly for network users.*

**Keywords**: Internet protocol address, remote system accessing, network security, instant messaging software, internet relay chat, netstat,

## INTRODUCTION

With the exponential development of computer network technologies and applications in all emerging fields of science and technology, innovations on remote system accessing and network security techniques carried out by previous researchers have been greatly recognized because of increasing demand both in number and severity. The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Usually, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service

Strict procedures for accessing to the machine room are used by various organizations, and these procedures are often an organization's only obvious computer security measures. Today, however, with pervasive remote terminal access, communications, and networking, physical measures rarely provide meaningful protection for either the information or the service; only the hardware is secure. Nonetheless, most computer facilities continue to protect their physical machine far better than they do their data, even when the value of the data is several times greater than the value of the hardware.

The U.S. Department of Defense has established its own definition of computer security, accepted in Trusted Computer System Evaluation Criteria (Department of Defense 1985), also called "the Orange Book" after the color of its cover /and hereafter shortened to "the Criteria"). The document employs the concept of a trusted computing base, a combination of computer hardware and an operating system that supports untrusted applications and users. The seven levels of trust identified by the Criteria range from systems that have minimal protection features to those that provide the highest level of security modern technology can produce (table1.1). The Criteria attempts to define objective guidelines on which to base evaluations of both commercial systems and those developed for military applications. The National Computer Security Center, the official evaluator for the Defense Department, maintains an Evaluated Products List of commercial systems that it has rated according to the Criteria. The Criteria is a technical document that defines many computer security concepts and provides guidelines for their implementation. It focuses primarily on general-purpose operating systems. To assist in the evaluation of networks, the National Computer Security Center has published the Trusted Network Interpretation (National Computer Security Center 1987), which interprets the Criteria from the point of view of network security. The Trusted Network Interpretation identifies security features not mentioned in the Criteria that apply to networks and individual components within networks, and shows how they fit into the Criteria ratings.

It is unfair to fault vendors entirely for this lack of attention to security. While customers may want improved security, they usually have second thoughts when security features adversely affect other, "more important" features. Since few customers are willing to pay extra for security, vendors have had little incentive to invest in extensive security enhancements.

A few vendors have taken steps to help the few security-conscious customers who are willing to invest in additional protection. These customers include not only the government but some banks, manufacturers, and universities. Several add-on security packages for major operating systems have been on the market for some time. The most notable of these are CGA Software Products Group's TOP SECRET, Uccel Corporation's ACF2, and IBM's RACF, all for IBM's MVS operating system. Stronger mandatory controls designed to be integrated into the operating system appear in SES/VMS, an enhancement to VMS offered by Digital Equipment (Blotcky, Lynch, and Lipner 1986), and are under development in the Sperry (now Unisys) 1100 operating system (Ashland 1985). These packages and enhancements are commercially sustainable in spite of their significant purchase and administrative costs. Several vendors have made a substantial investment in internal security enhancements to their operating systems without cost add-ons. These systems include DEC's VMS and Honeywell's Multics (Organick 1972; Whitmore et al. 1973). Control Data has also incorporated security enhancements into its NOS operating system. Honeywell was the first to offer commercially a highly secure minicomputer, the SCOMP (Fraim 1983), based on a security kernel. Gemini Computers offers the GEMSOS operating system, also based on a security kernel (Schell, Tao, and Heckman 1985). Thus, literature shows that some venders paid their attention to take initiative steps in connection with security-conscious customers who are willing to invest in additional protection. Likewise, several previous researchers confined their attention to contribute in connection with remote system accessing and network security. Some of these noteworthy researchers [1, 2, 4, 6, 8, 10, 18, 19, 21…23] are worth mentioning for their significant contribution in this direction. Some other researchers (e.g. [3, 7, 9, 11…14, 16, 19 & 20]) contributed to explore different techniques and cost benefit models in different framework of software testing and network security. Moreover, a worth mentioning textbook authored by Oollmann (1999) can be refereed on the subject. Intrusion Detection System (IDS) as a key technique in network security domain was suggested by Gandhi and Srivatsa [7]. It is worth mentioning hare that main purpose of IDS is to find out intrusions among normal audit data and this can be considered as classification problem. Intrusion detection systems (IDS) are an effective security technology, which can detect, prevent and possibly react to the attack. It performs monitoring of target sources of activities, such as audit and network traffic data in computer or network systems, requiring security measures, and employs various techniques for providing security services. With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more important than ever before. Symantec in a recent report uncovered that the number of fishing attacks targeted at stealing confidential information such as credit card numbers, passwords, and other financial information are on the rise, going from 9 million attacks in June 2004 to over 33 million in less than a year. One solution to this is the use of network intrusion detection systems (NIDS), which detect attacks by observing various network activities. It is therefore crucial that such systems are accurate in identifying attacks, quick to train and generate as few false positives as possible.

Here in the present paper, a brief discussion on everything related to Internet Protocol addresses and various useful accessing techniques have been demonstrated by which a system can be accessed in any network from any system outside that network. We remark here that the remote system accessing and network security techniques suggested in the present paper are very simple to understand and implement. Since any attacker or crackers can use any of these techniques, and cause a great harm to any other system administrator, it is necessary to all the networked users like LAN and Internet users to be cautious from these types of persons and activities while surfing in any network like LAN or Internet. Even, various types of counter-measures as precautions are also stated with these accessing techniques. Experimental results have demonstrated that this model is much more efficient in the detection of network intrusions, compared with network based techniques. It is recommended here to the entire Internet and other network loving persons to be alert from them as without knowing you the hackers or crackers used to break into your systems and play around as they feel like.

Table 1.1: Seven levels of trust identified by the Criteria range from systems

| Class | Title | Key Features |
|---|---|---|
| A1 | Verified Design | Formal top-level specification and verification, formal covert channel analysis, informal code correspondence demonstration |
| B3 | Security Domains | Reference monitor (security kernel), “highly resistant to penetration” |
| B2 | Structured Protection | Formal model, covert channels constrained, security-oriented architecture, “relatively resistant to penetration” |
| B1 | Labeled Security Protection | Mandatory access controls, security labeling, removal of security-related flaws |
| C2 | Controlled Access | Individual accountability, extensive auditing, add-on packages |
| C1 | Discretionary | Discretionary access controls, protection against accidents among cooperating users |
| D | Minimal Protection | Unrated |

## MATERIAL AND METHODS

### Basic Concepts of Internet Protocol (IP) Address

As people have home addresses, telephone numbers or some other identities that others can be used to contact them or uniquely identify them in a group of people, every system connected to the Internet or to a particular network has its own unique Internet protocol address or IP address. IP address is important because it represents our identity on the Internet. It is the address to which all data is sent and received. Later we shall be discussing everything that you would ever want to know related to IP addresses.

### Different Types of IP Addresses

You have learned that an IP address is a decimal notation of a computer's address in the computer’s world. The address of a computer does not necessarily have to be in the dotted-decimal format. It can be represented in several other ways, including the following:

- **Domain Name System (DNS)**: If an IP address is represented in the form of human-recognizable characters and names (for example, www.google.com), then it is said to be in the form of DNS.

- **DWORD Format:** DWORD (short for 'double word') basically consists of two bi-nary 'words' (or lengths) of 16 bits, but is almost always represented in the decimal number system (that is, having a base 10). An example of a DWORD IP address is 403A8ED4, which, when represented in the form of a decimal number system with a base 10, becomes 1077579476.
- **Octal System:** If an IP address is represented in the octal system, then it means that it is represented in the base-8 system (for example, http://Ol1O.0092.0117.0346).
- **Hexadecimal System:** If an IP address is represented in the hexadecimal system, as is 403A8ED4, then it is represented in the base-16 system.
- **Cross Breed:** If an IP address is represented using a mixture of two of any of the preceding systems, then it is said to be a 'cross breed.' (If you create a cross-breed lP address, note that browser compatibility may become an issue.)

**Special Cases of IP Addresses**

There are a few special IP addresses on the Internet which are used only under special circumstances:

- **The limited-broadcast IP address:** The limited broadcast IP address is 255.255.255.255. This special IP address is most commonly used during system setup, when the system has little idea about its own IP address and subnet address. It is also seen quite often in the routing tables of various systems. Keeping in mind IP routing, packets addressed to this address are never forwarded by routers.
- **The network-directed broadcast IP address:** This special IP address has the host part made up of all 255s, with its network part the same as that of the network to which it is applicable. A typical example is 203.255.255.255, where the network part of the IP address is 203 and the remaining part is the host-address part. Routers usually forward packets addressed to a network directed broadcast address.
- **The sub net-directed broadcast IP address:** In such an IP address, the host part of the address is represented by 255s, whereas the subnet part of the address stands for an actual sub net.
- **All-subnets-directed broadcast IP address:** Here, both the host and the subnet part of the address are represented by 255s. The subnet mask of the network must be known wherever such an address is being used.
- **The loopback IP address:** This special IP address stands for the local host system. A packet addressed to the loopback address is actually addressed to the same local machine from which it originated. In effect, both the source and destination IP addresses point to the same system, though their values might be different. All loopback addresses must have the network part as 127; the most commonly used loopback address is 127.0.0.1.
- **The zeros IP address:** Typically, the 0.0.0.0 IP address is used as the zeros IP address. Such an IP address is mostly seen in a system's log files. If you see packets being sent from the zeros IP address, it means that an attacker is trying to fingerprint the target system (that is, the system where the log files were examined).

**Conversion of a DNS IP Address into a Normal IP Address**

Now that you have seen the various forms in which an IP address can be represented, let's move on to learning how to convert DNS IP addresses into different forms, using the IP address www.yahoo.com as an example. First, let's convert www.yahoo.com to its normal decimal-dotted

IP address. You can easily get the IP address of a domain by simple method name as “ping”. On command prompt of a system that is connected to internet type ping as shown below and you will get normal decimal-dotted IP address as shown below:

```
• C:\Documents and Settings\ username>ping yahoo.com
• Pinging  yahoo.com [64.58.79.230] with 32 bytes of data:
• Reply from 64.58.79.230: bytes = 32  time = 702ms  TTL = 235
• Reply from 64.58.79.230: bytes = 32  time = 702ms  TTL = 235
• Reply from 64.58.79.230: bytes = 32  time = 702ms  TTL = 235
• Reply from 64.58.79.230: bytes = 32  time = 702ms  TTL = 235
• Ping statistics for 64.58.79.230: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds: Minimum = 712ms, Maximum = 781ms,
  Average = 555ms
```

- The preceding code snippet clearly shows that the decimal-notation IP address of the target system is 64.58.79.230.

### Ruling for Internet Protocol Address

How do you find out the IP address of your own system? Follow these steps:

- Step 1. Connect to the Internet
- Step 2. Launch MS-DOS
- Step 3. Type netstat -n at the prompt.

You will get an output similar to the following table 2.1:

Table 2.1: Active Connections

| Proto | Local Address | Foreign Address | State |
|---|---|---|---|
| TCP | 192.68.0.23:1230 | 46.149.75.83:80 | TIME WAIT |

The IP address shown in the Local Address field denotes the IP address of your system. For example, in this case the IP address of the local system is 192.68.0.23. First two octets of your IP address will not change whereas the last two octets probably.

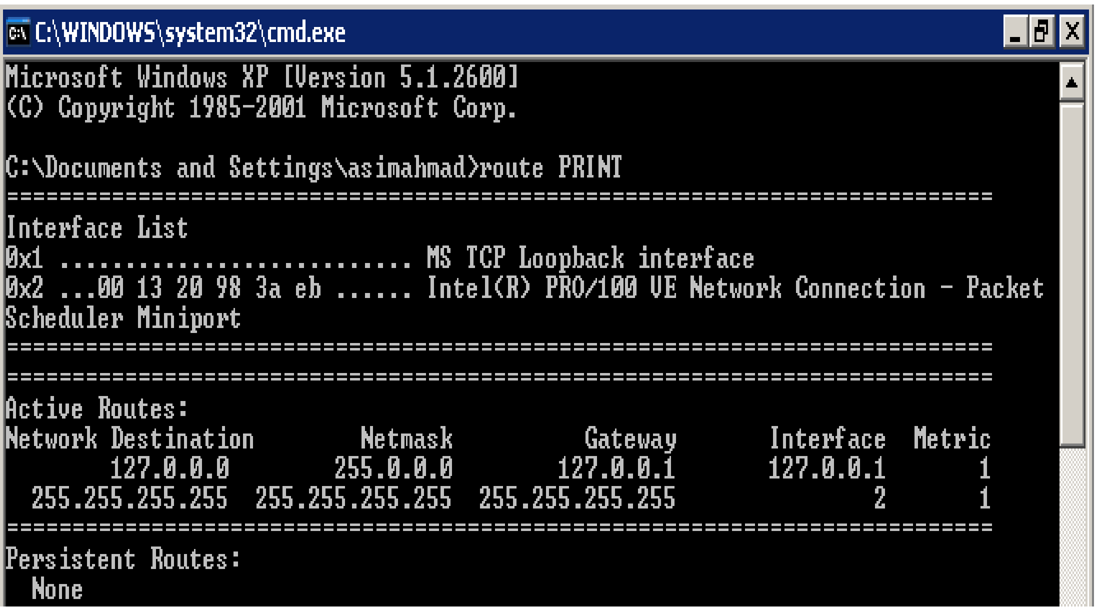
### Netmask Values for Network ID

A 'netmask value' is a 32-bit value containing one bits (255s) for the network ID and zero bits (Os) for the host ID. Using the netmask value, you can easily determine how many bits are reserved for the net ID and how many bits for the host ID. In other words, by studying the netmask value of an IP address, you can determine the class to which an IP address belongs. To find out the netmask value of an IP address, issue the following command:

```
C:\Documents and Settings\Asim Ahmad>route PRINT
```

And output is as shown below in table 2.2:

Table 2.2: Output for given Netmask values of Network ID



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\asimahmad>route PRINT
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 13 20 98 3a eb ...... Intel(R) PRO/100 VE Network Connection - Packet
Scheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
  255.255.255.255  255.255.255.255  255.255.255.255               2       1
===========================================================================
Persistent Routes:
  None
```

### Port Numbers and Sockets

Every system connected to the Internet has a number of ports open on it. Ports are basically virtual doors that allow the inflow and outflow of data packets. Without the opening of ports, no data communication can take place on a particular system. Typically, each time a client establishes a new connection over the network, a randomly chosen port number gets opened. Similarly, each time a service is enabled on a server, it automatically opens a predefined port number and listens for any clients who might want to establish a connection. Typically, port numbers are of three different types:

- Well-known port numbers
- Registered port numbers
- Dynamic/private port numbers

### Well-Known Port Numbers

Well-known ports are those that range in number from 0 to 1023. Each port in this range usually has a specific service running on it. In fact, an internationally accepted port numbers to services listing (known as Request for Comments or RFC 1700) fixes all services (like FTP, SMTP, POP and others) to their respective predefined port numbers. For example, by default the FTP service usually runs on Port 21 on most servers on the Internet. In other words, if you find that port 21 is open on a particular system, then it usually means that that system uses FTP to transfer files. However, it is important to note that system administrators are not forced to follow the service-to-port number rule. It is quite possible for a system administrator to choose to run the FTP service on a port other than 21.

We remark here that some smart system administrators run fake services on popular ports in order to make fool users. For example, a system might run a fake FTP daemon on port 21. Although the fake FTP daemon might present the same interface, banner and response numbers as a real FTP daemon, however, in reality it might actually record the intruder's presence sometimes even leading to the tracing of the intruder!

### Registered Port Numbers

Registered ports are those that range in number from 1024 to 49151. Ports in this range are not bound to any specific services. In fact, networking utilities such as your browser, email client and FTP client open random ports within this range to initiate communication with a remote server.

Port numbers within this range are what enable you to surf the Net, check your email and the like. That's why if you issue the netstat -a command and discover that a number of ports in this range are open, there's probably nothing to worry about. The ports are probably just opened temporarily by various applications to enable them to perform the tasks you want them to perform. They act as a buffer, transferring packets (data) to and from applications. For example; when you type www.hotmail.com in your browser, your browser randomly chooses a registered port and uses it as a buffer to communicate with the various remote servers involved. When you close the application, you will probably find that the port follows suit, closing automatically.

### Dynamic or Private Port Numbers

Dynamic or private ports are those that range in number from 49152 to 65535. This range of port numbers is rarely used by normal applications. Typically, on most occasions, port numbers in this range are used by malicious programs like Trojans, Keyloggers or spyware tools. However, on certain occasions, even legitimate applications use ports in this high range. For example, Sun starts its RPC ports at 32768. If you issue a netstat -a command and find that a port(s) in this range is open, then the following steps can be taken to detect the presence of any malicious tool installed on your system:

1.Check the Trojan list in Appendix C, 'Trojan Port Numbers,' to see if the open port numbers on your system match any of those listed.

2.If you have a match, it might mean that you have a Trojan installed on your system. You should use an appropriate Trojan removal tool to remove the Trojan infection from your system. If none of the open port numbers on your system match those listed in Appendix C, or if the Trojan-removal software indicates that no Trojan was found, then you have nothing to worry about.

### Remote System Accessing

To get access to a remote system an attacker's primary aim is to obtain remote system's IP address. An attacker can obtain the IP address of a remote system using a number of different, techniques. Some of the most popular enumeration techniques include the following:

- Through Instant Messaging software
- Through Websites
- Through HTTP and scripting methods
- Through Email Headers
- Through Internet Relay Chat (IRC)
- Through Netstat

Now we discuss these techniques of enumerating remote IP addresses and the countermeasures that you can be employed against them.

### Remote System Accessing Through Instant Messaging Software

The most common technique of enumerating the IP address of remote systems is through instant messaging software such as ICQ, MSN Messenger, Yahoo Messenger, AIM, and so on, some of which are discussed briefly in this section.

### ICQ

I Seek You, or ICQ, is among the most popular chatting software around. With it comes not only a fun and easy way to pass the time, but also security concerns. Specifically, whenever you start a chat session with a friend in ICQ, a direct connection between you and your friend is opened by the ICQ software with the help of the ICQ server. Thus, assuming that your IP address is xx.xx.xx.xx and your friend's IP address is yy.yy.yy.yy, all messages that you type are sent in the following manner:

ICQ has a built-in IP address hider, which, when enabled, should hide your IP address from those users with whom you are chatting. Like most software, however, IP-hiding software is not perfect. Indeed, you can find out the IP address of any ICQ user even if -IP hiding has been enabled by following these steps:

(i) Launch MS-DOS.
(ii) Type netstat -n to get a list of already open ports and the IPs of the machines with which a connection has been established. Jot down this list.
(iii)Launch ICQ, and send a message to the victim
(iv)While you are chatting, return to MS-DOS and again issue the netstat -n command. You will find a new IP signifying a new connection. This will probably be the victim’s IP address.

It should be remarkable here that this method of obtaining the IP address of the person with whom you are chatting is quite common because it works only with ICQ and other select instant messengers. However, it does not work with MSN messenger, Yahoo messenger, and other similar messengers.

### Other Instant Messengers

Whenever you start a chat session with a friend on other instant messengers like MS Messenger, an indirect connection between you and your friend is opened via the MS server. Thus, all me sage that you type first go to the MS server, which then forwards them to your friend and vice versa. Communication takes place in the following manner:

xx.xx.xx.xx ---------------------→ MSN server ---------------------→ yy.yy.yy.yy
(you) (your friend)

Similarly, all the messages that your friend types reach you in the following manner:

yy.yy.yy.yy ---------------------→ MSN server ---------------------→ xx.xx.xx.xx
(your friend) (you)

Because an indirect connection is established between your system (xx.xx.xx.xx) and your friend's system (yy.yy.yy.yy), issuing the netstat -n command does not reveal your friend's IP address. It instead displays the IP address of the MSN server. (The same is true for AOL Messenger, Yahoo Messenger and most other messaging software.) However, even utilities such as MSN Messenger are vulnerable to disclosing the IP address of the target system when the netstat -n command is issued. All you have to do is to follow these steps:

(i) Get the victim to come online and chat with you on MSN Messenger.
(ii) Use MSN Messenger's built-in file-transfer feature to send a file to the victim.
(iii)When the victim accepts the file transfer and the transfer process starts, launch MS-DOS and issue the netstat –n command. The victim’s IP address will be revealed because when files are transferred, a direct connection exists between you and the victim; there is no

mediating MSN server.

Here, we remark that an attacker will be able to find out a remote computer's IP address even if they send a request for a call and the victim accepts it.

### Counter Measures in Instant Messaging Software

Unfortunately, using messaging software does make your system vulnerable. If you are looking for a fool-proof counter-measure, or if you are really particular about remaining anonymous while instant messaging, then you should probably stop chatting! If that's not an option, there are a few ways to prevent from hackers.

First, and most simply, do not accept any file transfers-or call requests from people you do not trust. This will prevent those with malicious intent from getting a look at your IP address. Another thing you can do is to install on your system a firewall that does not respond to external packets coming from not-trusted sources. This will prevent attackers from sending malicious data packets to the victim.

### Cautions

Using a firewall will not prevent people from finding out your IP address, since it does not prevent attackers from using the netstat command. Also, some firewalls even filter out normal chat conversations, thus making the use of instant messengers impossible. The most fool-proof counter-measure you can take to prevent hackers from obtaining your IP address via instant messaging software is to chat through proxy servers like Wingate, WinProxy and many others. A proxy server acts as a buffer between you and the remote system on the other end. As a result all communication between you and the target system takes place via the proxy server. In the event someone on the target system tries to get your IP address, only the proxy server's IP address-not yours-will be revealed. Almost all instant messengers support the use of proxy servers.

For example, if you are using MSN Messenger to chat with your friends, you can connect via a proxy server by following these steps:

(i) Click on Tools > Options.

(ii) Click on the *Connection* tab.

(iii) Check the *Use a Proxy Server* option.

(iv) Enter the requested information about your proxy server in the space provided and click the OK button.

### Remote System Accessing Through Websites

Another common technique used by attackers to collect the IP addresses of innocent users is through Websites. It is quite easy to develop a Website and to track the IP addresses of all the people who visit it. One way to do so is to modify the following script to create a file that records IP address of each visitor: (this particular script will show the IP address only for systems with Netscape browsers with Java enabled):

```
<HTML>
<BODY>
<SCRIPT>
var ip = new java.net.InetAddress.getLocaIHost();
var ipStr = new java.lang.String(ip);
document. writeln(ipStr.substring(ipStr. indexOf('/') + I));
</SCRlPT>
```

```
</body>
 </HTML>
```

This proves that even while you surf your favorite sites, your privacy is at stake. This arises the question how exactly is a site that you are connected to able to get so much information about you? The answer to this question lies in the Hypertext Transfer Protocol (HTTP).

## Remote System Accessing Through HTTP Protocol

What exactly happens when you type a URL (uniform resource locator) in the location bar of a browser? First the browser performs a DNS query and converts the human-readable domain name (like hotmail.com) into a machine-readable IP address. Once the browser gets the IP address of the host, it connects to port 80 (which runs the HTTP daemon by default) of the remote host and uses HTTP commands to request the host for a particular document or page. (HTTP is the protocol used by browsers to communicate with hosts-that is, to ask for a particular file at a specific URL or to send or post data to the server.) One is never aware of this process, as it occurs in the background. In this section, we will learn how to manually carry out what the browser does automatically. Since the HTTP port is port 80, one must first telnet to port 80 of the server that stores the page or document that one wants to request, and then type the desired HTTP commands at the prompt. After each HTTP command, press Enter twice to send the command to the server or to invoke a response from a server. (It is just the way the HTTP protocol works).

When the browser asks for a file at a specific URL, it is said to request information. A typical HTTP request is as follows:
***get url HTTP/1.1***

For example, suppose you want to request the about.htm file from the Website www.gmail.com. This can easily be done by simply using the telnet utility to connect to port 80 of www.gmail.com and typing the following:

```
telnet www.gmail.com 80
get /about.htm HTTP/1.1
```

The preceding command requests the about.htm file, which is stored in the root directory (specified by the */)* on the server www.gmail.com. This command can be broken down into three parts:

- get. This specifies that the HTIP get method (as opposed to the post or head method) is to be used.
- /about.htm. This specifies that the request is for the file about.htm, stored in the root directory.
- HTTP/1.1. This specifies the version of the HTTP protocol to be used.

## Merits of the get, post, and head Methods

The **get** method, which is the most widely used method, is used by browsers to request pages or documents. With this method, the client (in this case, the browser) requests a page from the server (the host to which the browser is connected).

The **post** method is used to upload files to the server. This method is used when you upload your Website not by using the FTP service, but by uploading files through an HTML page. This method heralds a reversal of roles in which your browser becomes the server and the host to which your browser is connected becomes the client.

The **head** method is the least popular method; as such, few people know about it. You use the head method when you want to make sure a particular file exists at a particular URL without downloading the entire file. This method simply downloads the header information of a particular file, but not the entire file.

With all its methods and replies, the HTTP protocol gives away a lot of information about the sender of a particular HTTP message.

### Counter Measures

Although it's true that surfing the Internet can compromise your system, there are a few steps you can take to protect your privacy. The easiest way to do so is to connect to various Websites through an anonymous surfing service such as anonyrnizer.com or antionline.com. Such services not only hide your IP address from hosts that you visit, they also hide all other information about you, such as your browser name, operating system, and so on.

Another thing you can do to protect your identity is to surf via an anonymous Web proxy server. A proxy server is basically a server that acts as a buffer between the client (you) and the host to which you are connected, as illustrated here:

Client --------------→ Anonymous service/proxy server ----------------------→ Host

Host --------------→ Anonymous service/proxy server ----------------------→ Client

As you can see, there is never a direct connection between the client and the host; all communication takes place through the proxy server. If the host is running any malicious scripts, the information extracted by those scripts will be about the proxy server, not about you. Note, however, that unlike anonymous surfing services, proxy servers hide only your IP address; they do not filter out other client information such as the browser name, operating system, and so on.

Some Popular Anonymous Surfing Proxy Servers

(i) Utility Name: Anonymizer.com

Features: A very good online anonymous surfing proxy server that protects the identity of users. The most popular Websites are blocked in the freeware version and require registration.

**Download** URL: http://www.anonymizer.com

(ii) Utility Name: Anonymizer.ru

Features: Similar to previous one, but completely free.

Download URL: http://www.anonymizer.ru

### Remote System Accessing Through Email Headers

The email headers of every single email sent on the Internet contains the IP address of the person who sent that particular email. Hence, each time one receives an email one can easily study the email headers to reveal the identity of the person who actually sent that particular email. Ideally each time one receives an abusive email, one should follow the below easy steps and try to trace the source of the email:

(i) Open email headers of the email

(ii) Identify the Internet Protocol (IP) address of the computer that was used to send the email.

As soon as one receives an abusive email, then the first thing that one must do is to try and open its full email headers. One should go under the options or properties menu and ensure that the Full headers/Advanced Headers option has been selected. Once the full email headers have been enabled, then each incoming email is displayed with its respective full email headers. Moreover, on some email client programs, one can view the full email headers of an email by simply right clicking on it and selecting the properties option:

For example, in Outlook Express or Microsoft Outlook, one can view the full email headers by simply right clicking on the suspect email and selecting the properties option:

On the other hand, online email service providers like Yahoo, Hotmail, Gmail and others require users to enable the Full Headers/Advanced Headers option:

Once the full email headers of the suspect email have been opened, one should then try to obtain the IP address of the source system that was used to send the email. One of the most common techniques of finding the source IP address is to look for the following line:
X-Originating-IP: 210.62.15.92

This particular line contains the IP address of the source system that was used to send the suspect email. For example, in this case, the source IP address is 210.62.15.92. Unfortunately, not all email headers have the above line embedded in them. In those cases, where the above line is missing, one can find the source IP address in the last or bottom-most 'received' line.

## Counter Measures

There are a few counter-measures you can take to protect your privacy when you use email. For example, if you want to remain completely anonymous while sending email, your best bet is to use an anonymous re-mailer or to connect to your mail server using an anonymous proxy. Aside from that, you should be particular when choosing an email service. Look for ones that provide you some sort of security of your identity, if not complete anonymity.

## Remote System Accessing Through Internet Relay Chat (IRC)

You can determine the IP address or hostname of anyone on your IRC channel by simply typing the following command in your favorite IRC software command prompt:

/WHOIS *nicknameofvictim*

And the output generated contains “nicknameofvictim” followed by my dynamic IP address, which can be used for various malicious purposes.

## Remote System Accessing Through Netstat

Another common method of getting the IP address of someone on IRC is to initialize a direct client connection (DCC) with the target system for a chat session or for transferring a file, and then using the ever-so-friendly netstat command to get the victim's IP address. You can initiate a DCC session by using the following command:

/dcc send *nickname full_file_path*

This command initiates a DCC with nickname (replaced with the target's nickname) and sends the file whose full path is full_file_path (replaced with the target file's full path). Alternative command is as follows:

/dcc chat *nickname*

This command initiates a DCC with nickname (replaced with the target's nickname) for a chat session.

Once either of the preceding DCC sessions has been initialized, simply type the netstat command in the command prompt to reveal the IP address of the person with whom the DCC session has been established.

**Counter Measures**

One precaution is to use the built-in functionality provided by most IRC servers to hide your IP address. Hence it is a good idea to only choose those IRC servers that either hide your IP address or that provide some kind of security with regard to your identity (one such secure IRC network is suid.net). Either of the following commands (depending upon the IRC server that is being used) will work to hide your identity:

- /mode *your _nickname* +x
- /mode *your_nickname* +z

Also, regardless of what type of IRC software you use, you should never reveal our real full name and real email address in the options dialog box of the IRC software. Another way to protect yourself is to never accept DCC requests from people you don't know. Even if you have used the preceding commands to hide your IP address, you are still vulnerable if you accept DCC requests because in a DCC session, a direct connection is established between your computer and that of the IRC user who entered the DCC request.

Finally, you can protect your identity by bouncing your IRC session off a proxy server such as Wingate or a firewall so that all packet transfers between you and the IRC server occur via the proxy or firewall like so:

Your system -------------→ Proxy/Firewall ---------------------→ IRC server
IRC server -------------→ Proxy/Firewall ---------------------→ Your system

As a result, when the attacker tries to get information about you, he will instead get the IP address, hostname, and so on of the proxy or firewall.

## Hiding IP Addresses

As you know well that IP address act as our identity in any network (say Internet), so it is important to protect our IP address. There are two most common techniques of hiding IP address that are:

- Network Address Translation (NAT) Networks
- Proxy Servers

**Network Address Translation (NAT) Technique**

The current implementation of IP addressing provides users with a very limited number of IP addresses that can be used for connectivity purposes. To solve this problem of shortage in available IP address space, a number of organizations have started implementing NAT addressing which allows them to use a single public IP address for a large number of internal systems having unique private IP addresses. This allows organizations to register a single public IP address and yet be able to connect a large number of internal systems (with unique private IP addresses) to the Internet. Such networks are known as NAT networks. All internal systems in such a NAT network use a common public IP address to communicate with all external systems on the Internet. In other words, if an external system communicates with two internal systems in a NAT network at the same time, it will be impossible for it to differentiate between the two systems. This is because both the systems within the NAT network will be using a common public IP address for all their communication needs. Due to this reason, NAT networks have also started being used by individuals to protect themselves by hiding behind the safety of the public IP address.

Typically a NAT network consists of a large number of the internal systems which are connected to the Internet through a routing device known as a NAT box. It is this NAT box that acts as the core and controls all routing, addressing and interfacing requirements of the network.

Such a NAT network allows an internal system to communicate with any remote host on the Internet. At the same time, NAT networks are able to provide users with the added advantage of anonymity and IP protection. Hence, organizations often use such networks to protect the real identity of their internal computers. This technique of using NAT boxes is often also known as network masquerading or IP-masquerading.
The communication process that takes place in a NAT network can be recapitulated in the following manner:

(i) Internal Source System creates and sends a data packet to the external system.
(ii) The NAT box changes the source port number and IP address of the data packet to allow correct transmission and routing. It then forwards the data packet to the actual destination.
(iii) The destination sends back a reply to the public IP address of the NAT box and the new port number. This new port number is used by the NAT box to identify the actual internal source system.
(iv) The NAT box forwards the reply packet to the internal system and completes the transmission process.

There are a variety of different types of NAT networks, which differ mainly on the working of the NAT box shown in table 4.1:

Table 4.1: Different types of NAT networks '

| Type of NAT Network | Functioning of NAT Network |
|---|---|
| A Symmetric NAT | The functioning is similar to what we have discussed till now. A unique mapping ID is used for each session initiated by any internal system. |
| Full Cone NAT | Requests from a particular internal IP address and port number is mapped to the same external IP address and port number. External incoming traffic is allowed to connect to internal systems |
| Restricted Cone NAT | Same as previous except that external incoming traffic Is not allowed to reach the internal systems without the internal system first sending data to that particular external IP address. |
| A Port Restricted Cone NAT | Same as previous except that the incoming traffic is restricted to even a specific port number. |

### Proxy Servers

A proxy server protects the identity of your system from the wilderness of the Internet by acting as a buffer between you and the remote host to which you are connected. Instead of communicating directly with the host, your system establishes a direct connection with the proxy server. The proxy server, in turn, establishes a connection with the remote host to which you want to connect. Any messages sent to or from your system are routed through the proxy server, as shown below:

My System --------------→ Proxy server --------------→ Remote Host
Remote Host --------------→ Proxy server --------------→ My System

Some of the most popular proxy servers include the following:

- **Squid.** This is a great transparent proxy server for Linux platforms.
- **Wingate**. This proxy server is nearly equivalent to Squid but works on the Windows platform.
- **WinProxy**. Another extremely popular proxy server.
- **Microsoft Proxy Server.** Yet another popular proxy server for the Windows platform.

## CONCLUSION

Present paper provides a comprehensive analysis of everything related to IP addresses and Network system accessing. It also throws light on various forms of IP addresses and includes detailed discussion of various ways in which a user can find out a remote computer's IP address on any network say Internet. Conversely, it also explains the various techniques and methods of hiding IP address. Also this paper includes various counter measures that can be employed in any network to protect against various forms of IP tracing and remote system accessing activities. Finally with drawing these conclusions we summarize as following;

- Network Access Control is a key component of any network security solution. The need to understand the identity and health of an end system before it connects to the network is critical in ensuring business continuity and overall security.
- Enterasys offers an open-architecture, standards-based approach to Network Access Control and delivers a solution that meets the most critical security needs of any organization.
- The experimental techniques explored herein for remote system accessing and network security are much more simple and efficient in the detection of network intrusions, compared with network based techniques; therefore, the proposed experimental techniques are useful particularly for network users.
- The proposed experimental techniques provide a comprehensive approach to the requirements of assessing any end system, authorizing network usage based on a variety of important context, enforcing security and business communication policies, notifying out-of-compliance end users and assisting them in safe and secure remediation, and providing significant compliance data.

## ACKNOWLEDGEMENTS

Prof. (Dr.) Vishwa Nath Maurya; mentor author of the paper is presently working at Department of Mathematics, School of Science & Technology, University of Fiji, Saweni/Suva. Before joining the University of Fiji, he has served as founder Director of Vision Institute of Technology, Aligarh (G.B. Technical University, Lucknow (India) and as Principal/Director at Shekhawati Engineering College (Rajasthan Technical University, Kota) after having vast experience in the cadre of Professor & Head/Dean Academics from various Technical and Management Institutions and Universities in India such as at Institute of Engineering & Technology, Sitapur, UP, India; Haryana College of Technology & Management, Kaithal (Kuruchhetra University, Kuruchhetra); United College of Engineering & Research, Allahabad and Singhania University, Rajasthan (India). Moreover, he has been associated with leading Indian Universities-G.B. Technical University, Lucknow during 2005-2006 and Chhatrapati Shahu Ji Maharaj University, Kanpur for three terms during 2000-2004 for significant contribution of his supervision as Head Examiner of Central Evaluation for Theory Examinations of UG (B.Tech./B.Pharm.) and PG (MA/M.Sc.) programs. Instead of teaching and academic administration, Prof. Maurya has worldwide recognition in research contributions, innovative and creative activities. He is the Field Chief Editor, Advisory Editor & Reviewer of Editorial Boards of over 60 Indian and Foreign International peer-reviewed journals including of USA, Austria, Germany, Algeria, Nigeria, Hong Kong and many more of other European and African countries. He has been an active member of organizing committee of various International Conferences held in India, Japan, USA, Austria and Dubai, UAE among the others.

Dr. Maurya was born on 15th July 1974 in District Basti of Uttar Pradesh in India and he possesses an outstanding and meritorious academic record. He earned his M.Sc. (1996) with 1st Division and Ph.D. Degree (2000) in Mathematics & Statistics with specialization in Operations Research from Dr. Ram Manohar Lohia Avadh University, Faizabad, UP, India and thereafter he accomplished another two years Master's Professional Degree-MBA with specialization in Computer Science in 1st Division (B+ Grade) from NU, California, USA in 2003 in order to not only demonstrate and lead academic and administrative responsibilities in a better way but to make an optimum balance in his personal, social and corporate life. He did Ph.D. on topic titled "A Study of Use of Stochastic Processes in Some Queueing Models" under supervision of Prof. (Dr.) S.N. Singh, Ph.D. (BHU). During the last 20 years of his professional career in academics and administration, Prof. V.N. Maurya has authored six textbooks for students in higher education and published more than 75 scientific and academic research papers including 50 research papers as principal author based on his post-doctoral work and D.Sc. Thesis in Indian and Foreign leading International Journals in the field of Mathematical and Management Sciences, Computer Science, Engineering & Technology. His post-doctoral D.Sc. Thesis entitled "Performance Analysis and Inference of Mixed Poisson Queueing Models" has been published in Scholar's Press Publishing Co., Saarbrucken, Germany in the form of textbook. He has guided as Principal Supervisor and Co-Supervisor to several Research Scholars of M.Phil. and Ph.D. Most of his published research papers in India, USA, Algeria, Nigeria, Malaysia and other European and African countries are recognized as innovative contributions. By virtue of his innovative research contribution to many mathematical, statistical, computer science and industrial engineering related areas basic as well as application oriented, Prof. V.N. Maurya is known as an Indian academician and one of the leading experts in Applied Mathematics, Statistics and Operational Research. Apart from this, he is also on active role of Fellow/Senior/Life Member of various reputed National and International professional bodies of India and abroad including Operations Research Society of India, Kolkata; Indian Society for Technical Education, New Delhi; Indian Association for Productivity, Quality & Reliability, Kolkata; Indian Society for Congress Association, Kolkata; International Indian Statistical

Association, Kolkata; All India Management Association, New Delhi; Rajasthan Ganita Parishad, Ajmer and International Association of Computer Science & Information Technology, Singapore and many more.

Er. Avadhesh Kumar Maurya; has an outstanding academic record and accomplished his M.Tech. Degree with specialization in Digital Communication Engineering from Uttarakhand Technical University, Dehradun, UK and he graduated with B.Tech. Degree in Electronics and Communication Engineering from Rajasthan Technical University, Kota (Rajasthan). He is recipient of four First Divisions in his student career with flying colors. Since last one year, Er. A.K. Maurya is serving as an Assistant Professor & Head, Department of Electronics and Communication Engineering at Lucknow Institute of Technology, G.B. Technical University, Lucknow (India). Prior to resuming the post of Assistant Professor & Head at Lucknow Institute of Technology, U.P., he served as a Network Engineer for two years in National Informatics Centre, Department of Information Technology, Govt. of India with collaboration of HCL Co. He has worked on some technical projects such as Movable Target Shooter using Ultrasonic Radar and Hartley Oscillator. Apart from this, he has got industrial training in Door Darshan Kendra, Lucknow, U.P. in the field of TV Program Generation and Broadcasting of different channels for partial fulfillment of his Degree and published over 24 scientific research papers in various Indian and Foreign International journals of repute in the field of Electronics & Communication Engineering, Computer Science & Information Technology and Physical Sciences such as in International Journal of Electronics Communication and Electrical Engineering, Algeria; Journal of Advanced Computing, Columbia International Publishing, USA; World of Sciences Journal, Engineers Press Publishing Group, Vienna, Austria; International Journal of Information Technology and Operations Management, Academic and Scientific Publisher, New York, USA; International Journal of Engineering Research and Technology, Engineering Science & Research Support Academy (ESRSA), Vadodara, India; International Journal of Software Engineering and Computing, Serials Publications, New Delhi, India and many more.

Er. Asim Ahmad; author of this paper, accomplished M.S. with specialization in Cyber Security and Cyber Law from IMT Ghaziabad, affiliated to National Law University, Jodhpur, India and he graduated with B.Tech. in the branch of Information Technology from Gautam Buddha Technical University, Lucknow, India. Presently, Er. Asim Ahmad is working as an Assistant Professor in Department of Information Technology at Lucknow Institute of Technology (G.B. Technical University Lucknow) since July 2010. Prior to resuming the post of Assistant Professor at Lucknow Institute of Technology, U.P he has served as Customer Support Engineer and Network Engineer at HCL Infosystems, Lucknow. Also he has served Apple Computer Institute as a Teacher before joining HCL. He would also like to express his heartiest gratitude to Prof. (Dr.) V.N. Maurya, School of Science & Technology, University of Fiji, Saweni, Fiji Islands & Ex Founder Director, Vision Institute of Technology, Aligarh (G.B. Technical University, Lucknow, India) for his valuable guidance, inspiration and constant support.

## REFERENCES

[1]. Ashland R.E. **1985**. B1 Security for sperry 1100 operating system, *Proceedings of the 8th National Computer Security Conference*, pp. 105–107. Gaithersburg, Md.: National Bureau of Standards. A description of mandatory controls proposed for Sperry (now Unisys) operating systems.

[2]. Bace R.G., **2000**. Intrusion detection. Macmillan Technical Publishing.

[3]. Biermann E., Cloete E., and Venter L.M., **2001**. A comparison of intrusion detection systems, *Computers and* Security, Vol. 20, No. 8, pp. 676–683

[4]. Blotcky S., Lynch K.., and Lipner S., **1986**. SE/VMS: Implementing mandatory security in VAX/VMS, *Proceedings of the 9th National Computer Security Conference*, pp. 47–54. Gaithersburg, Md.: National Bureau of Standards. *A description of the security enhancements offered by Digital Equipment to upgrade security on its VMS operating system.*

[5]. Department of Defense, **1985**. DoD Trusted computer system evaluation criteria. DOD 5200.28-STD. Washington, D.C.: Department of Defense. (U.S. Government Printing Office number 008-000-00461-7.)

[6]. Fraim L.J., **1983**. SCOMP: A solution to the multilevel security problem, Computer, Vol. 16, No. 7, pp. 26–34.

[7]. Gandhi Meera and Srivatsa S.K., Detecting and preventing attacks using network intrusion detection systems, International Journal of Computer Science and Security, Volume (2) : Issue (1)

[8]. Herringshaw C., **1997**. Detecting attacks on networks, IEEE Computer Society, Vol. 30, pp.16 – 17.

[9]. Komninos T, Spirakis P., Stamatiou et al., **2004**. A software tool for distributed intrusion detection in computer networks (Helena) (Best Poster presentation in PODC 2004).

[10]. Komninos T., Spirakis P., **2003**. Dare the intruders, Ellinika Grammata and CTI Press.

[11]. Lippmann R., **2002**. The role of network intrusion detection, *Proceedings of the Workshop on Network Intrusion Detection*, H.E.A.T. Center, Aberdeen, MD

[12]. Maurya V. N., Bathla R.K., Maurya A.K., and Arora D.K., **2013**. A dynamic innovative scenario of automated regression testing using software testing tool, International Journal of Information Technology and Operations Management, Academic and Scientific Publishing, New York, USA, Vol. 1, No.1, pp. 1-10, ISSN: 2328-8582

[13]. Maurya V.N. and Bathla R.K., **2012**. Design and analytical study of module testing, Ph.D. Thesis, Department of Computer Science and Engineering, CMJ University, Shillong, Meghalaya, India.

[14]. Maurya V.N., Bathla R.K., Maurya A.K., Arora D.K., and Gautam R.A., **2013**. An alternate efficient sorting algorithm applicable for classification of versatile data, International Journal of Mathematical Modeling and Applied Computing, Academic & Scientific Publishing, New York, USA, Vol. 1, No. 1, pp. 1-10.

[15]. National Computer Security Center. **1987**. Trusted network interpretation. NCSC-TG-005. Ft.George G. Meade, Md.: National Computer Security Center. *An interpretation of the* Trusted Computer System Evaluation Criteria *for networks and network components.*

[16]. Ning P., and Xu D., **2004**. Hypothesizing and reasoning about attacks missed by intrusion detection systems, ACM Transactions on Information and System Security, Vol. 7, No. 4, pp. 591–627

[17]. Oollmann D., **1999**. *Cornpuler Security*, John Wiley & Sons.

[18]. Organick E.I., **1972**. *The Multics System: An Examination of Its Structure*, Cambridge, Mass.:MIT Press.*A description of Multics—at that time implemented on a processor without hardware- supported protection rings.*

[19]. Patwardhan A., Parker J., Joshi A., Karygiannis A., and Iorga M., **2005**. Secure routing and intrusion detection in Ad Hoc Networks", *Third IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, Hawaii

[20]. Rajender Kumar, Maurya V.N., and Maurya A.K., **2012**. A cost- benefit model for evaluating regression testing technique, International Journal of Software Engineering & Computing, Serials Publications, New Delhi, India, Vol. 4, No. 2, pp. 84-89, ISSN: 2229-7413

[21]. Schell R.R., Tao T.F., and Heckman M., **1985**. Designing the GEMSOS security kernel for security and performance, *Proceedings of the 8th National Computer Security Conference*, pp. 108–
[22]. Gaithersburg, Md.: National Bureau of Standards. *A description of a security kernel for the Intel iAPX 286 microprocessor offered by Gemini Computers.*
[23]. Weaver N., Paxson V., Staniford S., and Cunningham R., **2003**. A taxonomy of computer worms, Proceedings of the Workshop on Rapid Malcode (WORM 2003), held in conjunction with the10th ACM Conference on Computer and Communications Security, Washington, DC.

[24]. Whitmore J., Bensoussan A., Green P., Hunt D., Kobziar A., and Stern J., **1973**. Design for multics security enhancements, ESD-TR-74-176. Hanscom AFB, Mass.: Air Force Electronic Systems Division. (Also available through National Technical Information Service, Springfield, Va., NTIS AD-A030801.) *A description of the enhancements incorporated into Multics to support mandatory security controls.*