International Journal of Engineering Innovation & Research
Volume 3, Issue 1, ISSN: 2277 – 5668

Attacks & Defense Mechanisms for TCP/ IP Based Protocols

Alok Pandey
Sr. Systems Manager, Department of Computer Science Engineering, Birla Institute of Technology, Mesra, Jaipur Campus, Rajasthan, INDIA
Email: alokpandey1965@yahoo.co.in

Dr. Jatinderkumar R. Saini
Director (I/C) & Associate Professor, Narmada College of Computer Application, Bharuch, Gujarat, INDIA.
Email: saini_expert@yahoo.com

Abstract **- TCP/IP protocol suite is the most widely used communication protocol and has become the de facto standard for internet based communications. It is a set of robust protocols originally designed to provide reliable communication services that allow co-operating computers to share resources across networks.**

The networking of resources also brought in many potential threats to the network community like unauthorized access to private information, malicious break-in to other organizations' systems, to make them unusable or unreliable, due to some inherent security problems in the underlying protocols as their development was based upon the concept of implicit trust between the communicating systems.

Due to the design faults and faulty implementations of TCP / IP protocol suite several vulnerabilities have been reported. Different types of network based attacks have been identified which adopt the computer networks as transportation mechanism to carry out the intrusion or attack the communication system itself. Some of such attacks are sniffing, spoofing, denial of service, session hijacking, traffic redirection, authentication and routing attacks. Several tools and defence mechanisms have been developed to identify, analyse and mitigate such attacks. We describe some of these attacks against TCP/IP suite, analysis tools and various defence mechanisms.

Keywords **– Computer Security, Hacking, Network Security, Security Tools, TCP/IP Security.**

I. INTRODUCTION

TCP/IP suite is a collection of network based communication protocols that provide and support various kinds of services running over the network. It establishes, maintains and terminates connections between the end points and provides full-duplex end to end connectivity. It also formats data, addresses, routes the data packets over the network and ensures they are delivered to the recipient [1] [2]. Two main components of the TCP/IP protocol suite are Transmission Control Protocol TCP and Internet Protocol IP.

1.1 TCP/IP Protocol Hierarchy

TCP/IP protocol suite is designed through a highly structured and layered approach, with each layer responsible for a different facet of communications. This hierarchical architecture, as shown in fig. 1 & 1(a) makes it possible for each layer to provide a unique set of functions. Data encapsulation is achieved by various headers among different layers like IP header, TCP header or application headers as seen in fig. 1 & 1(a). These headers are critical and maintain specific set of information needed for functional & administrative reasons for that particular layer.

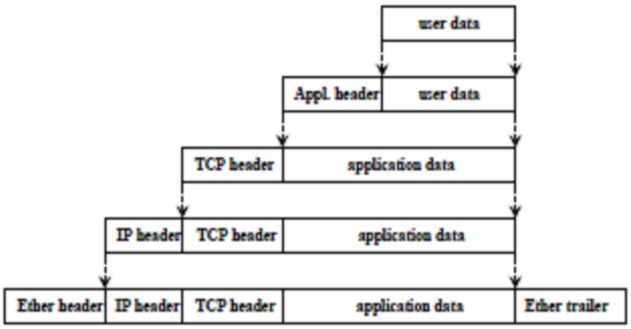

Fig.1. TCP/IP Protocol Stack

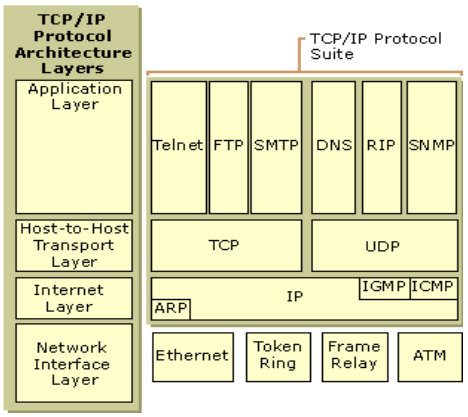

Fig.1. (a) TCP/IP Protocols

Internet Protocol (IP) **–** IP (Internet Protocol) is the workhorse protocol of the TCP/IP protocol suite, which provides an unreliable, connectionless datagram delivery service. All TCP, UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) and IGMP (Internet Group Management Protocol) data are transmitted as IP datagrams.

IP stands for the Internet Protocol that deals with routing packets of data from one computer to another or from one router to another till they reach the destination [3]. Neither does it engage in handshaking process nor does it provide flow control, error detection and control. Hence it does not provide any reliable connection between the hosts on a network. The structure of IP header is as shown in fig 2. The IP header contains important information like source IP address, destination IP Address etc. which help in routing the packet around the networks.

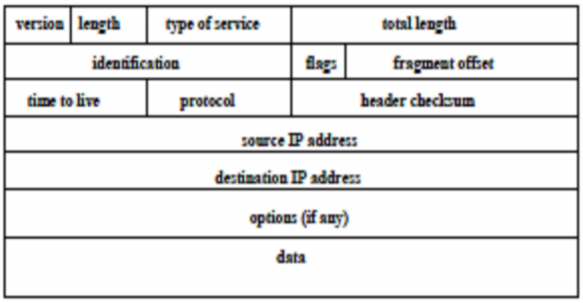

Fig.2. IP Header

User Datagram Protocol (UDP) - is a transport layer protocol, but it does not offer much more functionality other than port addressing. The checksum field in UDP header provides only a limited ability for error checking. The header of UDP is shown in Fig 3.

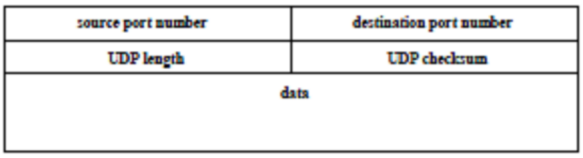

Fig.3. UDP Header

Transmission Control Protocol (TCP) – The user processes interact with the IP Layer through the Transport Layer. TCP is the most common transport layer protocol used in modern networking environments. Through handshaking and exchange of acknowledgement packets, TCP provides a reliable delivery service for data segments with flow and congestion control. The connection is uniquely defined by the unique combination of IP address of sender, TCP port number of the sender, IP address of the receiver, TCP port number of the receiver.

TCP provides a full duplex reliable connection between two end systems. It ensures the end to end delivery of the data packets. It also breaks the larger packets into smaller segments and numbers them properly and then passes them to the IP. At the receiving end TCP ensures that all the segments are received, arranged properly and reassembled after taking care of the error checking & retransmissions. It works on top of IP and provides flow control, error detection and error correction. It is responsible for the reliable delivery using the port numbers, sequence numbers, acknowledgement numbers and timers etc. A TCP Header is shown in fig 4.

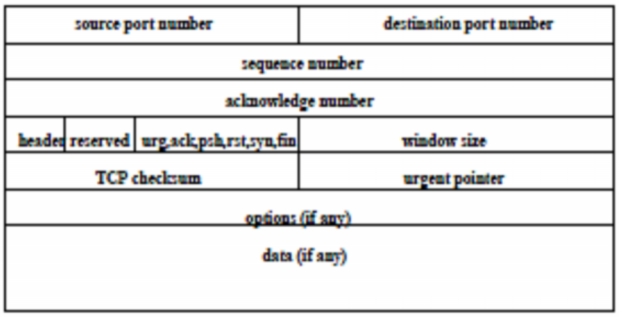

Fig.4. TCP Header

The TCP header contains the port numbers that are used to uniquely identify the process at the sending and receiving sides as TCP at the sending side is responsible for ensuring that the data segment is received at a specific port on the receiving side and properly acknowledged. Every byte that is sent by a host is marked with a sequence number and is acknowledged by the receiver using this sequence number. The sequence number is essential in keeping the sending and receiving datagram in proper order. There are six flag bits with the TCP header, namely URG, ACK, PSH, RST, SYN and FIN which play specific roles in the connection establishment, connection termination or other control purposes. For maintaining proper flow control, the size of the communication window is advertised between the communicating partners. Before actually transmitting data segments TCP follows the process of 3-way handshaking which ensures reliable transmission of the packets. Each packet sent is properly acknowledged [4].

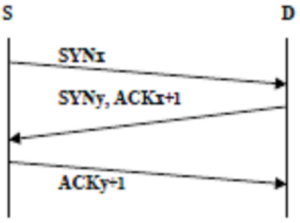

Fig.5. Three-way handshake

The process of 3-way handshake between a source and a destination can be seen in fig 5.The source system sends a SYN packet to destination system, telling its desire to establish a connection and setting its own ISN (Initial Sequence Number) in sequence number field.

Upon receiving the request packet, the destination host sends back a SYN_ACK packet with its own ISN and the incremented ISN from source host. Finally, the source host will transmit an ACK packet and data transfer can take place. If the sender S did not send any SYN packet but received a SYN_ACK packet from destination D, it would just send back a RST packet to reset the connection.

II. Some of the Hacking Techniques

The network hackers utilize the security holes of TCP/IP to perform various network attacks. Three of the commonly used hacking techniques used to exploit the vulnerabilities of TCP/IP protocol suite are as follows:-

2.1 IP Address Spoofing

Source and destination address contained in the IP header are the only information needed for routing the packet. Anyone who has access to the IP layer can easily spoof the packet's IP source address and then masquerade it as from another host in the network. The IP address spoofing is based upon maliciously creating TCP/IP packets using someone else's IP address as source address so as to either conceal own identity or impersonate the identity of the user of the spoofed IP address being used [5].

The packets are routed by the router to the destination. Upon receipt the recipient uses the IP address of the source to reply to the packet. Since the source address is spoofed, the recipient will reply to the spoofed address and not to the original sender who had deliberately changed his IP address in the original packet. Since the address has been changed intentionally it will be difficult to trace back to the attacker. Using this concept the following types of attacks are normally carried out.

2.1.1 Denial of Services Attacks (DoS)

Using the above trick the attacker can send a large number of packets to the victim [6]. As he will not receive any packet from the victim, all the replies will be directed towards the spoofed IP addresses and causes the victim to go out of services. Using DoS an attacker can disrupt the normal functioning of the network and carry out the following attacks:-

2.1.1.1 Storage Consumption Attacks – The attacker tries to consume all the available local storage space on the target machine to slowly bring it to a grinding halt. A simple trick of sending emails with very large attachments can be used for launching this type of DoS. Multiple large DVD VOB files and uncompressed JPEG or BMP (bitmap) images of very high resolution are common file types used to accomplish such attacks.

2.1.1.2. Subnet Mask Corruption Attacks – The attacker may send a message which causes the target machine to reset its subnet mask and so disrupt the target's subnet routing.

2.1.1.3. Connection Resources Consumption Attacks – By sending very large numbers of erroneous requests for TCP session establishment an attacker can consume all of the target's available connection resources thereby resulting in the target being unable to service any new authentic connection requests.

2.1.1.4. Buffer Overflow Attacks – A buffer overflow attack occurs when a process receives much more data than expected and if it has no programmed routine to deal with this excessive amount of data, it may act in unexpected ways that an attacker can exploit. There are numerous variations and forms of buffer overflow attack that have been formulated over the years, with the most common of all being the "Ping of Death".

2.1.1.5. Ping of Death Attacks - The Ping of Death attack is also referred to as the "Large Packet Ping Attack". The attacker initiates a "ping of death" attack by using network utility PING of Internet Control Message Protocol (ICMP) to "ping" the target with an illegally modified and very large IP datagram. This will result in overfilling of the target system's buffers causing the target to reboot or hang. PING can be configured to send the "illegal" IP datagram packets in bursts or as a continual stream. In the case of a continual stream the target will be immediately under attack once it reboots and will thus hang or reboot continually until something is done to stop it receiving the attacker's packets.

2.1.1.6. Long File or User Name Attacks – Another basic buffer overflow attack that can be initiated very easily by the attacker is done by sending the victim machine a large packet with user names or file names larger than 256 characters long. Email delivery processes are also a popularly exploited mechanism for deploying this type of excessively long file or user name attack.

2.1.1.7. SYN Attacks - A SYN attack occurs when an attacker exploits the use of the buffer space during the Transmission Control Protocol (TCP) session initialization - three-way handshake. The receiving machine (usually a server) can maintain multiple concurrent conversations all established using the same small "in-process" buffer pool.

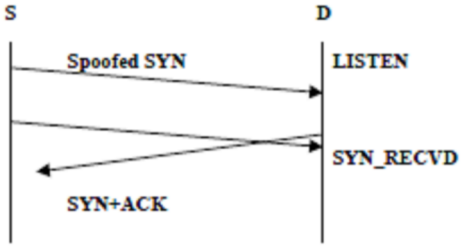

Fig.6. A SYN Attack

To instigate such attack an attacker simply floods the target system's queue with connection requests, but when the target system replies with a SYN-ACK acknowledgement packet the attacker simply ignores it (fig 6) rather than replying with an ACK packet which the target will be waiting for. By not responding deliberately to the SYN-ACK sent by the server he leaves the connections half opened. Thus the target system will "time out" as it will keep waiting for the proper response. The server will be unable to respond to further connection request because of exhaustion of resources and denial of service takes place [7]. The target will generally assume that either its SYN-ACK packet or the attacker's ACK reply packets have been lost in transit and so it will reissue its SYN-ACK packet.

After some time the target system will become unstable, hang, crash or become unusable. As a result the target system will have to be rebooted. Once rebooted; the attack will continue afresh for as long as the attacker wants or until the network administrator discovers that they are being attacked and take appropriate steps to counteract it.

2.1.1.8. Smurf Attacks – Here a combination of IP Address Spoofing and ICMP flooding are used to saturate a target network with traffic so that the normal traffic is disrupted thereby causing a Denial of Service (DoS) attack. Smurf attacks consist of the source site, the bounce site and the target site.

First the attacker selects a bounce site (usually a very large network). The attacker then modifies a PING packet so that it contains the address of the target site as the PING packet's source address.

Now the attacker sends the spoofed PING packet to the broadcast address of the target site. As a result the bounce site will broadcast the spoofed packet to all devices configured to receive messages from that broadcast address. The bounce site network devices receiving this misinformation will not know that it is false information

and so they will automatically respond to the ping request with a reply to the intended victim target site.

As a result the target site is overwhelmed by a large number of erroneous replies from the bounce site. This oversaturation of ping replies will consume all of the target site's "in-process" buffer resources and hang or reboot the system.

2.1.2. Defeating the Network Security – These attacks are aimed against IP based authentication environments, where the internal machines are configured to trust communication from internal IP addresses. No login or passwords are required for access [8]. By spoofing the connection an attacker can get unauthorized access to a victim machine without authentication.

2.1.3. Man- in-the-middle **Attack** - It is based upon hijacking an authenticated network session between two hosts. The attacker implants itself after they have finished the authentication steps. The attacker can spoof the IP address of a victim that was authenticated by other host or server and gets packets that pass between these hosts [9]. The attacker uses IP address of two hosts to receive and send packets

2.2 TCP Sequence Number Prediction

It is possible for the attacker to predict the sequence numbers based upon the ISNs which are being used for Sending and Acknowledging between two genuinely communicating hosts. Based upon this technique, the sessions can be hijacked by the attacker.

2.3 Port Scanning

It is not a technique used directly to perform an attack. Instead, its goal is to discover an exploitable communication channel and then launch the real attack. The reason for doing port scanning is that some vulnerable services may not use a fixed port number.

There are several ways to detect a potential communication channel. For a listening TCP server, the most basic approach is to try to make a real connection. Another method is SYN scanning, which sends a SYN packet to the victim as if it will create a real connection. As already discussed in TCP three-way handshake, a SYN_ACK packet will indicate an active server and a RST message tells a port with no listener.

These two methods above have obvious disadvantages. The first one is easy to be audited and the last one will not work with some firewalls or packet filters specially designed to block SYN packets to non-permitted ports.

Other way of port scanning is by TCP FIN scanning. Instead of sending SYN probes in SYN scanning, this method adopts FIN packet, then it waits for RST packet from a closed port. In case of an active listener, it will just discard this FIN packet silently without sending anything back.

UDP is a connectionless protocol. Its simplicity makes port scanning actually more difficult as there is no three-way handshake as in TCP, so UDP server will not acknowledge any probe packet. On the other hand, for a closed port, no UDP error message is returned. Most hosts send ICMP "port unreachable" message as a reply to the packets sent to an unused UDP port. This may give hackers some clues. Since UDP is unreliable hence neither UDP packets nor the ICMP messages are guaranteed to arrive.

III. DEFENDING MECHANISMS

Some simple prevention mechanisms like password protecting the system to avoid unauthorized use have become widely popular.

3.1 Firewalls - Firewalls are systems designed to prevent unauthorized access to or from a network. A firewall is a dedicated appliance or software running on a system which inspects network traffic passing through it and denies or permits passage based on a set of rules. Firewalls can be implemented in both hardware and software or a combination of both. Firewalls can be of the following types:-

Packet filter:- It inspects each packet entering or leaving the network and rejects or accepts based on defined rules. It is effective and transparent but difficult to configure. IP spoofing can be easily done for packet filter firewalls.

Application Gateway:- Decision to allow or disallow depends upon specific application for e.g. ftp, Telnet etc. It is very effective but imposes performance degradation.

Circuit-level Gateway:- It applies security mechanism when a TCP or UDP connection is established. After the connection establishment no further checking is done and packets could flow between hosts.

Proxy server:- It sits between the client and server. A client requires some services such as a file, connection web page or other resources available on a different server. The proxy server validates the request with its filter rules and after the request is validated by the filter, the proxy provides the resources by connecting to the relevant servers and requesting services on behalf of clients. Some of the commonly used firewalls are :-

Netfilter: It is an open source, firewall written in C that supports different IPV4 protocols and can be used with command line interface [10].

IPFilter: is an open source firewall that supports both IPv4 and IPv6. It works on different types of operating systems like AIX, BSD/OS, and some other flavours of BSD and Solaris [11].

3.2. A virtual private network (VPN) – A VPN is a private network that uses a public network such as internet to connect remote sites or users together. Instead of using a dedicated, real world connection such as leased line VPN uses "virtual" connections routed through the internet from the company's private network to the remote site. It is implemented as an additional logical layer on top of an existing larger network.

3.3. Authentication - Computer Security authentication means verifying the identity of a user logging onto a network. Authentication is the process of determining whether the person is genuinely the person whose identity he or she is claiming to be. In other words authentication is the process of verification of the identity of a user. It is typically based on:

- Something user knows: Passwords or PINs.
- Something user has: This could be a key or a token or a smart card or a disk or some other device.
- Something user is: It includes biometric authentication such as fingerprints, voice recognition, retina or iris scans.

Authentication procedures can be categorized as follows:

3.3.1. Two-party authentication:- In two-party authentication there are two ways

- *One way authentication* -The client authenticates with server by giving username and password. If it is correct then client is allowed to login to the server.
- *Two way authentication* - In two way authentication the client authenticates with server by giving username and password. Similarly the server authenticates with client by giving username and password. If it is correct then it is assured that the client is communicating with the correct server.

3.3.2. Third party authentication:- In third party authentication there is a third party security server. The clients communicate with security server by giving username and password. The security-server authenticates the client if the username and password are correct.

Similarly on the other side the server authenticates with security-server by giving username and password. After both the client and server are authenticated the client and server exchange keys for securely transmitting the data. After that the data is transferred in a secure way.

3.3.3. Single sign on: Users can access several network resources by logging on once to a security server.

3.4. Intrusion Detection System (IDS) – An intrusion detection system is a software / hardware designed to detect some unwanted attempts to access, manipulate and/or disable computer system. These attempts are generally generated from a network such as internet. It monitors network and/or system activities for malicious activities or policy violations. It is the process of monitoring the events occurring in a system or networks. It also analyzes them for violations of security policies. Intrusion Detection system can be of the following types:-

3.4.1. Network intrusion detection system (NIDS):- NIDS is an independent platform which examines network traffic and monitors multiple hosts. It gains access to network traffic by connecting to a hub or network switch which is configured for port mirroring or network tap.

3.4.2. Protocol-based intrusion detection system (PIDS):- PIDS is an intrusion detection system which is typically installed on a web server and is used in the monitoring and analysis of the communications protocol in use by the computing system.

3.4.3. Application protocol-based intrusion detection system (APIDS):- APIDS is an intrusion detection system that focuses its monitoring and analysis on a specific application protocol or protocols in use by the system.

3.4.4. Host based intrusion detection system (HIDS):- Host based intrusion detection system are run on individual hosts or devices on the network. A HIDS monitors the entire network traffic from the device and would alert the user or administrator whenever suspicious activities are observed.

3.4.5. Signature based Intrusion Detection System:- A Signature based Intrusion Detection System will monitor packets on the network and compare them against a database of signature or attributes from known malicious threats.

3.4.6. Anomaly based Intrusion Detection System:- An IDS which is anomaly based will monitor the network traffic and compare it against an established baseline. This baseline generally contains what is normal traffic for the network, what sort of bandwidth is generally used what protocols are used, what ports and devices generally connect to each other and it would alert an administrator when traffic detected is different or having an anomaly with the baseline.

3.4.7 Some commonly used IDS are :-

Firestorm: It is a Cross platform Network Intrusion Detection System that uses libpcap to capture, analyse and detect any malicious patterns in network traffic for different protocols [12]. It uses anomaly detection method and fully supports Snort [13] rules.

Prelude: Is a hybrid IDS, that uses several sensors in the network to capture and detect any malicious packet. It can work on Linux, BSD and some other operating systems [14].

Dragon: Dragon is a commercial host & network intrusion detection system, which uses rule and signature based detection techniques and has extensive libraries [15].

3.5. Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) uses rule based detection technique for detecting malicious traffic and preventing attacks. IPS is the advancement of intrusion detection system IDS.

3.6 Some popular IDS being used are :-

Snort: It is an open source IDS that works on application layer and network layer. It can detect and prevent different attacks like buffer overflow, denial of service attack, port scan, SMB probes and some other attacks.

Suricata: It is an open source network intrusion detection and prevention system that works on rule based and anomaly based detection concepts. It works on application and network layers [16].

3.7. Some commonly used mitigating techniques against IP Spoofing include use of encrypted session in router, using Access Control List for applying the security policies, application of defence mechanisms of upper layers [17].

3.8 Counteracting Ping of Death Attack – Techniques like changing the LAN IP address, use of filtering devices such as routers and dedicated firewall to drop all incoming (ICMP) packets are commonly used to defend against such attacks.

3.9. Mitigating Smurf Attack – For countering a smurf the commonly used techniques include “state-full”

inspection at firewall and to deny external ICMP traffic access to the internal network.

3.10. Countermeasures for Long File or User Name Attacks – Such attacks can be countered by configuring the network filtering device to automatically drop the traffic which contains file names and user names that are more than 255 character long.

3.11. SYN Attack Countermeasures - Identifying the source IP Addresses of the attack packets and then using a firewall or router to block all traffic from this source.

IV. TCP/IP Security Tools

Several Security tools are available. Some of the most common tools are :-

4.1 Network Sniffers

Network sniffers and analysers are software and / or hardware based tools that sniff data through a connection. They normally work in passive mode and are used to tap into a connection for listening to the ongoing packet exchange without altering or redirecting them.

Wireshark: It is an open source sniffer tool used for sniffing and analyzing packets. It captures live packets of Ethernet, IEEE 802.11, PPP, etc. and can analyze them in offline mode. It can work on Windows, Linux, Solaris, NetBSD, FreeBSD and others [18].

Tcpdump: It is a free software that can be used for analyzing packets on TCP/IP using a command line interface. This tool works on Linux, Solaris, BSD, Mac, AIX. For Windows it works through WinDump [19].

Ettercap: It is open source software for sniffing and analyzing packets written in C and works on Microsoft Windows, Linux, Mac, BSD and Solaris [20].

4.2. Vulnerabilities scanners

Vulnerability scanning is performed to know weaknesses in a system or network to attack it or it could be performed by a network administrator to know the weaknesses of a system or network so that he could reconfigure the network to secure it.

MBSA (Microsoft Baseline Security Analyzer: MBSA will scan the system and identify if there are any patches missing for products such as the Windows Operating System, Internet Information Server(IIS) etc.

Nessus: Nessus is a comprehensive vulnerability scanning program. Its goal is to detect potential or confirmed weaknesses on the tested network. It is a cross-platform tool and works on Linux, Mac OS X, and Microsoft Windows [21].

Retina: It is being used by industry for multi-platform vulnerability management as it identifies known & zero-day vulnerabilities along with detailed security risk assessment [22].

4.3 Penetration test tools

These are the tools which are used by both attackers and the penetration testing professionals to check the network. Following are some of the notable penetration testing tools for TCP/IP:

Nmap: It is a free open source tool used for network discovery, port scanning and security auditing of the target network [23]. It can also be used to do finger printing of operating system and network device.

Netcat: It allows reading and writing of data to network connections using the TCP/IP protocol. Packet can be constructed and dispatched using Netcat. Malformed packets can be crafted for testing the protocol responses [24].

hping: It is a command line open source TCP/IP packet assembler analysis tool. It supports multiple protocols including ICMP, TCP, UDP and RAW-IP protocols [25].

V. Conclusion

Several types of attacks based upon TCP /IP Protocols have been discussed in this paper. We have also highlighted some of the tools that are used for analyzing the different vulnerabilities of a network.

With a lot of emphasis on security these days, it becomes necessary that the networking professionals should not only know how to find the vulnerabilities of their network but also should know what are the techniques to guard against them.

With the implementation of IPV6 some of these security holes have been plugged, but a lot has to be done in this direction.

References

[1] Braden, Robert. "RFC-1122: Requirements for internet hosts." Request for Comments (1989): 356-363.

[2] Barden, R. "RFC 1123: Requirements for InterNet Hosts-Application and Support." InterNet Network Working Group (1989).

[3] Deering, Stephen, and Robert Hinden. "Internet protocol." (1998).

[4] Chappell, Laura. "Inside the TCP Handshake." NetWare Connection (2000).

[5] Tanase, Matthew. "IP spoofing: an introduction." Security Focus 11 (2003).

[6] Ferguson, Paul. "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing." (2000).

[7] CERT, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks," September 1996.

[8] Heberlein, L. Todd, and Matt Bishop. "Attack class: Address spoofing."Proceedings of the 19th National Information Systems Security Conference. 1996.

[9] Trabelsi, Zouheir, and Khaled Shuaib. "NIS04-4: Man in the Middle Intrusion Detection." Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE. IEEE, 2006.

[10] Yao, Xiaoyu, and Chen ZHAO. "Research on Implementation and Application of Linux Kernel Firewall Netfilter [J]." Computer Engineering 8 (2003): 042.

[11] Reed, D.: IP Filter. Online. http://coombs. anu. edu. Au / avalon/ip-filter.html (Last accessed 31 May 2013)

[12] Leach, John, and Gianni Tedesco. "Firestorm network intrusion detection system." Firestorm Documentation (2003).

[13] Roesch, Martin. "Snort-lightweight intrusion detection for networks."Proceedings of the 13th USENIX conference on System administration. 1999.

[14] Zaraska, Krzysztof. "Prelude IDS: current state and development perspectives."URL http://www. Prelude -ids. org/download/misc/pingwinaria/2003/paper. pdf(2003).

[15] Allan, Ant. "Enterasys Networks Dragon Intrusion Detection System (IDS)." (2002).
[16] "Suricata Intrusion Detection System", online, http://suricata-ids.org/ (last accessed 31 May 2013)
[17] Bellovin, Steven M. "A look back at." Computer Security Applications Conference, 2004. 20th Annual. IEEE, 2004.
[18] "Wireshark", online, www.wireshark.org.
[19] "TCPdump and libpcap", online, http://www.tcpdump.org/"
[20] "ETTERCAP", online, http://ettercap.github.io/ettercap
[21] "NESSUS vulnerability scanner", online, http://www.tenable.com/products/nessus
[22] "Retina Network Security Scanner", online, http://www.beyondtrust.com/Products/ Retina Network SecurityScanner
[23] "Nmap", online, http://nmap.org
[24] "What is netcat?", online, http://netcat.sourceforge.net
[25] "hping", online, http://www.hping.org

AUTHOR'S PROFILE

Alok Pandey

is Senior Systems manager and faculty member at B.I.T. (MESRA), Jaipur Campus. His qualifications include B.E.(EEE), MBA. He has also done MCSE, RHCE, CCNA, IBM Certified E-Commerce and diploma in Cyber law. He has a rich industrial working experience of more than 17 years and also a teaching experience of about 9 years in the areas of Data Communication and Computer Networks, Information Security, E-Commerce, Systems Management, ERP etc. He is also a member of CSI, IAENG and ISOC. His research interests include Computer Networks and Network Security.

Dr. Jatinderkumar R. Saini

is Ph.D. from Veer Narmad South Gujarat University, Surat, Gujarat, India. He secured first rank in all three years of MCA in college and has been awarded gold medals for this. He is also a recipient of silver medal for B.Sc. (Computer Science). He is an IBM Certified Database Associate-DB2 as well as IBM Certified Associate Developer-RAD. He has presented several papers in international and national conferences supported by agencies like IEEE, AICTE, IETE, ISTE, INNS etc. One of his papers has also won the 'Best Paper Award'. 11 of his papers have been accepted for publication at international level and 13 papers have been accepted for national level publication. He is a chairman of many academic committees. He is also a member of numerous national and international professional bodies and scientific research academies and organizations.