International Journal of Science and Modern Engineering (IJISME)
ISSN: 2319-6386, Volume-1, Issue-10, September 2013

TCP/IP Attacks, Defenses and Security Tools

Abdullah H. Alqahtani, Mohsin Iftikhar

Abstract: ***The TCP/IP protocol suite is the foundation of Internet and is ubiquitous in almost all networks worldwide. It was written as a robust protocol, which is able to communicate despite node failures. The design parameters of TCP did not weigh security as important and placed an implicit trust on nodes. The result was a protocol which was reliable and robust, but contained myriad inherent security flaws, open to be exploited by a malicious entity as was amply demonstrated by Morris worm [1] in the early days of what is Internet today. This problem was aggravated by various faulty implementations of the TCP/IP protocol. Many vulnerabilities and corresponding attacks have been identified targeting TCP/IP protocol suite including spoofing attacks, denial of service attacks, authentication attacks and routing attacks etc. Design flaws of TCP/IP can be mitigated by applying layers of security mechanism in a network. But this application itself is open to exploitation. Various tools have been designed to analyze and identify the presence of such vulnerabilities and avenues of exploitation in TCP/IP suite. We describe the spectrum of attacks against TCP/IP suite and discuss various defense mechanisms and tools like firewalls, intrusion detection systems, protocol analyzers, sniffers and vulnerability scanners etc. We conclude with an analysis of these tools.***

Keyword: Network security, TCP/IP security, security tools, hacking, computer security.

I. INTROCUTION

TCP/IP suite is a collection of various communication protocols operating over the Internet and other private communication networks and it supports most of the important services running over the network. It provides end to end connectivity by maintaining, establishing and releasing connections between the two sides. It provides for data formatting, addressing and routing of packets over the network to ensure that they are delivered to the recipient. [2][3]. The main two components of the TCP/IP protocol suite are Transmission Control Protocol TCP and Internet Protocol IP.

A. Internet Protocol IP

It is responsible for routing of packets or datagrams over the network to their destination [4]. Though part of the same conversation, different packets can take different

routes over a series of routers to reach to the destination. They may arrive in a different sequence than what they were sent in. When the packet passes through the intermediary node, the node determines the next hop leading to the destination and this decision depends on the particular routing protocol being used. This protocol is not reliable and called a connectionless protocol because it does not guarantee delivery of the packets to the destination and does not provide flow control and error detection / correction.

Manuscript received September 2013.

Abdullah H. Alqahtani, Computer Sciences, King Saud University/ Computer and Information Sciences, Riyadh, Saudi Arabia.

Dr. Moshin Iftikhar, Computer Sciences, King Saud University/ Computer and Information Sciences/ Riaydh, Saudi Arabia.

B. Transmission Control Protocol TCP

TCP works on top of IP and is responsible to break the data stream into segments before passing them it to IP and reassembling it at the destination. TCP is considered a reliable protocol because it guarantees packet delivery and incorporates error detection and correction mechanisms. Different mechanisms used by TCP to ensure packet delivery are sequence numbers, acknowledgements, three-way handshake and timers.

- *Three-way handshake*

It is the process used to establish connection between the two parties involved in a TCP connection [5]. Figure 1 shows an example of connection establishment between the browser and the Google website [6], where wireshark [7] is used to capture packets which are exchanged in a three-way handshake.

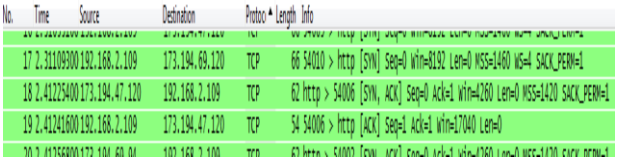

Figure 1: Packet capture of a TCP three-way handshake.

- A SYN packet is sent by the host with initial sequence number ISN to the server requesting for establishment of a connection.
- The server responds with a SYN ACK packet as acknowledgement of the SYN packet sent by the host and showing readiness to accept connection request.
- Host sends ACK packet as acknowledgment of the SYN packet sent by the server.
- Now both the parties have completed the connection setup and are ready for sending and receiving of packets.

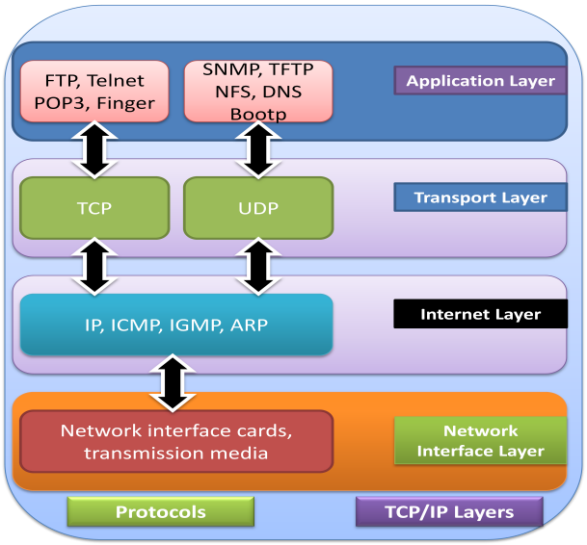

Figure 2: TCP/IP protocol stack

II. TCP/IP ATTACKS

A. *TCP "SYN" attacks*

This attack is caused by the three-way handshake mechanism used between host and the server to setup connection. A server has limited resources. Once it responds to a SYN request using SYN ACK it sets aside resources for this connection and listens for ACK from client. If the attacker sends multiple SYN within very short interval then the server will exhaust its resources. The attacker does not respond to SYN ACK sent by the server and the connections are left half opened. This ways server is unable to respond to further connection request because of exhaustion of resources and denial of service takes place [8].

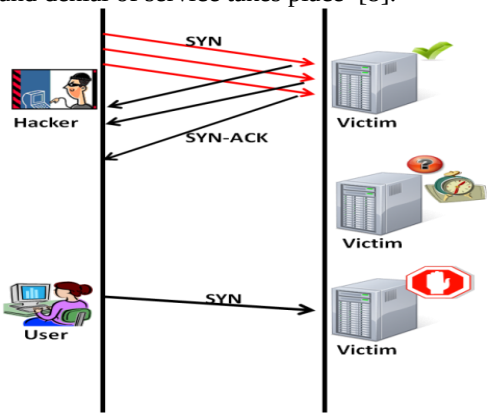

Figure 3: TCP SYN attack

B. *IP Spoofing*

IP address spoofing involves maliciously creating TCP/IP packets using other IP address as source address with the aim to either conceal own identity or impersonate the identity of the owner of the IP address used [10]. Routers use the IP address of the destination and forward the packet to it. The recipient uses the IP address of the source to reply to the packet. If the source address is spoofed, the recipient will reply to the spoofed address. Also the packet will be hard to be traced back to the attacker. But in this case if the attacker wants to access the reply also, he will have to sniff the traffic of the spoofed address also. This behavior of the recipient can be used to launch various attacks as described below:

- Denial of Service Attack (DoS)

The attacker can send a large number of packets to the victim when he does not care about the replies from the victim because he will not receive any packet from the victim [11]. All the replies will be directed towards the spoofed IP addresses. Also, the identity of attacker will also not be disclosed. This attack causes the victim to go out of service.

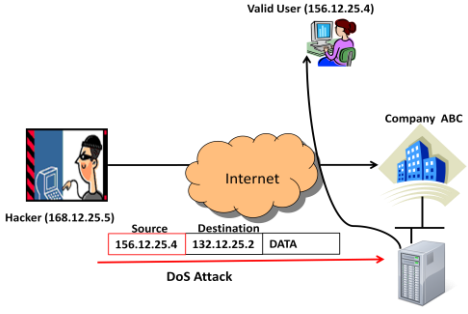

Figure 4: DoS Attack

- Defeating network security

This kind of attacks is mostly used against IP based authentication environments, where internal machines are configured to trust communication from internal IP addresses. There is no need for a login or password for access [12]. The attacker can spoof the connection between two machines to get unauthorized access to a victim machine without authentication.

- Man in The Middle Attack

It involves hijacking an authenticated network session between two hosts. The attacker when they finish authentication steps. The attacker can spoof the IP address of a victim that authenticated by other hosts or server and get packets that pass between these hosts [13]. The attacker uses IP address of two hosts and uses them to receive and send packets

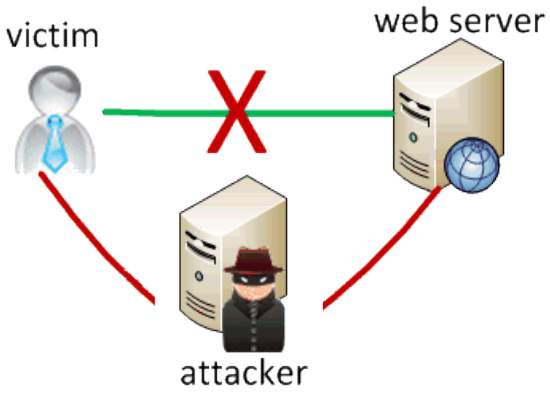

Figure 5: Man-in-the-Middle Attack

Defense against IP Spoofing

Following measures can be taken to prevent spoofing attacks [9]:

- *Use of encrypted session in router:* Through the use of encryption in the routers the trusted hosts can communicate securely with the local hosts. As the attackers will not be able to read the packets and will not be able to spoof packets.
- *Using Access Control List:* Access Control List (ACL) help in applying security policy. The ACL can be configured to block any traffic coming from outer network with an internal IP address and likewise blocking traffic from internal IPs to go to outside network so that these IP addresses are only used inside the network.
- *Filtering packets:* This involves blocking incoming packets which do not meet the security policy criteria, like ping requests from outside the network are filtered. Likewise outgoing packets can also be filtered based on the source or destination port / IP address criteria.
- *Using upper layer:* Incorporating defense mechanisms in upper layers can prevent IP spoofing like use of sequence numbers in TCP at transport layer so the attacker has to guess the sequence number also before spoofing the packet.

C. *Connection Hijacking*

Authentication between two hosts takes place during the initial stages of the connection setup. Thenceforth no authentication is required. As shown in Figure 6, the attacker can take advantage of this by sending a reset to the client and killing the connection for the client and then the attacker spoofs the client and continues session with server

using spoofed source address [14]. The other way of session hijacking is exploiting authenticated machine by stealing the cookies stored on that machine or stealing cookies by sniffing the unencrypted network traffic. Then these cookies can be used with the web server to establish an authenticated session.

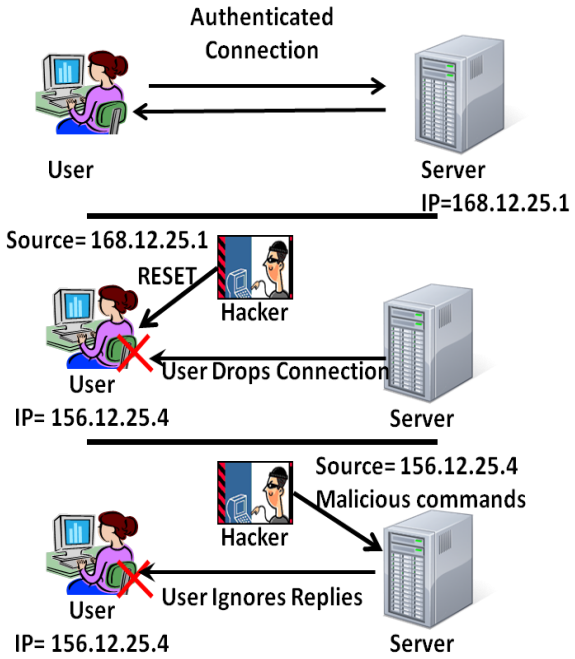

Figure 6: Session Hijacking

Defenses against Connection Hijacking Attacks [9]

- *Encryption:* Encryption secured the traffic between two hosts and an attacker may see the traffic but neither is he able to read the contents of the packets nor he can use them for session hijacking.
- *Using re-authentication:* Requirement of authenticating periodically after a specified period of time will cause the attacker to lose session after some time even if he initially succeeds. This may prevent further exploitation of the access.
- *Session timeouts:* Session timeouts are again a mechanism for enforcing re-authentication after a specified amount of time so that a hijacked session is not exploited perpetually.

D. Routing Information Protocol (RIP) Attacks

Routing Information Protocol (RIP) is a routing protocol used in TCP/IP suite to route packets based on hop count. Before making a routing decision RIP counts the number of hops on every path available and dispatches the packet on the path with minimum hops to the destination. Maximum hop count value can be 15 hops in RIP and any count greater than 15 is considered as an infinite route or unreachable path. This mechanism is used to prevent loops in routing. RIP does not employ authentication mechanism to receive routing updates. The attacker can forge RIP routing updates to advertise the least cost path to the target node. This will cause RIP to route all packets to the target node through attacker as he is considered the nearest to target node [15]. The attacker can use this to launch any attack on the target node.

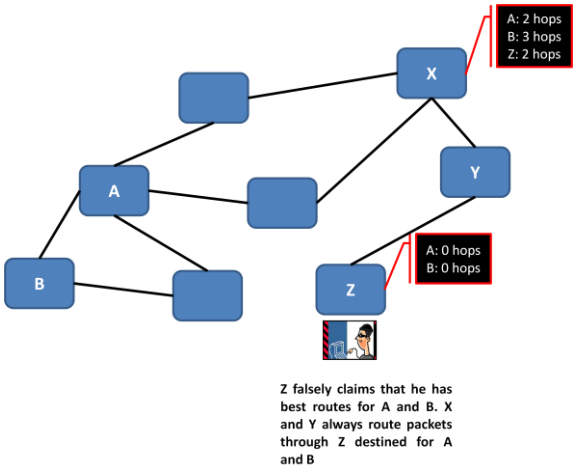

Figure 7: RIP attack

Defenses against RIP Attacks

The vulnerability in RIP protocol caused by the lack of authentication, the focus of most of the mitigation effort is on incorporating authentication into RIP. Following are some of the countermeasures against RIP Attacks [9]:

- Use of encryption.
- Filtering packets based on source and destination.
- Frequent log analysis aimed at anomaly detection.
- Check routes before acceptance.

E. ICMP Attacks

Internet Control Message Protocol (ICMP) is a protocol used in internet layer of TCP/IP protocol suite to send error messages and carryout network management tasks. Most familiar example of ICMP is the "Ping" tool which is used to send echo message so as to know the online status of the destination. The ICMP protocol does not have any authentication built-in and attacker can intercept ICMP packets. "Ping" can be used to launch DoS attacks also [9]. Defenses against ICMP attacks may include the following [9]:

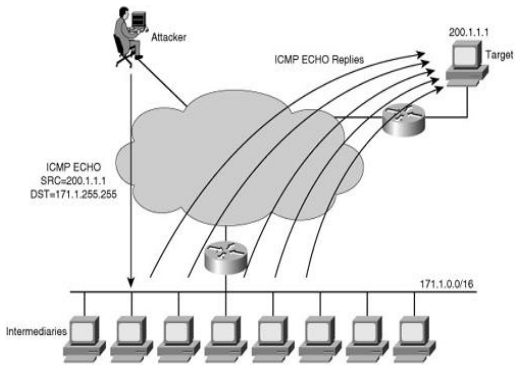

Figure 8: ICMP echo attack

- Checking if the packet belongs to the same connection or not.
- Changes in routes should be authorized to a particular connection.
- Reply packet should be accepted at a particular time.

F. DNS spoofing attacks

Domain Name System (DNS) is a service used in application layer to map an IP address to a domain name and vice versa [16] DNS spoofing attacks are launched by poisoning the DNS cache records to spoof a domain name

and binding it with attacker's IP address. If the client uses domain name to authenticate requests, then it will be compromised.

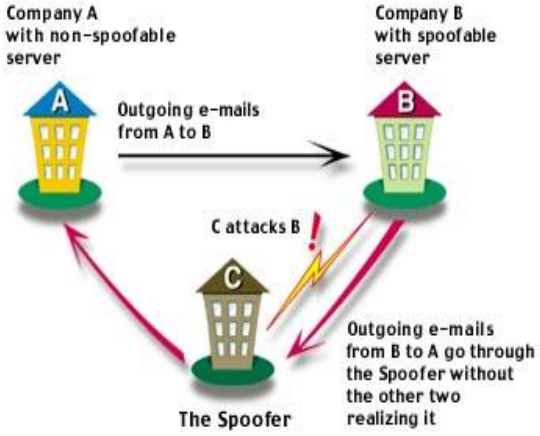

Figure 9: DNS spoofing attack

Defenses against DNS Spoofing attacks [16]

- Use IP address based authentication instead of using domain name based.
- Using encryption to prevent forging DNS.

III. TCP/IP SECURITY TOOLS

A. *Network Sniffers*

Network sniffers or network analyzers are tools, software or hardware, used to sniff data flow through a connection. They work in passive mode and only tap into the connection to listen into the packet exchange without altering or redirecting it. Sniffing tools can be used for analyzing network packets to solve problems in network and identify any malicious packets or behavior.

- *Wireshark:* Wireshark [7] is an open source sniffer tool used for sniffing and analyzing packets. It captures live packets, and can analyze them in offline mode. These packets can include Ethernet, IEEE 802.11, PPP, and loopback. Wireshark can work on many platforms like Windows, Linux, OS X, Solaris, NetBSD, FreeBSD and others. It provides GUI and command line interfaces.
- *Tcpdump:* Tcpdump [17] is free software used for analyzing packets on TCP/IP using a command line interface. This tool works mostly on Linux but also can work on other operating systems like Solaris, BSD, Mac OS X, HP-UX, AIX and Windows through WinDump.
- *Kismet:* Kismet [18] is not only a packet analyzer but also a network detector and intrusion detection system (IDS). It can capture packets on wireless network using 802.11a/b/g/n traffic and throughput. The outputs are shown using command line interface. Kismet is written in C++ and can work on Linux, Solaris, BSD, Mac OS X, HP-UX and AIX operating systems.
- *Ettercap:* Ettercap [19] is software for sniffing and analyzing packets with different protocols. It is open source written in C and works over various platforms like Microsoft Windows, Linux, Mac OS X, BSD and Solaris. It can work as man in the middle and launch attacks by sniffing information or passwords and may be used as network analyzer.

B. *Vulnerabilities scanners*

Vulnerability scanner is software used to look for vulnerabilities on a computer network, computer system, or computer applications. These tools are used by attackers to find any vulnerability, which can be exploited to launch attacks. On the other hand security administrators use it to find open vulnerabilities on their systems so that these can be patched and attacks can be prevented. Following are examples of some notable vulnerability scanners.

- *Nessus:* Nessus [20] is a network vulnerability scanner. It was open source and free up till 2005. Then it was transformed into a commercial product. Nessus works by analyzing the network to find any hole in the network, which can allow an attacker to launch an attack by exploiting this vulnerability. It is a cross-platform tool and works on Linux, Mac OS X, and Microsoft Windows. It contains a well designed Graphical User interface , making it a user friendly and easy to learn tool.
- *OpenVAS:* Open Vulnerability Assessment System OpenVAS [21] is a framework containin several services and tools forged from Nessus in 2005 when Nessus was launched as a commercial software. It works on Linux and Microsoft windows.
- *Core Impact:* It is a very powerful and commercial vulnerability scanner tool. It is used for penetration testing by finding any vulnerability on the system. After finding a vulnerability, it can exploit the machine to establish an encrypted tunnel to reach other boxes to exploit them [22].
- *Retina:* Retina is a vulnerability scanner tool used to lookup vulnerabilities on the network. Using GUI gives this tool more usability. The drawback with this tool is that it works only on Microsoft Windows and is a commercial tool [23].

C. *Attack Detection tools*

Some tools are used to detect attacks but they can't prevent attacks. This type of tool is called Intrusion Detection System (IDS) and a particular genre of IDS only operate at network layer and are called Network Intrusion Detection System (NIDS). These NIDS use signatures, anomaly detection or both as detection technique for their operation. Some notable IDS are listed below:

- *Firestorm:* This Network Intrusion Detection System has a high performance and is full of capabilities to detect various attacks. It can analyze many of protocols to detect any malicious patterns in network traffic by using libpcap for capturing packets [25]. It uses anomaly detection method and fully supports Snort [24] rules. Firestorm is cross-platform and works on Linux 2.x, FreeBSD 4.x, OpenBSD, and Solaris.
- *Prelude:* Is a hybrid IDS, which uses Snort rules and is capable of using other IDS rules. It uses several sensors in the network to capture and detect any malicious packet. It can work on Linux, BSD, and other operating systems [26].
- *Dragon:* Dragon is a network and host intrusion detection system, which uses rule based and signature based detection techniques. It is a commercial tool and comes with extensive library. It is functionality heavy and its different parts allow it to detect a wide range of malicious attacks. Both a user friendly GUI and command line can be used with Dragon [27].

- ***Bro:*** A free and open source network intrusion detection system used only on Unix. In addition on working on network layer it works on application layer and is able to detect attacks concealed using encrypted traffic or those which try to evade analysis and detection [28].

D. Attack Prevention tools

They are different than IDS, in that they employ various techniques to prevent attacks too. Many of attacks tools are used for attack prevention also. Different mechanism and methods are used for detecting malicious strings and then preventing attacks. Some examples of the Intrusion Prevention Systems (IPS) are listed below:

- *Intrusion Prevention System (IPS)*

An Intrusion Prevention System (IPS) uses anomaly or rule based detection technique for detecting malicious strings and then prevents attacks. Actually, IPS is the second generation of intrusion detection system IDS.

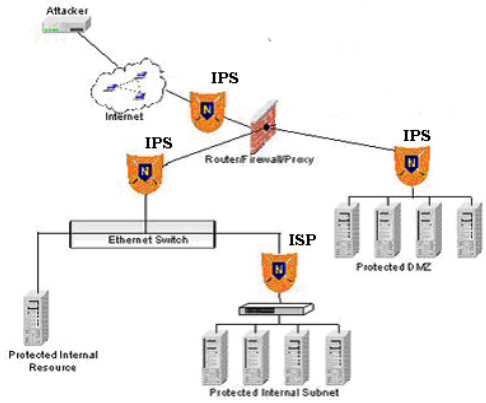

Figure 10: Intrusion Prevention System position in the network.

Snort: The most famous and powerful IDPS works on network layers and can also work on application layers. It can detect and prevent different kind of attacks like buffer overflow, denial of service attack, stealth port scan, CGI attacks, SMB probes and many of other attacks. Snort is open source tool which is widely used which and many research and development for it [24].

Suricata: Suricata [29] is a free and open source network intrusion detection and prevention system. It works on application layer in addition of network layers to detect and prevent variety of attacks. Suricata uses multithreading, which makes it faster than other IPS and IDS. The detection technique used by this tool is using rule based and anomaly based.

Firewall: Firewall is a software or hardware used to protect the network through analyzing the incoming and ongoing data, based on a rule set, if they have a malicious string or not. Most of operating systems uses software of firewall, and many routers uses component of firewall. Some kind of firewalls can operate on application layers in addition of network layer.

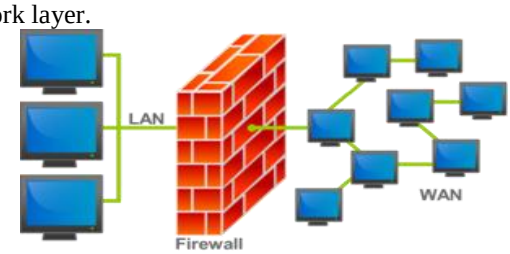

Figure 11:Firewall operation

Many of commercial and free firewalls differ in their capabilities and features. In the following some examples of open source and free firewall are given:

Netfilter: It is open source, written in C, and free firewall but works only on Linux. This firewall can be used with command line interface. It support different protocols on IPv4 and includes different modules for handling unruly protocols like FTP [30].

IPFilter IPFilter or short 'ipf ' is an open source and free firewall. It support IPv4 and IPv6 and can work on different types of operating systems like AIX, BSD/OS, DragonFlyBSD, FreeBSD, IRIX, HP-UX, Linux kernel, NetBSD, OpenBSD, OpenSolaris, QNX, Solarix, SunOS, and Tru46 [31].

E. Penetration test tools

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

- ***Nmap****:* It is the tool of choice for network discovery, port scanning and security auditing of the target network [32]. It is free and open source. It can carry out operating system and network device finger printing. It lets users build a complete picture of the target network. A large number of custom scripts for nmap are available to perform various pen-testing tasks.
- ***Netcat:*** This small and handy tool can be called the Swiss army knife of network pen-testing tools [33]. It allows reading and writing of data to network connections using the TCP/IP protocol. Any packet can be constructed and dispatched using netcat. It helps in creating malformed packets to test the protocol responses to them.
- ***hping:*** hping [34] is an open source and free TCP/IP packet assembler and analyzer. It does not have a graphical user interface and can only be accessed using the command-line interface. It supports multiple protocols including ICMP, TCP, UDP and RAW-IP protocols.

Tool	Category	Open Source	Free	Cross platform	GUI	Documentation	Maturity	Complexity	Active Support
Wireshark	Sniffer	Yes	Yes	Yes	Yes	Good	High	Low	Yes
Tcpdump	Protocol analyzer	Yes	Yes	Yes	CLI	Good	High	Medium	Yes
Kismet	Wireless sniffer/ IDS	Yes	Yes	Yes	3rd Party	Good	Medium	Medium	Yes
Ettercap	Sniffer/ Protocol analyzer	Yes	Yes	Yes	Yes	Sketchy	Low	High	Yes
Nessus	Vulnerabilities scanner	No	No	Yes	Yes	Good	High	Low	Yes
OpenVAS	Vulnerabilities scanner	Yes	Yes	Yes	Yes	Good	High	Low	Yes
Core Impact	Vulnerabilities scanner	No	No	Yes	Yes	Good	High	Low	Yes
Retina	Vulnerabilities scanner	No	No	Windows	Yes	Good	High	Low	Yes
Firestorm	IDS	Yes	Yes	Yes	CLI	Good	Medium	Medium	Yes
Prelude	IDS	Yes	Yes	Yes	Yes	Good	High	Medium	Yes
Dragon	IDS	No	No	Unix	Yes	Good	Medium	Medium	Yes
Bro	IDS	Yes	Yes	Unix	Yes	Good	High	Medium	Yes
Snort	IPS /IDS	Yes	Yes	Yes	3rd Party	Good	High	Medium	Yes
Suricata	IPS	Yes	Yes	Yes	3rd Party	Good	High	Low	Yes

Table 1: Comparison of various network tools

IV. CONCLUSION

The design flaws of TCP/IP suite of protocols have been responsible for most of the attacks on the Internet. Since then through concerted efforts various loopholes have been plugged and attack surface has been reduced considerably. But it always requires security to be applied as an external layer to the TCP/IP suite and this approach causes various problems itself and makes the things complex and vulnerable. With the introduction of IPV6 and IPSec various security problems of TCP/IP suite are likely to get solved on permanent basis. This paper has presented various attacks directed at TCP/IP and focused on the tools and defense mechanisms to identify the vulnerabilities that cause these attacks and ways to plug them.

REFERENCES

[1] Spafford, Eugene H. The internet worm incident. Springer Berlin Heidelberg, 1989.
[2] Braden, Robert. "RFC-1122: Requirements for internet hosts." Request for Comments (1989): 356-363.
[3] Barden, R. "RFC 1123: Requirements for InterNet Hosts-Application and Support." InterNet Network Working Group (1989).
[4] Deering, Stephen, and Robert Hinden. "Internet protocol." (1998).
[5] Chappell, Laura. "Inside the TCP Handshake." NetWare Connection (2000).
[6] "Google", online, http://google.com (last accessed on 2 Jun 2013)
[7] "Wireshark", online, www.wireshark.org. (last accessed on 25 May 2013)
[8] CERT, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks," September 1996.
[9] Bellovin, Steven M. "A look back at." Computer Security Applications Conference, 2004. 20th Annual. IEEE, 2004.
[10] Tanase, Matthew. "IP spoofing: an introduction." Security Focus 11 (2003).
[11] Ferguson, Paul. "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing." (2000).
[12] Heberlein, L. Todd, and Matt Bishop. "Attack class: Address spoofing."Proceedings of the 19th National Information Systems Security Conference. 1996.
[13] Trabelsi, Zouheir, and Khaled Shuaib. "NIS04-4: Man in the Middle Intrusion Detection." Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE. IEEE, 2006.
[14] Harris, B., and R. Hunt. "TCP/IP security threats and attack methods."Computer Communications 22.10 (1999): 885-897.
[15] Barbir, A., S. Murphy, and Y. Yang. "Generic threats to routing protocols." (2006).
[16] Yan, Boru, et al. "Detection and defence of DNS spoofing attack." Jisuanji Gongcheng/ Computer Engineering 32.21 (2006): 130-132.
[17] "TCPdump and libpcap", online, http://www.tcpdump.org/"(last accessed on 26 May 2013)
[18] "KISMET", online, http://www.kismetwireless.net/ , (last accessed on 25 May 2013)
[19] "ETTERCAP", online, http://ettercap.github.io/ettercap/, (last accessed on 25 May 2013)
[20] "NESSUS vulnerability scanner", online, http://www.tenable.com/products/nessus (last accessed on 25 May 2013)
[21] "Open VAS- Open Vulnerability Assessment System", online, www.openvas.org (last accessed on 25 May 2013).
[22] "Core-impact", online, http://www.coresecurity.com/core-impact-pro (last accessed on 25 May 2013).
[23] "Retina Network Security Scanner", online, http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/ (last accessed 28 May 2013)
[24] Roesch, Martin. "Snort-lightweight intrusion detection for networks."Proceedings of the 13th USENIX conference on System administration. 1999.
[25] Leach, John, and Gianni Tedesco. "Firestorm network intrusion detection system." Firestorm Documentation (2003).
[26] Zaraska, Krzysztof. "Prelude IDS: current state and development perspectives."URL http://www. prelude-ids. org/download/misc/pingwinaria/2003/paper. pdf(2003).
[27] Allan, Ant. "Enterasys Networks Dragon Intrusion Detection System (IDS)." (2002).
[28] Bro, I. D. S. "Homepage: http://www. bro-ids. org." (2013).
[29] "Suricata Intrusion Detection System", online, http://suricata-ids.org/ (last accessed 31 May 2013)
[30] Yao, Xiaoyu, and Chen ZHAO. "Research on Implementation and Application of Linux Kernel Firewall Netfilter [J]." Computer Engineering 8 (2003): 042.
[31] Reed, D.: IP Filter. Online. http://coombs.anu.edu.au/~avalon/ip-filter.html (Last accessed 31 May 2013)
[32] "Nmap", online, http://nmap.org/. (last accessed 1 Jun 2013)
[33] "What is netcat?", online, http://netcat.sourceforge.net/, (last accessed 1 Jun 2013)
[34] "hping", online, http://www.hping.org/ (last accessed 1 Jun 2013)