TITLE OF ASSIGNMENT: SECURITY VULNERABILITIES AND COUNTERMEASURES IN TCP/IP LAYERS

NAME : MWAMI MUGALA

COURSE NAME : MASTER OF NETWORK ADMINISTRATION AND SECURITY

DATE : 03.05.2014

INTRODUCTION

The purpose of this paper is to expose the many security loopholes in the TCP/IP protocol layers and its implementation. Both the protocol level problems and implementation flaws are explored in this research paper, giving the dangers they pose, the probable attacks and the controls that can be enforced to overcome them. The security vulnerabilities and solutions are highlighted at each layer of the TCP/IP protocol model. By gaining the understanding of the security loopholes at each layer, developing a secure network can be made possible by taking a layered approach of designing and deploying security mechanisms.

JUSTIFICATION

The TCP/IP protocol suite was created as an internetworking solution with little or no regard to security aspects. The development of TCP/IP protocol suite was focused on the creating a communication protocol standard that can interoperate between different hardware devices and software independent. Other major goals included; failure recovery and the ability to handle high error rates, efficient protocol with low overhead, routable data and the ability to add new networks to an already existing network without disrupting the existing network (TCP/IP Foundations, Sybex, San Francisco and London. Andrew G Blank. 2004.).

Its main emphasis was providing a suite Security was not given priority in the creation of this protocol suite. Hence, by default, TCP/IP has security flaws at both the protocol level and implementation. The major types of possible attacks that are highlighted in ths paper are denial of service.

TCP/IP Protocol Model

TCP/IP is made up of various layers that each performs distinct tasks. These layers have protocols that are needed for devices on a network to communication. According to the TCP/IP model, there are four layers; Application, Transport, Internetwork, Network access layer. At each layer, there are some security weaknesses that can be exploited by attackers. By understanding the most fundamental flaws in TCP/IP and its implementation, a network

security expert can enhance the security controls to protect both the network applications and the actual network itself.

Both the protocol and implementation flaws can be mitigated by applying layers of security mechanisms in the network.

APPLICATION LAYER

The application layer of the TCP/IP model is a combination of the application, presentation and the session layer of the OSI model. It offers the first step of getting data onto the network and interacts directly with the user. It consists of software programs that users deploy to communicate over a network. The presentation layer is in charge of formatting the data in way that can be interpreted by the appropriate device on the destination device, data compression and decompression, encryption and decryption of data.

There are a number of application layer protocols that provide the exchange of user information. Some of these protocols are; Hypertext Transfer Protocol (HTTP), Telnet, Simple Mail Transfer Protocol (SMTP), Dynamic Host Control Protocol (DHCP), File Transfer Protocol (FTP), Domain Name System (DNS). Each of these protocols has vulnerabilities that will be highlighted and explored.

Hyper Text Transfer Protocol and Web applications and Browsers

Every day we need to communication using the internet and the most common way to do so is via the usage of web browsers. Web browsers by default use HTTP as the communication protocol to transfer files that make up the web pages from the web servers. These transfers are done in plain text and thus an intruder can easily read the data packets.

Instead of using the traditional HTTP, web browser developers deploy HTTPS (Hyper Text Transfer Protocol Secure). HTTPS is managed by a security protocol called Secure Socket Layer (SSL). SSL provides encryption of data transmitted between the web server and the web client or browser. It uses a public-key encryption to exchange a symmetric key between

the client and the server; this symmetric key is used to encrypt the HTTP transaction (both the request and the response.)
The data transmitted will be unreadable to an attacker using packet capturing tools to eavesdrop.

With SSL incorporated in HTTP, the data can even travel on a less secure network but still maintain integrity and confidential.

Web application and browser security vulnerabilities

Caching

Web browsers and web application can also have security problems that can be exploited. Web browsers perform caching of the web pages a use has visited. The contents in the cache are saved temporarily on the user's machine for easy access in case the user wants to view the web page again, the files will load from the local hard drive. The cache can contain images, passwords and user names. If the user's computer was compromised, an attacker can view all the contents and the user's browsing habits without any need of being authenticated and thus can be a privacy concern.
It is important to clear the cache once in a while and also disable the auto saving feature in the browser of passwords and user names in the cache.

Session hijacking

Hijacking is an attack that can happen when the attacker steals an HTTP session after observing and capturing the packets using a packet sniffer. A successful hijack enables the attacker to have full access to the HTTP session; and the communication changes from the client to the web server to attacker to the web server.
Hijacking is possible when there is weak authentication between the client and the web server during the initializing of the session.

Cookie Poisoning

Cookies are used to maintain the state of a session to avoid the user to retype in their credentials every time they visit a site or change web pages. Cookies are used by many web applications (including browsers) to save information. This information is stored

permanently or temporarily on the client machine. Cookie poisoning is the modification or theft of cookie in a user's machine by an attacker in order to release personal information. If the attacker gets hold of a cookie containing a password and username, they can use the cookie on their machine and the web server will not request any authentication because the cookie will issue out the username and password automatically. With cookie poisoning, an attacker can gain access to unauthorized information about a user and possibly steal their identity.

Web Application Firewalls (WAF) are able to detect and block cookie poisoning attacks. Web Application Firewalls are able to inspect the HTTP sessions and can trace down the parameters set in the cookies that have been issued by the web server.

Replay attack

This involves a man-in-the-middle attack in which the sent data is repeated sent to the server. This is more than a hijack; the data resent can be modified and can bring different results.

Furthermore, the attacker can spoof the client's IP address and thus redirect his/her machine. The web browser should be able to tell that replayed traffic is not legitimate. This can be done by the web browser having a good way of keeping track of sessions.

Cross-Site Scripting

This attack involves the hacker injecting malicious code in a web application or browser and is executed at the client side. The essence of this attack is to perform a session hijack by stealing session tokens and cookies of a legitimate user's session.

The best defence is to disable scripts to run on the website. However, this control means that some functions and features on the website will not be available. Another alternative is to enhance the security controls when dealing with cookie based user authentication.

Domain Name System

Domain Name System is used to resolve host domain names to IP addresses. We depend of DNS functionality every day we browse the internet or type in a URL in a web browser.

An attacker's aim is to modify a DNS record so that it resolves to an incorrect IP address; they can cause all traffic for that site to the wrong computer. There are a two ways a hacker

can exploit DNS; he first being protocol attacks and he second is by attacking the DNS server.

DNS Protocol Attacks

These are based on the flaws found in the DNS protocol; which is the actual way DNS works on the network. There are three common attacks in this category, namely; DNS cache poisoning, DNS spoofing and DNS ID Hijacking.

DNS cache poisoning is an integrity attack that involves manipulating the information saved in the DNS cache giving it wrong information. This false information will offer a name to IP mapping to a wrong IP address. The aim is to divert the requests to another site. This attack can lead to pharming. The new web site might be bogus and offers the same similar products or services as the real web site. If the user does not notice anything, enters the user name and password, the attacker can steal their credentials.

DNS spoofing refers to faking the IP address of a computer to match the DNS server's IP address so that requests can be directed to that wrong machine. In this attack, the hacker's machine is considered to be a legitimate DNS server by clients and other servers. It will impersonate the DNS server and reply to all incoming requests from the clients thus misdirecting them.

Most of the DNS attacks have been fixed in the patches. It is important to make sure the DNS server's operating systems is up to date. DNS security DNSSEC is a set of extensions to the DNS system that are designed to prevent DNS attacks.

Dynamic Host Configuration Protocol (DHCP)

DHCP is used to automatically assign temporal IP addresses to client machines logging into an IP network. The DHCP server is configured with a pool of IP addresses that are leased to client machines after a request.

This protocol can be misused by an attacker by making this service unavailable. DHCP starvation attack is the consuming of the IP address space allocated by the DHCP server. The attacker can send a lot of DHCP request broadcasts using spoofed MAC addresses. The DHCP server simply leases its IP addresses one by one until it runs out of IPs to give out.

When a genuine user wants to access the network, the server will not offer an IP address automatically and the user will not be granted access into the network. This is a denial of service attack.

To prevent DHCP starvation, port security can be used because it only allows a specified number of MAC addresses per port.

TRANSPORT LAYER

Transport Layer is responsible for process to process delivery by ensuring that applications on two or more nodes are able to communicate. It hosts three protocols which offer different features that can be required by particular types of application. These protocols are; Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Stream Control Transmission Protocol (SCTP).

TCP is a connection oriented protocol, meaning that for to be sent from a sender to a receiver, a connection must be established. The sender needs to know if the receiver is available, and negotiate some parameters for sending the data. To archive this, TCP uses the three way handshake.

Three way handshake security flaws

In the three way handshake procedure, the client sends SYN segment to the server requesting to establish a connection, the server replies with a SYN-ACK segment acknowledging the client's request, the client then sends an ACK segment and there after the connection is established.

TCP Sequence Number Prediction

The security weakness in this the three way handshake is the ability to predict TCP sequence numbers. This is possible because the sequence number is incremented by a constant amount per second and by half that amount each time a connection is initiated. If an

attacker manages to gain access and connect to the server legitimately, he can easily guess the next sequence number, which can lead to a session hijack and TCP injection attacks. Sequence number prediction can be overcome by randomizing the generation of initial sequence number increment.

Another form of Hijacking that can be done is called TCP blind spoofing. In this attack, the attacker manages to somehow guess both the port number and sequence number of the session that is in process. If the correct port and sequence number is acquired, the attacker can carry out an injection attack.

SYN Flood

Another flaw that the three way handshake has is the SYN flood attack. In this attack, multiple SYN packets are spoofed using a source address that does not exist. They are then sent to the target server. After receiving the fake SYN packets, the server replies with a SYN ACK packet to the source address that is unreachable. This situation creates a lot of half-opened sessions due to the fact that the expected ACK packets are not received by the server to properly initiate a session. This can cause the server to be overloaded or can eventually crash. The server will not allow any further connections to be established and legitimate user connection requests will be dropped, thus leading to a denial of service attack.

SYN floods can be eradicated by using a firewall to act as a proxy between the server and the client. The firewall will be responding to the SYN packets from the clients. Hence the SYN ACK packets will be sent on behalf of the server to the client. The firewall will only allow connections to the server after it receives an ACK packet from a client. This process eliminates all possible client/server half-opened connections.

UDP Flood attack

This is a denial of service attack that takes advantage of UDP services that reply to requests. For instance UDP port 7 is an echo port. Another UDP port that replies to queries is the chargen port (http://www.cve.mitre.org). An attacker can overwhelm the target machine with multiple requests to these ports creating a lot of traffic on the network.

To prevent UDP flooding attacks, an intrusion detection system can be deployed to perform network traffic monitoring. Any anomaly in the flow of traffic will cause an alarm and a firewall or an intrusion prevention system can be implemented take action.

INTERNETWORK LAYER

The internetwork layer performs routing functions. The main protocol at this layer is the Internet Protocol or IP. IP is implemented in two versions; IPv4 and IPv6. Other protocols that exist at this layer are; Address Resolution Protocol (ARP) Internet Control Message Protocol (ICMP) and Internet Group Multicast Protocol. These protocols pose some serious security vulnerabilities.

IP addresses together with a subnet mask uniquely identifies devices on a network. However, an attacker can easily spoof an IP address and from this, it is possible to carry out a man-in-the-middle attack. Alternatively, an attacker can hijack a connection session.
Overcoming this attack can be done by deploying route policy controls that use a strict anti-spoofing and route filters at the edge of the network. Setting up a firewall with strong filter and anti-spoofing policies can also mitigate such an attack (Computer Networks – Basics and Security Issues, Barak Ekici, Yasar University, Turkey.)

IP source route involves a packet listing the specific routers it took to reach its destination; this path can be used by the recipient to send the data back to the sender. In a source route attack, the attacker can modify the source route option in the packet. This can lead to a loss of data confidentiality as the attacker will be able to read the data packets. Dropping or forwarding packets that carry the source route option can solve this issue.

RIP Security Attacks

Routing Information Protocol is a dynamic routing protocol and an interior gateway protocol that is used to propagate routing information on local networks. The messages sent are unchecked by the receiver, and so, an attacker can take advantage of this and easily send incorrect routing information or simply forge RIP messages. The attacker's intent can be to

impersonate a route to a particular host that is unused. The packets can be sent to the attacker for sniffing or perform a man in the middle attack.

The way around to disable RIPv1 and use RIPv2 and enable MD5 based authentication. Another alternative is completely getting rid of RIP and replacing it with Open Shorted Path First (OSPF). OSPF also uses MD5 authentication.

OSPF uses five message types and these messages have security vulnerabilities that can be exploited. (Network Infrastructure, Authentication, management and routing protocols that run your network, Jeremy Rouch)

Internet Control Message Protocol (ICMP)

ICMP is a basic network diagnosis or management protocol of the TCP/IP. It is used to send error and control messages regard the status of a host or router. ICMP is an integral part of the IP network implementation and thus is present in very network setup. ICMP can be abused to wage an attack on a network. There are two kinds of attacks that can be initiated by exploiting ICMP protocol; passive and active attacks.

ICMP Passive Attacks.

A passive attack involves monitoring of traffic and available hosts on a network. If successful, a hacker is able to read unencrypted data and can use the information gathered to perform another type of attack.

Network reconnaissance attacks can be categorised in the group of passive attacks. The essence of network reconnaissance is an attempt to determine network topology and paths into the network. It uses ICMP packets to offer information that is being probed for. It gives the attacker a true picture of the network to enable proper planning before launching an active attack. An attacker will be able to better understand the environment and gather information about the target so as to plan the attach approach. He or she is able to determine the number of hops to reach a specific device, where the firewalls are placed on the network, applications and hosts running on the network.

ICMP sweep, Ping sweep or IP sweep involves discovering all the host IP addresses which are alive in the entire target's network. Instead of pinging each individual host, a ping sweep will probe all hosts simultaneously in a given network range with a single command. There

are many free downloadable applications that offer ICMP sweep; one example is nmap. This makes it very easy for an attacker to know the alive host IP addresses in a network.

Port scanning attack is also another method used for reconnaissance. The attacker can deploy a scanning tool that checks for listening or open UDP/TCP ports on target hosts, and is able to determine whether the hosts are using the ports to provide services. If the port is opened, it means that a certain application is running and from this information an attack can pin point which particular vulnerability that application has and exploit it. Apart from gain the knowledge of which services are running, port scanning also gives out information such as; what users own those services, whether anonymous logins are supported, and whether certain network services require authentication (SANS Institute of InfoSec Reading Room – Port Scanning Techniques and the Defense Against Them.)

Furthermore, it is also possible to know which operating system is being used on a host machine. This is called operating s fingerprinting. Each operating system has a different way in which it handles network traffic. ICMP can be used to determine the underlying operating system.
A defence against port scanning is to disable all the ports that are not in use on a server or client. Deploying TCP wrappers can restrict the information gained from port scans. TCP wrappers allow a network administrator to permit or deny access to the services based upon IP addresses or domain names. It is advisable to carry out a port scan on a device before it goes public online.

A perfect tool that can accomplish a passive attack is traceroute. Trace route is a popular ICMP utility that is used to map a target networking by describing the path in real time from the client to the remote host being contacted (Computer Desktop Encyclopedia.)
Using the traceroute, the attacker is not only able to trace the path taken by a packet as it travels to the target but also gives information on the topology of the target network. This will allow the attacker to plan his approach when attacking the network.

ICMP Active Attacks

This type of attack is more than monitoring and analysing of traffic. An attacker actually tries to bypass or break into the network and can result in a denial of service.

One important tool used in network diagnosis is the ICMP ping. Ping echo packets can be sent to a broadcast address on a target network which can eventually lead to a traffic overload which can impede normal traffic and can lead to a denial of service. This is called an ICMP smurf attack, Ping Flood or ICMP storm attack.

Deploying a firewall can stop ICMP floods from happening. The firewall can check the rate of ICMP packets destined for a specific destination address. There should be threshold rate and if it is exceeded, then all such subsequent ICMP packets should be dropped.

Another security vulnerability that ICMP poses is ICMP redirect attacks. ICMP redirects are used by gateways or routers to advice the hosts of better routes. ICMP redirect attacks send incorrect messages to hosts on a subnet to request the hosts to change their routing tables. The changes made in the hosts routing tables will interfere with their normal forwarding of IP packets.

Using an Intusion Detection System (IDS) policy to provide notifications of attempts to modify the routing tables. The IDS policy can also be used to disable ICMP redirects. By doing so, ICMP redirect packets will be dropped.

Ping Of Death Attack

This attack involves sending IP packets that exceeds 65,535 bytes to the target device. The malformed packets can be sent as ping messages with 56bytes or 84 bytes with the IP header is considered. The target computer will not be able to handle this packet properly and can cause the operating system to crush. This is called a kernel panic attack. Eventually this leads to a denial of service attack [Denial of service attacks, Gary C. Kesseler & Daine E. Levine, 2013]

To fix this operating system glitch, it important to patch up the operating system. Current operating system updates have fixed this problem.

Teardrop attack

This is also another denial of service attack in which an attacker sends a series of fragmented packets that the target machine will not manage to reassemble due to a bug in the TCP/IP fragmentation reassembly and the packets will overlap one another [http://security.radware.com/knowledge-center/DDoSPedia/teardrop-attack/]

Other versions of the teardrop attack are; NewTear, Nestea, SynDrop and Bonk.

Patching up the operating system with the latest security updates can mitigate this problem.

NETWORK ACCESS LAYER (Data-Link and Physical layer)

Data link layer

The data link layer has two basic functions; allowing the upper layer protocols to access the media and to control the placement of data on the media. Data link layer devices are switches and these are mainly implemented as the access points of end users to the network. (Network Fundamentals, CCNA 2008. Mark A. Dye)

Redundancy in a network is very important. In case one link goes down, the second link can pick up. However, this concept in a switched environment can cause loops, in which packets keep going in circles. Switches offer the spanning tree protocol (STP) to prevent loops. This protocol may be purposely or accidentally tempered with some errors causing it to transmit packets in an infinite loop.

Eavesdropping via sniffing is possible at the data link layer. Since all broadcasts are sent to all switch interfaces except the originating port, subnets using broadcasts are sent to all network interface cards attached to that switch. This means that packets can be analysed or stored for later inspection by an attacker. Tools such as wireshark are capable of capturing packets.

Physical or MAC addressing is done at the data link layer. For the switching process to be a success, each packet that requires delivery needs to have a physical address.

Switches use a cam table to store information such as the Mac addresses available on physical ports with their associated VLAN parameters (Security, CISCO Systems 2002.) The table can only store a fixed size of information. A hacker takes advantage of the fixed

memory size by maxing it with more entries than it can handle causing to overflow. This attack is called cam flood or mac flooding attack.

ARP Attack

Data link layer uses the Address Resolution Protocol (ARP) to translate the IP address to the MAC address. The client begins by first sending a broadcast ARP message, requesting for a MAC address for a given IP address. The switch broadcasts the ARP message to all ports except for the source port. When the intended destination IP address gets the ARP, it replies with its MAC address and all other hosts on the switch will drop the packet. From there, the sender updates its ARP table with the new physical to logical binding.

Gratuitous ARP is another flavour of the traditional ARP. It is used by hosts to "announce" their IP address to the local network and avoid duplication of IP addresses on that network (Hacking Layer 2: Fun with Ethernet Switches, Sean Convery, Cisco Systems, 2002.)

Gratuitous ARP can be abused by a hacker. There is no authentication in the ownership of IP or MAC address. So an attacker can spoof an ARP packet to announce an IP and MAC address of an already existing host. This can cause an IP conflict on the network and the legit user can be kicked out of the network causing a denial of service. Furthermore, this attack can allow the switched environment to start delivering traffic to the wrong hosts because the cam table has been altered with wrong IP and Mac bindings.

ARP keeps its physical to logical bindings in an ARP cache. An attacker can modify this table and give incorrect mappings. This attack is called ARP cache poisoning. When a client machine wants to send data, it looks up at the poisoned cache and sends the data to an attacker. ARP cache poisoning requires that the attacker is on the same subnet as the target machine because ARP does not cross the router boundaries. To combat against an attack, it is important to enhance the physical security.

Vlans are implemented on switches and their main purpose it to divide a layer 2 network into multiple broadcast domains. This increase the network performance by reducing the broadcast domains and the collision domains. An attacker's aim will be to access traffic of another Vlan which he has no access to. Such an attack is called Vlan hopping. This kind of

attack allows the sending of data traffic to hosts that belong to another Vlan. The attacker generates traffic and tags it with a valid VLAN ID of a target VLAN. This lets traffic cross Vlans.

Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium [Data Communications and Networking By Behrouz A. Forouzan] This layer consists of the actual connections to and within the network; routers, switches, servers, cables and wireless media.

The type of attack that can be performed at this layer is dependant of the communication media being used; wired or wireless communication environments.
If an attacker is about to gain access to any of them, then he or she can easily cause a denial of service attack by making the causing the organisation application unavailable to users or simply sniff the actual media by tapping into the network. Ethernet copper twisted pair cables are relatively easy to hack into. An attacker needs to have knowledge of the Ethernet cabling standards (568A or 568B). With this information, a cable can be easily tapped into without being detected.

One other security vulnerability with twisted pair cables is that they emit electromagnetic energy that can be picked wit sensitive equipment without the need for physical tapping into the media. Optic fiber cables emit not electromagnet waves and are hard to tap. They can be used in place of Ethernet cables.

Physical theft of data and hardware equipment is a possible result of poor physical security. A simple thing like removing or cutting a network cable can cause a lot of havoc on the network.

In a wireless networking environment, an attacker can easily eavesdrop. Wire Equivalent Privacy (WEP) is one of the most common wireless authentication standards that is widely used. However, it uses a very weak RC4 encryption algorithm and a determined hacker can easily crack it by using dictionary attacks or brute force. Wi-Fi Protected Access overcomes

the weakness that WEP has. It offers a sophisticated hierarchy that generates new encryption keys each time a mobile device connects to the network (Computer Desktop Encyclopaedia)

Wireless access points can be spoofed. An attacker can set up a rogue access point, give it the same service set identifier (SSID) of the genuine network and also configure the wireless network authentication password to be the same. When users login to this network, the attacker has full access to their machines.

Wireless media is susceptible to radio frequency interference. An attacker can jam the wifi's radio frequency by placing a device that can distort the wave length and amplitude of the signals making the network unusable.

To mitigate physical layer attacks, certain aspects need to be considered. The physical layer addresses the actual physical security to equipment and media. To combat these attacks, there is need to control the physical access to the networking devices. For instance, the server should be locked and only authorized individuals should be allowed inside. This can include setting up physical locking systems using door locks and/or biometric security systems. Backup power should also be available in case there is a power outage. The equipment should be free from fire and water, as this can easily damage the devices. Other environmental issues that should be avoided in server rooms are food stuffs and drinks. Hardware failure is sometimes inevitable. However, to avoid data loss, there is need to backup the data at regular intervals and have a good disaster recovery plan. The backups should also be tested to ensure integrity and make sure they are working according and can work if used to restore the system. These backups should be stored in a remote site in case the server room has some catastrophe.

CONCLUSION

This paper has exposed some of the many security vulnerabilities that exist in the TCP/IP Protocol layers and its implementation. Various security flaws are shown on a layer by layer basis.

The TCP layers follow the domino effect which means that if one layer is hacked, the other layers will not be aware and communication will be compromised. If an attack is done at the data link layer, the application layer will not be aware of such an attack. It is for this reason that security controls be deployed on each layer. It is possible to deploy security measures at every TCP layer. For such controls to be implemented, it is important to understand and address the security vulnerabilities and threats at each layer. This can effectively reduce the risk of the exploits to be successful.

Physical security to network infrastructure is sometimes overlooked. Unauthorised physical access to media and equipment should be restricted.

From this paper, it can be seen that the development of TCP/IP was mainly focused on providing a stack of layers that offer communication possible. Security was not highlighted in its infancy. This is why defence in depth security systems should be deployed; which has a layered approach in protecting the network system.

REFERENCES

San Fransisco and London Andrew G Blank. (2004). *TCP/IP Foundations*. Sybex.

Ronald Krutz and James W. Conley. (2005) *Network Security Bible*. Canada. Wiley Publishing, Inc.

Computer Desktop Encyclopaedia-(iPhone Application) 2013.

Common Vulnerabilities and exposures, Retrieved from http://www.cve.mitre.org

Barak Ekici. (2012) *Computer Networks – Basics and Security Issues*. Yasar University, Turkey

Behrouz A. Forouzan. (2013) *Data Communications and Networking* 5th edition. McGraw-Hill Forouzan Networking Series. USA.

Mark A. Dye. (2008) *Network Fundamentals CCNA Exploration Companion Guide*. Cisco Press. Indianapolis, USA.

Radware Limited. (2013). *Teardrop Attack*, http://security.radware.com/knowledge-center/DDoSPedia/teardrop-attack

Gary C. Kesseler & Daine E. Levine. (2013) *Denial of service attacks*. Retrieved from all.net/CID/**Attack**/papers/DCA.html

SANS Institute of InfoSec Reading Room.(2001). *Port Scanning Techniques and the Defense Against Them. Retrieved from http://www.sans.org/reading-room/whitepapers/auditing/port-scanning-techniques-defense-70*

Jeremy Rouch. Network Infrastructure Insecurity. Theauthentication, management and routing protocols that run your network. Retrieved www.blackhat.com/presentations/bh-usa-00/Jeremy/JeremyRauch.ppt

Sean Convery. (2002) Hacking Layer 2: Fun with Ethernet Switch. Cisco Systems.