

COMPREHENSIVE GUIDE ON NETWORK SECURITY WHITEPAPER



PREPARED BY

Mr.Venkatesh
Security Engineer
@briskinfosec Bint lab



PRESENTED BY

NCDRC
(National Cyber Defence
Research Centre)
in collabration with
BINT Lab
www.ncdrc.res.in

1.INTRODUCTION

Welcome to the world of 'network security' which is an unavoidable term in cybersecurity. This white paper of 'Network security' encompasses the most significant and predominantly used networking security concepts which are highly important for maintaining your network environment secure.

Go on to read it!

CONTENTS

- Wireless encryption standards
- Authentication and security on a wireless network
- Network attacks and threats
- Securing networking devices
- Mitigation techniques
- TCP/IP Security
- Organizational Security
- Troubleshooting the Network.



2. WIRELESS SECURITY

In this section, we will focus our attention on the importance of wireless security, and then we'll dive in to learning and understanding about various wireless encryption standards and technologies that are used to help in securing the transmission of traffic on a wireless network. We will also look at different wireless authentication and authorization methods that will aid you in designing and implementing a safer wireless network for your home or office.

2.1 WIRELESS ENCRYPTION STANDARDS

In this section, we are going to dive in to various encryption standards that are used on wireless networks.

2.1.1 WIRELESS EQUIVALENT PRIVACY (WEP)

WEP is an encryption standard that was used in early generations of wireless networks. WEP uses the RC4 cipher, which provided a 40-bit key for data encryption. In 2002, various security flaws were discovered, which allowed an attacker to compromise the encryption key. Due to weak encryption key, WEP can be compromised within a few hours. It's not recommended to use a WEP encryption standard on wireless networks anymore.

2.1.2 Wi-Fi PROTECTED ACCESS (WPA)

WPA was created in 2002 to fix the security flaws of Wired Equivalent Privacy (WEP). WPA uses Temporal Key Integrity Protocol (TKIP), which applies the RC4 encryption cipher for data privacy. Furthermore, the initialization vector (IV) is larger on each packet and uses a hash value to produce an encryption key of 128-bits. TKIP uses the secret key combined with the initialization vector IV; this produces the TKIP value, which changes frequently between the client and the wireless router/access point.

Additionally, a sequence counter is used as a countermeasure for any replay attacks that are attempted by a hacker or a malicious user. Each packet sent between the wireless router/access point and the client device contains integrity checking, which is done through a 64-bit key to prevent and detect any modifications of packets between the sender and receiver. However, with a lot of technologies, TKIP has its vulnerabilities and was later disapproved during wireless security implementations in 2012.



2.1.3 WI-FI PROTECTED ACCESS 2 (WPA2)

The WPA2 wireless security encryption standard uses the Advanced Encryption Standard (AES) for data encryption rather than the RC4. This is an upgrade for data security. Furthermore, WPA2 applied the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which replaced the need for TKIP. The CCMP uses a 128-bit key for its data encryption by using the AES, which creates data blocks of 128-bit in size. Due to larger data blocks and stronger encryption algorithms being used in WPA2, more computing resources are required.

CCMP provides the following during wireless transmissions:

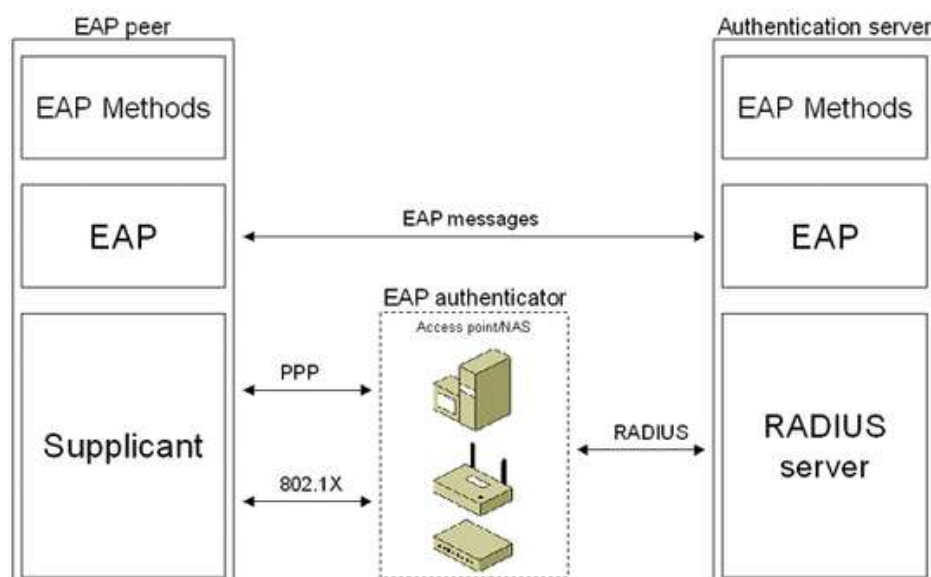
- Confidentiality
- Authentication
- Access control

3. AUTHENTICATION AND SECURITY ON WIRELESS NETWORK

In this section, we will cover various wireless authentication and security methods on a wireless network.

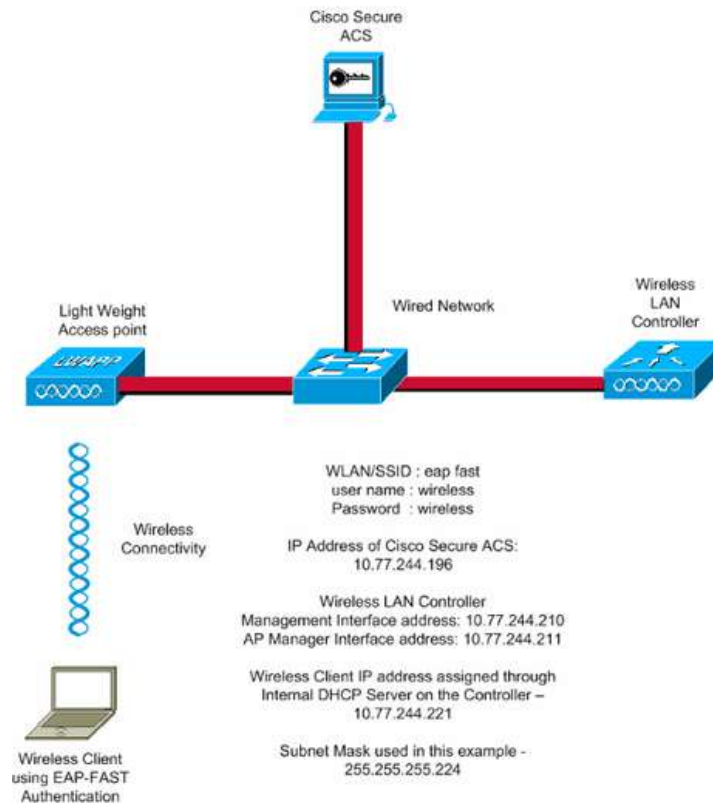
3.1 EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

EAP is a framework that allows a client to authenticate to a wireless network. The Internet Engineering Task Force (IETF) has many Request For Comments (RFC) standards for the EAP framework.



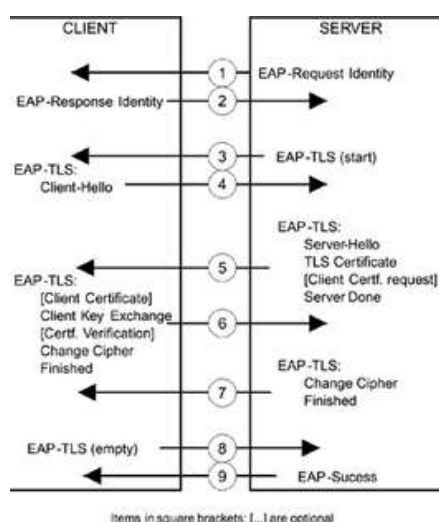
3.2 EAP FLEXIBLE AUTHENTICATION VIA SECURE TUNNELLING (EAP-FAST)

One version of EAP Cisco that was proposed was the Lightweight EAP (LEAP), which was considered to be lightweight and secure. However, Cisco has since updated their framework to the EAP-FAST, which has improved security on the wireless networks.



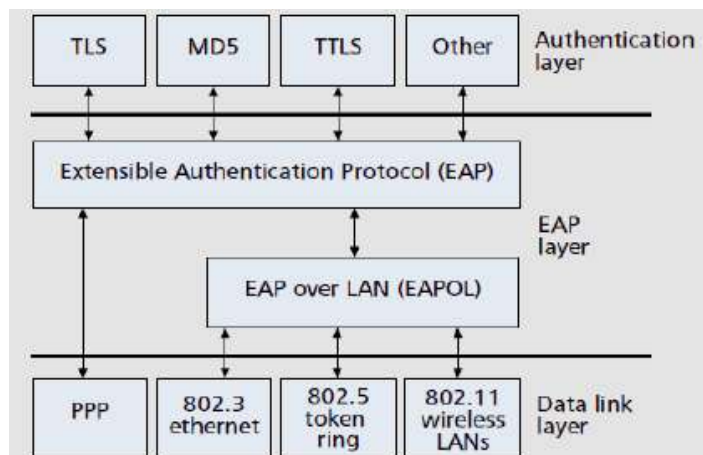
3.3 EAP TRANSPORT LAYER SECURITY (EAP-TLS)

The EAP-TLS provides strong security. TLS has since gained popularity as the successor of the Secure Socket Layer (SSL). With improved security features, EAP-TLS was widely implemented in wireless devices.



3.4 EAP TUNNELED TRANSPORT LAYER SECURITY (EAP-TTLS)

This version of the TLS tunnel allowed organizations to tunnel other authentication methods and protocols through the EAP tunnel.

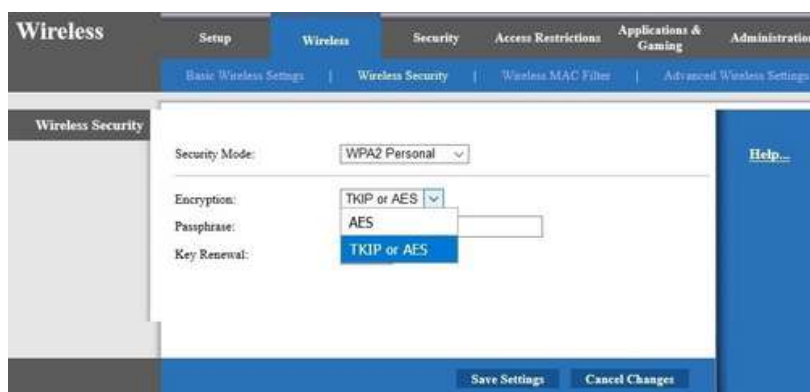


3.5 PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL (PEAP)

PEAP was developed by various technology vendors such as Cisco, RSA security, and Microsoft. PEAP allows EAP within a TLS tunnel.

However, it was most commonly implemented in EAP-MSCHAPv2 on Microsoft systems, which allows for authentication to Microsoft's MS-CHAPv2 databases

On your wireless router or access point, under the Wireless security settings, you will have various security modes to choose from WEP, WPA, WPA2, and so on. After choosing a security mode, the device will allow you to choose an encryption standard, such as TKIP, AES, or both:



After choosing the encryption mode, the device will allow you to set a Pre-Shared Key (PSK) (better known as a WPA2-PSK), which is used during the authentication phase between the wireless router/access and the client. The WPA2 security mode uses a 256-bit key for data encryption of all traffic to and from the client.

3.6 MAC FILTERING

A wireless router can filter a Media Access Control (MAC) address, which either allows or denies access to the wireless network. However, attackers have found a way to spoof an authenticated client's MAC address. This allows an attacker to bypass the filtering access control list feature on the wireless router/access point. The below screenshot shows the client devices (stations) that are currently authenticated to a wireless router (Basic Service Set Identifier (BSSID), with the MAC address and the Extended Service Set Identifier (ESSID) -the name of the network).

```
CH 2 ][ Elapsed: 2 mins ][ 2018-10-28 18:58
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
38:4C:4F:	0	0	565	103 0	2	195	WPA2	CCMP	PSK	_WiFi_T28R

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
38:4C:4F:	B0:C0:90:	-1	1e- 0	0	43	
38:4C:4F:	5C:C3:07:	-82	1e- 1e	0	35	
38:4C:4F:	DA:A1:19:	-92	0 - 1	0	17	_WiFi_T28R

3.7 GEOFENCING

Geofencing is where you restrict or allow features, when the device is in a particular area using a client's Global Positioning System (GPS) location service. For example, if a wireless client is outside a geographical area, some features may not work. Therefore, geofencing ensures that users are in a particular area so that they can use a device or feature.



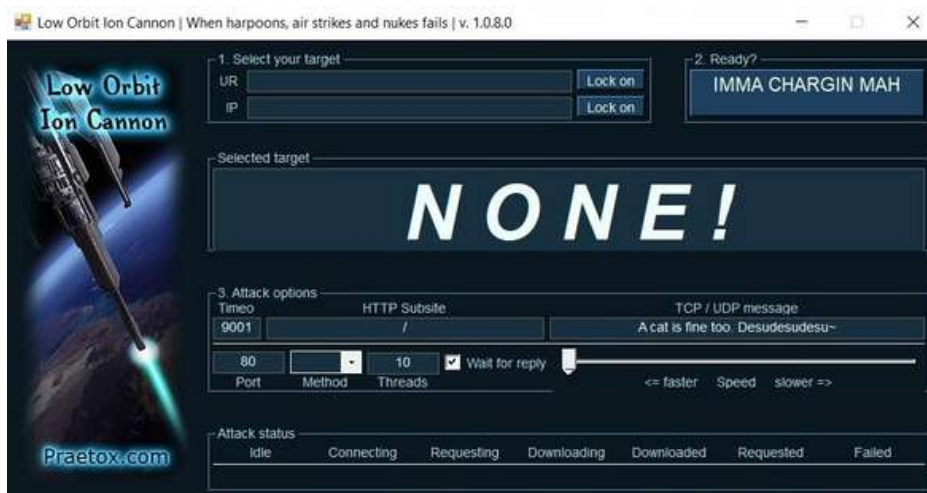
4. NETWORK ATTACKS AND THREATS

In this section, we will dive in to understanding various network security attacks and threats that attacker's use in an attempt to destroy a service, or compromise an organization's assets for various reasons.

4.1 DENIAL OF SERVICE (DOS) ATTACKS

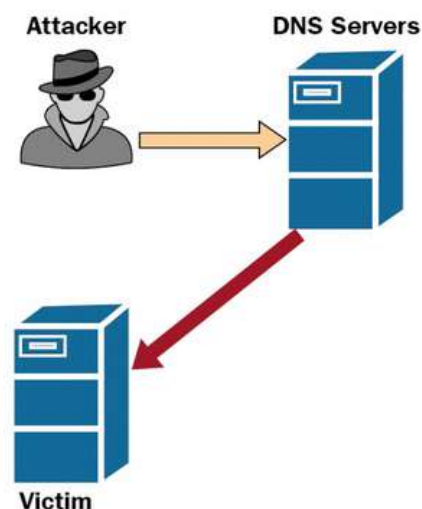
In various places around the world, whenever a government or an organization does something of which citizens or employees don't generally accept, they usually start a protest or a corporate strike. At times, these protests lead to planning an organized strike where the citizens or employees of an organization plan don't show up at their relevant workplace. In digital world, a DoS attack is also applicable. Let's take a look at a simple case study of the famous hacktivist group 'Anonymous'. Just to clarify, hacktivism is the use of computers to promote some sort of political agenda or a social change either locally or internationally. Back in 2003, Anonymous was formed through the famous image board website (<http://www.4chan.org>). During this time, 4chan allowed members to create threads and post without using a particular username. This allowed everyone to post as Anonymous, and therefore a person's identity could be concealed for privacy and anonymity. Some of their attacks involved a network stress test tool, named as Low Orbit Ion Cannon (LOIC).

The tool was used to send a continuous stream of TCP or UDP packets to a single server or website. The recipient, upon having received each packet, will need to process and respond accordingly and eventually, stopping to respond for legitimate requests.



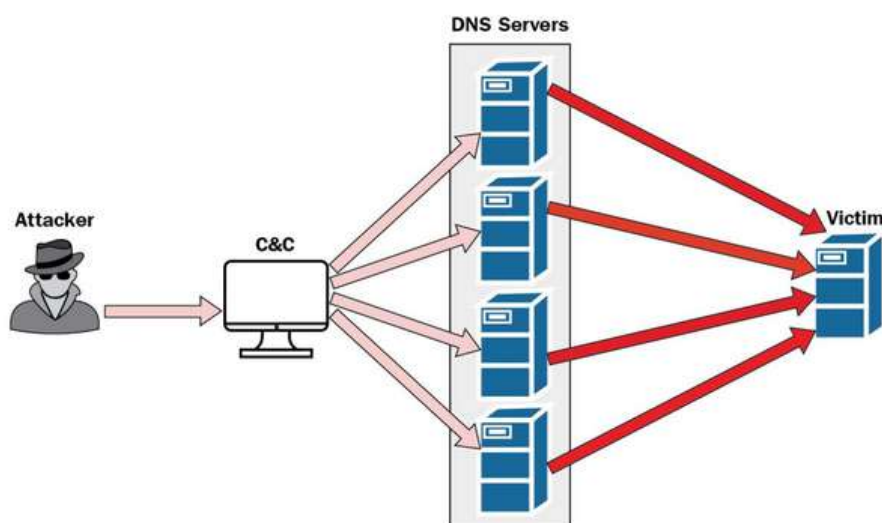
4.1.1 REFLECTIVE:

In a reflective attack, the attacker sends unsolicited requests to a server by using the victim's IP address as the attacker's source IP address. This impersonation process is known as spoofing. When the server receives the request from the attacker, it sends its replies to the source IP address within the IP packets it has received. Therefore, all of the responses will go to the victim's machine and not to the attacker's.



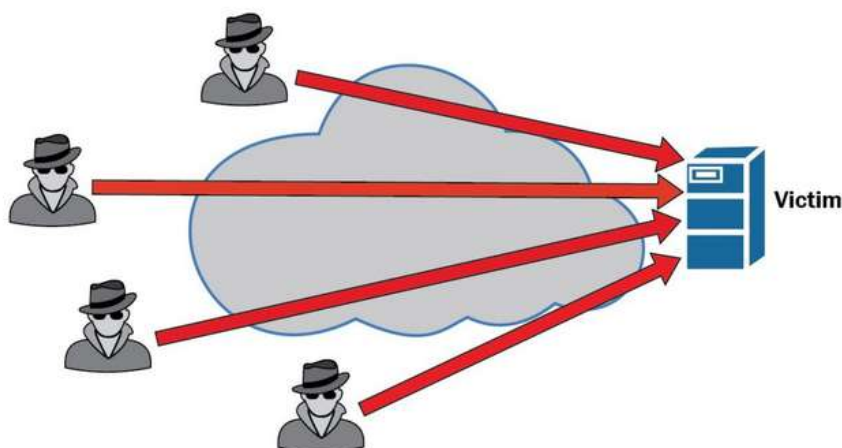
4.1.2 AMPLIFIED:

The amplified attack is similar to the reflective attack. In an amplified attack, the attacker spoofs the IP address of the victim and sends a continuous stream of unsolicited messages (requests) to multiple servers such as DNS servers. When each server processes each packet, they all respond to the victim's machine. The victim's machine will constantly be flooded with messages from various online servers.



4.1.3 DISTRIBUTED:

In a Distributed Denial-of-Service (DDoS) attack, the victim receives a continuous stream of unsolicited messages from multiple sources. This type of attack is similar to the amplified attack. On 1st March 2018, the Hacker News (www.thehackernews.com) reported one of the biggest DDoS attacks to ever take place. This was 1.35 TB humongous, which hit the famous GitHub website (www.github.com).



4.2 SOCIAL ENGINEERING

Social engineering is the art of manipulating or convincing a person to reveal private or confidential information about someone or something. Most of the time, the victim inadvertently provides sensitive information to the attacker.

The following are the phases in which an attacker executes a social engineering attack:

- The attacker performs reconnaissance on the target/potential victim.
- The attacker develops a relationship with the victim (employees). This is used to build trust.
- Finally, the attacker exploits their relationship with the victim.

To prevent social engineering attack, an organization must ensure the following:

- Sufficient training is provided to each employee.
- Presence of appropriate security policies, procedures, and controls in place.
- Existence of regulated access and monitoring of information.

4.3 INSIDER THREAT

In each organization, whether large or small, there is at least one employee who is disgruntled about their current position within the organization. A disgruntled employee is one of the biggest threats to any company, as this person already knows the organization's procedures, systems, and has access to the company's assets such as financial and customer records, confidential information, and so on. A lot of time, whenever an employee leaves a company on bad terms, they usually have the idea of causing the organization some sort of harm upon their resignation or termination.

4.4 LOGIC BOMB

A logic bomb is a type of virus that remains in a dormant state until a particular action is executed on the system it has infected. How can a logic bomb be used in a real-world situation?

Let's imagine a hacker has compromised a server that has very important and confidential data on the local drives. The hacker installs a backdoor and a logic bomb. As I've previously mentioned, a backdoor is a doorway in the operating system that is used to allow a hacker, gain entry into the system. When the hacker has completed his objectives on the compromised system, the last step is to cover their tracks, remove any logs, files, and traces as they would reveal what the hacker has done in the system.



At times, an organization may have an internal incident response team or hire an external team to perform digital forensics on the compromised system to determine what happened and who did the crime. This is where the logic bomb plays its role. During the acquisition phase (obtaining evidence) which is performed by the forensics experts on the live system, the logic bomb may be triggered to unleash its payload, which may wipe the entire hard drive of the Organization and remove any further evidence.

4.5 ROGUE ACCESS POINT (AP)

One of the many popular methods of wireless hacking is setting up a rogue AP. A rogue AP is used by a hacker who uses a wireless router of his/her own, and creates a Service Set Identifier (SSID) or a network name in the hopes of attracting people to connect to it. The name of the SSID would be something that would definitely attract users, such as VIP Access, free Wi-Fi, or even the name of a popular coffee house. The goal is to get people to connect and while they are browsing the internet, the hacker intercepts all their network traffic, looking for any sensitive or confidential information.

A simple mitigation technique is to not connect to any wireless networks that has a suspicious name or something that you don't trust. Sometimes, upon seeing an open wireless network, somebody might think it's a gold mine that has free internet access. However, to a hacker, it's a bait, and their gold mine would be the victim's traffic and data that's intercepted.



4.6 EVIL TWIN

An Evil twin is similar to the rogue access point model, but the evil twin is either a wireless router or an access point that's deployed on a company's network, by a hacker or a malicious user. This method allows the hacker to capture sensitive data while mobile users access the company's network. This little, pocket size device is used by both hackers and penetration testers for auditing wireless networks.



The above device is known as the Wi-Fi Pineapple. Countermeasures for both rogue APs and Evil twin deployments are as follows:

- Conduct regular wireless audits using a Wi-Fi spectrum analyser such as the insider (www.metageek.com), to scan for any suspicious wireless routers in range.
- Train staff in wireless security awareness.

4.7 WAR-DRIVING:

Some of us, upon getting our first Wi-Fi enabled device such as a laptop, would probably have the thought of driving around the neighbourhood, looking for anyone with an open wireless network for free internet access. A hacker would probably attempt to do the same, driving around a community or neighbourhood looking for any open wireless networks, connecting to it and intercepting the traffic, or compromising the network devices with malicious intentions.

Usually, the devices used in a war-driving scenario would be a laptop either preloaded with a penetration testing Linux distribution such as Kali Linux (www.kali.org), and a high-gain wireless antenna, which supports wireless packet injection and monitoring.

The following are some countermeasures for war-driving:

- Ensure that your wireless network is secured by using strong encryption standards.
- Ensure that your password for the wireless network is very strong.
- Do not leave your wireless network open.
- Do not place wireless routers or access points close to the outer perimeter of a compound or a building.

4.8 RANSOMWARE

Hackers usually compromise an online server and inject their malicious codes into the server or files on the server. Then, a regular user (potential victim) accesses the resources on the server or simply visits the website, and the user downloads a malicious file without knowing it is harmful on his system. Apropos of that, the malicious code on the web server attempts to push itself on the potential victim's systems. Regardless of which method is used, once the malicious file executes on the victim's system, it immediately begins to encrypt the entire local drives using a secret key (passphrase or a digital certificate). While this is being done, it attempts to spread across the network. When the system is encrypted with ransomware, it become unusable with a single screen presented to the victim, informing them to pay a ransom. The ransom would be something of monetary value, either asking the victim to provide their credit card details or to pay through some sort of crypto-currency, such as Bitcoin.



Some countermeasures for ransomware are as follows:

- Implement a next generation firewall.
- Implement endpoint security and ensure that virus definitions are up-to-date.
- Implement anti-ransomware protection on end devices.
- Ensure that your systems have the latest patches and updates installed.
- Implement data backup and retention policies. If a victim does not pay the ransom, he can still restore data from a last known good backup.

4.9 DNS POISONING

If a hacker is able to compromise a DNS server and modify the DNS records, an unsuspecting user may visit an incorrect website, even though the host name is accurate. At this point, you may be wondering what the impact and effects of an attacker performing DNS poisoning on an organization or an individual are. For a security incident of this nature to occur, the DNS records of the DNS server used by the victim were compromised and modified, or the DNS Server IP configurations were modified on the victim's computer and were resolving entries on the attacker's DNS server.

There are many records in a DNS server. The following are the most commonly used entries:

Record Type	Description
A	The Address Mapper or the "A" record is used to map a hostname to an IPv4 address
AAAA	The quad A records maps a hostname to an IPv6 address
CNAME	The CNAME is used to create alias for the domain name
MX	The MX records is used to specify the mail exchange servers
NS	The Name Server (NS) records is used to specify the authoritative name server
PTR	The Pointer (PTR) record is used to resolve an IP to a hostname
SOA	The Start of Authority (SOA) record has information stored in the DNS zone and its recorrrds
TXT	The Text (TXT) record contains text string which my used to proof identity on a domain



Using the nslookup command on Windows, you can troubleshoot DNS issues. By simply executing the nslookup command, your current DNS server settings will be presented:

```
C:\>nslookup
Default Server: one.one.one.one
Address: 2606:4700:4700::1111
```

4.10 ARP POISONING

One of the most popular protocols that exists between the Data Link and the Network Layers of the OSI reference model is the Address Resolution Protocol (ARP). ARP mostly operates at the Data Link layer, with its purpose meant to resolve IP address to Media Access Control (MAC) addresses. You may be wondering, why do devices on a network need to resolve IP addresses to MAC addresses?

A switch is a layer 2 device, and is only able to read the layer 2 header of the frame. This part of the frame contains only MAC addresses, and so if devices are using the Internet Protocol (IP) to communicate on a local network, the switches will not be able to read the Network Layer header which contains the IP addresses. Therefore, all communication that occurs on a local network uses layer 2 addressing, instead of using MAC addresses.

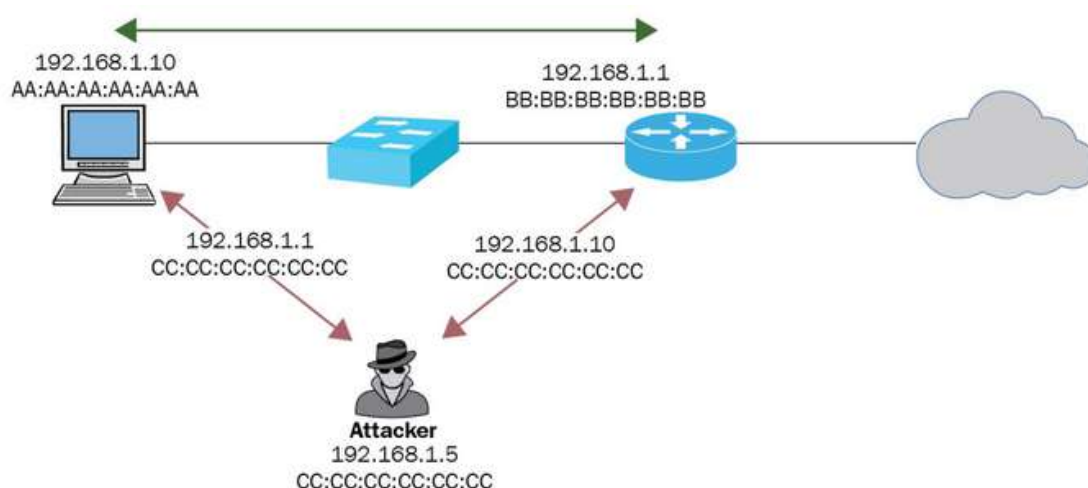
Using the arp -a command on Windows, we can see the current ARP entries of the local device:

```
C:\>arp -a

Interface: 172.16.17.8 --- 0x17
 Internet Address      Physical Address      Type
 172.16.17.6           f0-27-2d-             dynamic
 172.16.17.18          9c-3d-cf-             dynamic
 172.16.17.255         ff-ff-ff-ff-ff-ff     static
 224.0.0.22            01-00-5e-00-00-16     static
 224.0.0.251           01-00-5e-00-00-fb     static
 224.0.0.252           01-00-5e-00-00-fc     static
 239.255.255.250       01-00-5e-7f-ff-fa     static
 255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ARP poisoning is where an attacker sends intentional gratuitous ARP messages to a potential victim's machine, in effect, causing the victim's machine to update the ARP cache.

Let's take a look at the following diagram to get a better understanding of an ARP poisoning attack. Whenever PC1 wants to send traffic out to the internet, it sends BB:BB:BB:BB:BB:BB to its default gateway by using the router's MAC address. The router, in return, will record the PC1 MAC address, AA:AA:AA:AA:AA:AA. Let's imagine that an attacker has joined the network, as shown in the following diagram. The attacker is attempting an ARP cache poisoning attack. The attacker's machine will send a Gratuitous ARP message to PC1, telling it that the default gateway's IP-to-MAC mapping has been updated to 192.168.1.1 – CC:CC:CC:CC:CC:CC.



The effect of this change on PC1 will be that all of the traffic destined outside of the local network and the default gateway will now be sent to the attacker's machine. Furthermore, the attacker will send a Gratuitous ARP message to the router, informing the MAC that the address of 192.168.1.10 has been updated to CC:CC:CC:CC:CC:CC. Therefore, returning traffic for 192.168.1.10 will now be sent to the attacker's machine. This is both an ARP cache poisoning and a Man-In-The-Middle (MITM) attack, as all traffic between PC1 and the router will be passing through the attacker.

4.11 DE-AUTHENTICATION

Whenever we connect to a wireless network using devices like smartphone, laptop, and others, this connection is known as an association between the client and the wireless router/access point. A de-authentication attack focuses on bumping out all of the wireless devices that are connected to a wireless router/access point. From an attacker's point of view, the attacker machine does not need to be connected/associated to the target wireless network, instead of being within range of the wireless signal. The effect of this type of attack is to create a Denial-of-Service (DoS) attack for the clients whom are connected to the wireless network.

4.12 BRUTE FORCE


Let's imagine you're a construction worker who's been hired to break down a wall. Unfortunately, you don't have any heavy machinery equipment to aid in the process, but you have a sledge hammer. You know this won't be enough, because after the first strike at the wall, you haven't done any damage. If you continue striking the wall with the same sledge hammer, you'll eventually notice that the wall begins to crack and shatter. This is the effect of brute force. So, how does a brute force attack work in the digital world? Let's imagine that an attacker is trying to crack a password for a login portal for a victim's web server. Let's take a look at the following login page for the Joomla web framework:

Joomla! Administration Login

Use a valid username and password to gain access to the administrator backend.

[Go to site home page.](#)



User Name	<input type="text"/>
Password	<input type="password"/>
Language	Default <input type="button" value="v"/>
<input type="button" value="Log in"/> 	

If an attacker has figured out the credentials of a user, he can try all of the possible passwords in the Password field on the portal. This is provided that the website administrator has not modified the administrator in any way. This would mean that the attacker machine will slam in all password possibilities until the correct password is found. A brute force attack is always or mostly successful. However, the downside is that the time it takes to crack the system is very long.

5. TCP/IP SECURITY

In early days, during the creation of protocols and TCP/IP, security wasn't a huge concern. Cyber criminals and cyber terrorists weren't even a thing to be petrified, and the term hacker referred to a person who was a computer wizard and not what is known for today. As time passes and the technology evolves, there are more cyber threats each day.

The former CEO of Cisco Systems once said the following: **"There are two types of companies: those that have been hacked, and those who don't know they have been hacked."**

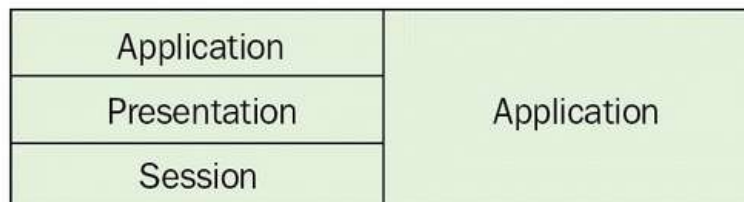
5.1 VULNERABILITIES ON EACH LAYER OF TCP/IP STACK

- Vulnerabilities at the Application Layer
- Vulnerabilities at the Transport Layer
- Vulnerabilities at the Internet Layer
- Vulnerabilities at the Network Access/Link Layer.



5.1.1 VULNERABILITIES AT THE APPLICATION LAYER

The Application Layer of the TCP/IP stack consists of the Application, Presentation, and Session Layers of the OSI reference model. As we've learned before, whenever a computer wants to send traffic (datagrams) to the network, the creation of the Protocol Data Units (PDUs) begins at the top of the TCP/IP stack, the Application Layer:



The following are some of the application layer protocols which we must give intense close attention to on our network:

- File Transfer Protocol (FTP)
- Telnet
- Secure Shell (SSH)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Hypertext Transfer Protocol (HTTP)

Each of these protocols was designed to provide the function it was built to do, and with a lesser focus on security. Malicious users and hackers are able to compromise both the application that utilizes these protocols and the network protocols themselves. Here is the list of major problems that occurs in Application Layer:

PROBLEMS

- Cross Site Scripting (XSS)
- SQL injection (SQLi)
- Lightweight Directory Access Protocol (LDAP) injection
- Cross-Site Request Forgery (CSRF)
- Session hijacking
- Cookie poisoning

DNS

- Distributed Denial-of-Service (DDoS)
- Registrar hijacking
- Cache poisoning
- Typosquatting / URL Hijacking

5.1.2 VULNERABILITIES AT THE TRANSPORT LAYER:

FINGERPRINTING

Fingerprinting isn't always used by hackers or those with malicious intent. This technique is also used by system/network administrators, network security engineers, and cyber security professionals alike. Imagine you're a network administrator assigned to secure a server; apart from applying system hardening techniques such as patching and configuring access controls, you would also need to check for any open ports that are not being used. Each network protocol running at the Application Layer of the TCP/IP stack binds itself with a logical port within the operating system to accept incoming traffic.

Let's take a look at a more practical approach to fingerprinting in the computing world. We have a target machine, 10.10.10.100, on our network. As a hacker or a network security professional, we would like to know which TCP and UDP ports are open, the services that use the open ports, and the service daemon running on the target system. In the following screenshot, we've used n-map to help in discovering the information we are seeking. The n-map tool delivers specially crafted probes to a target machine:

```
root@kali:~# nmap -sV 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-09 15:33 EST
Nmap scan report for 10.10.10.100
Host is up (0.00026s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

ENUMERATION

In a cyberattack, the hacker uses enumeration techniques to extract information about the target system or network. This information will aid the attacker in identifying system attack points. The following are the various network services and ports that stands out for a hacker:

- Port 53 : DNS zone transfer and DNS enumeration
- Port 135 : Microsoft RPC Endpoint Mapper
- Port 25 : Simple Mail Transfer Protocol (SMTP)

DNS ENUMERATION

DNS enumeration is where an attacker is attempting to determine whether there are other servers or devices that carry the domain name of an organization. Let's take a look at how DNS enumeration works. Imagine we are trying to find out all the publicly available servers that Google has on the internet. Using the host utility in Linux and specifying a host name, host www.google.com, we can see the IP address 172.217.6.196, has been resolved successfully. This means there's a device with a host name of www.google.com active. Furthermore, if we attempt to resolve the host name, gmail.google.com, another IP address is presented but when we attempt to resolve mx.google.com , no IP address is given. This is an indication that there isn't an active device with the mx.google.com host name as shown below:

```
root@kali:~# host www.google.com
www.google.com has address 172.217.6.196
www.google.com has IPv6 address 2607:f8b0:4006:800::2004
root@kali:~# host gmail.google.com
gmail.google.com is an alias for www3.l.google.com.
www3.l.google.com has address 172.217.7.14
www3.l.google.com has IPv6 address 2607:f8b0:4006:819::200e
root@kali:~# host mx.google.com
Host mx.google.com not found: 3(NXDOMAIN)
```

DNS ZONE TRANSFER

DNS zone transfer allows the copying of the master file from a DNS server to another DNS server. There are times when administrators do not configure the security settings on their DNS server properly, which allows an attacker to retrieve the master file containing a list of the names and addresses of a corporate network.

MICROSOFT RPC ENDPOINT MAPPER

Not too long ago, CVE-2015-2370 was recorded on the CVE database at <https://cve.mitre.org>. This vulnerability took advantage of the authentication implementation of the Remote Procedure Call (RPC) protocol in various versions of the Microsoft Windows platform, both in desktops and server operating systems. A successful exploit would allow an attacker to gain local privileges on a vulnerable system.

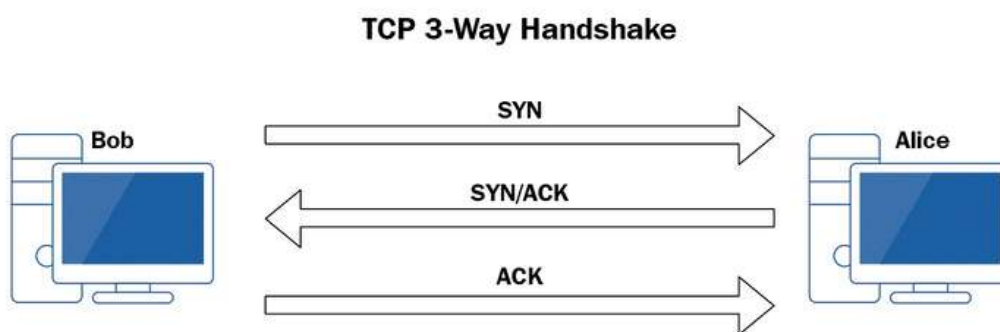
SMTP

SMTP is used in mail servers, as with the POP and the Internet Message Access Protocol (IMAP). SMTP is used for sending mail, while POP and IMAP are used to retrieve mail from an email server. SMTP supports various commands, such as EXPN and VRFY. The EXPN command can be used to verify whether a particular mailbox exists on a local system, while the VRFY commands can be used to validate a username on a mail server. An attacker can establish a connection between the attacker's machine and the mail server on port 25. Once a successful connection has been established, the server will send a banner back to the attacker's machine displaying the server name and the status of the port (open). Once this occurs, the attacker can then use the VRFY command followed by a user name to check for a valid user on the mail system using the VRFY bob syntax.

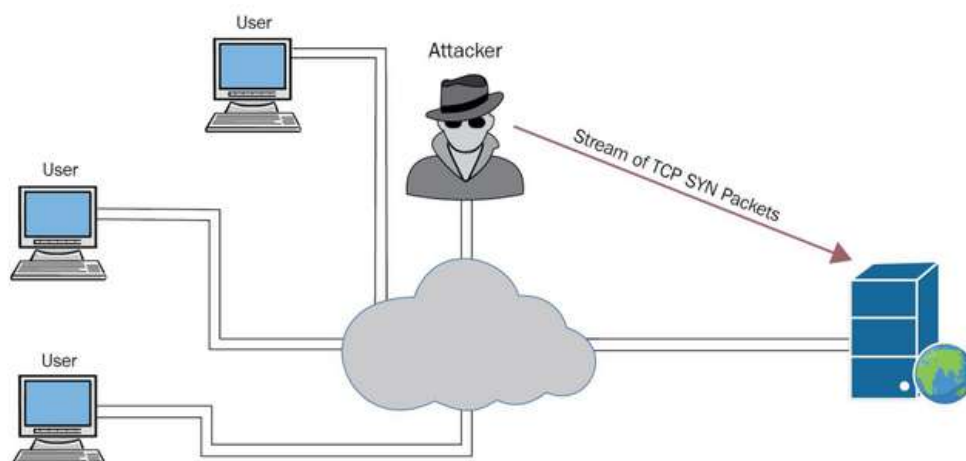


SYN FLOODING

One of the protocols that exist at the Transport Layer is TCP. TCP is used to establish a connection-oriented session between two devices that want to communicate or exchange data. Let's recall how TCP works. There are two devices that want to exchange some messages, Bob and Alice. Bob sends a TCP Synchronization (SYN) packet to Alice, and Alice responds to Bob with a TCP Synchronization/Acknowledgment (SYN/ACK) packet. Finally, Bob replies with a TCP Acknowledgement (ACK) packet. The following diagram shows the TCP 3-Way Handshake mechanism:



For every TCP SYN packet received on a device, a TCP ACK packet must be sent back in response. One type of attack that takes advantage of this design flaw in TCP is known as a SYN Flood attack. In a SYN Flood attack, the attacker sends a continuous stream of TCP SYN packets to a target system. This would cause the target machine to process each individual packet and respond accordingly. Eventually, with the high influx of TCP SYN packets, the target system will become too overwhelmed and stops responding to any requests.



5.1.3 VULNERABILITIES AT THE INTERNET LAYER

The Internet Layer (TCP/IP stack) and the Network Layer (OSI model) are the places where the Internet Protocol (IP) resides. The Internet Layer and the Network Layer are responsible for IPv4 and IPv6 addressing, and routing IP packets. Various routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System-Intermediate System (IS-IS), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP) operates here. There are many weaknesses/flaws which an attacker can leverage by simply exploiting the design of the Internet Protocol (IP).

ROUTE SPOOFING

Route spoofing is where an attacker attempts to inject fake routes into the routing table of a device. The routing table is used as a forwarding database for a local device such as a computer, multiple layer switch, router, or firewall to determine a path for sending traffic to a specific destination. If an attacker has successfully injected spoofed/fake routes into a target device, this will cause the victim's machine to re-route its outgoing network traffic to another path, which may allow the attacker to intercept it.

On a Windows system, to view the routing table, simply use the route command in Command Prompt:

IPv4 Route Table					
=====					
Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	172.16.17.18	172.16.17.8	35
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
	172.16.17.0	255.255.255.0	On-link	172.16.17.8	291
	172.16.17.8	255.255.255.255	On-link	172.16.17.8	291
	172.16.17.255	255.255.255.255	On-link	172.16.17.8	291
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
	224.0.0.0	240.0.0.0	On-link	172.16.17.8	291
	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
	255.255.255.255	255.255.255.255	On-link	172.16.17.8	291
=====					

To view the routing table of a Cisco IOS router, you can use the “show ip route” command, as shown in the following screenshot:

However, it is recommended to ensure route authentication is turned on between routers that are participating in RIP, EIGRP, OSPF, and BGP routing. It is a good practice to ensure only authenticated routing information is exchanged between peer routers on a network.

```
R1:TT#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/1
L       192.168.2.1/32 is directly connected, GigabitEthernet0/1
```

IP ADDRESS SPOOFING

An IP spoofing attack is where an attacker modifies the source IP address of traffic originating from his machine. The purpose of this attack is to mask the attacker's identity and make the attack seem to originate from another source, or to cause a reflective attack.

Both IPv4 and IPv6 are vulnerable to IP spoofing attacks, and the protocols that use the IP are:

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

ICMP is a very useful protocol that helps network professionals to determine whether there are any issues in a network segment and their possible causes. Even though one of the main functions of this protocol is to aid systems and networking professionals in their troubleshooting and diagnostics when checking connectivity on a network, this protocol can also be used for malicious activities by an attacker like:

- DoS vulnerability in ICMP
- Smurf attack
- Teardrop attack
- Ping of Death (PoD)

DOS VULNERABILITY IN ICMP

In 2004, a DoS security vulnerability was published by the National Vulnerability Database (<https://nvd.nist.gov>) with the ID CVE-2004-1060. This recorded security vulnerability allowed an attacker to cause a reduction in network performance by sending unsolicited and fake ICMP packets with a low next-hop Maximum Transmission Unit (MTU) value.

SMURF ATTACK

A Smurf attack is a form of DDoS attack that takes advantage of the ICMP. In a Smurf attack, the attacker sends a continuous stream of ICMP messages to an IP network using an IP broadcast address as the destination, while spoofing the IP address of the potential victim's machine as the source IP address. Therefore, each device that receives an ICMP message from the attacker with the spoofed IP address will attempt to respond. If there are a lot of devices on the broadcast network, they all will be replying to the spoofed packets. This will result in a DDoS attack on the victim.

TEARDROP ATTACK

A Teardrop attack is another type of DoS attack. It leverages the design flaw in the TCP/IP fragmentation reassembly process. In a teardrop attack, the attacker sends fragments of packets to a potential victim. As noted on older operating systems such as Windows 3.1 x, Windows 95, Windows NT, and versions of the Linux kernel 2.1.63, the receiving machine cannot reassemble the packets due to a bug in TCP/IP fragmentation reassembly. Since the receiving system cannot reassemble the packet, the packets will eventually begin to overlap each other. The host operating system will not be able to handle this type of fragmentation, and it will crash.



PING OF DEATH (POD)

In a PoD attack, the attacker sends a specially crafted ping packet greater than 65,536 bytes to a victim machine. Since TCP/IP supports fragmentation of packets across a network, a malicious user is able to take advantage of this feature by breaking down a packet of 65536 or more bytes into smaller pieces. This would allow the attacker to send these smaller pieces to a victim. When the victim's machine reassembles the pieces, many operating systems won't know how to process this large packet and will either freeze, reboot, or crash. This is another form of DoS attack.

5.1.4 VULNERABILITIES AT THE NETWORK ACCESS/LINK LAYER

The Data Link Layer (layer 2) is responsible for error checking, reassembly of frames, delivery of frames, Media Access Control (MAC) addressing, flow control of frames as they are sent and received on the network. The Physical Layer (layer 1) is responsible for the electrical and mechanical functions and for delivering the bits from one device to another. As the name suggests, the Physical Layer is the physical media used for transmission of the bits, such as the cables, hubs, radio frequency, and so on.

We will group the vulnerabilities under the Data Link and the Physical Layers of the OSI reference model.

OSI Model	TCP/IP Stack
Data Link	Network Access/Link
Physical	

DATA LINK LAYER

Here, we will be discussing about the vulnerabilities that affects the Data Link Layer:

- Address Resolution Protocol (ARP) poisoning
- Sniffing
- Broadcast storms
- VLAN hopping

ARP POISONING

The ARP was designed to resolve IP address to MAC address on a network. All devices on a Local Area Network (LAN) use MAC addresses for communication between one device and another. However, there are times when a device has only the IP address of its destination. In this situation, the sender device would send an ARP request out on the LAN and if a device has the IP address contained in the ARP request message, it responds with its MAC address. The IP is now bound to the MAC address in the local ARP cache of the sender.

An attacker may attempt to modify the ARP cache of a victim's machine by sending a Gratuitous ARP with an update containing a change to the MAC address of an existing entry within the victim's ARP cache. If the change is successful on the victim's machine, any traffic destined for the IP address will now be sent to the device that has the new MAC address specified in the Gratuitous ARP message. This would allow the attacker to either intercept traffic or re-route the victim's traffic on the network.

SNIFFING

Sniffing is the monitoring of data packets as they pass through the network or between devices. A Sniffer is usually a software/application that has the ability to present raw network traffic as human-readable information for analysis. Sniffers are used by both, good and the bad guys. The good guys, such as network engineers, use a sniffer to help in determining problems on a network. A security engineer would use a sniffer to monitor network traffic for any type of security intrusion, such as malware traversing the network. However, an attacker would use a sniffer to determine the types of services that are being used on a victim's network and to find any confidential or sensitive information passing across the network.



BROADCAST STORMS

A broadcast storm is an extremely concentrated amount of broadcast traffic being flooded either by one or multiple devices on a network. Each device on a network receives a broadcast message and processes it accordingly. Imagine there are hundreds of people within a single room (network) and everyone is shouting at another person (broadcasting), but no one in the room will be able to process and communicate properly as there would be a lot to process and noise. This is how a broadcast storm works on a network. Eventually, after a few minutes, the network's performance will degrade gradually and it may eventually become crippled.

VLAN HOPPING

VLAN hopping allows an attacker to access the network resources and traffic of other VLAN's that are normally inaccessible. VLAN hopping attacks occur on switches with their physical ports configured to convert into a trunk port automatically. A trunk allows multiple VLAN traffic to pass across simultaneously. The Cisco Dynamic Trunking Protocol (DTP) is susceptible to VLAN hopping attacks. The attacker can establish a physical connection to a switch and inject specially crafted IEEE 802.1Q frames into the switch port. If auto-trunking is enabled, the port will be converted into a trunk. This would then allow the attacker to access all VLANs on the network.

PHYSICAL LAYER

Here, we will outline and discuss various vulnerabilities at the physical layer.

WIRETAPPING

Wiretapping is a type of sniffing that involves the monitoring of a telephone system and internet conversations. This allows an attacker to actively or passively monitor, intercept, and record any conversations on the wire.

Wiretapping is done by placing a physical component inline, on the telephone wire or the network cable.

OTHER PHYSICAL ISSUES

The other physical issues are as follows:

CABLE CUTTING

The cutting of network cables can definitely cause a network outage, which will result in a physical form of DoS for legitimate users on a network.

POWER INSTABILITIES

Power outages are a critical concern for daily operations of businesses. If a device's power supply blows out, the device will be down until the power supply is replaced. If the building loses power, all components will lose power. However, a lot of companies invest in Uninterruptible Power Supply (UPS) for their core and mission critical network appliances and servers. A UPS can supply power to a component for a very short period of time. Therefore, a backup generator is recommended to counteract a power outage in a building or compound. Another type of power instability is an electrical surge, which can short out or blow electrical components. Using a power surge protector or an automatic voltage regulator (AVR), we can protect network appliances from such abnormal spikes in electrical current.

6. SECURING NETWORKING DEVICES

As an upcoming network professional, it is very important to understand how to secure and mitigate these threats and vulnerabilities on a network infrastructure. In this section, we are going to take a look at applying some simple and effective controls on a system and network to assist in preventing and mitigating these security threats.



6.1 CHANGING DEFAULT CREDENTIALS

Whether you have purchased a computer or a network appliance, these devices have default accounts that allow the owner to log in to the administrator or root account. In some cases, users do not change or disable the default accounts or passwords that have been implemented, which is usually classed as a security vulnerability on a network. Failing to change the default configurations on a device could lead to a security breach on the network, and the complexity of the attack would be simple for either guessing the password, or checking the manufacturer's website for default account and password information.

6.2 AVOIDING COMMON PASSWORDS

In 2014, we had the privilege of looking at a router's configuration files after a cyberattack had occurred at a reputable organization in the region. The attack is known as toll-fraud, which results in a company's telephone bill being extremely high due to unaccountable international calls. After reviewing the configurations of the compromised router, it seemed that the person who had made the configurations or set the device password, actually used a very common and a guessable password.

This was a clear indication that the attacker didn't have the need to perform any sort of complex attack or password cracking techniques, but simply just needed to guess the password based on the manufacturer of the device. As a result of not having a proper password policy and applying basic security practices, the organization had to spend thousands of dollars remediating any damage that was done within their network and the high cost of the telephone bill. This is the result of setting common passwords on devices.



6.3 DEVICE HARDENING

Firmware is a piece of software that is permanently programmed into the Read-Only Memory of an electronic component. It's quite important to update/upgrade the firmware on a system since an updated version will contain fixes for any bugs within the program and security issues, and will implement newer features from the vendor. Firmware updates can be found on the device manufacturer's website.

Installing device updates, patches, hotfix, and service packs on an operating system will assist in minimizing the attack surface and reduce the threat landscape within an organization. These updates are frequently released by software companies as a continuous service to ensure that any bugs and security issues are resolved as quickly as possible.

Device hardening is not only focused on installing updates, but also on applying baseline policies across all systems and devices within the organization. This ensures that the minimum security standards are applied to everyone and each device aids in minimizing security threats and risk.

6.4 DISABLING UNNECESSARY SERVICES

As learnt in previous chapters, whenever there are services running on an operating system, there are logical network ports assigned to each unique service. Having unnecessary services active on a system poses a security vulnerability on the device. From an attacker's point of view, each open port on a system is a doorway into the operating system. Leaving a doorway open in reality can be an invitation for an intruder.

6.5 DISABLING PHYSICAL PORTS

We've been talking about logical ports a lot thus far, but we must not forget about disabling any unused physical ports on a device either. Leaving physical ports active can allow a malicious user or hacker to access physically connected specialized devices to a network for creating physical backdoor access.



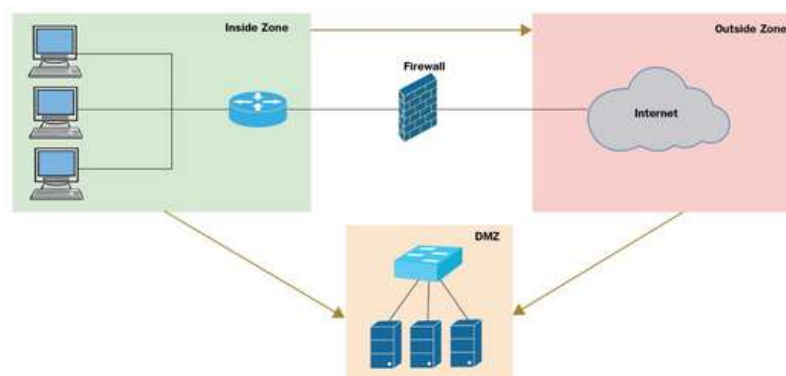
7. MITIGATION TECHNIQUES

Let's talk about the various mitigation techniques that are used for security threats on a network infrastructure a little bit more.

7.1 NETWORK SEGMENTATION - DEMILITARIZED ZONE

Most organizations have servers that are accessible by users of the public internet. Some of these servers are web servers and email servers. It's definitely not recommended to allow any traffic originating from the internet to access your internal, private network. Creating a DMZ to place these publicly accessible servers is highly recommended.

The DMZ is a semi-trusted segment of the company's network that allows users from the internet limited access to devices in this area, which is why it's the best possible location to place the publicly accessible servers on the organization's network.



7.2 NETWORK SEGMENTATION - VLANS

As an upcoming networking professional, leaving all ports on the same VLAN will result in a logical flat network without any segmentation. This would lead to unnecessary broadcast messages, which will reduce the network's performance and increase the risk of a network security incident.

VLANs on a physical network will assist in improving the security posture of the network. Let's imagine that each department within an organization is on a unique VLAN. If an intruder plugs his attacker machine into a switch port, only that logical segment may be compromised until the attacker finds a way to perform VLAN Hopping.

Having multiple VLANs also allows Access Control Lists (ACLs) to be implemented on the routers that handle the inter-VLAN routing of traffic. The ACLs can be used to either permit or deny traffic originating from one VLAN to another.

7.3 SPANNING TREE PROTOCOL (STP) THREAT MITIGATION TECHNIQUES

STP threat mitigation techniques are as follows:

7.3.1 BRIDGE PROTOCOL DATA UNIT (BPDU) GUARD

BPDU guard is used to prevent BPDUs from entering a switch port. These features are recommended, if the switch is using 'Portfast' on a particular interface. It assists in preventing a hacker from injecting malicious BPDU messages into the switch in the hopes of adjusting the root bridge to the attacker's machines and manipulating layer 2 traffic.

7.3.2 ROOT GUARD

The root guard is placed at the local interfaces of both the root bridge and the secondary root bridge that connects to other switches except themselves. The root guard's features is used to enforce the placement of root bridges on a network.

7.4 MITIGATING SECURITY THREATS

To secure an organization's network, one must first identify the assets of the company. Assets can be categorized into the following:

- Tangible
- Intangible
- Employees

7.4.1 IMPLEMENT A NEXT-GENERATION FIREWALL

- Built-in Intrusion Prevention System (IPS)
- Virtual Private Network (VPN) capabilities
- Botnet filtering
- APT filtering
- Prevent zero-day breakouts
- Deep packet inspection
- Malware and ransomware prevention

7.4.2 IMPLEMENT AN IPS

Another type of security appliance is an IPS. An IPS has the ability to detect and block attackers and other anomalies that other security appliances cannot find. Within an IPS, there are rules that govern how the appliance monitors and filters network traffic, and these rules can be customized by a security engineer to detect and stop certain activities that are of interest to a single organization. Since an IPS is usually placed behind a firewall, it blocks malicious traffic that were missed by the firewall appliance.

7.4.3 IMPLEMENT WEB SECURITY APPLIANCE (WSA)

Protecting our users also means providing web security for both outgoing and incoming traffic. A WSA is a web content security appliance that has the ability to mitigate threats, handle content filtering, and allows secure access to the web. When a user enters a URL in their web browser, data is sent to the WSA for further analysis and validation of the data, leaving the organization and the intended website/server. If the web traffic or website is harmful, the WSA will prevent the malicious traffic from entering the organization's network and restrict access to the malicious website/server.



7.4.4 IMPLEMENTING EMAIL SECURITY APPLIANCE

There are many types of threats for which attacker use email as their delivery platform. These threats are as follows:

- Spam
- Malware
- Phishing
- Spear-phishing

Using an Email Security Appliance will process both incoming and outgoing emails from an organization to help stop cyberattacks that are delivered by email messaging. The incoming emails go through various processing and analysis stages, such as anti-spam filtering, antiviruses for virus detection, content filtering, and so on. The outgoing emails go through a very similar process to prevent any internally compromised systems within the organization from spreading malware or distributing any sort of threat.

7.4.5 IMPLEMENT LAYER 2 SECURITY ON SWITCHES

Securing layer 2, the switch network, is a very important aspect when implementing network security. Many people I've encountered within the IT industry from IT techs to managers, haven't realized the importance of securing a network using a layered approach, such as DiD. Having a next-generation firewall isn't going to stop all threats. What about preventing an insider threat, which a lot of us forget about? Over 90% of cyber-attacks happen from the inside, within a network, rather than originating from the internet.

The following are recommended as some of the best network security practices:

- Applying port security on a switch's port will prevent a Content Addressable Memory (CAM) table overflow. CAM table has been mentioned in Chapter 3 Ethernet.
- Block all switch port negotiations to prevent an attacker from performing a VLAN hopping attack.
- Remove all ports from VLAN 1 and do not use VLAN 1 for anything.
- Implement DHCP snooping on the switches to prevent a malicious user or attacker from installing a rogue DHCP server on the network.

- Implement BPDU guard to prevent an attacker from injecting specially crafted BPDU messages into a switch port to become the role of a root bridge.
- Implement Dynamic ARP Inspection (DAI) to prevent ARP spoofing on the layer 2 network.

7.4.6 IMPLEMENT VIRTUAL PRIVATE NETWORKS (VPNS)

Implementing a VPN can help in protecting the data in motion, as it transits from one location to another. This will aid in preventing anyone who is attempting to eavesdrop on the network. A VPN allows secure access to a corporate network for members of staff who are traveling, working out in the field, or even working remotely.

7.4.7 OTHER IMPORTANT SECURITY CHECKS

The other important security checks are as follows:

- Implement an Authentication, Authorization, and Accounting (AAA) server for user management on network and security appliances. AAA is used for central management of user accounts, privileges, policies, and log management in a single unified system.
- Train and educate employees to have a better understanding of cyber security.
- Install the latest updates to fix any bugs and security flaws in the software on a system.
- Keep regular backups of data in the event of a ransomware attack or system crash.
- Disable any unnecessary services on appliances and systems.
- Encrypt and apply passwords on sensitive data.
- Perform regular vulnerability assessments on the network infrastructure to determine risk rating and mitigation.
- Perform penetration testing regularly, both announced and unannounced, to find any hidden vulnerabilities on a system and network before a real attacker discovers and takes advantage of them.



8. TROUBLESHOOTING A NETWORK

In order to illustrate the entire network troubleshooting methodology, we will examine common hardware and software tools that are utilized to gather data on issues, and also discuss some everyday problems that plague both wired and wireless networks. Finally, we will explore a number of typical network service issues that are prevalent across many networks. This phase will aid you in connecting the concepts to the real-life issues you'll face in administering a network, allowing you to quickly and confidently diagnose and resolve many of these issues.

8.1 HARDWARE-BASED TROUBLESHOOTING TOOLS

- Crimper
- Punchdown tools
- Tone and probe tool
- Loopback adapter
- Multimeter

8.2 SOFTWARE-BASED TROUBLESHOOTING TOOLS

- packet sniffer
- port scanner
- Wi-Fi analyzer
- arp tool
- ping tool
- tracert tool
- nslookup tool
- ipconfig tool
- iptables
- route tool
- netstat tool
- Network Mapper (Nmap) tool



8.3 COMMON ISSUES ON WIRED AND WIRELESS NETWORKS

Common issues on wired networks

- Link lights/status indicators
- Damaged cables and connectors
- Incorrect TX/RX alignment
- Crosstalk and EMI
- Bad ports/transceivers



COMMON ISSUES ON WIRED AND WIRELESS NETWORKS

- Physical layer issues
- Antenna issues
- Signal power issues
- Interference
- Client configuration issues

8.4 COMMON NETWORK SERVICE ISSUES

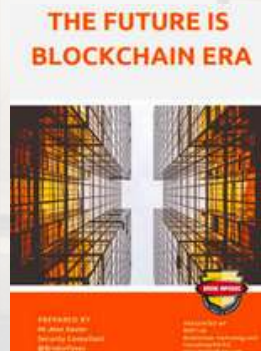
- IP address duplication
- MAC address duplication
- Incorrect gateway and netmask
- Incorrect DNS/NTP servers
- Expired IP address
- Untrusted SSL certificate
- Incorrect network or host firewall settings.

9. CONCLUSION

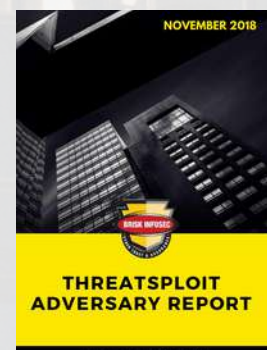
Whether you're a seasoned network engineer, an IT technician, an enthusiast, or simply starting your studies in networking, security threats and attacks exist everywhere. No network infrastructure exists that's fully secure because each minute, hour, or day, a new cyberthreat emerges. If your network isn't protected, it's a gold mine for hackers to steal assets of immeasurable value. So, securing it is obviously mandatory. To do this, reaching out to a successful cybersecurity organization is the sanest choice.

We have been listed as one among the “Top 20 Most Promising Cyber Security Provider.” We have also set the “India Book of Records for identifying most number of vulnerabilities”. Last but not the least, we are a CERT Contact us to gain in-depth insight on Cybersecurity.

YOU MAY BE INTERESTED ON OUR PREVIOUS WHITEPAPER



YOU MAY BE INTERESTED ON OUR PREVIOUS WORKS



REFERENCES ABOUT BRISKINFOSEC



CASE STUDIES



SOLUTIONS



SERVICES



RESEARCH



COMPLIANCES



BLOGS



This White Paper is proudly presented by

BRISKINFOSEC TECHNOLOGY AND CONSULTING PVT LTD

Feel free to reach us for all your cybersecurity needs
contact@briskinfosec.com | www.briskinfosec.com

|USA|INDIA|UK