Security at Network Layers

Title	Page Number
1. **Introduction**	3
2. **Layer 1: Cabling and Hubs**	4
2.1. Cabling Security Issues	4
2.2. Hubs Security Issues	5
3. **Network Sniffers**	6
3.1. Detecting Sniffer	7
3.2. Sniffing Legitimately	7
3.3. Sniffer Safeguards	7
4. **Layer 2: Switches**	8
4.1. Address Resolution Protocol (ARP)	9
4.2. Sniffer in Switch Environment	10
4.3. ARP Vulnerability	10
4.4. Mac Flooding	13
4.5. Switch Safeguards	14
5. **Layer 3: Routers**	14
5.1. IP Spoofing	15
5.2. Reflected Denial of Service Attack (DoS)	16
5.3. IP Spoofing Safeguard	16
5.4. Routing Information Threats	17
6. **Layer 4: TCP, UDP, ICMP Issues**	17
6.1. SYN Flooding Attack	18
6.2. TCP Denial of Service + IP Spoofing	19
6.3. UDP Flooding Attack	21
6.4. The Internet Control Message Protocol (ICMP)	22
6.5. ICMP Security Vulnerabilities	23
6.6. Securing Against Denial of Service Attacks	24
7. **Exercises**	26
8. **References**	31

Learning Objective

After studying this chapter, you should be able to:

- Understand the different components that are likely to be found in a network.
- Study the major network protocols (focussing on TCP/IP networks).
- Develop an awareness of the inherent security risks of using these components and protocols.
- Study a few ‘classic’ attacks on networks: ARP spoofing, TCP Denial of Service, network sniffing.

1.Introduction

Network infrastructure devices are the components of a network that transport communications needed for data, applications, services, and multi-media. These devices include cables, hubs, switches, routers, firewalls, servers, load-balancers, intrusion detection systems, domain name systems, and storage area networks. These devices are ideal targets for malicious cyber actors because most or all organizational and customer traffic must pass through them.

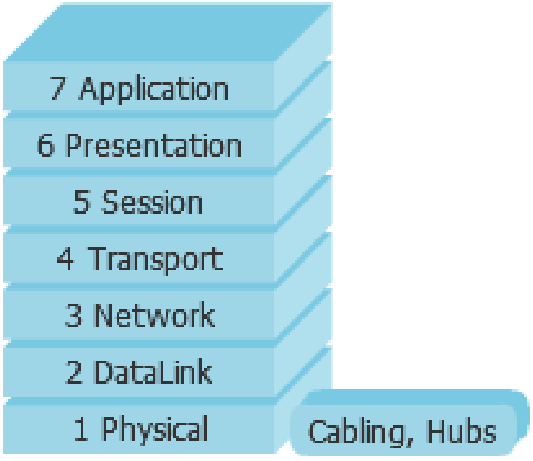
In this chapter, we take a layer-by-layer look at the most important network components and protocols, and associated security issues:

- Cabling and Hubs (Layer 1), Sniffers
- Switches and MAC (Layer 2)
- Routers and IP (Layer 3)
- TCP, UDP and ICMP (Layer 4)

2.Layer 1: Cabling and Hubs

Network cables are used to connect and transfer data and information between computers, routers, switches and storage area networks. These cables are essentially the carrier or media through which data flows. There are different types of communications cables, and the appropriate type to use will depend on the structure and topology of the overall architecture of the system. These cables are ideal targets for malicious cyber actors because most or all organizational and customer traffic must pass through them.

Hub interconnects all devices connected to it, retransmitting every received message to each port (except of the port the message was received on). In this way everyone, gets a copy of all the traffic transmitted over a hub. However, there is a limitation to it, due to the nature of the hub, which can carry only one signal at a time. Therefore, devices connected to a hub cannot receive and transmit at the same time.



Figure(2.1): Hubs and Cabling in OSI Protocol Stack

2.1.Cabling Security Issues

All four fundamental threats can be realized by attacks on cabling:

- Information Leakage: attacker taps cabling and reads traffic, any intrusion into network cables may threaten your information systems and hence the confidentiality of your information.
- Integrity Violation: attacker taps and injects traffic, or traffic corrupted in transit.

- Denial of Service: Cables may be damaged with a resultant reduction in reliability and / or the loss of your network.
- Illegitimate Use: attacker taps cabling and uses network resources.

Some contributory factors in assessing risk:

- Single or multi-occupancy building?
- How is access controlled to floor/building?
- Does network cabling pass through public areas?
- Is the network infrastructure easily accessible or is it shared?
- What is the electromagnetic environment like?
- Is there any wireless connection in your network infrastructure?

Safeguards:

- Consider separating the network wiring from all other wiring, so as to protect and monitor it more easily, and to reduce the danger of accidental electronic interference.
- Where rodent damage is possible, consider installing armored cable.
- For very high-security situations, consider laying the cable in transparent conduit, thereby allowing ready identification of any interference.
- Ensure that all devices such as data scopes, that may facilitate tapping of communications lines, are controlled effectively.
- Ensure that network access points are disabled if equipment is removed.
- Ensure that the incoming and outgoing services, including communications lines, are hidden from view and are adequately protected against damage.
- Ensure applying the security policy of wireless connections.

2.2.Hubs Security Issues

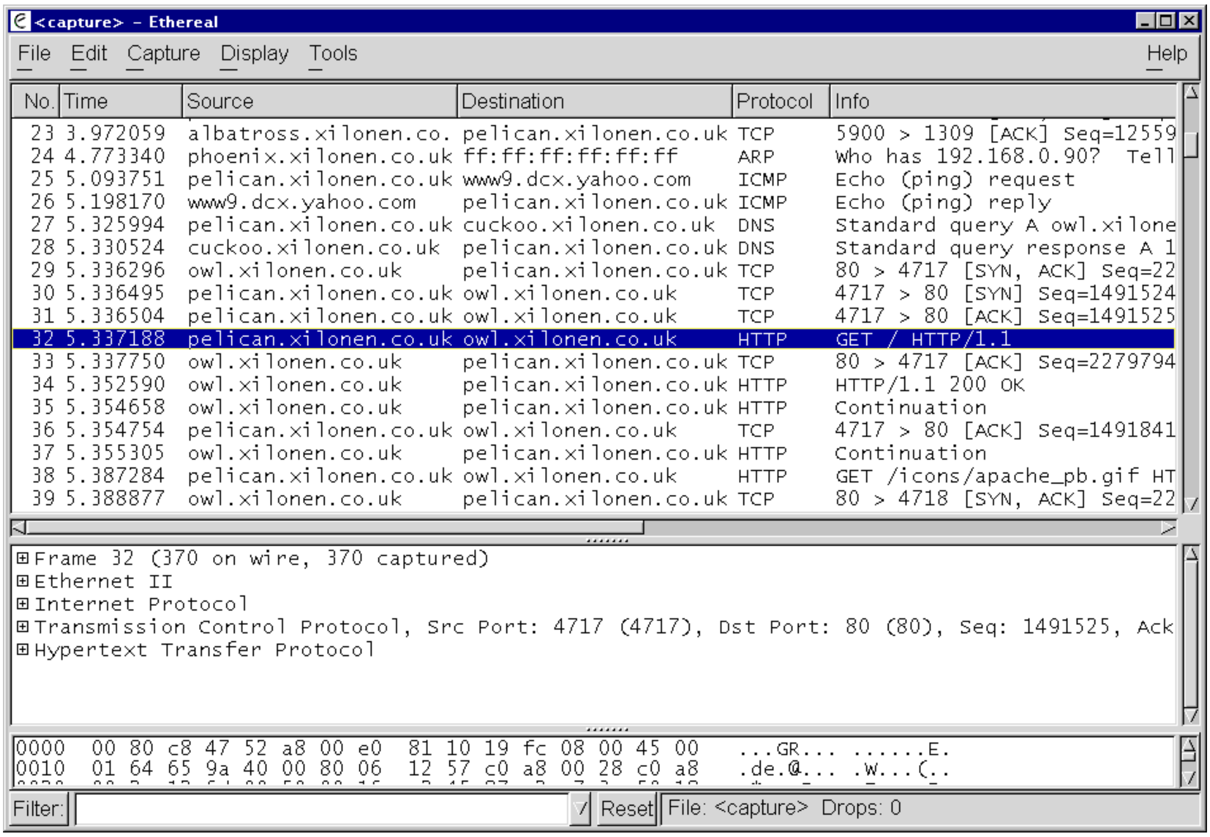
- Data is broadcast to all devices on the hub, threat: Information Leakage.
- Easy to install and attach additional devices. Good from a network management perspective.
- Unless hub physically secured, anyone can plug into hub.
- Even if hub secured, attacker can unplug existing device or make use of currently unused cable end.
- Threats: All four fundamental threats are enabled.

To perform an attack the attacker needs to connect attacked devices through a hub and connect a sniffer to the hub.

In addition to the security issues, hubs do not support speeds faster than 100 BASETX, they work only in half duplex mode. For these reasons, hubs are outdated, and rarely used in modern networks.

3.Network Sniffers

Network Interface Cards (NICs) normally operate in non-promiscuous mode. i.e. they only listen for frames with their MAC address. A packet sniffer is a software application that uses a NIC in a promiscuous mode to capture all network packet sent across a network segment, i.e. Reads frames regardless of MAC address. Many different sniffers are available free online, examples: Tcpdump, Snort, and Wireshark.



```
No. Time      Source                Destination           Protocol Info
 23 3.972059  albatross.xilonen.co. pelican.xilonen.co.uk TCP      5900 > 1309 [ACK] Seq=12559
 24 4.773340  phoenix.xilonen.co.uk ff:ff:ff:ff:ff:ff     ARP      Who has 192.168.0.90?  Tell
 25 5.093751  pelican.xilonen.co.uk www9.dcx.yahoo.com    ICMP     Echo (ping) request
 26 5.198170  www9.dcx.yahoo.com    pelican.xilonen.co.uk ICMP     Echo (ping) reply
 27 5.325994  pelican.xilonen.co.uk cuckoo.xilonen.co.uk  DNS      Standard query A owl.xilone
 28 5.330524  cuckoo.xilonen.co.uk  pelican.xilonen.co.uk DNS      Standard query response A 1
 29 5.336296  owl.xilonen.co.uk     pelican.xilonen.co.uk TCP      80 > 4717 [SYN, ACK] Seq=22
 30 5.336495  pelican.xilonen.co.uk owl.xilonen.co.uk     TCP      4717 > 80 [SYN] Seq=1491524
 31 5.336504  pelican.xilonen.co.uk owl.xilonen.co.uk     TCP      4717 > 80 [ACK] Seq=1491525
 32 5.337188  pelican.xilonen.co.uk owl.xilonen.co.uk     HTTP     GET / HTTP/1.1
 33 5.337750  owl.xilonen.co.uk     pelican.xilonen.co.uk TCP      80 > 4717 [ACK] Seq=2279794
 34 5.352590  owl.xilonen.co.uk     pelican.xilonen.co.uk HTTP     HTTP/1.1 200 OK
 35 5.354658  owl.xilonen.co.uk     pelican.xilonen.co.uk HTTP     Continuation
 36 5.354754  pelican.xilonen.co.uk owl.xilonen.co.uk     TCP      4717 > 80 [ACK] Seq=1491841
 37 5.355305  owl.xilonen.co.uk     pelican.xilonen.co.uk HTTP     Continuation
 38 5.387284  pelican.xilonen.co.uk owl.xilonen.co.uk     HTTP     GET /icons/apache_pb.gif HT
 39 5.388877  owl.xilonen.co.uk     pelican.xilonen.co.uk TCP      80 > 4718 [SYN, ACK] Seq=22

⊞Frame 32 (370 on wire, 370 captured)
⊞Ethernet II
⊞Internet Protocol
⊞Transmission Control Protocol, Src Port: 4717 (4717), Dst Port: 80 (80), Seq: 1491525, Ack
⊞Hypertext Transfer Protocol

0000   00 80 c8 47 52 a8 00 e0  81 10 19 fc 08 00 45 00   ...GR... ......E.
0010   01 64 65 9a 40 00 80 06  12 57 c0 a8 00 28 c0 a8   .de.@... .W...(..

File: <capture>  Drops: 0
```

Figure(2.2): Wireshark Screen Shot

3.1.Detecting Sniffer

One question that most people ask is “How can I tell if a machine is in promiscuous mode?” Well, if you have physical access to the machine you could look at the settings for the network card. Over a network it is more difficult, some approaches include:

- Sending large volumes of data, then sending ICMP ping request and observing delay as sniffer processes large amount of data.
- Sending data to unused IP addresses and watching for DNS requests for those IP addresses.

There is a program called AntiSniff that you can run to determine if a specified machine or group of machines have their network card in promiscuous mode. AntiSniff performs three classes of tests: operating system specific tests, DNS tests, and network latency tests. All of the tests may be run together to give a high degree of certainty as to whether or not a computer is packet sniffing. It is important to realize that these methods are not 100 percent accurate.

3.2.Sniffing Legitimately

If you are an administrator and are allowed to legitimately run a sniffer, you can run it to:

- Enforce your company’s security policy.
- It can be used as network analyzers or protocol analyzers, which is the key maintain an optimized network and detecting security issues.
- With complex networks, they are used for fault investigation and performance measurement. It allow you to capture data from the network packet by packet, decode the information, and view it in an easy to understand format.
- Useful when understanding how a product uses the network.
- Network-based Intrusion Detection Systems (NIDS), Monitor network traffic, looking for unusual behavior or typical attack patterns.

3.3.Sniffer Safeguards

When intruders use sniffers, it considered as passive attack. They use sniffers mostly to capture user names and passwords, collect confidential data, and map the network. In addition, sniffers are common component of rootkit, and a tool to control backdoor programs. To protect from sniffer, we can:

- Use of non- promiscuous mode interfaces.
- Use of switched environments. Switches offer some, but little protection against sniffers (see next sections).
- Encryption of network traffic. Encryption is the best method of protecting your data from sniffers.
- One-time passwords, e.g. SecurID, skey, limiting usefulness of information gathered by sniffer.

4.Layer 2: Switches

A hub is a simple device that requires virtually no overhead to operate. But it is also inefficient. When a network is experiencing a high level of traffic, a hub compounds the problem by taking any incoming frame and retransmitting it out to all connections. In contrast, the switch uses addresses and processing power to direct a frame out of a particular port, thus reducing the amount of traffic on the network. The switch has one primary function: to direct the data frame to only the addressed receiver. Thus, the switch needs to know where all the devices are so that it can send the data out the appropriate link. It does not send the frame out all links, as the hub does (unless the data frame is a broadcast message). Thus, the switch acts as a filter. A filter examines the destination address of a frame and forwards the frame appropriately, depending on some address information stored within the switch, this address is called Media Access Control (MAC) address. As a frame of data moves across the first local area network and enters the switch, the switch examines the source and destination addresses stored within the frame. These frame addresses are assigned to the NIC when the NIC is manufactured. (All companies that produce NICs have agreed to use a formula that ensures that every NIC in the world has a unique NIC address). This unique address is 48 bit value. The first 24 bits indicate vendor.

For example, 00:E0:81:10:19:FC

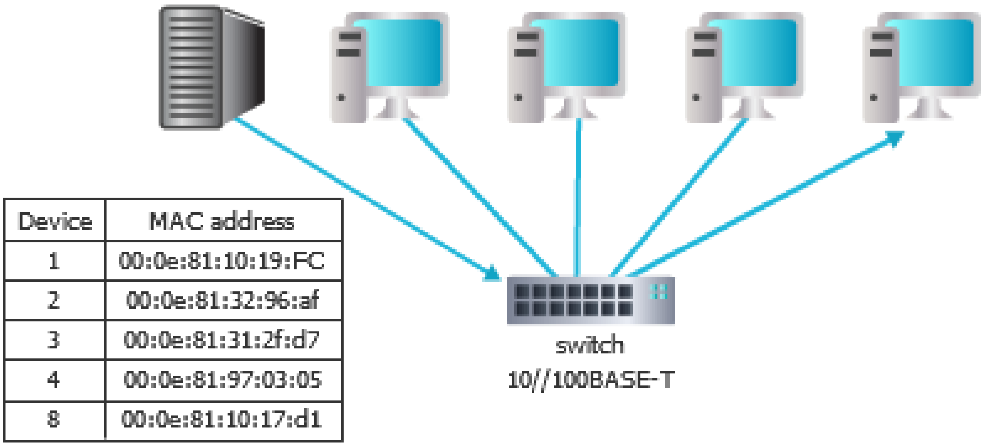
00:E0:81 indicates Tyan Corporation.

10:19:FC indicates 1,055,228th NIC.

As a sequence:

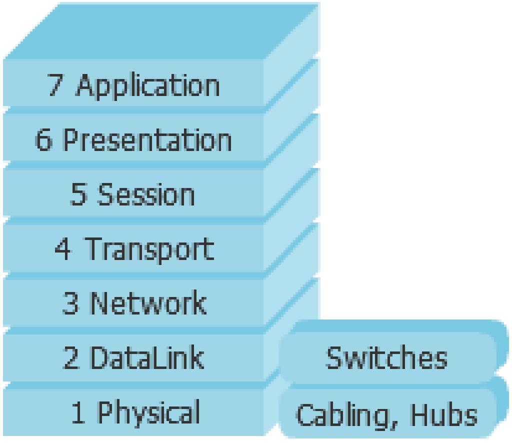
- Switches operate at Layer 2
- Switches reduce effectiveness of basic sniffing tools

- Now a promiscuous NIC only sees traffic intended for it



Device	MAC address
1	00:0e:81:10:19:FC
2	00:0e:81:32:96:af
3	00:0e:81:31:2f:d7
4	00:0e:81:97:03:05
8	00:0e:81:10:17:d1

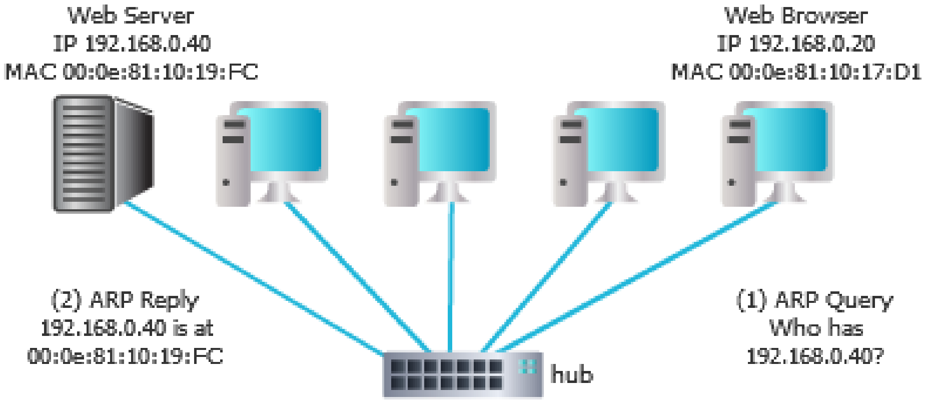
Figure(2.3): Switch Operations



Figure(2.4): Switches in OSI Protocol Stack

4.1.Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) takes an IP address in an IP datagram and translates it into the appropriate medium access control layer address (MAC address) for delivery on a local area network. Every workstation that has a connection to the Internet is assigned an IP address. This IP address is what a packet uses to find its way to its intended destination. There is one problem, however, when a workstation is on, for example, an Ethernet. The frame in the data link layer consists of a number of fields of information, none of which is an IP address. If the frame is supposed to go to a particular workstation with a unique IP address, but the frame does not contain an IP address, how does the frame know where to go? ARP provides the answer to this question. After an IP datagram enters a LAN through a router, ARP broadcasts a message on the LAN asking which workstation belongs to this IP address. The workstation that recognizes its IP address sends a message back saying, "Yes, that is my IP address, and here is my 48-bit (NIC) address. Please forward that IP packet to me via my address". The 48-bit NIC address is stored in a buffer just in case it will be needed again in the near future.



Figure(2.5): ARP Query & ARP Reply

4.2. Sniffer in Switch Environment

We mentioned earlier that the use of switches in the network makes sniffing more difficult. In theory, on a switch you should only see traffic destined for your own computer. There are ways to trick a switch, or get round its technology, the following list describes several ways in which a switch can be defeated.

4.3. ARP Vulnerability

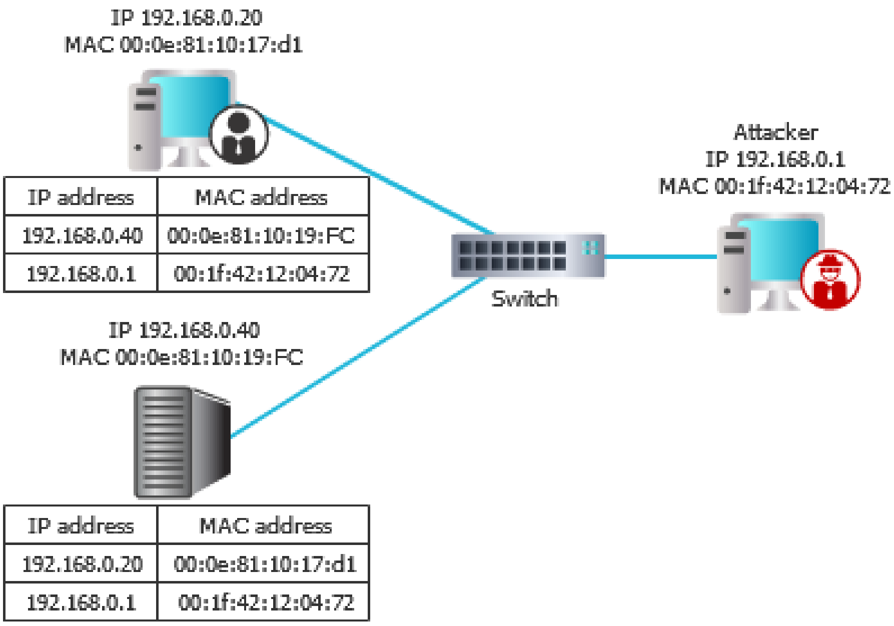
- As we have mentioned earlier, when a computer needs to know the MAC address of another computer, it will send an ARP request. Each computer maintain an ARP table to store the MAC addresses of other computers that it has talked to. ARPs are broadcast on switch, so all computers on that switch will see the request and the response. There are several methods that use ARP to trick a switch into sending traffic somewhere it should not. The most used is by using gratuitous ARPs:

  - Sent by legitimate hosts on joining network or changing IP address.
  - Not in response to any ARP request.
  - Associates MAC address and IP address.
  - The attack can be realised by issuing gratuitous ARPs.
  - ARP replies have no proof of origin, so a malicious device can claim any MAC address.

The attack is performed as follows, see Figures(2.6, 2.7) and (2.8):

- Attacker sends gratuitous ARPs claiming that 192.168.0.20 and 192.18.0.40 are associated to a new MAC address (the attacker MAC address).
- Attacker keeps a relay index: a table containing the true association between MAC addresses and IP addresses.
- But the two devices at 192.168.0.20 and 192.18.0.40 update their ARP caches with false information.
- All traffic for 192.168.0.20 and 192.168.0.40 gets sent to attacker by layer 2 protocol (Ethernet).
- Attacker can re-route this traffic to the correct devices using his relay index and layer 2 protocol.
- So these devices (and the switch) are oblivious to the attack
- Enables all fundamental threats

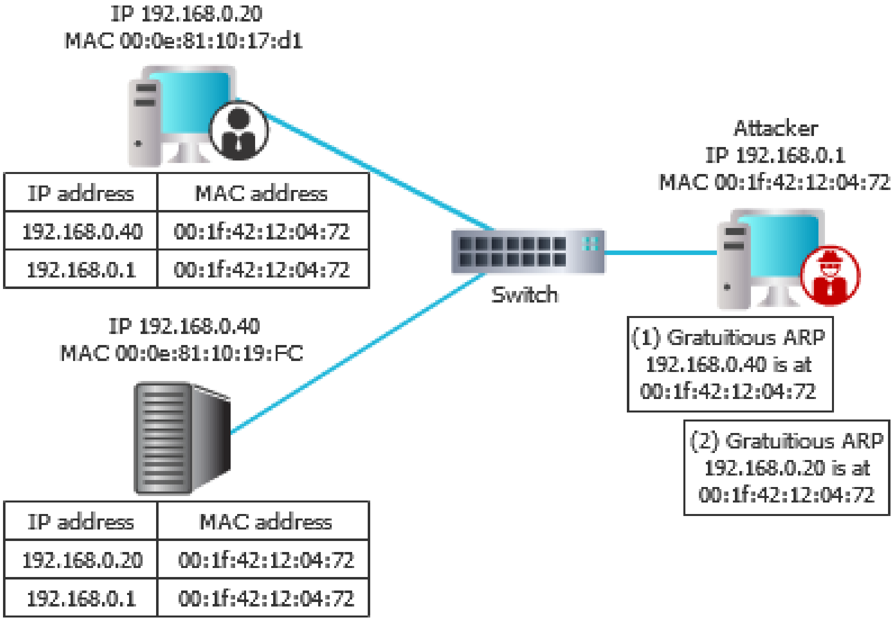
The attacker can subvert a switch by sending out an ARP claiming to be someone else as the MAC address. The attacker can also send an ARP claiming to be the router, the gateway, in which case computers will try to send their packets through the attacker's computer. All of these tricks will allow an attacker to see, and modify information that he is not supposed to see. So sniffing is possible in a switched environment. This attack implemented in Dsniff tools.



IP address	MAC address
192.168.0.40	00:0e:81:10:19:FC
192.168.0.1	00:1f:42:12:04:72

IP address	MAC address
192.168.0.20	00:0e:81:10:17:d1
192.168.0.1	00:1f:42:12:04:72

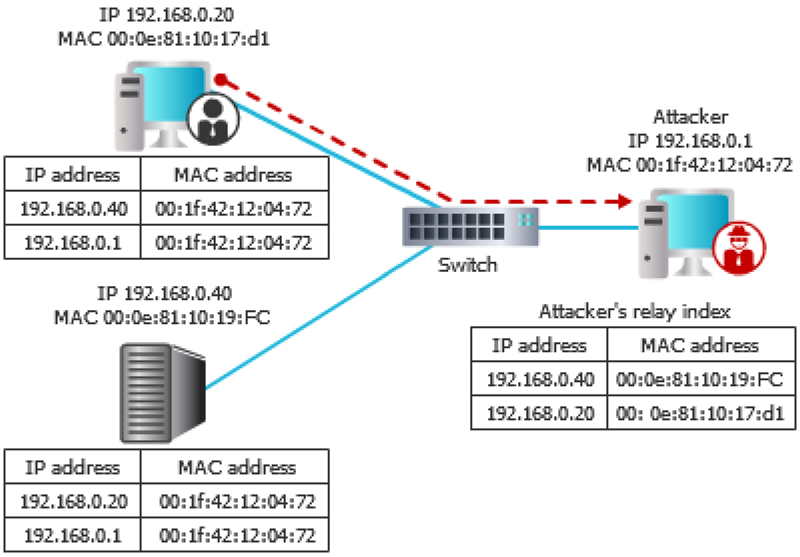
Figure(2.6): Before ARP Spoofing



IP address	MAC address
192.168.0.40	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

IP address	MAC address
192.168.0.20	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

Figure(2.7): After ARP Spoofing



IP address	MAC address
192.168.0.40	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

IP address	MAC address
192.168.0.40	00:0e:81:10:19:FC
192.168.0.20	00: 0e:81:10:17:d1

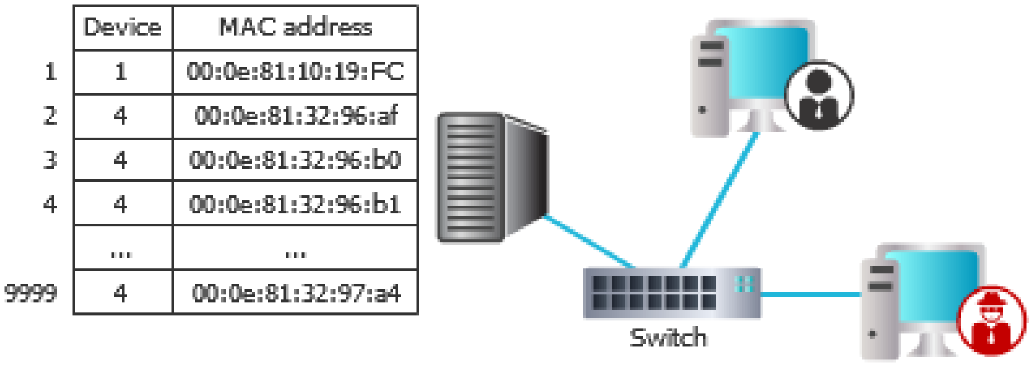
IP address	MAC address
192.168.0.20	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

Figure(2.8): Effect of ARP Spoofing

4.4.Mac Flooding

When a malicious device connected to switch, and sends multiple gratuitous ARPs. Each ARP claims a different MAC address. When index fills:

- Some switches act like a hub, where all packets are broadcast to all computers. This is known as a device *failing open,* thus removing all security provisions.
- Devices that *fail close* will incorporate some sort of security measures, such as shutting down all communications, and ignore any new devices attempting to connect.



	Device	MAC address
1	1	00:0e:81:10:19:FC
2	4	00:0e:81:32:96:af
3	4	00:0e:81:32:96:b0
4	4	00:0e:81:32:96:b1
	...	...
9999	4	00:0e:81:32:97:a4

Figure(2.9): Mac Flooding

4.5.Switch Safeguards

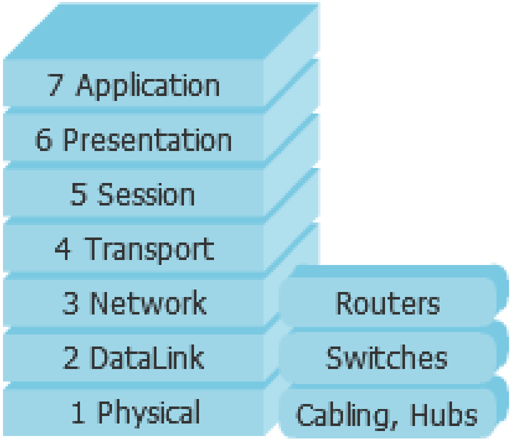
- Physically secure the switch: Prevents threat of illegitimate use
- Switches should failsafe when flooded
  - New threat: Denial of Service
  - Provide notification to network admin
- Arpwatch: is a computer software tool for monitoring Address Resolution Protocol traffic on a computer network. It can.
  - Monitor MAC to IP address mappings
  - Issue alerts to network admin
- Use static ARP caches: These are address resolutions that are manually added to the cache table for a device.
  - Loss of flexibility in network management
- Port security: specify MAC addresses for each port, or to learn a certain number of MAC addresses per port. Upon detecting of an invalid MAC the switch can be configured to block the offending MAC or just shut down the port.
  - Loss of flexibility in network management and performance hit

5.Layer 3: Routers

Sending and receiving IP packets is a primary way in which networked computers and other devices communicate, and constitutes the basis of the modern internet. All IP packets contain a header which precedes the body of the packet and contains important routing information, including the source and destination addresses. A router is a Network layer device, it examines the IP address of the packets that pass through it. And because IP addresses have both a network and a host address, a router can determine what network a message is coming from and going to. Routers employ routing tables, which are Information about possible destinations and how to reach them.

When a datagram reaches a router, there are three possible actions for the datagram:

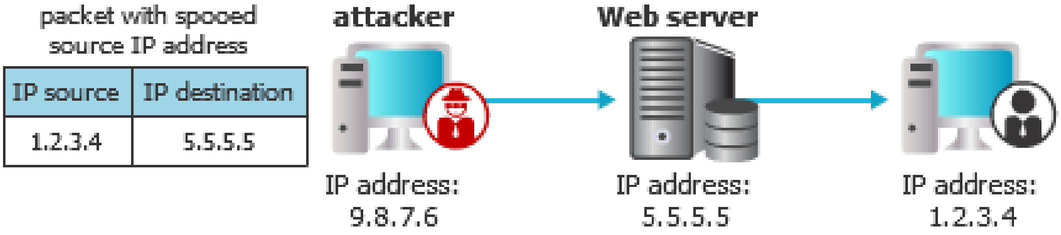
- Sent directly to destination host
- Sent to next router on way to known destination
- Sent to default router



Figure(2.10): Routers in OSI Protocol Stack

5.1.IP Spoofing

In a normal packet, the source IP address is the address of the sender of the packet. Any station can send packets pretending to be from any IP address. Replies will be routed to the appropriate subnet, route asymmetry. Analogy, nothing prevents you from physically mailing a letter with an invalid return address, or someone else's, or your own. Likewise, packets can be inserted in the network with invalid or other IP addresses. IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. The ability to modify the source IP is inherent to the design of TCP/IP, making it an ongoing security concern.



Figure(2.11): IP Spoofing

5.2.Reflected Denial of Service Attack (DoS)

A reflected DoS attack uses IP spoofing to generate fake requests, apparently on behalf of a target, to produce responses from under protected intermediary servers. The perpetrator's goal is to amplify their traffic output by triggering large responses from much smaller requests. Common reflected DoS attack methods include:

- DNS amplification: An ANY query originating from a target's spoofed address is sent to numerous unsecured DNS resolvers. Each 60 byte request can prompt a 4000 byte response, enabling attackers to magnify traffic output by as much as 1:70.
- Smurf attack: An ICMP Echo request is sent from a target's spoofed address to an intermediate broadcast network, triggering replies from every device on that network. The degree of amplification is based on the number of devices to which the request is broadcast. For example, a network with 50 connected hosts results in a 1:50 amplification.
- NTP amplification: A get monlist request, containing a target's spoofed IP address, is sent to an unsecure NTP server. As in DNS amplification, a small request triggers a much larger response, allowing a maximum amplification ratio of 1:200.

5.3.IP Spoofing Safeguard

While IP spoofing can't be prevented, measures can be taken to stop spoofed packets from infiltrating a network. A very common defence against spoofing is ingress filtering. Ingress filtering is a form of packet filtering usually implemented on a network edge device which examines incoming IP packets and looks at their source headers. If the source headers on those packets don't match their origin or they otherwise look fishy, the packets are rejected. In addition, by using ingress filter we can Forbid inbound broadcasts from the internet into our networks, and forbid inbound packets from non-routable networks. Some networks will also implement ingress filtering, which looks at IP packets exiting the network, ensuring that those packets have legitimate source headers to prevent someone within the network from launching an outbound malicious attack using IP spoofing. In addition to drop outbound broadcasts.

We can also use Log files to monitor any unlawful activities on our network.

5.4.Routing Information Threats

The router's primary functions are to learn and propagate route information, and ultimately to forward packets via the most appropriate paths. Successful attacks against routers are those able affect or disrupt one or more of those primary functions by compromising the router itself, and/or the routing information.

Routers are subject to the same sort of attacks designed to compromise hosts and servers, such as password cracking, privilege escalation, buffer overflows, and even social engineering.

For most routing protocols routers cannot exchange route information unless they establish a neighbour adjacency. Some attacks attempt to break established sessions by sending the router malformed packets, resetting TCP connections, consuming the router resources, etc. Attacks may also prevent neighbour adjacencies from being formed by saturating queues, memory, CPU and other router resources.

Finally, routing can also be compromised by the injection of false route information, and by the modification or removal of legitimate route information. Route information can be injected or altered by many means, ranging from the insertion of individual false route updates to the installation of bogus routers into the routing infrastructure. Potential denial of service conditions may result from intentional loops or black-holes for particular destinations. Attackers may also attempt to redirect traffic along insecure paths to intercept and modify user's data, or simply to circumvent security controls.

6.Layer 4: TCP, UDP, ICMP Issues

At this layer, two types of connections can be made: TCP or User Datagram Protocol (UDP). TCP requires acknowledgment for establishing connection but UDP does not. While the IP establishes the connection across the network, the port defines the type of connection and the protocol used by that connection. When a user application wants to establish a communication link with a remote host, it must provide source/destination port numbers for the TCP layer and the IP address of the destination for the IP layer. When a port is paired up with the IP address of the remote machine whose port we are interested in, the paired entity is known as a socket. That socket may be referred to as the destination socket or the remote socket. A pairing of the source machine IP address with the port used by the TCP layer for the communication link would then be referred to as the source socket. The two sockets at the end-points uniquely define a communication link.

The ports are vulnerable to either banning or scanning. Port banning occurs when the accessed port provides information on the protocol running on the port, the device's operating system and application, etc. Port scanning helps the attacker in obtaining valuable information of the network, including IP address, list of open ports and the applications running on those ports.

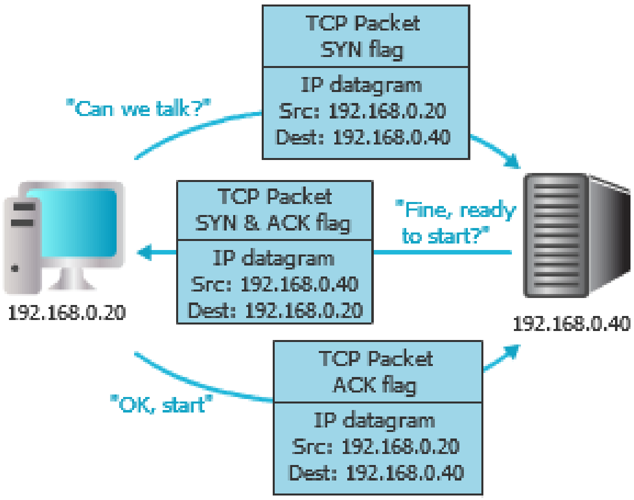
This layer is greatly susceptible to attacks that target the TCP or UDP, such as SYN flooding or UDP flooding.

6.1.SYN Flooding Attack

To explain SYN flooding attack, we first recall the TCP connection structure. For application layer connections to be established, the sender and receiver are required to engage in a process of mutual verification, known as a TCP three-way handshake. The process consists of the following exchange of synchronization (SYN) and acknowledgement (ACK) packets (see figure 2.12):

- A SYN packet from sender to receiver. “Can we talk?”
- An SYN/ACK packet from receiver to sender. “Fine – ready to start?”
- An ACK packet from sender to receiver. “OK, start”

The packet type is indicated by a flag in the packet header. The destination host has to track which machines it has sent a “SYN+ACK” to keep a list of TCP SYN packets that have had a SYN+ACK returned. When ACK is received, packet removed from list as connection is open.



Figure(2.12): TCP Handshake

What if the sender does not answer with an ACK?

- A SYN packet from sender to receiver. “Can we talk?”
- An SYN/ACK packet from receiver to sender. “Fine – ready to start?”
- ……………….nothing……………….

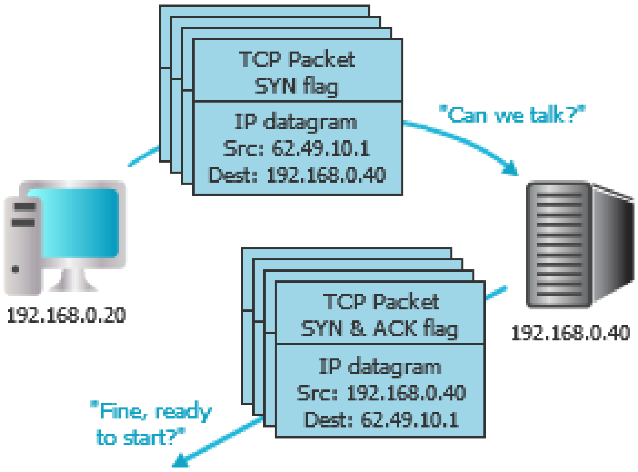
If the sender sends 100 SYN packets per second. Eventually receiver runs out of memory to track the SYN+ACK replies. “SYN flooding”

If the attacker hits a host periodically with a square wave of short duration DoS, you can bring down a TCP engine to its knees and essentially make it inoperative for all TCP communications. What makes this type of attack so insidious is that it can be much more difficult to detect than the more run-of-the-mill DoS attacks that involve hitting a targeted host with heavy traffic so as to cause resource/bandwidth exhaustion at the target. This attack requires hitting a targeted host with periodic DoS traffic. It is possible for the on/off ratio of the DoS traffic to be such that such an attack would fly under the radar — in the sense that it would not be detectable by a traffic monitor that is looking for heavy traffic associated with the more common DoS attacks.

6.2.TCP Denial of Service + IP Spoofing

The attacker uses fake IP addresses to send continuous SYN requests to the target device on its different ports. Assuming all requests as genuine, the target system sends the acknowledgment (SYN_ACK) packets to each requesting fake IP. This creates a scenario where the port remains open until the connection times out, when another fabricated SYN request is received. This overwhelms the target system's resources and prevents legitimate users from establishing connections. This type of attack has an advantage (to an attacker) over the previous attack that: No-one knows who sent the packets.

Another consequence of this type of attack is that, as soon as the attack is detected, the admins of the targeted network will block the source IP addresses (by quickly adding to the firewall packet filtering rules, as described in the coming lectures). If it should happen that the forged IP addresses are legitimate, in the sense that those addresses have actually been assigned to hosts in the internet, such packet filtering would amount to a denial of service (DoS) to the otherwise legitimate users/systems at those IP addresses.



Figure(2.13): TCP DOS Attack + IP Spoofing

Safeguard

While modern operating systems are better equipped to manage resources, which makes it more difficult to overflow connection tables, servers are still vulnerable to SYN flood attacks. There are a number of common techniques to mitigate SYN flood attacks, including:

SYN Cookies: using cryptographic hashing, the server sends its SYN-ACK response with a sequence number that is constructed from the client IP address, port number, and possibly other unique identifying information. When the client responds, this hash is included in the ACK packet. The server verifies the ACK, and only then allocates memory for the connection.

RST Cookies: for the first request from a given client, the server intentionally sends an invalid SYN-ACK. This should result in the client generating an RST packet, which tells the server something is wrong. If this is received, the server knows the request is legitimate, logs the client, and accepts subsequent incoming connections from it.

Stack Tweaking: administrators can tweak TCP stacks to mitigate the effect of SYN floods. This can either involve reducing the timeout until a stack frees memory allocated to a connection, or selectively dropping incoming connections.

Obviously, all of the above mentioned methods rely on the target network’s ability to handle large-scale volumetric DoS attacks, with traffic volumes measured in tens of Gigabits (and even hundreds of Gigabits) per second.

6.3.UDP Flooding Attack

UDP is a networking protocol that is both connectionless and session-less. Unlike TCP, UDP traffic does not require a three-way handshake. As such, it requires less overhead and is perfectly suited for traffic such as chat or VoIP that does not need to be checked and rechecked. The same properties that make UDP ideal for certain kinds of traffic also make it more susceptible to exploitation. Without an initial handshake to ensure a legitimate connection, UDP channels can be used to send a large volume of traffic to any host.

A UDP flood is a form of volumetric DoS attack where the attacker targets and overwhelms random ports on the host with IP packets containing UDP packets. Each time a new UDP packet is received by the server, resources are used to process the request. The first step in this process involves the server determining if any programs are running at the specified port. If no programs at that port are receiving packets, then the server issues an ICMP packet (“Destination Unreachable”) to notify the sender that the destination could not be reached. The cumulative effect of being bombarded by such a flood is that the system becomes inundated and therefore unresponsive to legitimate traffic. The attacker may also choose to spoof the IP address of the packets. This ensures that the return ICMP packets are not able to reach their host, while also keeping the attack completely anonymous.

What make this type of attack dangerous is that: There are no internal protections that can limit the rate of a UDP flood. As a result, UDP flood DOS attacks are exceptionally dangerous because they can be executed with a limited amount of resources.

Safeguard

Preventing a UDP flood attack can be challenging. Most operating systems attempt to limit the response rate of ICMP packets with the goal of stopping DoS attacks. The downside to this form of mitigation is that it also filters out legitimate packets. In the case of a truly high volume flood, even if the server's firewall is able to mitigate the attack, congestions or slowdowns will in-all-likelihood occur upstream, causing disruption anyway.

6.4.The Internet Control Message Protocol (ICMP)

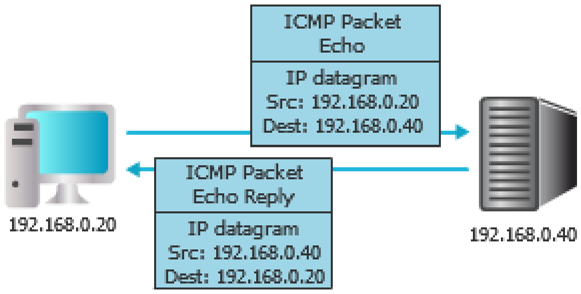
ICMP is a transport layer protocol (some references classify it as a network protocol) used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.

What is ICMP Used For?

The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination.

A secondary use of ICMP protocol is to perform network diagnostics, the commonly used terminal utilities traceroute and ping both operate using ICMP. The traceroute utility is used to display the routing path between two Internet devices. The routing path is the actual physical path of connected routers that a request must pass through before it reaches its destination. The journey between one router and another is known as a 'hop', and a traceroute also reports the time required for each hop along the way. This can be useful for determining sources of network delay.

The ping utility is a simplified version of traceroute. A ping will test the speed of the connection between two devices and report exactly how long it takes a packet of data to reach its destination and come back to the sender's device. Although ping does not provide data about routing or hops, it is still a very useful metric for gauging the latency between two devices. The ICMP echo-request and echo-reply messages are commonly used for the purpose of performing a ping.



Figure(2.14): Ping Operation

6.5.ICMP Security Vulnerabilities

Although ICMP is a handy tool for network management and fault diagnostic, network attacks can exploit this process, creating means of disruption, which include but are not limited to:

Ping sweep: A type of attack that uses ICMP echo request messages to enumerate live hosts on a network.

Ping flood: Utilized to launch a DoS, where the attacker sends ICMP requests in a rapid succession without waiting for the targeted system to respond. Ping floods aim to consume both incoming and outgoing bandwidth as well as utilize CPU resources to degrade the system's performance.

ICMP tunneling: A method used to establish a covert communication channel between remote systems, most times between a client and a proxy. All communications are sent via ICMP requests and replies. ICMP tunneling could be used to bypass firewall rules.

Forged ICMP redirects: Network traffic could be fraudulently redirected to an attacker via a forged ICMP redirect message. The attacker would send an ICMP redirect message, which informs a host of a direct path to a destination, to the victim that contains the IP addresses of the attacker's system. This allows an attacker to compromise network traffic via a man-in-the-middle attack or cause a DoS.

Due to all of the possible attacks involving ICMP, and the fact that TCP/IP "mostly" works even when ICMP traffic is blocked, network administrators sometimes block ICMP traffic on their firewalls as a "quick fix" security measure. Disabling the full ICMP protocol may not be a good approach in securing network devices. Instead disabling a subset of ICMP types provide fine-grained control over which types of ICMP messages network devices could request, receive, and respond to.

6.6.Securing Against Denial of Service Attacks

It is very difficult to defend against a sophisticated DoS attack launched by a determined adversary. The more difficult is that attacks are perpetrated by means of using several source devices, i.e. requests made to target services come from a large number of different devices which may even be geographically separated. This type of attack is called distributed denial-of-service attack (DDoS attack) and is usually carried out with the help of botnets. A botnet, in simple terms, is a network of infected computers that are controlled as a single entity by a malicious actor. That means the actor can have all the computers in the infected network carry out the same instructions at the same time.

How to Mitigate DoS Attacks

Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services.

Attack Detection: The first step of any mitigation strategy is understanding when you are the target of a DoS attack. Analyzing incoming traffic and determining whether or not it is legitimate is the first step in keeping your service available and responsive. Early detection of an attack dramatically increases the efficacy of any mitigation strategy.

IP Whitelisting/Blacklisting: The simplest defense against a DoS attack is either whitelisting only legitimate IP addresses or blocking ones from known attackers. For instance, if the application is meant to be used only by employees of a specific company, a hardware or software rule could be created to disallow any traffic, not from a specific IP range. For example, 192.168.0.0/16 would allow any IP address between 192.168.0.0 and 192.168.255.255. The rule rejects any IP address outside that range. Inversely, IP blacklisting adds a rule to reject traffic from specific IP addresses. It is important to remember that blocking IP addresses in this way may prevent legitimate traffic from those IPs. Blacklisting IP addresses is also dangerous in that you may end up blacklisting all users sharing an IP address, even if many of those users are legitimate. Also, this strategy may not be effective against DDoS attacks or DoS attacks using spoofed IP addresses.

Rate Limiting: Rate limiting is the practice of limiting the amount of traffic available to a specific Network Interface Controller (NIC). It can be done at the hardware or software level to mitigate the chances of falling victim to a DoS attack. At the hardware level, switches and routers usually have some degree of rate-limiting capabilities. At the software level, it is essential to have a limit on the number of concurrent calls available to a specific customer.

Upstream Filtering: One of the best mitigation strategies is to filter requests upstream, long before it reaches the target network. There are many providers of "Mitigation Centers" that will filter the incoming network traffic. For example Amazon Shield and Cloudflare both offer products that allow for protection against DoS and DDoS attacks by checking incoming packet IPs against known attackers and botnets and attempt to only forward legitimate traffic.

Exercises:

True or False

Question	True	False
1. UDP provides unreliable transfer of datagrams between client and server.		
2. Both UDP and TCP require that the applications recognize their own data formats.		
3. All datagrams contain 2 ports.		
4. A Denial-of-Service attack can be performed by bombarding a server with connection requests.		
5. IP Sniffing is the ability to inject packets into the Internet with a false source address.		

Multiple Choice Questions

1. Due to a previous IP spoofing attack, you want to make some changes to the network to prevent future attacks. Which of following actions should you take?

   A. Install antivirus software

   B. Set up IP address filters

   C. Install certificates on clients and servers

   D. Block all ports on the router

2. ARP spoofing attack can be performed in:

   A. Hub environments

   B. Switch environments

   C. Router environments

   D. A and B only

   E. All of the above

3. Sync flooding attack depends on:

   A. Vulnerability attack

   B. Bandwidth flooding

   C. Connection flooding

   D. User forgery

4. A type of attack that overloads the resources of a single system to cause it to crash or hang.

   A. Resource Starvation

   B. Active Sniffing

   C. Passive Sniffing

   D. Session Hijacking

5. A mode that causes the controller to pass all traffic through the CPU, this mode is used for packet sniffing and can be used by a single device to intercept and read all packets.
   A. Collision Domain
   B. Passive Sniffing
   C. Promiscuous Mode
   D. Summary Display

6. A place where IP addresses, MAC addresses, and a timer are used to reduce the amount of ARP traffic on the system.
   A. Address Resolution Protocol (ARP) Cache
   B. DNS Security Extensions (DNSSEC)
   C. Address Resolution Protocol (ARP) Poisoning
   D. Session Hijacking

7. Type of attack that involves an attacker changing the MAC address and attacks a LAN by forging ARP request and reply packets on the target computer resulting in frames being sent to the attacker's computer first compromising the data and security.
   A. Address Resolution Protocol (ARP) Poisoning
   B. Resource Starvation
   C. Address Resolution Protocol (ARP) Cache
   D. Session Hijacking

8. Sniffing performed on a switched network by injecting packets onto the network to create traffic bypassing the switch.
   A. Passive Sniffing
   B. Session Hijacking
   C. MAC Flooding
   D. Active Sniffing

9. Sniffing performed on a hub, that does not require the injection of packets onto the network.

A. Session Hijacking

B. Passive Sniffing

C. MAC Flooding

D. Active Sniffing

10. What is the purpose of a Denial of Service attack?

A. Exploit a weakness in the TCP/IP stack

B. To execute a Trojan on a system

C. To overload a system so it is no longer operational

D. To shutdown services by turning them off

11. What is the sequence of a TCP connection?

A. SYN–ACK–FIN

B. SYN–SYN ACK–ACK

C. SYN–ACK

D. SYN–SYN–ACK

12. Why would a ping sweep be used?

A. To identify live systems

B. To locate live systems

C. To identify open ports

D. To locate firewalls

13. Services running on a system are determined by ______________.

A. The system's IP address

B. The Active Directory

C. The system's network name

D. The port assigned

14. Multiple TCP streams can distinguished on a given machine using __________.

A. Ports

B. DNS addresses

C. network interface cards

D. All of the above responses are correct

15. The ability to inject packets into the Internet with a false source address is known as __________________ .

A. IP spoofing

B. IP sniffing

C. IP phishing

D. Man–in–the–middle attack

References

1. Stallings, W., Brown, L. : Computer Security: Principles and Practice 4th edn. Prentice Hall (2018).
2. Stallings, W.: Network Security essentials: application and standards, 6th edn. Pearson India Education Services Pvt. LTD (2017).
3. https://www.imperva.com/learn/application-security/ip-spoofing/.
4. https://developer.okta.com/books/api-security/dos/how/.

Number of the Question	True	False
1	✓	
2	✓	
3	✓	
4	✓	
5	✓	

Number of the Question	Answer
1	B
2	D
3	C
4	A
5	C
6	A
7	A
8	C
9	B
10	C
11	B
12	A
13	D
14	A
15	A