Network & Perimeter Security

OSI Model

Now, going back to your Network+ studies, you probably remember the mnemonic of Please Do Not Throw Sausage Pizza Away.
This represents the seven layers of the OSI Model, going from the bottom to the top. This is:

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application.

Switch

Now, this is because hubs were dumb. They had no intelligence. As networks got larger, hubs caused a lot of collisions and slowed down the network. To solve this problem, something came along called a bridge, and this was used to separate physical LANs or WANs into two logical networks, or connect two logical networks together.
Now, switches are the evolution of hubs and bridges. Essentially, every single port on a switch acts as if it was a bridged hub on each one. This means that it improves the data transfer and security through the intelligent use of MAC addresses, being able to figure out where a device is and only sending the information out that particular port of the switch and ignoring the rest.

Now, switches are subject to three main types of attack:

1. MAC flooding
2. MAC spoofing
3. Physical Tampering

Routers

Now, routers are devices that make routing decisions and they do this by using IP addresses. These layer three IP addresses are used to determine what network a particular host is on and what path the traffic should take to go across the wide area network until it reaches its destination network.

Network Zones

Most networks are segmented into at least three different zones:

1. LAN
2. WAN
3. DMZ.

Extranet

is a specialized type of DMZ that's created for your partner organizations to access over a wide area network.

Intranet

An Intranet is something that allows you to expand your internal network within your organization across multiple areas. This is usually done using VPN tunnels.

Jumpbox

Now, any kind of hosts you put in the DMZ should really be what we consider a Bastion Host. This is a host or serve that we put into the DMZ, which is not configured with any services that run on the local network. So, I don't want to run something like Active Directory inside the DMZ. That's an internal network service. Instead, I only want to run things that should be on the Internet, things like email, things like web, things like remote access.

Now when we want to configure our devices inside the DMZ, what are we going to do?
Well, we're going to use something known as a **jumpbox**.
Now, a **jumpbox** is a hardened server that provides access to other hosts within the DMZ.
And what ends up happening is the administrator will connect to the jumpbox, and then the jumpbox will connect to the host in the DMZ. So, we call it a jumpbox cause we're almost pivoting off of it.

Network Access Control

Network Access Control or NAC is used to protect your network from both known and unknown devices. With NAC, a device is scanned to determine its current state of security prior to it being allowed access to your network. Now, NAC can be used for computers that are within your internal network that are physically located in your buildings and connected to it or it can be applied to devices that are connected into your network remotely through a VPN.

VLANs

VLANs are implemented to segment our network, reduce collisions, organize our networks, boost performance and increase security. Unfortunately, attackers have created VLAN hopping which allows them to break out of our VLANs and access other VLAN data, though.

Subnetting

Subnetting is the act of creating subnetworks logically through the manipulation of IP addresses. So, if I take a large chunk of IPs, like a 256 block, I can break it down into four blocks of 64 IPs, or eight blocks of 32 IPs, however you want to break it down in your subnetting. Now, subnetting has some benefits to our network.

NAT

Network Address Translation or NAT is the process of changing an IP address while it transits across a router. Now in Network+, we discussed how this was used because we wanted to conserve public IP addresses because they were limited in IPv4.

Class A is anything that starts with a 10, so 10.0.0.0 all the way up through 10.255.255.255.

Now in class B, we have IP addresses that start with 172.16.0.0 all the way up through 172.31.0.0, essentially, anything that starts with a 172.16 all the way up through 172.31.

Class C is really easy to remember as well, and it's probably what you are using at home. It's 192.168.0.0 all the way up to 192.168.255.255.

Telephony devices

Telephony is a term that's used for a device that provides voice communication to your end users. Originally, telephony was used in networks to make connections with the outside world such as through your modem. So, a modem was this old device that we used to use that would allow us to modulate and demodulate digital information into an analog signal that could transmit over a standard dial-up connection.

War dialing

War dialing is simply when an attacker starts dialing random phone numbers to see if any modems would answer on the other side. So, a lot of servers back in those days will have dial-up modems so that remote technicians could dial into the server, gain access, and make changes to due support.

PBX

A PBX equipment is something you're going to find much more often in your networks than you are going to find modems. A PBX system stands for a Public

Branch Exchange. Essentially, this is the telephone system that runs all of the internal phone lines for your company.

VoIP

Well, it's Voice Over Internet Protocol. VoIP is much cheaper than the traditional PBX system and it's a lot more secure and easier to run if you can figure it properly. Some organizations will actually run two different networks now. One for data and one for the VoIP network.

Firewalls

1. software-based
2. hardware-based
3. embedded firewalls

Software-based firewalls are run as a piece of software on a host or a server. In fact, if you're running a Windows server, those have a built-in Windows Firewall that you can enable.

Hardware firewalls, on the other hand, are a standalone device that's actually an appliance that's installed into your network. It looks like another switch or another router that goes into your network stack.

Embedded firewalls work as a single function out of many on a single device. So, if you have a small office, home office router or a unified threat management device, these are examples of an embedded firewall.

Packet Filtering

Packet filtering is going to inspect each packet as it passes through the firewall, and it'll accept it or reject it based on the rules that it's been given.

There are two types of packet filtering:

1. stateless

2. stateful.

With stateless packet filtering, it's simply going to accept or reject packets based on the IP address and the port number that was requested. So, if I'm running a web server and you requested to come in on port 80, I would allow that, but if you requested to come in on port 53, I would deny it because it's not in my access control list.

Now, a stateful packet filter, on the other hand, is going to keep track of requests that leave through the firewall. So, if I make a request from a host through the firewall, it will temporarily open up a port number that I made the request from, some random high port number like 50,000 or 56,000. By using stateful packet inspection, you can almost entirely eliminate IP spoofing as a threat because the firewall is going to inspect the header of each packet being received. It's then going to compare that against what it was expecting based on the request that recently went out, and then, it's going to make its accept or reject decisions based on this additional information.

NAT filtering

This is going to filter traffic according to the port, whether it's a TCP or UDP port. This filtering can be done by simply checking the endpoint connections, by matching the incoming traffic to the requesting IP, and by matching the incoming traffic to the requesting IP address and port.

ALG

This is going to apply security mechanisms to specific applications such as FDP or Telnet. Now, instead of blocking traffic based on the Telnet port of port 23, instead, it's going to inspect each packet and determine which application it was meant for, and if it finds out that it was meant for Telnet, it would block it because that was unauthorized. This is a resource-intensive process, but it is a powerful layer of security that can be added onto your network.

Circuit-level gateway

which works at the session layer of the OSI model and applies security mechanisms when a TCP or a UDP connection is first established. Now, once that connection is established, the packets can then be sent or received without any further inspection or checks because all of that was done during the session establishment.

MAC filtering

We use MAC filtering, this is going to filter out computers and prevent them from accessing beyond the firewall based on their MAC addresses. This is used as part of your local area network before it gets out into the routing and Layer 3 logical addresses that go out beyond the network.

More recently, though, application firewalls have begun rising in popularity. These application firewalls operate at Layer 7 of the OSI model, the application layer, and this makes traffic control decisions based on the applications being used, things like FTP, HTTP, Telnet, and others.

WAF

Now, one modern type of firewall you may come across is known as a web application firewall, or WAF. A web application firewall is installed on a server in your environment, and it provides traffic control in the data that's being sent to and from your web applications. These are useful in helping to mitigate threats like cross-site scripting and SQL injection attacks because these web application firewalls are designed to specifically look for these type of threats and block them.

Proxy Server

There are four types of proxies in use today:

1. IP Proxy
2. Caching Proxy
3. Content Filter

4. Web Security Gateways.

IP Proxy

An IP Proxy is used to secure a network by keeping machines behind it anonymous. When your work computer decides to connect to Dion Training through the proxy in my example above, my server doesn't know which particular computer is actually connected to it from your company's network. All I see is the proxy server itself. This is because your proxy is using NAT to translate your request from your machine into a request from the proxy.

Caching Proxies

Caching Proxies are used to attempt to serve client requests without actually connecting to the remote server each time. Let's say that you went to my website at diontraining.com, and then your coworker, five minutes later, tried to go to diontraining.com, just like you did.

PAC, a Proxy Auto-Configuration file. This file contains the settings needed for a host to connect to the proxy server. Unfortunately though, these files are subject to modification, and could be used to redirect the user to an attacker's control proxy instead of your organization's. For this reason, it is better to disable the PAC files, and manually configure your proxy settings on your host machines, or you can push these out using a global policy object, or GPO update.

Internet Content Filter

These are used in large organizations as a way to prevent users from getting to stuff that they don't want you to access at work. It can filter out all types of different Internet activities, such as websites that aren't allowed to be accessed, email services they don't want you to get to, or even instant messaging.

Web Security Gateway

And this type of proxy acts as a go-between for devices that will scan them for viruses, filter out contents like ads, and then can act as a data loss prevention device as well. This type of proxy is looking at what's being sent out of the network, and what is coming back into the network to ensure that it aligns with your organization's policies.

Honeypots and honeynets

Honeypots and honeynets are used to attract and trap potential attackers to counteract any attempts at unauthorized access to your organization's network.

Now, a honeypot is generally a single computer, but it could also be a file, a group of files, or an area of unused IP address space that might be considered attractive to a would-be attacker.

A honeynet, on the other hand, is one or more computers, servers, or an area of the network. And often, this is used when a single honeypot is not deemed to be sufficient for your purposes.

Data loss prevention

Data loss prevention, or DLP systems, are designed to protect data by conducting content inspection of your data as it's being sent out of your organization's network. While data loss prevention is the most commonly used term, it's also referred to as ILP for Information Leak Prevention, or EPS, Extrusion Prevention Systems. Usually, these systems are installed as a network-based DLP or a Cloud-based DLP. For example, my company happens to use a Cloud-based DLP through Google's G Suite. Anytime one of our employees tries to send information outside of our own domain through email, that email is flagged and they have to verify that they understand the data is being sent outside of Dion Training.

NIPS & NIDS

Now, we've already spoken a little bit about intrusion detection and intrusion prevention systems earlier on in this course. In this lesson, though, we're going to focus on the differences between a network-based IDS and a network-based IPS.

A Network Intrusion Detection System, or a NIDS, is a type of IDS that attempts to detect malicious network activities, for example, port scans and denial of service attacks. Generally, your Network Intrusion Detection System will be placed into what's known as promiscuous mode. This allows it to see all of the traffic that crosses the network instead of just the traffic that's destined for its own Mac address.

A Network Intrusion Prevention System, or NIPS on the other hand, is a type that's designed to inspect traffic and based on its configuration or security policy, it can also remove, detain, or redirect that malicious traffic.
That means a NIPS can not only detect it and log it like an IDS does, but it can also stop that ongoing attack by blocking the IP address that's causing issues or shutting down the connection.

Now, a NIPS or a NIDS may have a built-in protocol analyzer embedded into their system. This is usually done to allow the device to decode application layer protocols like HTTP, SMTP, FTP, Telnet, and others. And then, it passes that data that's contained in those protocols, over to the signature engine of the NIDS or the NIPS for further analysis. This allows the devices to create their own baseline of what normal looks like for the network and also helps to identify what abnormal might be for its behavioral or anomalous traffic detection functions.

UTM

The unified threat management or UTM system is a newer concept that was introduced in the last five to 10 years. Basically, security professionals realize, as I'm sure you're realizing now too, that relying on a single firewall is not enough to protect our networks, and so a UTM was created. Now, a unified threat management system is a combination of network security devices and technologies that are added to a network to better protect it. Simply put, a UTM is a single device that combines many other devices and technologies into it. For example, your UTM might include a firewall, a network intrusion detection system, or a network intrusion prevention system, a content filter or a proxy, an antivirus or anti-malware gateway, a data loss prevention system, and maybe even a site-to-site VPN, if you have the need.

You may have also heard the term, **Next Gen Firewall, or Next Generation Firewall, also known as NGFW.** If you've heard this term, it's because it's being used in the industry instead of using the term **UTM** or unified threat management. These are those all-in-one security devices and that's all a Next Generation Firewall is.