Hoofd1-8

Hoofdstuk : OSPF Features and Characteristics

OSPFv2 is used for IPv4 networks

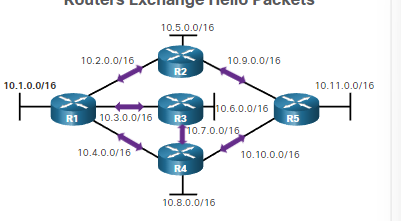
SPF has significant advantages over RIP in that it offers faster convergence and scales to much larger network implementations.rip kan niet werken in larger networks

A link is an interface on a router. A link is also a network segment that connects two routers, or a stub network such as an Ethernet LAN that is connected to a single router. Information about the state of a link is known as a link-state. All link-state information includes the network prefix, prefix length, and cost.

Components of OSPF :

* Routing protocol messages : hello packets,database description packet, linkstate request packet and link state update packet and link state acknowledge packet => doel neighbor discovery
* Database structure : ospf databases => adjency database : neighbor table, link state database : topology table , forwarding database : routing table
* Algoritm : he SPF algorithm is based on the cumulative cost to reach a destination, OSPF places the best routes into the forwarding database, which is used to make the routing table.

Link-State Operation

* he following are the link-state routing steps that are completed by a router:
* 
  + **Establish neighbor adjacensie** : hello packets => om tew eten of er neighbors zijn (ospf enabled routers) If a neighbor is present, the OSPF-enabled router attempts to establish a neighbor adjacency with that neighbor.
  + **Exchange link state advertisement** : Afbeelding met tekst, schermopname, diagram, lijn

    Automatisch gegenereerde beschrijving

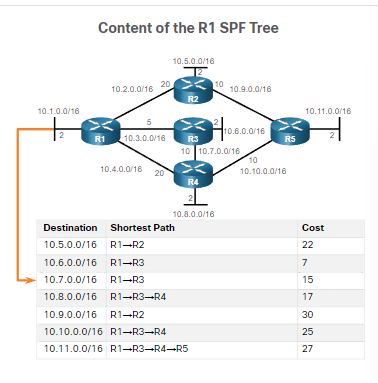
Na de adjecensie dan word er lsa’s gestuurd soor elke router. De ls geeft de state en de cost van elke connected link.

* + **Nadat de lsa is gedaan** dan gaat de router een topology table maken zodat ze weten hoe de netwerk in de ospf eruit ziet van die area
  + **Execute the spf algoritm** : spf algotritm word dan gebruikt om de spf tree te maken

Afbeelding met tekst, diagram, schermopname, ontwerp

Automatisch gegenereerde beschrijving

* **Choose best path** : maakt de beste pad naar waar je wilt gaan. Dit gebuerd naar de spf tree



**Single-Area OSPF** - All routers are in one area. Best practice is to use area 0.

**Multiarea OSPF -** OSPF is implemented using multiple areas, in a hierarchical fashion. All areas must connect to the backbone area (area 0). Routers interconnecting the areas are referred to as Area Border Routers (ABRs).

**Multiarea OSPF**

For instance, any time a router receives new information about a topology change within the area (including the addition, deletion, or modification of a link) the router must rerun the SPF algorithm, create a new SPF tree, and update the routing table. The SPF algorithm is CPU-intensive and the time it takes for calculation depends on the size of the area.

Als uw lsdb te groot is dan gaat de load of de cpu increasen : oplossing :

Afbeelding met tekst, Lettertype, schermopname, informatie

Automatisch gegenereerde beschrijving

Ospfv3 :

Gebruikt ipv6 addressen ,

OSPFv3 has the same functionality as OSPFv2, but uses IPv6 as the network layer transport, communicating with OSPFv3 peers and advertising IPv6 routes. OSPFv3 also uses the SPF algorithm as the computation engine to determine the best paths throughout the routing domain.

Ospfpackets :

Afbeelding met tekst, Lettertype, schermopname

Automatisch gegenereerde beschrijving

Linkstate update :

Lsu worden gebruikt wanneer er een lsr word gestuurd maar ze worden ook gebruikt wanneer de osf routing updates dan word er lsu’s gestuurd.

Een lsu contains one or more lsa’s

Lsa contains route information for the destination

Hello packkets :

Discover neighbors

Advertise parameters on which two routers must become neighbours

Elect dr,bdr on multiaccess networks

Point to point state do not require dr en bdr

Laat zien wat allemaak in de ospfpacket hello packet :

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

Ospf operation :

Ospf operational states

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Establish neighbor adjencensie

When OSPF is enabled on an interface, the router must determine if there is another OSPF neighbor on the link. To accomplish this, the router sends a Hello packet that contains its router ID out all OSPF-enabled interfaces. The Hello packet is sent to the reserved All OSPF Routers IPv4 multicast address 224.0.0.5. Only OSPFv2 routers will process these packet

router ID is a 32-bit number formatted like an IPv4 address and assigned to uniquely identify a router among OSPF peers.

When a neighboring OSPF-enabled router receives a Hello packet with a router ID that is not within its neighbor list, the receiving router attempts to establish an adjacency with the initiating router

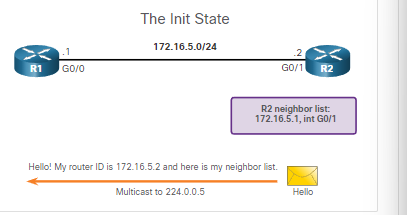
Down state to initstate =

Afbeelding met tekst, schermopname, diagram, lijn

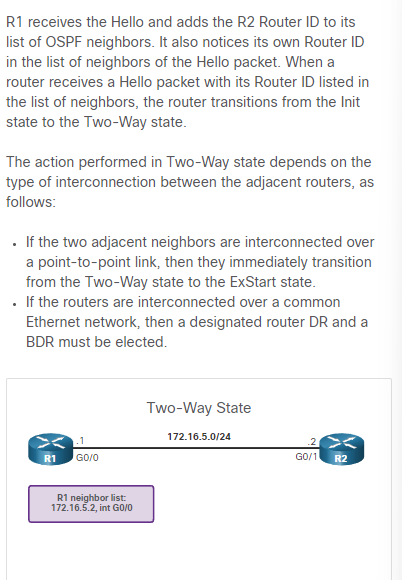
Automatisch gegenereerde beschrijving

The inti state =

Zet de router id van r1 in de neighbor table en dan stuurt een hello terug naar r1



Two way state = In the "Two-Way" state, routers have received Hello packets from each other, and they have confirmed that they can reach each other. However, they have not yet agreed to form a full neighbor relationship.



Elect the d rand bdr :

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Synchronizing OSPF Databases :

After the Two-Way state, routers transition to database synchronization states

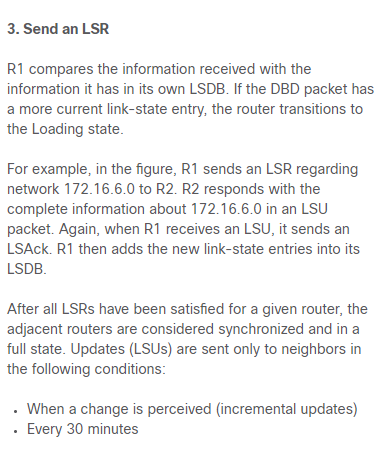
Decide first router = with higher router id die router suurt als eerst de dbd paketten in de exhchange state

Exchange dbd =

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Send a lsr =



Why is there a need for a DR:

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Afbeelding met tekst, Lettertype, schermopname, algebra

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, nummer

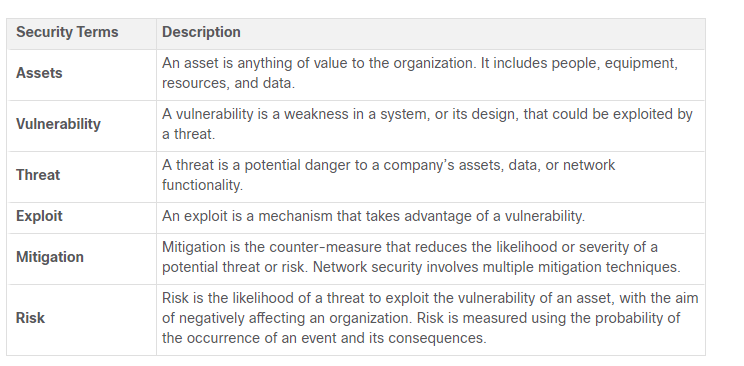
Automatisch gegenereerde beschrijving

Als je een dr hebt en bv router 1 is een dr en router 2 wilt een lsa sturen dan gaat de lsa naar de dr en de dr stuur de lsa naar iedereen.op dit mannier stuurt niet elke router een lsa maar alleen de dr

Hoofstuk : network security concepts :

Current state of cyber security

Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people’s privacy, and compromise the integrity of information. These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and can even threaten public safety.



Assets must be identified and protected. Vulnerabilities must be addressed before they become a threat and are exploited. Mitigation techniques are required before, during, and after an attack.

Vectors of Network Attacks

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure. For example, threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.

Afbeelding met tekst, diagram, schermopname, ontwerp

Automatisch gegenereerde beschrijving

DoS attack occurs when a network device or application is incapacitated and no longer capable of supporting requests from legitimate users.

An internal user, such as an employee, can accidentally or intentionally:

* Steal and copy confidential data to removable media, email, messaging software, and other media.
* Compromise internal servers or network infrastructure devices.
* Disconnect a critical network connection and cause a network outage.
* Connect an infected USB drive into a corporate computer system.

Internal threats zijn gevaarlijker dan external threats want die internal heeft direct acces to de building and its infrastructure decvices.

Data Loss

Data is de belangrijkste asset van een organisatie.

Data loss is wanneer de data perongeluk of express word verloren of gestolen of geleaked naar de buiten wereld.

Gevolgen van data loss:

* Brand dammage of loss reputation
* Loss of competitive advandatage
* Klanten kwijt
* Loss of revenu
* Litigation/legal action resulting in fines and civil penalties
* Significant cost and effort to notify affected parties and recover from the breach

Hoe data loss kan gebueren

* Email/social networking : email of im messages opvangen en revalen van confidential information
* Unencrypted devices : de dief kan makkelijk aan de confindetial info als er geen encrytion op is
* Cloud storage devices : Sensitive data can be lost if access to the cloud is compromised due to weak security settings.
* Removable media : One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another risk is that a USB drive containing valuable corporate data could be lost
* Hard copy : confidential data should be shredded when no longer needed
* Improper access control : password of zwakke password is gecomprimes waardoor de threat actor makkelijk aan de corporate data kan.

Network security professionals must protect the organization’s data. Various Data Loss Prevention (DLP) controls must be implemented which combine strategic, operational and tactical measures.

Threat actors

The hacker

Originally the term referred to someone who was a skilled computer expert such as a programmer and a hack was a clever solution.

White hat hackers : these hackers users their programming skills voor legak purposes. Zoekt security vulnerabilities and reports to developers for them to fix before the vulnerabilities can be exploited.

Gray hat hacker : These are individuals **who commit crimes and do arguably unethical things**, **but not** for personal gain or to cause damage. Gray hat hackers may **disclose a vulnerability to the affected organization after having compromised their network.**

**Black hat hacker :** These are unethical criminals who compromise computer and network **security for personal gain, or for malicious reasons, such as attacking network**

In this course, we will not use the term hacker outside of this module. We will use the term threat actor. The term threat actor includes hackers. But threat actor also includes any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack.

Evolution of hackers :

Modern hacking terms :

**Script kiddies** : gebruikt een **exisitening script** to cause harm. Not for profit

**Vulnerability broker** : gray hat hacker => **discover exploit** and report to vendors soms voor geld

**Hacktitvis :** gray hat hacker => **publicly protest organizations** or governments by posting articles, videos, leaking sensitive information, and performing network attacks.

**Cyber criminals** : black hat hackers => **self employed** of werken voor een **groote cyber crime organisation**

**State-sponsored** : white hat hacker of black hat hacker => who **steal government secrets**, gather intelligence, and sabotage networks. **Their targets** **are foreign governments**, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

Cyber Criminals

It is estimated that cyber criminals steal **billions of dollars from consumers and businesses**. Cyber criminals operate in an **underground economy where they buy, sell, and trade attack toolkits**, zero day exploit code, botnet services, banking Trojans, keyloggers, and much more. They also **buy and sell** the **private information and intellectual property they steal**. Cyber criminals target small businesses and consumers, as well as large enterprises and entire industries.

Hacktivists

Two examples of hacktivist groups are Anonymous and the Syrian Electronic Army. **Although most hacktivist groups are not well organized,** they can cause significant problems for governments and businesses. Hacktivists tend to rely on fairly basic, freely available tools

State-Sponsored Hackers

State-sponsored hackers create advanced, customized attack code, often using previously **undiscovered software vulnerabilitie**s called zero-day vulnerabilities. An example of a state-sponsored attack involves the Stuxnet malware that was created to damage Iran’s nuclear enrichment capabilities.

Threat actor tools :

Evolution of Security Tools

Penetration testing tool :

**Password crackers** : crack or recover password. Password **repeadetly make geusses** until it cracks the password. John the ripper

**Wireless hacking tools** : hack into a wireless network **to detect security vulnerabilities**. Vb kismet

**Network scanning and hacking tools** : probe network devices, servers, and hosts for open TCP or UDP ports**. Vb nmap**

**Packet crafting tool : robe** and test a firewall’s robustness using **specially crafted forged packets**.vb Hping

**Packet sniffers : capture** and **analyze packets within** traditional Ethernet LANs or WLANs.wireshark

**Rootkit detectors :** his is a directory and **file integrity checker** used **by white hats to** detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter. White hacker

**Fuzzers to search** vulnerabilities : **discover computer security vulnerabilities** vb skipfish

**Forensic tools** : white hackers => **sniff any trace of evidence of a existing computer** vb HELIX

**Debuggers :** black hat hacker : **reverse engineer binaru files** when **writing exploits**.word ook gebruikt bij white hat **hackers om malware te anylazinge.vb** winDbg

**Hacking operarting systems** : os made for hacking vb kali linux. **Pre installed hacking tools in os**

Encryption tools : **openssh, openssl**

**Vulnerability exploitation tools** : identify whether **a remote host is vulnerable to a security attack**. Vb metaspoit

**Vulnerability scanners** : scan a network system to identify open ports . kan ook gescanned worden voor known vulnerability and scan vm’s vb NIPPER

Many of these tools are UNIX or Linux based; therefore, a security professional should have a strong UNIX and Linux background.

Attack Types

**Eavesdropping attack :** listen to network traffic => andere naam is sniffing of snooping

**Data modification attack :** If threat **actors have captured enterprise traffic**, they can alter the data in the packet without the knowledge of the sender or receiver.

**Ip address spoofing attack** : A threat actor **constructs an IP packet** that appears to originate from a valid address inside the corporate intranet

**Password based attack** : if threat actors **discover a valid user account**, the threat actors have the **same rights as the real user.** Threat actors could use that valid account to obtain lists of other users, network information, change server and network configurations**, and modify, reroute, or delete data.**

**Denial of service attack (dos) :** A DoS attack prevents normal use of a computer or network by valid users. A DoS attack can **flood a computer or the entire network with traffic** until a shutdown occurs because of **the overload**. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.

**Man in the middle attack** : this attack occurs when threat actors have positioned themselves **between a source and destination.** They can now actively monitor, capture, and control the communication transparently.

**Compromised key attack** : threat **actor obtiain secrect key.** That key becomes a **compromised key**. A compromised key can be used to gain **access to a secured communication** without the sender or receiver being aware of the attack.

**Sniffer attack** : sniffer is an application or device that can **read, monitor, and capture network data** exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

Malware

Viruss and trojan horsa

Virus

The first and most common type of computer malware is a virus. **Viruses require human action to propagate and infect other computers**. For example, a virus can infect a computer when a victim opens an email attachment, opens a file on a USB drive, or downloads a file.

Viruses can:

* Alter, corrupt, **delete files**, or erase entire drives.
* Cause computer **booting issues**, and corrupt applications.
* Capture and **send sensitive information** to threat actors.
* Access and use **email accounts** to spread.
* Lay dormant until summoned by the threat actor

**Boot sector virus** : attacks boot sector,file partion, file system

**Firmware viruss** : attacks device firmware

**Macro virus** : Virus uses the MS Office or other applications macro feature maliciously.

**Program virus** : Virus inserts itself in another executable program.

**Scritp viru**s : Virus attacks the OS interpreter which is used to execute scripts.

Trojan horse :

Threat actors use Trojan horses to compromise hosts. **A Trojan horse is a program that looks useful** but also carries malicious code. Trojan horses are often provided with free online programs such as computer games. Unsuspecting users download and install the game, along with the Trojan horse.

**Several types of trojan horses :**

* **Remote access** : Trojan horse enables unauthorized remote access.
* **Data-sending** : trojan horse provides , the threat actor with sensitive data, such as passwords.
* **Destructive : c**orrupts or deletes files
* **Proxy :** use a victim device as a source device to attack and preform illegal activities
* **ftp :** enables unauthorized file transfer services on end devices
* **security software disabler** : stops antivirus programs or firewalls
* **dos** : slows or halts network activity
* **keylogger :** steal confidential info such as credit card

Viruses and Trojan horses are only two types of malware that threat actors use. There are many other types of malware that have been designed for specific purposes.

Other types of malware :

**Adware** : usually distributed **by downloading online software**., **Pop-up windows** may be difficult to control as new windows can pop-up faster than the user can close them

**Ransomware** : **denies user access to their files bc of encryption** by the threat actor and ask for ransom for the key , users without up to date backups must pay ransom, payment usually crypto

**Rootkit** : **admin level access to a computer, difficult to detect** , They can provide a backdoor to threat actors giving them access to the PC, and allowing them to upload files, and install new software to be used in a DDoS attac,

**Spyware** : similar to **addware, but used to gather information about the user and send to** threat actors without the user’s consent., Spyware can be a low threat, gathering browsing data, or it can be a high threat capturing personal and financial information.

Worm : worm is a self-replicating program that propagates automatically without user actions by exploiting vulnerabilities in legitimate software**. The intent of a worm is usually to slow or disrupt network operations.**

Common network attacks :

Reconnaissance attack :

Reconnaissance = means gather info about the enemy doel om de zwakheden te vinden

Threat actors use reconnaissance (or recon) attacks to **do unauthorized discovery and mapping of systems, services, or vulnerabilities. Recon attacks precede access attacks or DoS attacks.**

Some of the techniques used by malicious threat actors to conduct reconnaissance attacks are described in the table:

**Preform an info query of a target :** initial info about the target vb tool googlesearch

**Initate a ping sweep of the target network** : reveals target network address . with ping sweep you can know which ip address is active

**Intitate a port scan of active ip addresses** : to deteminis which port or sercices are available ; vb netscan

**Run vulnerability scannners** : to determine the type and version of the application and operating system that is running on the host. vb Nipper

**Run exploitation tools** : discover vulnerable services that can be exploited. Vb metaspoit

Access attacks :

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services.

**Doel =**> retrieve data, gain access, or to escalate access privileges to administrator status.

**Password Attacks** : hreat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.

**Spoofing attacks :** , the threat actor device **attempts to pose as another device by falsifying** data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing. These spoofing attacks will be discussed in more detail later in this module

**Other Access attacks include:**

* **Trust exploitations** : threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.
* **Port redirections :** In a port redirection attack, a threat actor uses a compromised system as a base for attacks against other targets. The example in the figure shows a threat actor using SSH (port 22) to connect to a compromised Host A
* **Man-in-the-middle attacks : is al uitgelegd**
* **Buffer overflow attacks :** In a buffer overflow attack, the threat actor exploits the buffer memory and overwhelms it with unexpected values. This usually renders the system inoperable, creating a DoS attac

Social engineering attack :

Social engineering is an access attack that attempts **to manipulate individuals** into performing actions or divulging confidential information. Some social engineering techniques are **performed in-person while others may use the telephone or internet.**

**Social engineers often rely on people’s willingness to be helpful. They also prey on people’s weaknesses.**

**social engineers techniek :**

**pretexting** : A threat actor **pretends to need personal** or financial data to confirm the identity of the recipient

**phishing** : A threat actor sends fraudulent email **which is disguised as being from a legitimate**, trusted source to trick the recipient into installing malware on their device

**spear phising** : A threat actor creates a targeted phishing attack tailored **for a specific individual** or organization.

**Spam :** Also **known as junk mail**, this is unsolicited email which often contains harmful links, malware, or deceptive content.

**Baiting :** A threat actor leaves a **malware infected flash drive in a public location.** A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware

**Impersonation :** This type of attack is where a **threat actor pretends to be someone they are** not to gain the trust of a victim

**Tailgating :** This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.

**Shoulder surfing :** This is where a threat actor **inconspicuously looks over someone’s shoulder to steal their passwords or other information.**

**Dumpster diving** : This is where a threat actor rummages through **trash bins to discover confidential** documents.

**he Social Engineering Toolkit (SET) was designed to help white hat hackers and other network security professionals create social engineering attacks to test their own networks.**

**DoS and DDoS Attacks**

Afbeelding met tekst, Lettertype, lijn, schermopname

Automatisch gegenereerde beschrijving

DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled threat actor.

A Distributed DoS Attack (DDoS) : s **similar to a DoS attack, but it originates from multiple, coordinated sources**. making it a zombie that can communicate with the CnC system. The collection of zombies is called a botnet. **When ready, the threat actor instructs the CnC system to make the botnet of zombies carry out a DDoS attack.**

**IP Vulnerabilities and Threats**

IPv4 and IPv6

IP does not validate whether t**he source IP address contained in a packet actually came from that source**. For this reason, threat actors can send packets using a spoofed source IP address.

**Icmp attacks** : Threat actors use Internet Control Message **Protocol (ICMP)** echo packets (pings) to **discover subnets and hosts on a protected network**, to generate DoS flood attacks, and to alter host routing tables.

**Amplification and reflection attacks** : Threat actors attempt **to prevent legitimate users** from **accessing information or services using DoS** and DDoS attacks.

**Address spoofing attacks :** Threat actors spoof the source IP address in an IP packet to perform blind **spoofing or non-blind spoofing**.

**Man in the middle attack** :  or alter packets and forward them to their original destination.

**Session hijacking** : Threat actors gain access to the physical network, and then use an MITM attack to hijack a session.

**ICMP Attacks**

Threat actors use ICMP for **reconnaissance an**d scanning attacks. They can launch information-**gathering attacks to map out a network topology,** discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors also **use ICMP for DoS attacks.**

**Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the interne**

Common ICMP messages of interest to threat actors are listed in the table:

**CMP echo request and echo reply :** This is used to **perform host verification** and DoS attacks.

**ICMP unreachable** : This is used to perform network reconnaissance and scanning attacks.

**ICMP mask reply** : This is used to map an internal IP network.

**ICMP redirects :** This is used to lure a target host into sending all traffic through a compromised device and create a MITM attack.

**ICMP router discovery :** This is used to inject bogus route entries into the routing table of a target host.

Amplification and Reflection Attacks

Threat actors often use amplification and reflection techniques to create DoS attacks. The example in the figure illustrates how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.

Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving

: Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.

Address Spoofing Attacks

IP address spoofing attacks occur when a threat actor **creates packets with false source IP address** information to either hide the identity of the sender, or to pose as another legitimate user. The threat actor can then gain access to otherwise inaccessible data or circumvent security configurations. Spoofing is usually incorporated into another attack such as a Smurf attack.

**Non-blind spoofing** : can see the traffic between the host and the target. the threat actor uses non-blind spoofing **to inspect the reply packet from the target victim**. Non-blind spoofing determines the **state of a firewall and sequence-number prediction.** It can also hijack an authorized session.(has some knowledge about the target system)

**Blind spoofing** : The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks**.(has no knowledge of the targer system**)

In both cases, the term "spoofing" generally refers to the act of pretending to be someone or something else to gain unauthorized access or deceive a system. Common examples include IP spoofing, email spoofing, or MAC address spoofing.

TCP and UDP Vulnerabilities

TCP Services

**Reliable delivery : TCP** incorporates acknowledgments to guarantee delivery, instead of relying on upper-layer protocols to detect and resolve errors. If a timely acknowledgment is not received, the sender retransmits the data.

**Flow control** : TCP implements flow control to address this issue. Rather than acknowledge one segment at a time, multiple segments can be acknowledged with a single acknowledgment segment.

**Stateful communication :** TCP stateful communication between two parties occurs during the TCP **three-way handshake**. Before data can be transferred using TCP, a three-way handshake opens the TCP connection, as shown in the figure. **If both sides agree to the TCP connection, data can be sent and received by both parties using TCP.**

**Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving**

TCP Attacks

TCP SYN Flood Attack : The TCP SYN Flood attack exploits **the TCP three-way handshake.** The figure shows a threat actor continually **sending TCP SYN session** request packets with **a randomly spoofed source IP address to a targe**t. The target device **replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet**. Those responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections, and **TCP services are denied to legitimate users**.

Afbeelding met tekst, schermopname, diagram, ontwerp

Automatisch gegenereerde beschrijving

**TCP Reset Attack** : TCP reset attack can be **used to terminate TCP communications** between two hosts. TCP can terminate a connection in a civilized (i.e., normal) manner and uncivilized (i.e., abrupt) manner.

**TCP Session Hijackin : TCP session hijacking is another TCP vulnerability. Although difficult to conduct, a threat actor takes over an already-authenticated host as it communicates with the target. The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host. If successful, the threat actor could send, but not receive, data from the target device.**

**UDP Segment Header and Operation**

UDP is commonly used by DNS, TFTP, NFS, and SNMP. UDP is a connectionless transport layer protocol. It has much lower overhead than TCP because **it is not connection-oriented** and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that provide reliability. The UDP segment structure, shown in the figure, is much smaller than TCP’s segment structure.

Overhead means extra data

UDP Attacks :

UDP is not protected by any encryption. he lack of encryption means that anyone can see the traffic, , and send it on to its destination. Changing the data in the traffic will alter the 16-bit checksum, , but the checksum is optional and is not always used. When the checksum is used, the threat actor can create a new checksum based on the new data payload, and then record it in the header as a new checksum. The destination device will find that the checksum matches the data without knowing that the data has been altered. This type of attack is not widely used.

**UDP Flood Attacks** :

A program sends a flood of UDP packets from a spoofed host to a server on the subnet sweeping through all the known UDP ports looking for closed ports. This will cause the server to reply with an ICMP port unreachable message

IP Services