**Hoofdstuk 1 : ospf**

* Ospfv2 => ipv4
* Spf is beter dan rip want spf kan werken in grotere netwerken
* A link is a interface in the router , also a segement or a stub network
* State of a link => linkstate

Components of ospf

* Routing protocol message , hello messages, linkstate request …
* Database structure => ospf database , adjencensie table
* Algorithm => choose best route

Linkstate operation ;

* Establish neighbor adjencie : hello packet => zoekt neighbors als er is => establish neighbor adjencie
* Exchange linkstate advertisement
* Topology table
* Spf algorithm
* Choose best path

Single area ospf : alle routers in one area => area 0

Multi area ospf ; multiple areas , must be connecte to the backbone area 0, ABRS

Multi area ospf:

* Topology change in a area new spf algoritim to update the routing table. It takes time depending on the size of the area

Lsdb is te groot oplossing:

* Smaller routing table
* Reduced link state update overhead
* Redueced frequency of spf calculations

Ospfv3

* Ipv6 addressen
* Doet het zelfde als ospfv2

Ospf packets :

* Hello packets
* Database description packet
* Link state request packet
* Linkstate update packet
* Linkstate acknowledgement packet

Linkstate update packet

* Lsu word gebruikt wnr er lsr word gestuurd , ze worden ook gebruikt wnr de ospf routing updare wilt sturen
* Een lsu contain one or more lsa’s
* Lsu contains routing info for the destination

Hello packets

* Discover neighbors
* Elects dr,bdr alleen op multiacces networks
* Point to point networks dont need dr en bdr

Ospf states:

* Down state => no hello, router sends hello,
* Init state => hello received from neighbor, router id of the sending neighbor
* Two-wat state => biderctional,elect dr, bdr,
* Exstart state => point to point decide who send the dbd(hoogste router id)
* Exchange state => echange dbd,full state
* Loading state => ls ren lsu voor extra of nieuwe info,spf algrothim
* Full state => fully synchronized

Establish neighbor adjencie:

* Send to all router ospf router interfaces to see if there are neighbors : 224.0.0.5
* Router id 32bit
* Als de ospf router de hello packet krijgt en ziet dat die router id niet in de neighbor lijst zit dat maakt de router een establish neighbor adjencie with the other router

Exhange dbd’s

* Router 1 sends dbd to r2
* R2 acknowleges the dbd using lsACK packet
* R2 sends dbd to r1
* R1 acknowledges r2

Lsu are only send when a change is perceived and every 30 minutes it wil send a lsu automatically

Why is there a need for dr:

* Zonder dr wanneer je flooding lsa doet dan krijg je :
  + Creation of multiple adjencie
  + Extensive flooding of lsa’s
* Flooding lsa : lsa word gestuurd naar alle routers en triggers dat alle router ook lsa’s hierdoor gaat trafiek chaotisch worden
* Lsa’s dr : 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 2 : network security concepts

Current state of cyber security :

* Assets : value
* Vulnerability : weakness
* Threat : potential danger
* Exploit : take advantage of vulnerability
* Mitigation : counter-measure
* Risk : negativily affecting the organnistion . probabililty of occurrence of a event and its consequences

Vectors of network attacks :

* Attack vector => path to gain access to a server host or network
* Vector => insider or outside
* Dos => cant no more support legitimate users

An internal user such as employees can accidently or intentionly

* Steal and copy confidentaily data
* Compromise internal servers
* Disconnect a network
* Connect a infected usb
* Internal threats zijn gevaarlijker dan external

Data loss :

* Data is de belangrijkste asset
* Gevolgen :
  + Brand dammage
  + Loss of commpetitive advantage
  + Klanten kwijt
  + Loss of revenu
  + Fines and civil penalties
  + Cost
* Hoe kan dit gebeuren :
  + Email social networking
  + Unencrypted devices
  + Cloud storage
  + Removable media
  + Hard copy
  + Improper acces control
* Dlp

Threat actors:

* White hat hacker : legal purpose
* Grey hat hackers : commit crimes but not for personal gain or to cause damage
* Black hat hackers : crimes for personal gain or malicious reasons
* Threat actor => hacker

Evolution of hacking:

* Scritp kiddies
* Vulnerabilitie broker
* Hackitivist
* Cyber criminals
* State-sponsored

Cyber criminals

* Steal billions of dollars of businesses , operate in underground economy,targets are small businesses and consumers as well as large businesses

Hactivist :

* Not well organized
* Use fairly basic and free tools

State sponsored :

* Advanced code n undiscoverd software vulnerabilities

Threat actor tools

* Password crackers => repeadetly make guesses
* Wireless hacking tools => security vulnerabilities
* Network scanning and hacking tools => probe network devices
* Packter crafting tool => robe and test firewalls
* Packet sniffer => capture and anylize packets
* Rootkit detectors => file integrity checker
* Fuzzers to search => discover computer security vulenerbilities
* Forensic tools => SNIF ANY TRACE OF EVIdence of a existing computer
* Debugger : write exploit
* Hacking os => os with hacking tools
* Vulnerability exploits tools
* Vulenbility scanner

Many tools ar unix or linux based

Attack types :

* Eavesdropping attack => listen to network
* Data modification => alter data
* Ip address snooping attack => construnt a ip packet
* Password based attack =
* Denial of service
* Man in the middle
* Compromised key attack
* Sniffer attack

Malware

Virus

* Human action to progate and infect other computers
* Viruses can :
  + Delete files
  + Booting issues
  + Send sensitive data
  + Access email accounts
* Boot sector virus
* Firmware virus
* Macro virus
* Program virus
* Script virus

Trojan horse

* Program that looks useful but has malicious code => free online programs
* Types of trojan horses :
  + Remote access
  + Data sending
  + Desctructive
  + Proxy
  + ftp
  + security
  + dos
  + keylogger

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
* ransomware
* rootkit => admin leve access to a computer
* spyware => get info and send to threat actor
* worm => to slow or disrupt network operations

common network attacks:

raconnaisance attack :

* means gather info
* access or dos attacks
* techniques for reconnaissance attack :
  + info querie on target
  + intiate ping sweep
  + intiat port scan of active ipaddress
  + run vulnerability scanners
  + run exploitation tools

access attack :

* passoword attacks
* spoofing attack : attempts to pose as a other devide by falsifying data
* trust exploitations : use unauthorized privileges to gain access to the system
* port redirections :use compromised system as a base to attack other targets
* man in the middle
* buffer overflow attack: exploits the buffer memory and overwhelm it with unexpected values

social engineering attack :

* manipulate individuals
* in person or telephone or internet
* prey on people’s weakness
* telephone scammers

social engenieering techiniek

* pretexting
* phising
* spear phising
* spam
* baiting
* impersonation
* tailgating
* shoulder surfing
* dumpster diving

**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 end dos attacks**

* overwhelming quantity of traffiq
* maliciously formatted packets
* ddos almost the same as dos but the attacks originates from multiple coordinated sources=> zombie that can communicate with the cnc , the treat actor uses the cnc so that the zombies carry the ddos attack.

Ip vulnerabilities and threats

Ipv4 en 6

* IP does not validate whether the 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 attack => discover subnets and hosts to generate dos
* Ampliciatiion and reflection attacks : prevent legimate use to access services => dos
* Address spoofing attacks
* Man in the middle
* Session hijacking

Icmp attack :

* Gather info
* Counter measure is icmp acls
* Icmp messages that interest the threat actor:
  + Cmp echo request en reply
  + Icmp unreachable
  + Icm mask reply
  + Icmp redirects
  + Icmp router discovery

Amplification and reflection

* Create dos attacks
* Dns amplification and reflection en ntp amplification and reflection

Address spoofing attacks :

* False source ip addres , to pose as a legimate user
* Non-blind spoofing : inspect the reply packet from the target , can see the traffic being sent between host and target
* Blind spoofing : cannot see the traffic that is being sent between host and target => use dos attacks

Tcp and udp vulnerability

* Tcp services
  + Reliable deliviery : guarantee delivery
  + Flow control : multiple segment can be acknowledged with a single acknowledgement segment
  + Staefull communinication
  + Three way hand shake: if both side aggree to tcp connection only then data can be sent
* Tcp attacks
  + Tcp syn flood attack : exploit the three way handshake: so the threat actor send multiple syn request to a webserver the webserver sends multiple syn acks and wait but then the legimate user send a syn reques and now is the webserver confused en hierdoor kan de legimate user niet naar de webserver gaan
  + Tcp reset attack : terminate tcp communications
  + Tcp session hijacking : a threat actor takes over an already-authenticated host as it communicates with the target.

Udp segment header and operations

* No retransmisioon because not connection oriented , je krijgt geen replys
* Udp attack : uDP is not protected by any encryption. he lack of encryption means that anyone can see the traffic.
* Udp flood attack : gewoon vorm van dos

Ip services :

* Arp vulnerbilities :
  + Unsolicited arp reply (gratuitous arp)
  + First boot => inforl new mac address
  + Arp => doel is mack wetel van device
  + Arp cashe poisoning : doel target a victim host, and have it change its default gateway to the threat actor’s device. This positions the threat actor in between the victim and all other systems outside of the local subnet.
  + Passive arp poisoning => steal data
  + Active arp poisoning => modify data

Dns attacks :

* Dns resolver attack :
  + Dns cashe poisoning : spoofed records info to dns resolver to redirecto user to malicious sites
  + Sns amplification and reflection : use dos attacks
  + Dns resource utilization attack : consumes the resources of the dns opensolver
* Dns stealth attack : hide identity
  + Fast flux
  + Double ip flux
  + Domain generatio algorithm :
  + Dns shadowing attacks
* Dns tunnelling
  + It’s a method od sending data covertly by hiding it within the dns protocol
  + Opendns blocks dns tunnelling

Dhcp

Dhcp attacks

* Dhcp spoofing attack

Network security best pactrices:

* Confidentialy
* Integrity
* Availability

The defense in depth approach

* Secure communication across both public and private networks
* Vpn
* Ips
* Esa/was
* Aaa server

Firewalls

* Access control policy between networks
* All firewalls share common properties
  + Resisitant to networks attacks
  + All traffic flows through the firewall
  + Enforce the access control policy
* Benefits of firewall
  + Prevent the exposure of sensitive hosts, resource and applications to trusted users
* Limitations
  + Misconfigured firewall can have serious consequences=> single point of failure
  + Can slow down
  + Unauthorized traffic can be tunneled or hidden
* Ids e nips detect pattern in network traffic usiding signatutes, => to detect malicious activity
* Signature patterns Single packet en multi packet

Content security appliance :

* Esa : check emails
* Was : controlling web traffic

Cryptography :

* Four element of secure information
  + Data integrity
  + Origin authentication
  + Data confidentiality
  + Data non-repudiation
* Hash function
  + Md5 128 bit , niet aangeraden gebruike sha2 of 3
  + Sha hashing algoritm 160bit
  + Sha-2
  + Sha-3
  + Man in the middle kan de hash veranderen
* Hashing algorithms only protect against accidental changes and does not protect the data from changes deliberately made by a threat actor.
* Origin aurhincation : hmac
* Data confidentiality
  + Symmetric encryption : des , 3des , aes and uses one key
    - Block cypher and stream ciphers
  + Asymmetric : public and private key, rsa, difie helmann dss, dh

Hoofdstuk : acl concepts