# **Firewall:**

1. Rules ACL

IP port

**3 soorten firewalls:**

1. Packet Filter:

Als de destination poort boven poort 1024 is , doe laat die da door. Maar zo laat ge teveel poorten openstaan

1. Statefull Firewall

OSI-Model laag 5: Sessie laag

* De socket informatie (IP met poort) , communicatie van socket naar socket.
* Na contact komt die terug bij de firewall, Als die sessie in de firewall staat dan laat die die door.

1. Proxy Firewall (Deep Packet Inspection)

OSI-Model lag 7: Data lag

Proxy server gaat modules hebben, als die bv op http moet filteren moet die een http module hebben, voor ftp ftp modules, op email smtp/ pop3 /Imap modules,…

Maar hoe hoger de security hoe slechter Usebility.

Als hacker: Overload de proxyserver zodat die zijn eigen uitzet wegens hoge CPU usage 🡪 netwerk firewall valt uit 🡪 gateway blijft open dus hacker kan erin.

**Op’t examen de 3 verschillende kunnen uitleggen**

# **Virussen en Wormen:**

Basis van een virrus en een worm:

Wat is het doel ervan: Replicatie / kopiëren zodat ze meerder systemen kan infecteren

Ze hebben verschillende soorten payloads en triggers.

Virus doet aan replicatie door een user interaction, een worm kopieerd zijn eigen, deze gebruikt meestal network vurnibilatys. 🡪 voila exploit 🡪 dan kijkt die bv bij u thuis , ziet vurnibilatys en exploit dan andere pc’s

2 Belangrijke kenmerken van virussen en wormen:

1. Ze moeten Stealth zijn
2. Ze moeten polimorph zijn

Een virus dat zich gewoon op et internet bevint noemt men een virus in the wild. (Der is een Virus Wild List)

Stealth cababilies, verbergen voor virus scanners 🡪 hoe doen ze dit?

Niet direct uwe payload uitvoeren, niet direct triggeren. Deze pas later uitvoeren.

Virussen gaan zich ergens nestelen ipv echte code

Polimorph zijn is u eigen kopieren maar iedere keer een beetje anders zodat ze niet direct alles ineens kunnen deleten. Want u Byte code veranderd.

2 virussen kennen:

1. Boot Sector Infector
2. Memetisch Virus

Boot Sector infector is een virus die in de bootcode gezet staat.

Een memetisch virus een virus of the mind 🡪 hoax 🡪 een soort van kettingbrief 🡪 bv als je zoekt op system 32 , da is een virus 🡪 deleten.

**Trojan**

Bv een free antivirus die zegt ge hebt zoveel virussen maar tegelijk opent die ne backdoor

Voor het examen moet je kennen dat er verschillende nieveaus van trojan, maar je komt redelijk snel bij rootkits.

15 jaar geleden: RAT (Remote Acces Tool) 🡪 wat nu Remote acces Trojan noemt) Backdoor maken in een programma zodat ge kon inloggen voor u gebruiker te helpen, maar hackers vonden dit ook.

Application Level Trojan gaan op u target een extra service instaleren, het probleem was als die client een service instaleerd heeft die maar een stomme windows firewall. Dus op moment dat men target een bepaalde service is geinstaleerd die een bericht stuurt naar ‘de hacker’ zodat ge eens sessie hebt en dan kunt ge door die firewall. Bij exploits gebruitk ge hiervoor Reverse TCP binding.

Volgende evoluties van Trojan: Rootkits

Rootkits was ne hacker die veel aant spelen was op zijn pc, en wa die proeerde was rootacces krijgen. En op moment da die op die pc zat ging die keyloggers instaleren enzo. Maar al die programma’s moesten steatlh zijn. Vandaag wordt dat gebruikt voor stealth mode. Een rootkit gaat ge nodig hebben voor u ding te shielden van virus scanners. Maar de service die ge gaat instaleren op u target gaat ge hiden van virus scanners. Ge gaat een service pakken die essentieel is voor u operating system en u backdoor hernoemt ge naar da. Als u virus scanner da da probeert de deleten delete die iets essentieel.

De volgende evolutie van rootkits gaan ze in de kernerl proberen te zetten.

Kernel Based Rootkits: virus scan wilt bepaalde bytecode scanenen , dus die gaat bepaalde services van de kernel moeten opvragen voor de scan te doen van bytcode (die in de hardware zitten) , dus als gij in de kernel zit als rootkit gaat ge dat hooken: “ Aaah ge wilt die code gaan checken , oke is goed hier is het antwoord” zo heeft de virusscanner niks door. Ge kunt dit niet zien in taskmaneger want ge zit in kernel mode.

# **Sniffers (Protocol analyser)**

U netwerk kaart gaat filteren op Destination Mac adress, maar als sniffer wilt ge net da ge alle data net hebt. Dit noemt Promiscuous mode 🡪 overspel modus.

Dus een hacker moet selectief te werk gaan, die gaat vooral TCP protocollen vangen. (200-300 eerste bytes hebben want daar staat u login gegevens in)

**Hoe beveiligt ge u daar tegen ?**

2 soorten beveiling:

1. Netwerk beveiling
2. Data beveiliging

Netwerk:

1. Alle netwerkkaarten pollen 🡪 op moment dat ge een host tegen komt die in promiscuous mode zit 🡪 blocken
2. Hashes maken van de belangrijkste systeem bestanden 🡪 dus als ge aan’t sniffen zijt dan is die hash veranderd, dus als gij da ni hebt gedaan is da malicious code
3. Segmentatie gaan doen: Veel switchen en routers erin zetten. Een switch is een filter, op wat gaat een switch filteren, mac adressen 🡪 hacker krijgt die data dus nooit. Maar hoe omzeilt ge dat? 🡪 Mac adress tabel volsteken , als die vol zit u eigen mac adres toevpoegen, kan der niet in , dus die switch gaat flooden.

Data:

1. Encrypteren