# Spoofing

Is u gaan voordoen als iemand anders

**TCP/IP**

IP tabel: rhost file (linux) hier wordt ingezet 🡪 hebt ge dit IP krijgt ge die rechten. Of geinstaleerd u eigen een backdoor.

TCP werkt volgens de 3 way handshake:

|  |  |  |
| --- | --- | --- |
| Client |  | Server |
| Eerste stap:  Ieder bericht heeft een Sequence nummer (random) en een ack nummer. bv seq nr= 50 en acknowledge nummer is leeg  Laatste stap:  Seq = 51 en ack is 81  Wilt ge spoofen moeten al die nummers kloppen. | SYN🡪 | Tweede stap:  Sequence number wordt random gekozen bv: 80  Acknowledge number: 51  (ik heb tot 50 ontvangen en moet nu 51 hebben zogezegt) |
| 🡨 Syn + ACK |
| ACK 🡪 |

Stap 1:

We gaan ons voordoen als Parren: 192.168.0.2

Eigen IP = 192.168.0.2

Parren gaat ons resetten als die da doorheeft, dus ge moet Parren “uitschakelen”

1. Parren lamleggen (DDoS) 🡪 SYN-flood

Ik ben hacker en ik ga een synvraag doen aan Parren

Parren geeft SYN + Ack

Ik reageer niet meer, dus TCP stuurt een bericht terug

Doet die 3 keer en dan reset die connectie, dus ge vraagt dat gewoon super veel aan.

Dan na een tijd gaat die buffer vollopen en die CPU gaat idle worden

1. SYN bericht naar de blade sturen

Non-blind spoofing vs. Blind spoofing

1. Non blind

Bercith wordt als hacker naar mij gestuurd

Berichtje moet langs mij komen zodat ge de sequence nummer kunt zien zodat je het acknowledge nummer kunt invullen.

ARP Poisoning, IP Source Routing

1. Blind Spoofing

Berichtje wordt niet naar de hacker gestuurd maar naar Parren, deze gooit het bericht weg.

1. Je moet het random getallee vinden , hoe doe je dit:

Het getal is pseudo random (Zijn afhankelijk van de system time)

Dus op voorhand een paar 1000 keer kijken welk getal gegenereert wordt (via een client pc)

Dan kan je kijken welke sort pseudo random functie gebruikt gaat worden

Enzo kan je voorspellen welk getal random gekozen wordt. Eens de connectie gemaakt is kan je gewoon met je TCP verkeer beginnen.

1. Backdoor instaleren (of in de rhost file zetten)

ARP is binding tussen Mac-Adress en IP-adres

ARP poisoning :

In u netwerkkaart wordt een tabel gezet met ARP shizle, dus gij stuurt gewoon over het netwerk hey dit IP-adres is mijn mac adress en deze zijt gij, nu komt al het verkeer via u ipv van de gateway bv.

In de host file kunt ge dingen veranderen zodat als ge surft ge naar een andere site gaat.

**Examen:**

DDoS: Gebruiken vanzoveel mogelijk system resources gebruiken zodat ze geen normale service meer kunnen doen:

SYN-Flood 🡪 veel open connecties maken

Smurf-Attack: reflected DDoS attack, ik stuur een ping naar het broadcast adres naar het pxl network, dan stuurt iedereen een antwoord terug naar mij en lig ik lam, dus ik gebruik spoofing en ik zeg dat de ping origineel gestuurd was van een andere PC (bv Parren) end an wordt parren plat gelegt.

Zo gebruik je gewoon meerdere netwerken voor dit te doen.

Ping Of Death: een gewone ping is 64 bytes groot, deze wordt over het ethernet netwerk gestuurd, MAX 1,5 Kb , MAX ip pakket 64 Kb

Gewoon een ping sturen van 1 Terrabyte, ge fragemnteerd die in stukskes van 64 kb , na een tijd loopt de buffer vol 🡪 index out of bounds 🡪 netwerk kaart gaat plat

DDOS technieken voor webserver:

Als je SQL aan’t draaien bent, heel grote querry’s doorsturen, zodat je de server plat krijgt: bv sorteren op meeste seeders, scriptje die doet up down up down up down up down enzovoort.

Een formke gewoon volsteken met tekst 🡪 HDD volpompen

Mailing Lists attacks : er staan op bepaalde hacking site emails van subsriptions, ik schrijf geoon iemand ander zijn email adres op al die newsletters in.

BOTNETS: Hacker 🡪 master 🡪 slaves 🡪 aanval ergens op

Beveiliging tegen spoofing:

EXAMEN: Ingress en Egress filtering

1. Ingress

Filteren op inbound verkeer 🡪 verkeer dat binnenkomt, deze hebben al een ip adress die van intern is, dit kan niet.

1. Egress

Filteren op outbound verkeer maar die heeft al een ip adress die van buiten af