Seguridad de Redes de Computadores

Redes de Computadores

FIEC04705

Sesión 24

Agenda

- Terminología
- Seguridad en capa de red

Terminología

Terminología

- Datagrama: una unidad independiente en conmutación por paquetes.

Ataques a LAN

Ataques a LAN

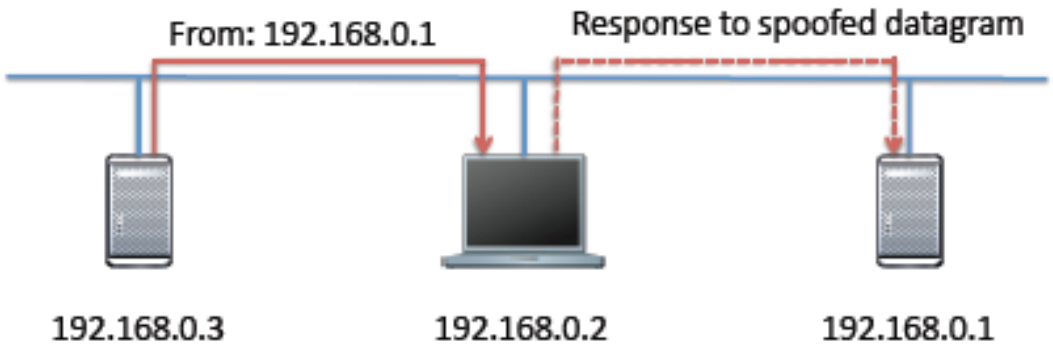
Ataque	Violación de seguridad	Objetivo del intruso
Sniffing	Confidencialidad	Acceso a la información
Spoofing	Autenticidad	Hacerse pasar por un host confiable
Hijacking	Confidencialidad, integridad y autenticidad	Hacerse pasar por un host confiable, acceso a la información
Denial of Service	Disponibilidad	Interrupción

Sniffing

- El intruso configura su tarjeta de red en modo *promiscuo*, de modo que todos los paquetes pueden ser recibidos (y no solo aquellos dirigidos al host intruso)
- Se puede acceder a todo el tráfico en el segmento

IP spoofing

- Un host se hace pasar por otro, enviando un datagrama que tiene la dirección de algún otro host como dirección de remitente
- El intruso sniffs la red buscando por respuestas desde el host atacado
- Las respuestas serían dirigidas al spoofed host



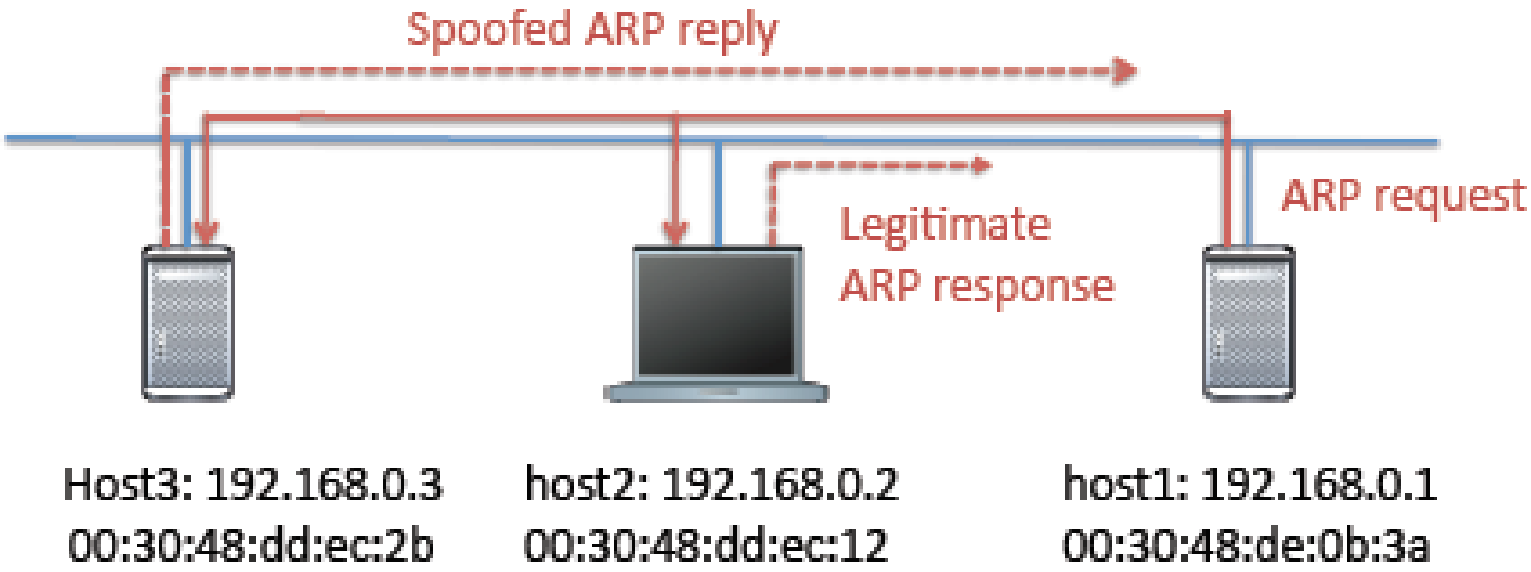
Objetivos del IP spoofing

- Hacerse pasar por fuentes de información de seguridad crítica. Por ejemplo: un servidor DNS o un servidor NFS.
- Explotar una autenticación basada en direcciones.

Hijacking

- Sniffing y spoofing son las bases para el hijacking
- El intruso espera por un requerimiento del cliente
- Luego, compite contra el legítimo host para prducir una respuesta que sea aceptada por el cliente.
- Variaciones de este ataque para ARP, UDP y TCP.

Hijacking ARP



ping

```
$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=52 time=8.16 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=52 time=8.24 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=52 time=8.02 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=52 time=8.02 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=52 time=8.16 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=52 time=8.02 ms

--- 192.168.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time
25082ms
rtt min/avg/max/mdev = 8.021/8.106/8.245/0.125 ms
```

Ataques basados en ICMP echo: scanning

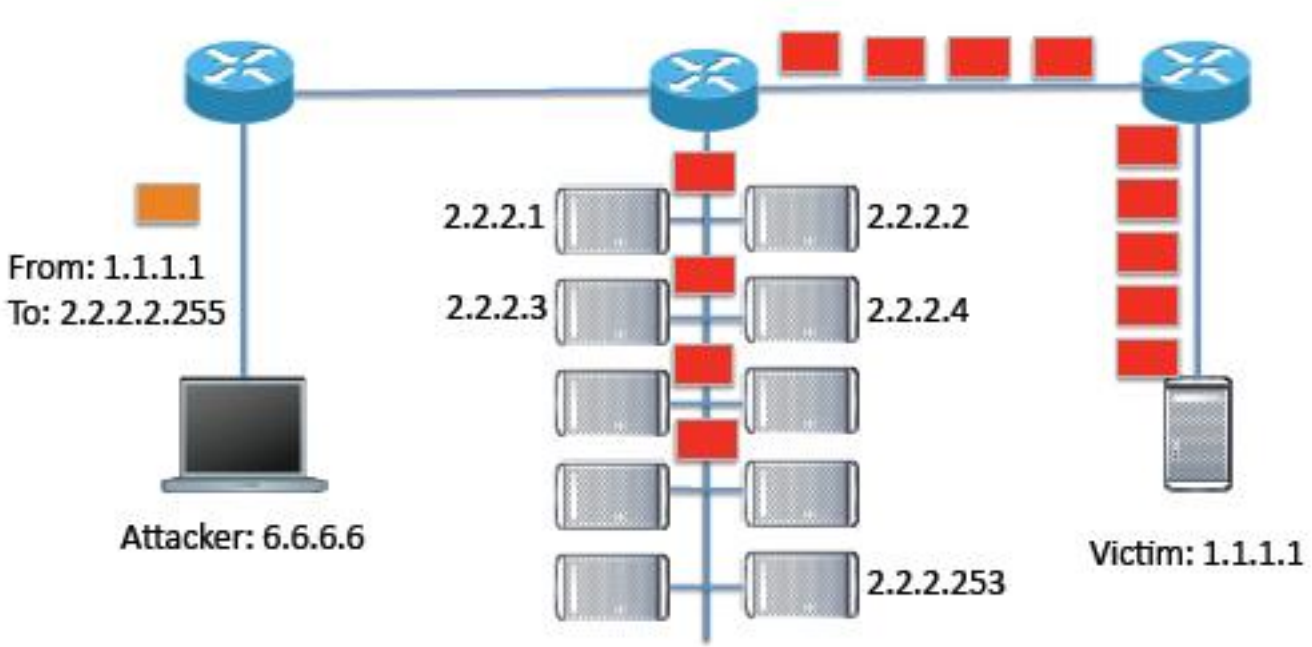
- El intruso desea saber que hosts están corriendo en una subred
- Se envía un ping a todos los posibles hosts en las subred (pingsweep)
- Se recibe las respuestas de todos los hosts activos

```
$ nmap -sP 172.16.48.0/24

Starting Nmap 5.00 ( http://nmap.org ) at 2011-01-12 09:48 PST
Host 172.16.48.1 is up (0.0024s latency).
Host 172.16.48.2 is up (0.00077s latency).
Host 172.16.48.130 is up (0.0065s latency).
Host 172.16.48.139 is up (0.00014s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.54 seconds
```

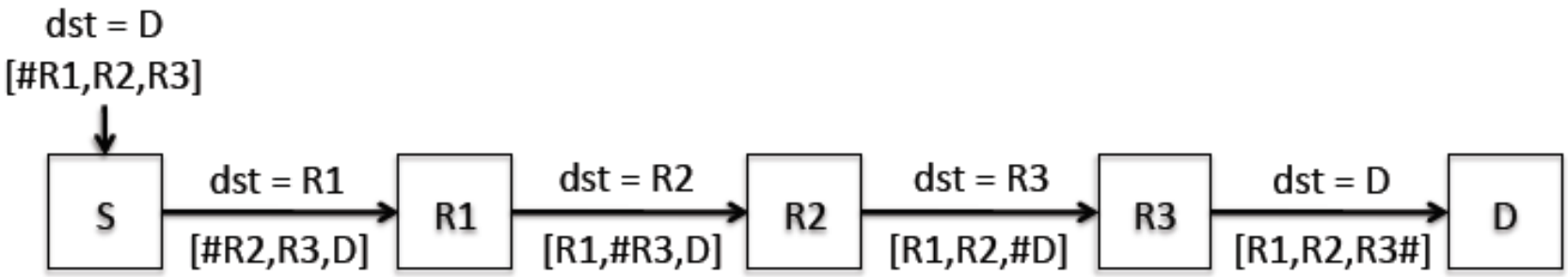
Ataques basados en ICMP echo: smurf

- Enviar un ping a una dirección de broadcast
- Todos los hosts en la subred responderán con un echo reply



Ataque al ruteo en origen

- El ruteo en origen es perfecto para ataques de spoofing
  - Alice: 1.1.1.1
  - Bob: 2.2.2.2
  - Malice: 6.6.6.6
- Malice envía un datagrama a Bob estableciendo la dirección de origen como la de Alice (spoofing) y especifica el gateway de Malice (6.6.6.1) en la lista de ruteo
- Cuando Bob responde, los datos pasan a través del gateway de Malice



Puntos para recordar

- Spoofing
- Sniffing
- Hijacking
- Pruebas de estos ataques solo se deben realizar sobre redes en las cuales se haya obtenido el permiso correspondiente.

Próxima Sesión

- Seguridad en capas de aplicación y de transporte: PGP, SSL