Práctica Redes

NMAP (http://www.insecure.org/nmap)

Nmap Free Security Scanner
Network-wide ping sweep, portscan, OS Detection
Audit your network security before the bad guys do
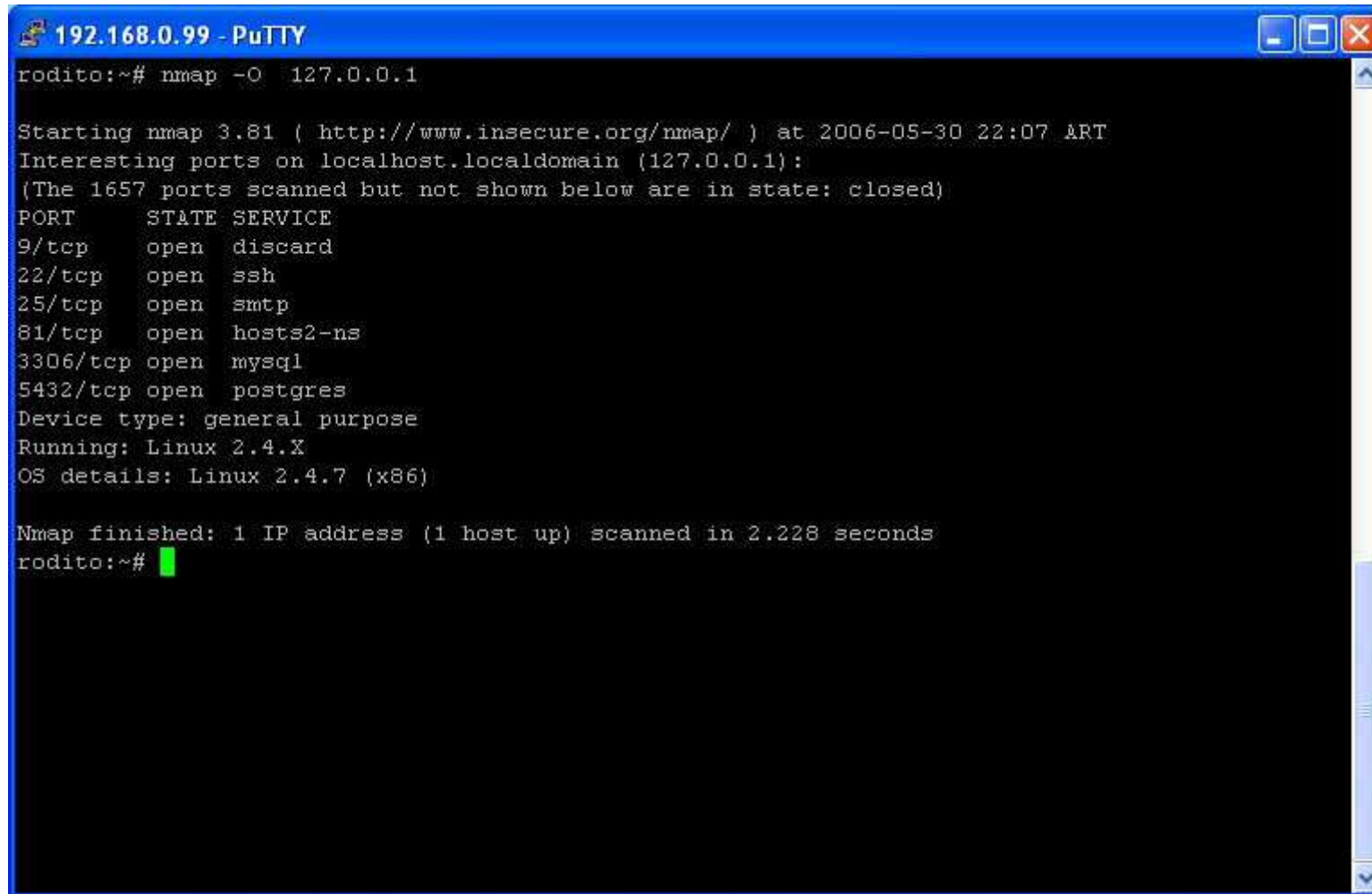
Nmap ("Network Mapper") es una utilidad open-source para explorar redes. Fue diseñada para escanear redes en forma rápida y puede determinar qué servicios (puertos) están habilitados, qué sistema operativo se está utilizando, si existe algún dispositivo de filtrado en el medio, etc. Puede determinar el tipo de servicio que escucha en cada puerto detectado, y provee un potente lenguaje de scripting: NSE.

Ejemplo Nmap

Nmap soporta:

- Vanilla TCP connect() scanning,
- TCP SYN (half open) scanning,
- TCP FIN, Xmas, or NULL (stealth) scanning
- TCP ftp proxy (bounce attack) scanning
- SYN/FIN scanning using IP fragments (bypasses some packet filters)
- TCP ACK and Window scanning
- UDP raw ICMP port unreachable scanning
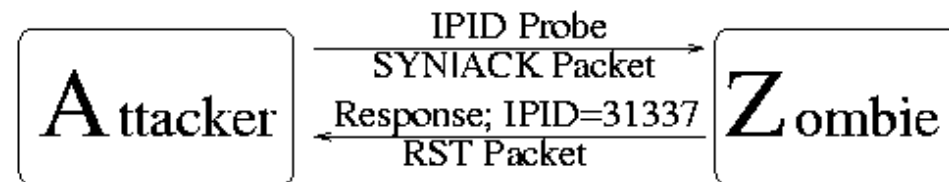- ICMP scanning (ping-sweep)
- TCP Ping scanning

Nmap soporta: (cont.)

- Direct (non portmapper) RPC scanning
- Remote OS Identification by TCP/IP Fingerprinting, and
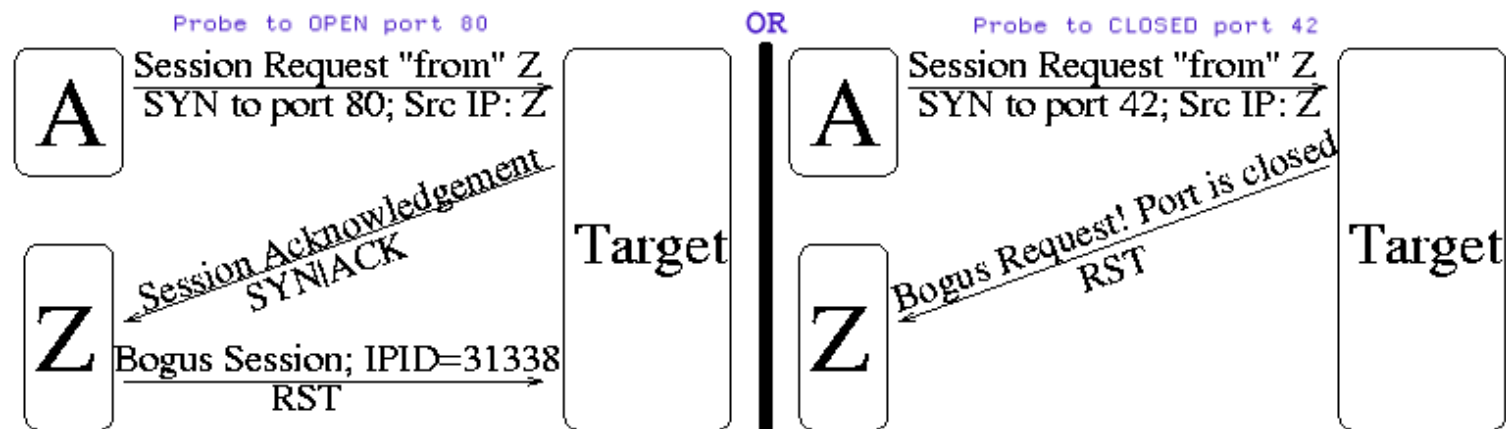- Reverse-ident scanning.

Nmap Idle Scan

Nmap Idle Scan Technique (Simplified)
http://www.insecure.org

Step 1: Chooze a "zombie" and probe for its current IP Identification (IPID) number:

Step 2: Send forged packet "from" Zombie to target. Behavior differs depending on port state:

Probe to OPEN port 80   OR   Probe to CLOSED port 42
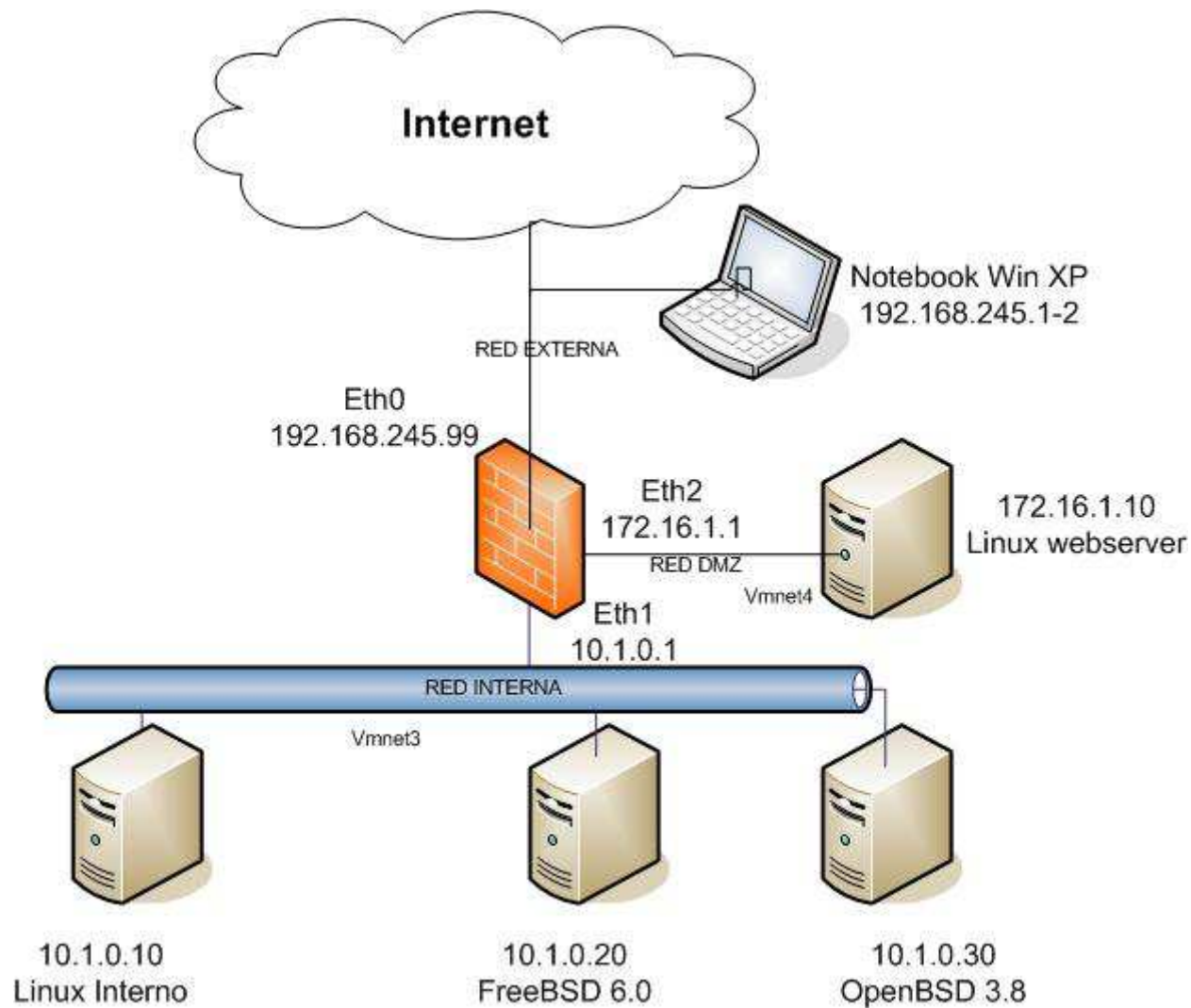
Step 3: Probe Zombie IPID again:

IPID increased by 2 since step #1, so port 80 on target must be open!

IPID only increased by 1, port 42 is CLOSED!

Esquema Demo Firewall

TOR - The Onion Router

https://www.torproject.org/

http://www.onion-router.net/Publications/tor-design.pdf

https://blog.torproject.org/blog/top-changes-tor-2004-design-paper-part-1

https://blog.torproject.org/blog/top-changes-tor-2004-design-paper-part-2

https://www.torproject.org/about/overview.html.en#thesolution

https://trac.torproject.org/projects/tor/wiki/doc/TorALaymansGuide

Tails Live System

https://tails.boum.org/contribute/design/

https://tails.boum.org/doc/about/warning/index.en.html