

Práctica Redes

- **Cifrado: wep, wpa1, wpa2 y wpa3**
- **Ocultar SSID y Mac filter?**
- **Wireless IDS**
- **Auth: WPS, personal(psk), enterprise**
- **Wifiphiser (Rogue AP)**
- **WIFI Jammer**
- **Cuestiones de privacidad**

Deep Web vs. Dark Web vs. Surface Web



Surface Web

- Google, Youtube, Reddit, ETC.
- Anything accessible through a link.

Deep Web

- Private Emails, Dropbox, Public Records, ETC.
- Anything you can't directly link to, or has security.

Need Special Tools to Access

Dark Web

- Markets, Hidden Sites, Tor Sites
- Purposefully hidden, special access material.

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>

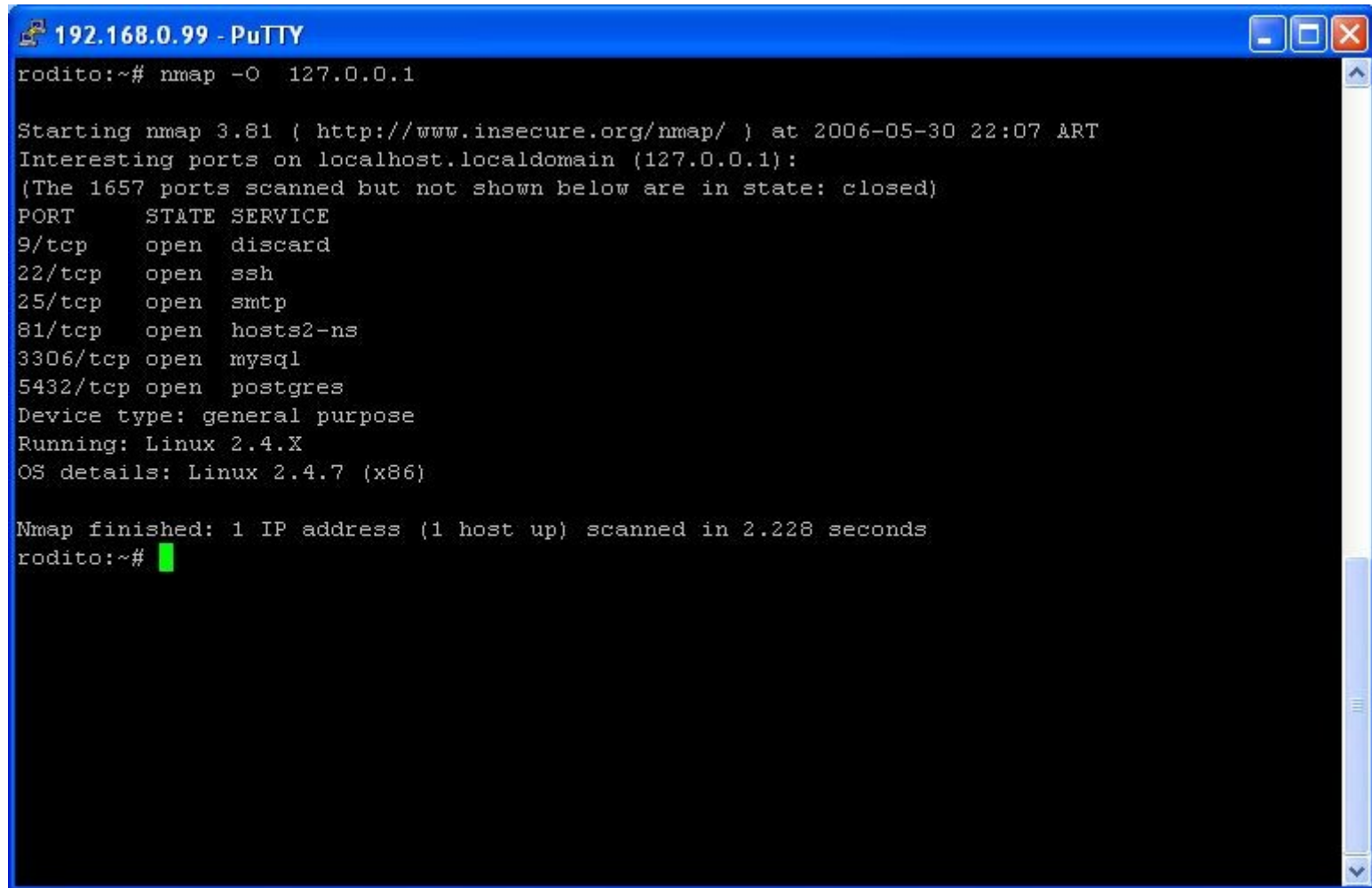
Tails Live System

<https://tails.net/>



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



```
192.168.0.99 - PuTTY
rodito:~# nmap -O 127.0.0.1

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-05-30 22:07 ART
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1657 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
9/tcp     open  discard
22/tcp    open  ssh
25/tcp    open  smtp
81/tcp    open  hosts2-ns
3306/tcp  open  mysql
5432/tcp  open  postgres
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.7 (x86)

Nmap finished: 1 IP address (1 host up) scanned in 2.228 seconds
rodito:~#
```

Nmap implementa técnicas que permiten identificar en forma remota que sistema operativo está utilizando un equipo. Las técnicas se basan en pequeñas variaciones en la construcción de paquetes y la respuesta del equipo ante la recepción de dichos paquetes.

<https://nmap.org/nmap-fingerprinting-article.txt>

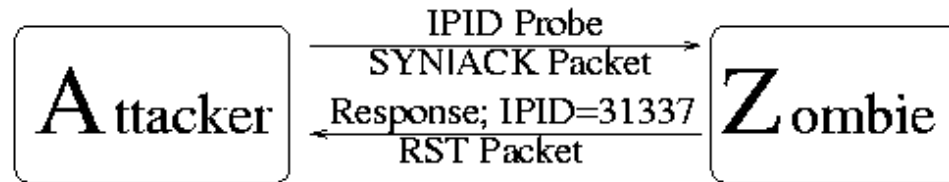
Nmap soporta:

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

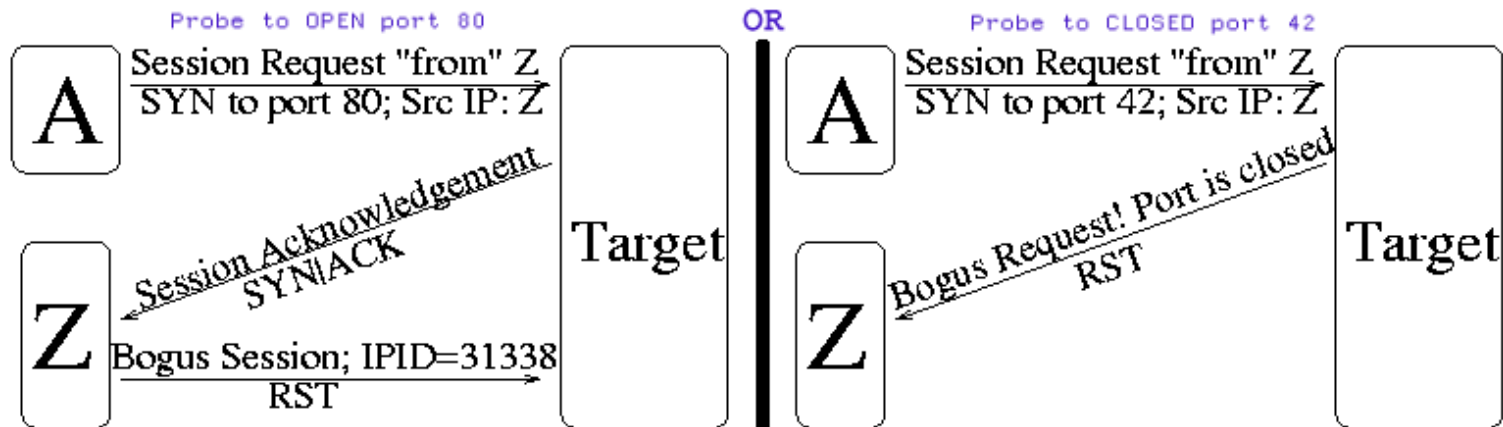
Nmap Idle Scan

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

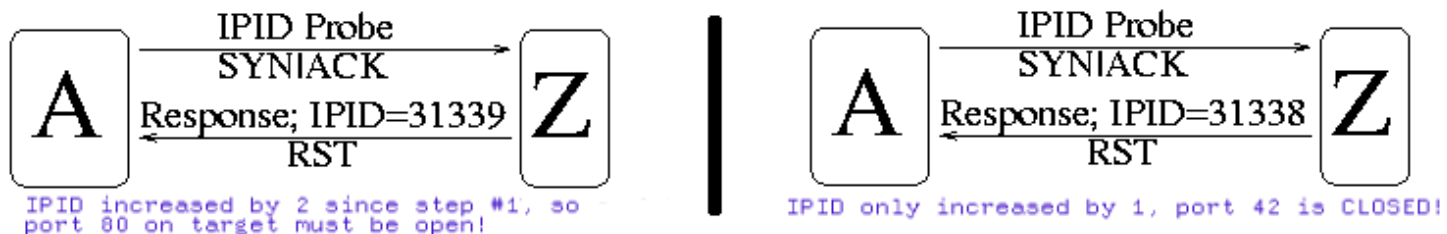
Step 1: Choose a "zombie" and probe for its current IP Identification (IPID) number:



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



Step 3: Probe Zombie IPID again:



Nmap NSE

Los scripts de Nmap son pequeños programas escritos en el lenguaje Lua que se utilizan para realizar tareas específicas durante un escaneo con Nmap. Clasificados según categorías: auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, and vuln.

```
nmap -sC example.com
```

```
nmap --script smb-os-discovery example.com
```

```
Nmap --script http-enum example.com
```

```
nmap --script-help ssl-enum-ciphers
```

```
Nmap --script auth example.com
```

```
Nmap --script vuln example.com
```

<https://nmap.org/book/nse-usage.html>

Laboratorio de Redes - Seginf

