
Scanning & Enumeration Phase
(…poke, poke, poke)
http://www.JasonDion.com

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Scanning & Enumeration

- Scanning
  - Actively connecting to the system and get response to identify open ports & services
- Enumeration
  - In-depth information gathering
    - Open shares
    - User accounts information
    - Software versions
- Compile the information gathered to build a target map before beginning your attack

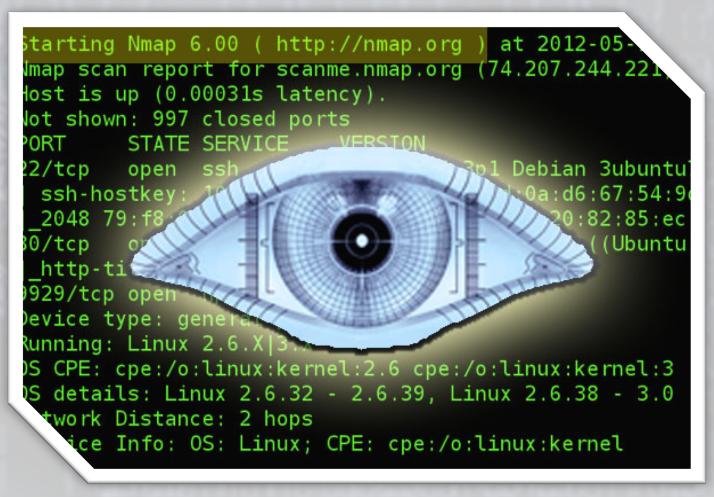
What tool should I use?

- No single tool is sole solution

- Some tools are:
  - Free and open-source
  - Easily detected
  - Crash services on the target machine
  - Provide false results

nmap

- Used in our labs
- Most popular scanning program in the world
- Free and open-source
- Great GUI with Zenmap

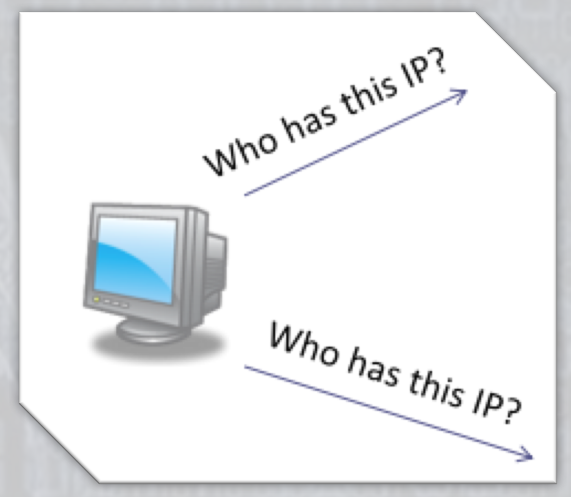


Scanning for Targets

- ARP
- Ping
- Netbios
- Passive Collection

ARP

- nmap –PR <IP ADDRESS>
- Sends ARP to local subnet only
- Advantages:
  - Low level
  - Looks like legitimate traffic
  - Never blocked by a target
- Disadvantages:
  - Cannot route across subnets



ping (ICMP)

- Ping <IP ADDRESS>
- nmap –sn <IP ADDRESS>

- Advantages:
  - Used locally or to other subnets
  - Layer 3 protocol, receives TTL

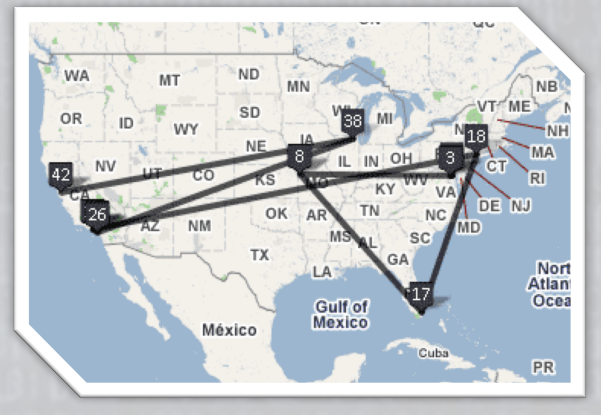
- Disadvantages:
  - Blocked by many firewalls
  - Some Network IDS log this activity
  - Typically used by SYSADMIN or Hackers

traceroute

- nmap –traceroute <IP ADDRESS>

- Advantages:
  - Resolves IPs to router names

- Disadvantages:
  - Blocked by many firewalls



NetBIOS

- nbtstat –A <IP ADDRESS>

- Advantages:
  - Blends into Windows environment
  - Gives us lots of details on the host
    - Workgroup/domain name
    - Hostname
    - MAC address
    - Networking & Print Sharing

- If you send it to UNIX, its noticeable!

Fingerprinting

- Simplest method is based on TTL
- Not accurate, since defaults can be changed
- Based on TTL, though, we can narrow our port scanning
  - Linux, Mac OS X (64)
  - Windows (128)
  - Solaris, Cisco (255)

Enumeration

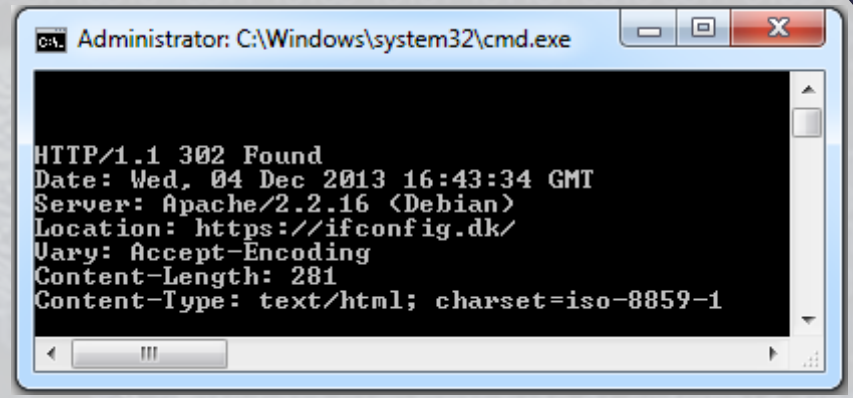
- Determine the OS and Service Pack
- Identify the machine's role
  - Workstation, Server, Router, etc.
- Use this information to find vulnerabilities for identified services
- You use this to be quieter!

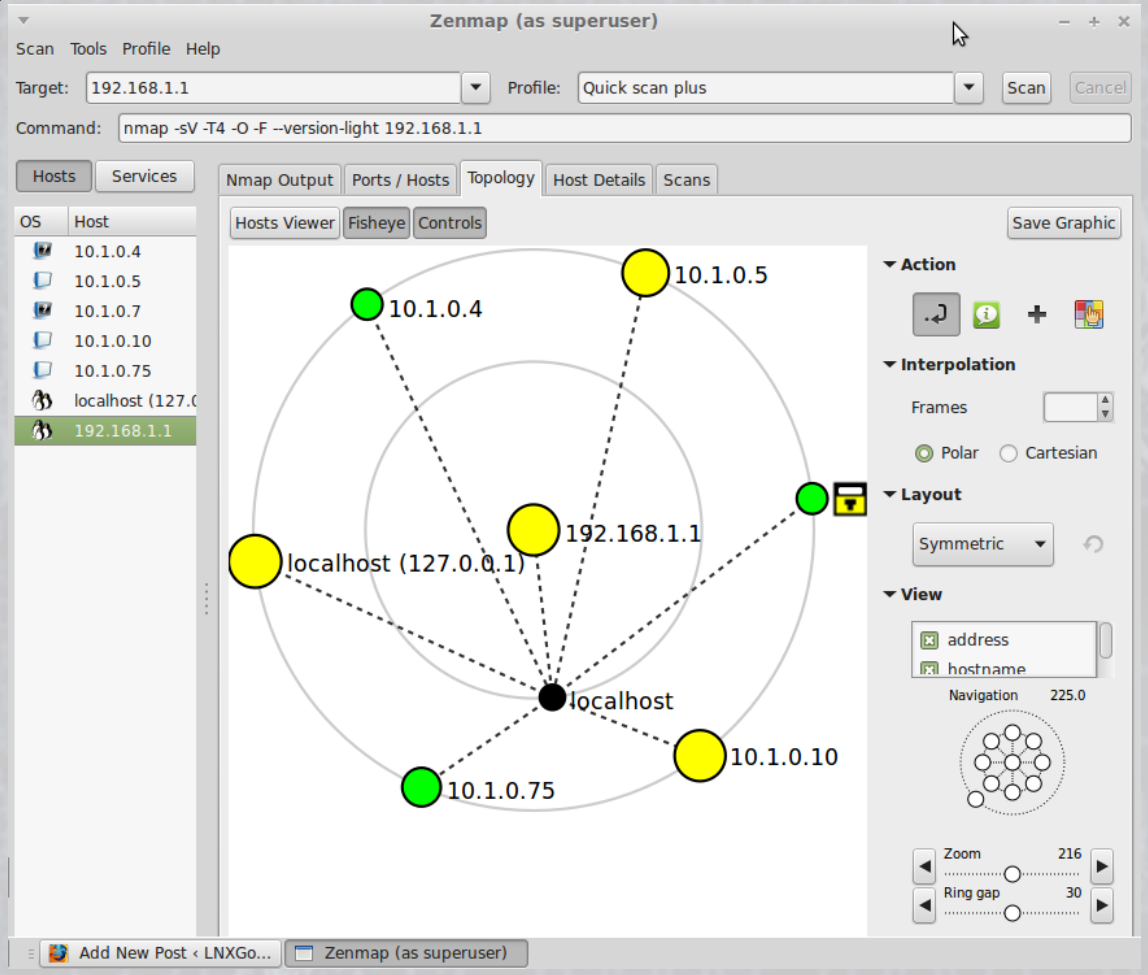
What ports should I look for?

- Web services (80, 443)
- FTP (20/21)
- SSH (22)
- SMTP (25)
- Remote Desktop (3389)
- NetBIOS (135, 139, 445)
- RPC Mapper (111)
- Cups (631)
- NFS (2049)

Banner Grabbing

- Manual enumeration
- Connect to the target
- Service provides a “welcome banner”
- Determine OS based on banner
- Common in FTP, SSH, Telnet, and HTTP/HTTPS.



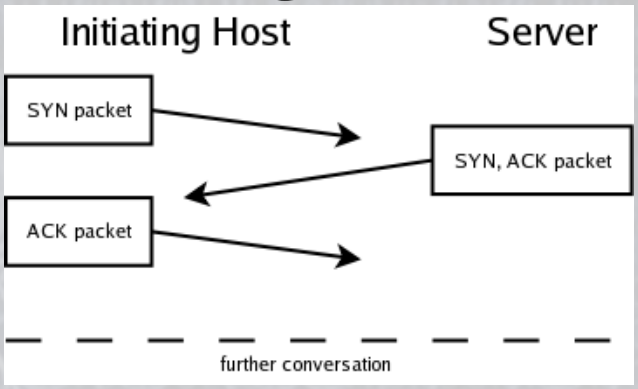


Zenmap

- PING
- TRACEROUTE
- NETBIOS
- TCP/UDP

NMAP manipulates the TCP flags

- URG (Urgent! Even if out of order)
- ACK (Acknowledges SEQ #)
- PSH (Push buffered data)
- RST (Reset the connection)
- SYN (Agrees on intial SEQ #)
- FIN (Session is finished)



OS Detection in NMAP

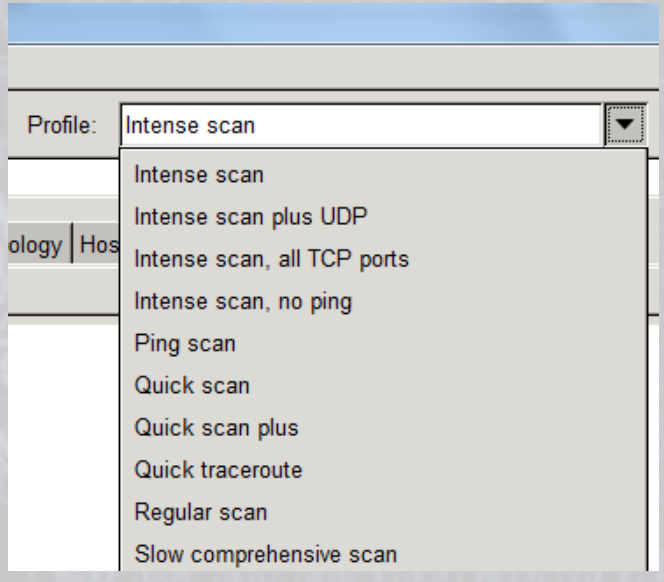
- Noisy process…scans 1000 ports (twice)
  - 6 TCP Packets with SYN flag
  - 2 ICMP Echo packets
  - 1 UDP Packet to a closed port
  - 6 TCP Packets with various flags

Version Scans

- Scan takes a long time, so use less ports
- Sends SYN flag, if a SYN/ACK is received, it sends RST to build a port list
- Then, sends another SYN to create a full connection and review the response

ZENMAP

- Default profiles:
  - Ping
  - Quick
  - Regular
  - Intense
  - Slow Comprehensive



Common Vulnerabilities and Exposure

- Find a vulnerability based on the information gathered in your scanning and enumeration
- Match an exploit in Metasploit in order to exploit the vulnerability and gain access!
- https://cve.mitre.org

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level


Scanning & Enumeration Phase
(…poke, poke, poke)
http://www.JasonDion.com