



Port Scanning

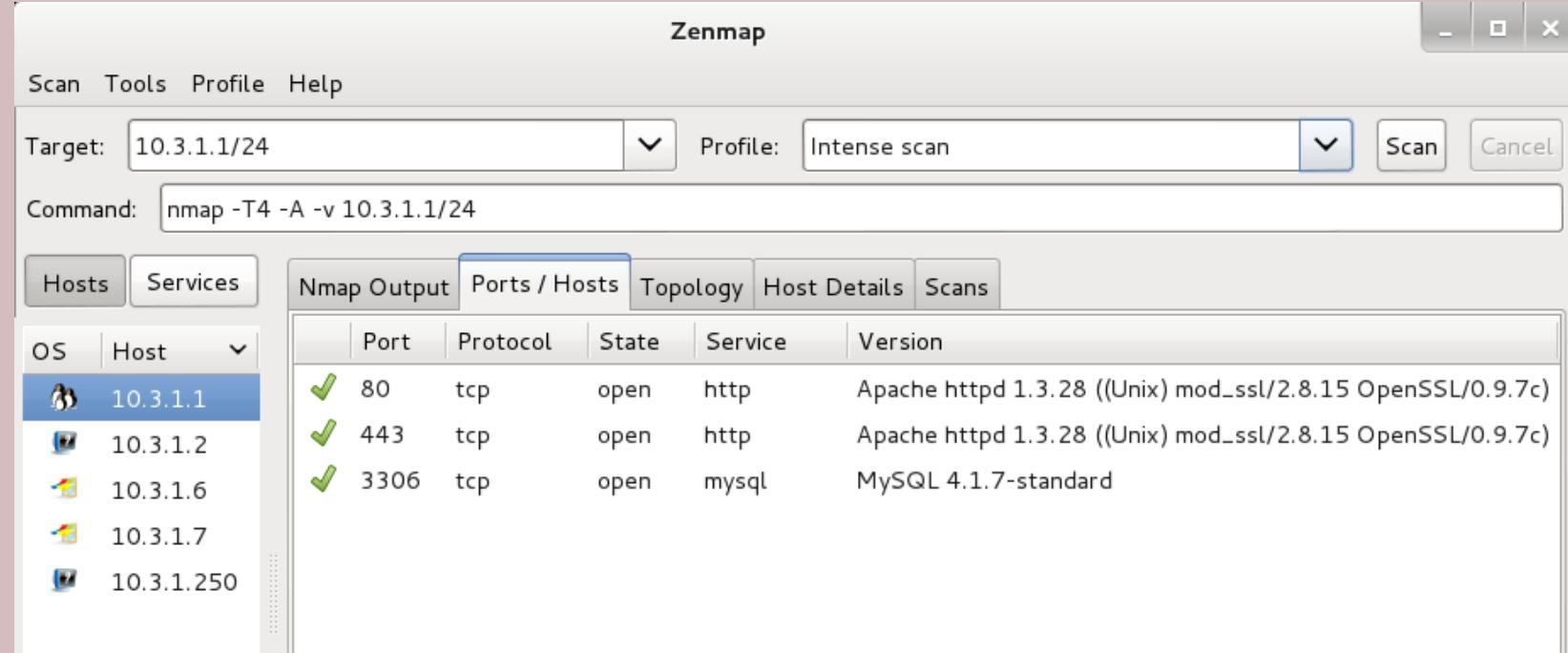
THREAT MANAGEMENT

Port Scanning

- Most common method to gather information on a network and devices
- Port scanners perform:
 - Host discovery
 - Port scanning and service identification
 - Service Version identification
 - Operating System Identification
- Port scanners also used for network inventory tasks and security audits



Service Scanning (Zenmap)



Zenmap

Scan Tools Profile Help

Target: 10.3.1.1/24 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 10.3.1.1/24

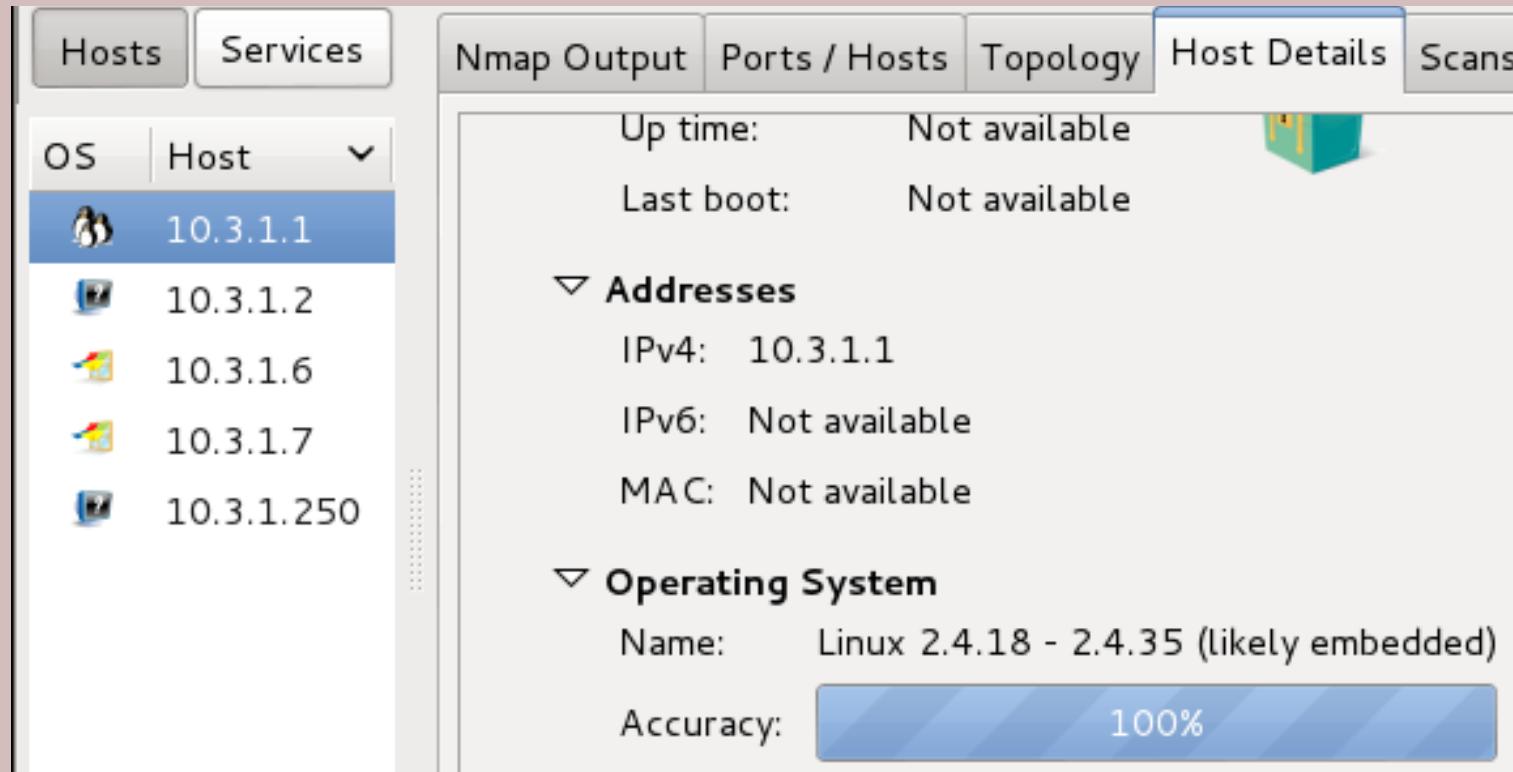
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host	Port	Protocol	State	Service	Version
	10.3.1.1	80	tcp	open	http	Apache httpd 1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
	10.3.1.2	443	tcp	open	http	Apache httpd 1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
	10.3.1.6	3306	tcp	open	mysql	MySQL 4.1.7-standard
	10.3.1.7					
	10.3.1.250					

Service identification attempts to identify the service and its version through banner grabbing or comparing TCP/UDP packet responses to known signatures



OS Scanning (Zenmap)



The screenshot shows the Zenmap interface with the 'Host Details' tab selected. On the left, a sidebar lists hosts by IP address: 10.3.1.1, 10.3.1.2, 10.3.1.6, 10.3.1.7, and 10.3.1.250. The host 10.3.1.1 is selected and highlighted in blue. The main panel displays the following host details:

- Up time: Not available
- Last boot: Not available
- Addresses**
 - IPv4: 10.3.1.1
 - IPv6: Not available
 - MAC: Not available
- Operating System**
 - Name: Linux 2.4.18 - 2.4.35 (likely embedded)
 - Accuracy: 100%

OS fingerprinting uses TCP/IP stack responses from the TCP and UDP packets sent to identify Windows, Linux, or OSX, and if possible, the version



Importance of Port Numbers

- Well-known ports (0-1023)
- Registered ports (1024-49151)



Where you scan from matters...

- Internal scans will see more information than an external scan
- If you are trying to simulate a cyber attack during a PenTest, you should be scanning from the outside the network to match the attacker's perspective

