JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

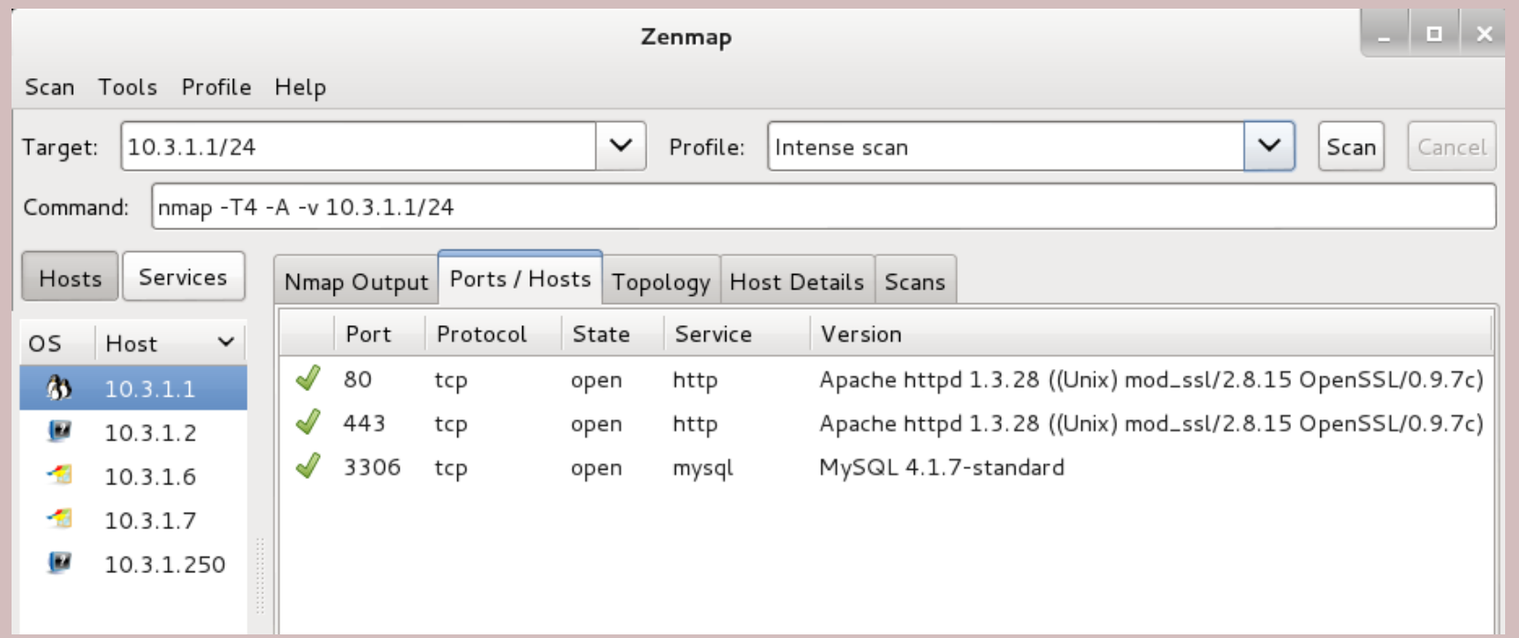
Port Scanning

THREAT MANAGEMENT

Port Scanning

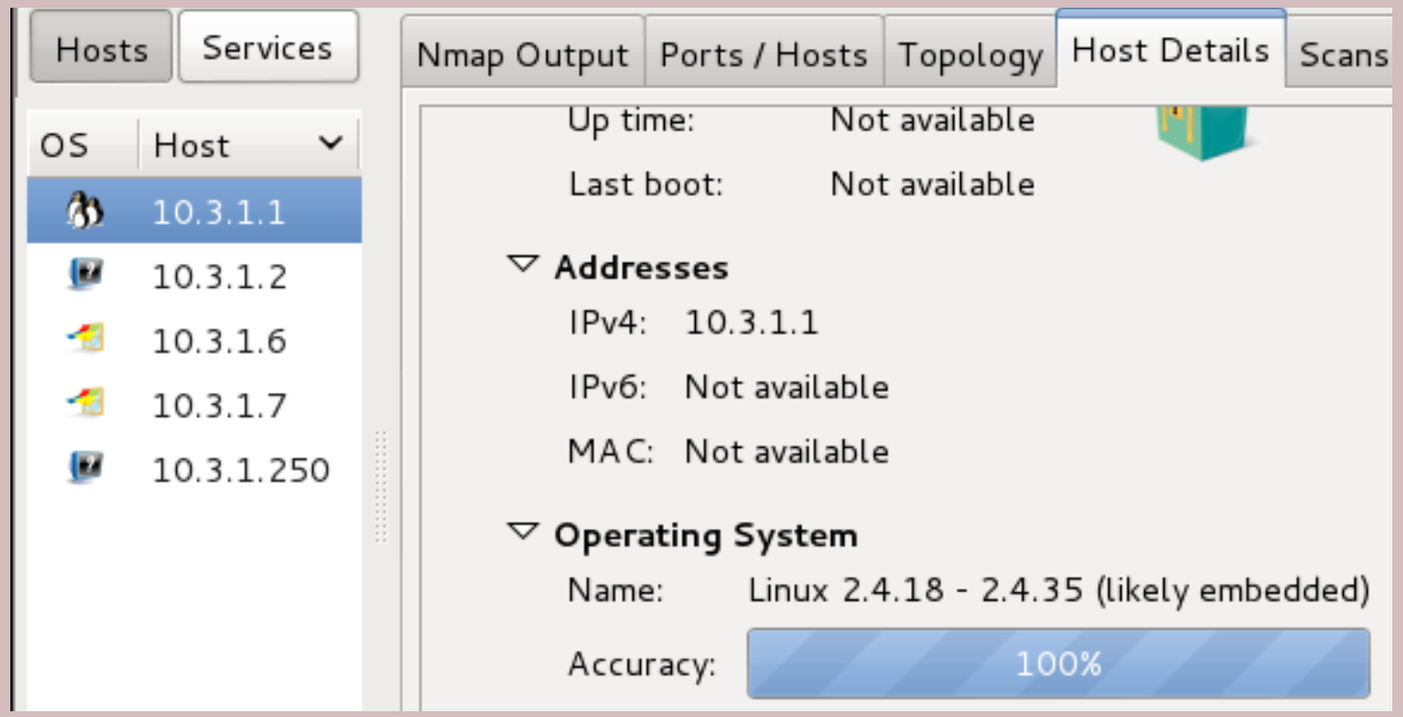
- Most common method to gather information on a network and devices
- Port scanners perform:
  - Host discovery
  - Port scanning and service identification
  - Service Version identification
  - Operating System Identification
- Port scanners also used for network inventory tasks and security audits

Service Scanning (Zenmap)



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)



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

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE