Network Security Tools

Hit the Ground Running

Rik Farrow
rik@spirit.com

Three Useful Tools

- ethereal – see what is on your network
- nmap – determine which ports are open
- nessus – search for vulnerabilities

Ethereal

- Open Source network protocol analyzer
  - ethereal.com
- Key points:
  - run as root, but use su (not su -)
  - use filters in busy networks
  - analyze stored traffic or live traffic
  - have permission to sniff traffic first

Ethereal

- Good points:
  - Large list of decoded protocols
  - Easy to use interface
- Bad points:
  - Filter language difficult to use (and important)
  - May crash in heavy traffic (capture traffic using tethereal or tcpdump for later analysis)

nmap

- The continually updated Open Source tool for network exploration and security assessments
  - nmap.insecure.org
- Written by a security consultant, Fyodor
- Basically a port scanner
  - but will do much more

Host Discovery

- nmap is useful for discovering in-use IP addresses
  - quickly send ICMP Echo with -sP to check to see which hosts are up and respond
  - ARP scans can be used in the local network, and are very fast and quite reliable (-PR)
  - other types of scans are possible, such as ACK scans to port 80 (-PA -p 80)

Port Scanning

- Port scanning detects open ports
  - Open ports represent listening services
  - Listening services are potentially vulnerable services
- Use port scanning to
  - check for compliance to policy, ie, no Web servers on desktops
  - unusual services, or service list differing from netstat, an indication that a rootkit has been installed

nmap Port Scanning

- Traditional port scan displays the port number and service name
- nmap can attempt to identify application version
  - adds reliability to service name identification
  - provides additional information to port scan
  - based on banner grabbing

nmap OS Identification

- nmap will attempt to identify the OS version of scanned systems
  - requires discovering one open and one closed port
  - examines responses to packets sent to open and closed ports
  - collects other information, such as ISN, IP id, window size, and order of TCP options
  - 1707 fingerprints in version 3.95

nmap Pros and Cons

- Pros
  - fastest, much flexible, scanner
  - OS and application version info
  - accepts IP address ranges, lists, file format
  - frontend available for the commandline inhibited
- Cons
  - scanning may be considered hostile
  - SYN scans have been known to crash some systems

Nessus Vulnerability Scanner

- Nessus is a tool that has commercial counterparts
  - still available for free use -- nessus.org
- Nessus works by
  - locating hosts starting with a target file
  - port scanning the targets located
  - probing for vulnerabilities in applications listening at open ports

Nessus

- Client-server architecture
  - client requests scans and formats results
  - server accepts scan requests, authenticates clients, performs scans
  - scans based on large and constantly updated vulnerability list

Nessus

- Pros
  - free vulnerability scanning
  - check for effectiveness of patching
- Cons
  - some UI issues
  - less open than it once was
  - definitely appears hostile when used

Summary

- Ethereal – ethereal.com
- nmap – nmap.insecure.org
- Nessus - nessus.org