

*Portscanning
and the use of nmap in
assessing network vulnerabilities*

Keith Callenberg
Linux Users Group at SJSU

Ports

Ports are numbers used by TCP/IP to map packets to services

If an IP address is an apartment building, ports are each resident's mailbox, via which the residents send and receive messages

21 – FTP

22 – SSH

23 – Telnet

25 – SMTP

53 – DNS

80 – HTTP

110 – POP3

443 – HTTPS

465 – SMTPS

Port States

- open – actively accepting connections
 - closed – accessible, but no application listening
 - filtered – cannot determine whether it's open because of packet filtering
 - unfiltered – accessible, but whether it's open or closed has not yet been determined (ACK scans)
 - open|filtered – open port that doesn't give a response, possibly due to packet filtering
-
-

Basic nmap usage

`nmap [scan type] [options] {target specification}`

`-v` verbose output

`-O` detect operating system

`-sV` service version detection

`-T {paranoid|sneaky|polite|normal|aggressive|insane}`

`-p` specify ports you want to scan

`-F` Fast scan: only scan ports mapped to services

Specifying targets

Wildcard: `192.168.1.*`

Range: `10.0.2.1-20`

Single host: `192.168.0.1`

TCP Flags

and their related nmap scans

- SYN – initiate -sS SYN scan
 - ACK – acknowledge -sT TCP connect scan
 - RST – error -sN Null scan
 - FIN - finish/terminate -sF FIN scan
 - PSH -sA ACK scan
 - URG
-
-

Resources

- www.insecure.org - nmap and Fyodor's Top 100
- www.antonline.com - tutorials and forums
- www.securiteam.com - news and exploits
- www.milw0rm.com - exploits and tutorials

