


# Port Scanning

Matt Bishop  
Department of Computer Science  
University of California, Davis


December 1, 2000 Slide #1



# Outline

- ◆ What is port scanning?
- ◆ How do you do it?
- ◆ Why should you do it?
- ◆ Is it ethical?
- ◆ Some random thoughts

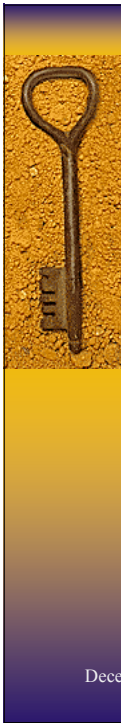
December 1, 2000 Slide #2



## Port Scanning by Analogy

- ♦ Look at the door of a building
- ♦ By looking at the type of door, you may gain information about what the site does
  - Door with counter halfway up: fast food
  - Door with heavy glass and sliding tray: drive-up teller
  - Door with iron bars: jail
  - Door with multiple locks: “secure” facility


December 1, 2000 Slide #3



## In Computer Terms

- ♦ Servers make your computer available to “outsiders”
- ♦ The functions your computer will perform is reflected by the servers you run
- ♦ Good place for attackers to check out your computer

December 1, 2000 Slide #4




## Original Port Scanner

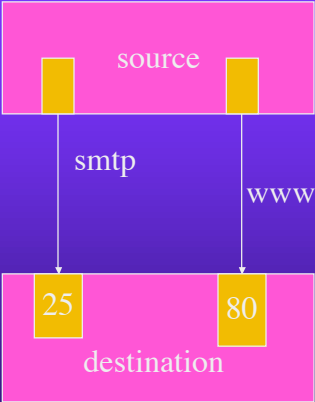
### Big Bad Wolf

1. Knocked on doors to see if anyone was there
2. Detected type of server (a pig)
3. Attacked at weakness based upon information gleaned from probe (huffed and puffed)

December 1, 2000 Slide #5




## What is a port?



- ◆ Each communication (connection or datagram) goes to a *port* (mailbox) on a system
- ◆ Port “opened” when a server is listening for a message

December 1, 2000 Slide #6

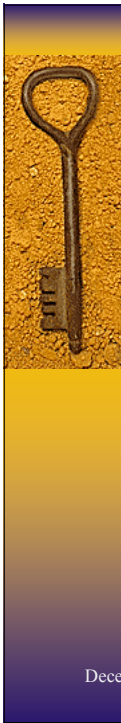


## What is port scanning?

- ♦ Send a message to port 1
  - If rejected, no server listening
  - If accepted, a server listening
- ♦ Repeat for some set of ports

Symptom: connection/messages to large number of ports, especially from a single source

December 1, 2000 Slide #7



## What you learn

- ♦ Port number gives function
  - Examples: 25 is smtp, 80 is WWW server
- ♦ May give useful information


220 xxx.yyy ESMTP Sendmail 8.9.3/8.9.3; Sun, 26 Nov 2000 21:34:49 -0800 (PST)

UNIX system running *sendmail*

220 zzz.yyy Microsoft ESMTP MAIL Service, Version: 5.0.2195.1600 ready at Sun, 26 Nov 2000 21:29:29 -0800

Windows system running Microsoft's mail server


December 1, 2000 Slide #8



## Attackers

- ◆ Figure out the operating system
  - Look for known attack tools, security holes
- ◆ Figure out which servers are being run
  - Look for known holes
  - Obtain information (user names, *etc.*) about site
- ◆ Scope out what site is doing
  - If running *amd* server, probably an NFS server
  - Does it relay mail? (Good for spam)

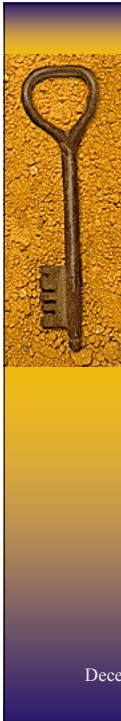
December 1, 2000 Slide #9



## How do you do it?

- ◆ Freeware scanners
  - Best is *nmap*; does TCP, UDP scanning
    - Can use a variety of probes
  - Many others available
    - Do web search on “network+port+scanner”
- ◆ Often included with other programs
  - SATAN, SARA has one

December 1, 2000 Slide #10




## Example

```
# nmap -sN -v -F -f bait

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host bait.cs.ucdavis.edu (11.22.33.44) appears to be up ... good.
Initiating FIN, NULL, UDP, or Xmas stealth scan against bait.cs.ucdavis.edu
(11.22.33.44)
The UDP or stealth FIN/NULL/XMAS scan took 2 seconds to scan 1062 ports.
All 1062 scanned ports on bait.cs.ucdavis.edu (11.22.33.44) are: closed
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```


December 1, 2000 Slide #11



## Why you should do it

- ◆ Learn what attackers will see
  - These are starting points of attack
- ◆ Look for unauthorized services
  - Someone may be running a server with known problems
  - Someone may be running an unauthorized server on a high port
  - Someone may be running unauthorized server on legitimate port

December 1, 2000 Slide #12




## Examples

- ♦ Enable *ftp* over port 25
  - Looks like mail, but allows file transfers
- ♦ Tunneling
  - Encapsulate *ftp* messages into email, send it over, and recipient's email system throws it over to *ftp*
  - Known technology; BITNET, CSNET allowed *ftp* by email

December 1, 2000

Slide #13




## What about firewalls?

- ♦ Idea: block probes from outside
- ♦ Problem: if a client can get through, so can a probe
  - Firewall may be programmed to allow connection/datagram (probe) through
  - Firewall may be mis-configured
  - Policy may be incorrect

December 1, 2000

Slide #14




## Is It Ethical?

- ♦ Consider our door
- ♦ If you check the doors of your house to see which are unlocked, that's fine
- ♦ If you check the doors of your neighbor's house, that's questionable
  - Is it illegal if you don't open the door?

December 1, 2000

Slide #15




## Random Thoughts

- ♦ When is it port scanning?
  - Can be done very slowly
  - Unintentional connections, messages to various ports
- ♦ What does it mean?
  - Curiosity
  - Precursor to attack

December 1, 2000

Slide #16



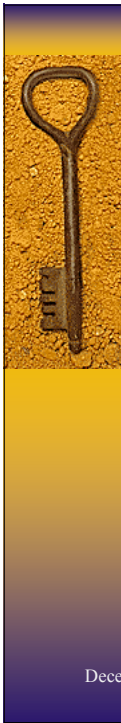


## Doing It Right (Attacking)

- ◆ Port scan from multiple hosts
  - Ideally, from different networks
- ◆ Port scan a single host over a period of days or weeks
  - This makes it harder for monitoring tools to detect
- ◆ Scan ports in random order
  - Use different types of probes (TCP, half-open, FIN, Christmas tree, *etc.*)

December 1, 2000

Slide #17




## What You Can Do

- ◆ Realize you *cannot* prevent this
  - If it's critical to run dangerous services, limit their visibility to outsiders using a firewall
- ◆ Keep system up to date with all security patches
- ◆ If possible, monitor traffic to critical hosts and infrastructure components to detect these
  - May not be feasible

December 1, 2000

Slide #18



## A Final Thought

When it seems hopeless, remember Dorothy Parker's words:

```
Razors pain you;  
Rivers are damp;  
Acids stain you;  
And drugs cause cramp.  
Guns aren't lawful;  
Nooses give.  
Gas smells awful;  
You might as well live.
```

December 1, 2000 Slide #19



## Contact Information

Matt Bishop  
Department of Computer Science  
University of California at Davis  
Davis, CA 95616-8562  
*phone: (530) 752-8060, (530) 752-1286 (lab)*  
*email: bishop@cs.ucdavis.edu*

December 1, 2000 Slide #20