Chapter 6
Phase 2: Scanning

War Dialer

- Tool used to automate dialing of large pools of telephone numbers in an effort to find unprotected

THC-Scan 2.0

- Full-featured, free war dialing tool
- Runs on Win9x, WinNT, and Win2000
- Released by The Hacker's Choice group
- Available at http://thc.inferno.tusculum.edu
- Keeps track of number of carriers (discovered modems)
- Detects repeat dial tones
- Nudges discovered modems
- Jamming detection

MS-DOS Prompt - THC-SCAN

8 x 12

TIME

Start » 16:49:50
Now » 16:51:25
ETA » 16:56:58

Timeout » 2/50
Rings » 0/6

FOUND!

STATISTIC

Done :	2
To Do :	8
Dials/H:	114
Carrier:	0
Tones :	0
VMB :	0
Voice :	0
Custom :	0
Busy :	0
Others :	2
2ndary :	0

LOG WINDOW

```
16:49:50 Auto Saving DAT File ...
16:49:50 UnDialed : 10
16:49:50 Excluded : 0
16:49:50 Done     : 0
16:49:50 To Do    : 10
16:49:50 Dialmask : 751102X
16:49:50 Scan Mode: Carrier
16:49:50 Dialing  : undialed, busy
16:49:50 Scan started
16:49:50 7511020 Fax(0) 13sec
16:50:06 7511027 Timeout(0) 50sec
16:51:04 7511021
```

MODEM WINDOW

```
ATH
OK
ATDT7511027
NO CARRIER
ATH
OK
ATDT7511021
```

* FINAL * THC-SCAN v2.00 (c) 1996,98 by van Hauser/THC * FINAL *

Figure 6.1 THC-Scan 2.0 screen

Demon Dialer

- Tool used to attack just one telephone number with a modem by guessing passwords
- THC LoginHacker available at http://thc.inferno.tusculum.edu

Defenses Against War Dialing

- Provide documented policy forbidding use of modems on desktop machines in offices without approval from security team
- Periodically scan all analog lines and digital PBX lines
- Perform desk-to-desk check of modem lines to computers

Network Mapping

- Finding live hosts
  - ICMP pings
  - TCP/UDP packets

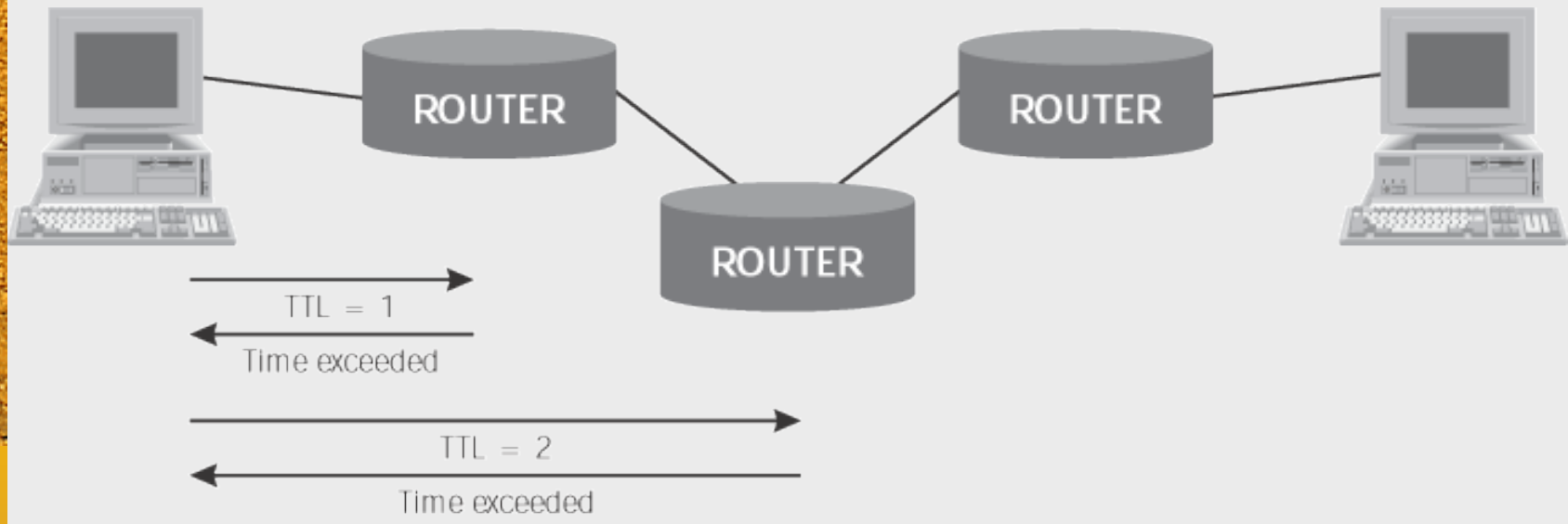


Figure 6.2 Using traceroute to discover path from source to destination

Traceroute

- Traceroute utility on most Unix platforms sends out UDP packets with incremental TTL values to trigger ICMP Time Exceeded messages
- Tracert utility on Microsoft platform sends out ICMP packets with incremental TTL values to trigger ICMP Time Exceeded replies

Command Prompt

```
D:\> tracert 10.15.15.1

Tracing route to 10.15.15.1 over a maximum of 30 hops:

  1    <10 ms    <10 ms    <10 ms  10.1.1.1
  2    <10 ms     10 ms     10 ms  10.2.160.1
  3     50 ms     50 ms     60 ms  10.3.123.1
  4     30 ms     31 ms     30 ms  10.206.13.21
  5     30 ms     40 ms     40 ms  10.130.92.177
  6     50 ms     50 ms     50 ms  10.111.23.242
  7     30 ms     40 ms     40 ms  10.63.18.30
  8     40 ms     50 ms     50 ms  10.163.23.145
  9     50 ms     60 ms     50 ms  10.24.193.245
 10     60 ms     40 ms     60 ms  10.70.9.139
 11    130 ms    150 ms    141 ms  10.74.4.225
 12    150 ms    130 ms    151 ms  10.71.164.19
 13    150 ms    160 ms    141 ms  10.75.167.6
 14    140 ms    160 ms    150 ms  10.151.12.5
 15    150 ms    150 ms    140 ms  10.15.15.1

Trace complete.

D:\>
D:\>
D:\>_
```

Figure 6.3 Windows NT tracert output

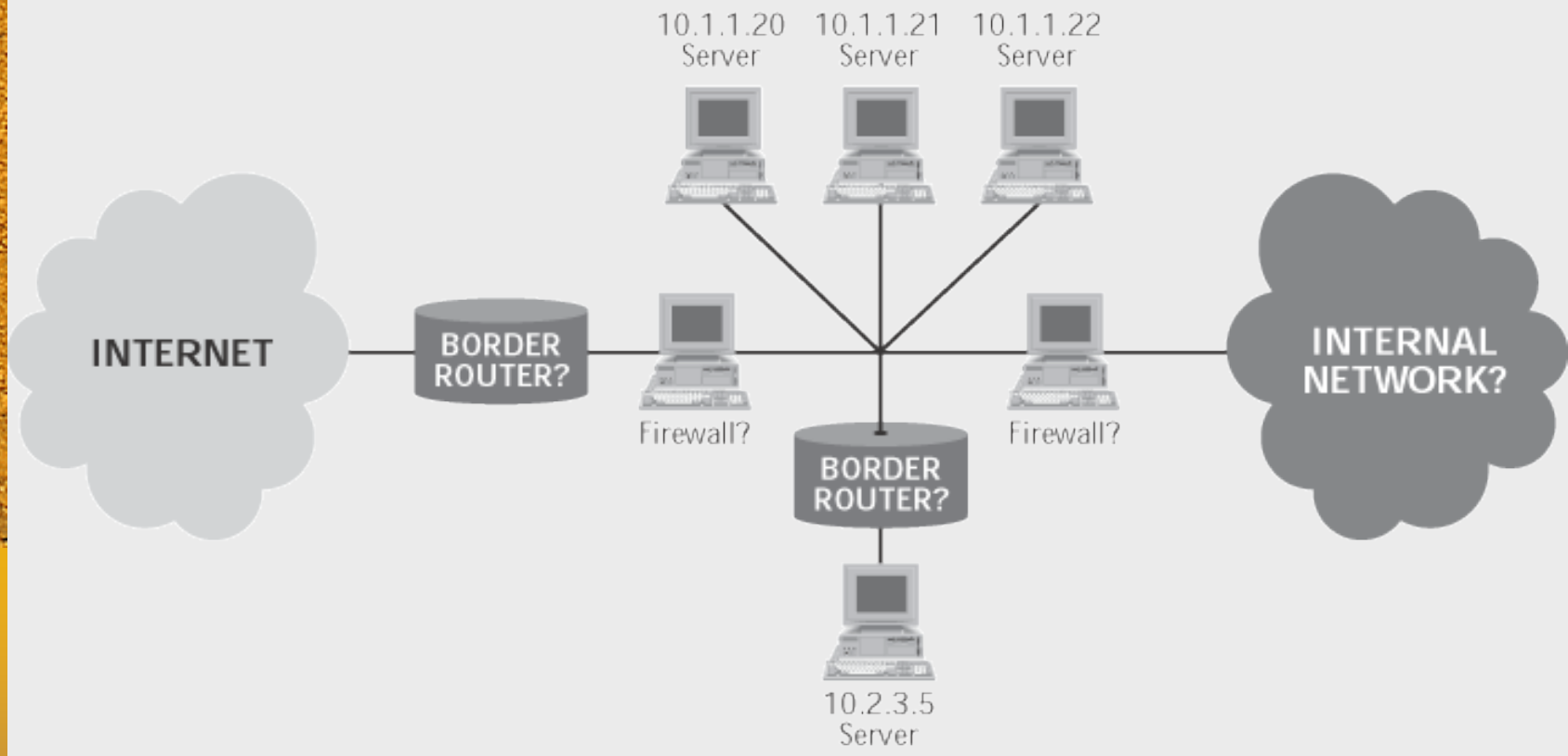


Figure 6.4 Network diagram created by attacker using ping and traceroute

Cheops

- A nifty network mapper tool
- Available at http://www.marko.net/cheops
- Runs on Linux
- Generates network topology by using ping sweeps and traceroute
- Supports remote operating system identification using TCP Stack Fingerprinting

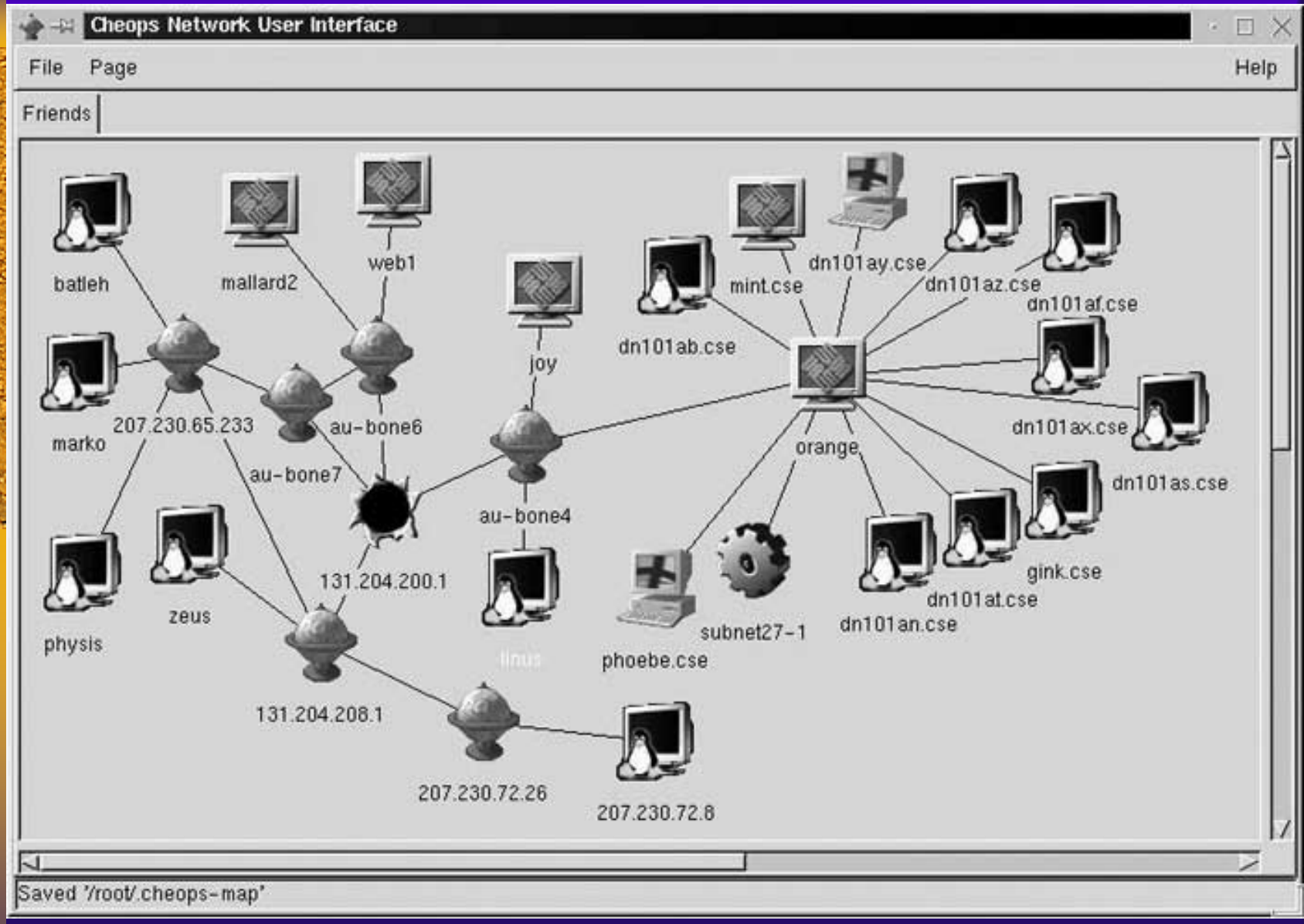


Figure 6.5 The Cheops display

Defenses against Network Mapping

- Block incoming ICMP messages at Internet gateway to make ping ineffective
- Filter ICMP Time Exceeded messages leaving your network to make traceroute ineffective

Port Scanning

- Used to find open ports
- Free port scanning tools
  - Nmap available at www.insecure.org/Nmap
  - Strobe at http://packetstorm.securify.com/UNIX/scanners
  - Ultrascan for NT available at http://packetstorm.securify.com/Unix/scanners

Nmap

- Full-featured port scanning tool
- Unix version available at http://www.insecure.org/Nmap
- Windows NT version available at http://www.eeye.com/html/Databases/Software/Nmapnt.html

Nmap Front End v1.6

File Output Help

Host(s): xanadu vectra playground Scan. Exit

Scan Options: General Options:

connect() Don't Resolve TCP Ping Fragmentation
SYN Stealth Fast Scan TCP&ICMP Get Identd Info
Ping Sweep Range of Ports: ICMP Ping Resolve All
UDP Port Scan Don't Ping OS Detection
FIN Stealth
Bounce Scan: Use Decoy(s): Input File: Send on Device:
antionline.com

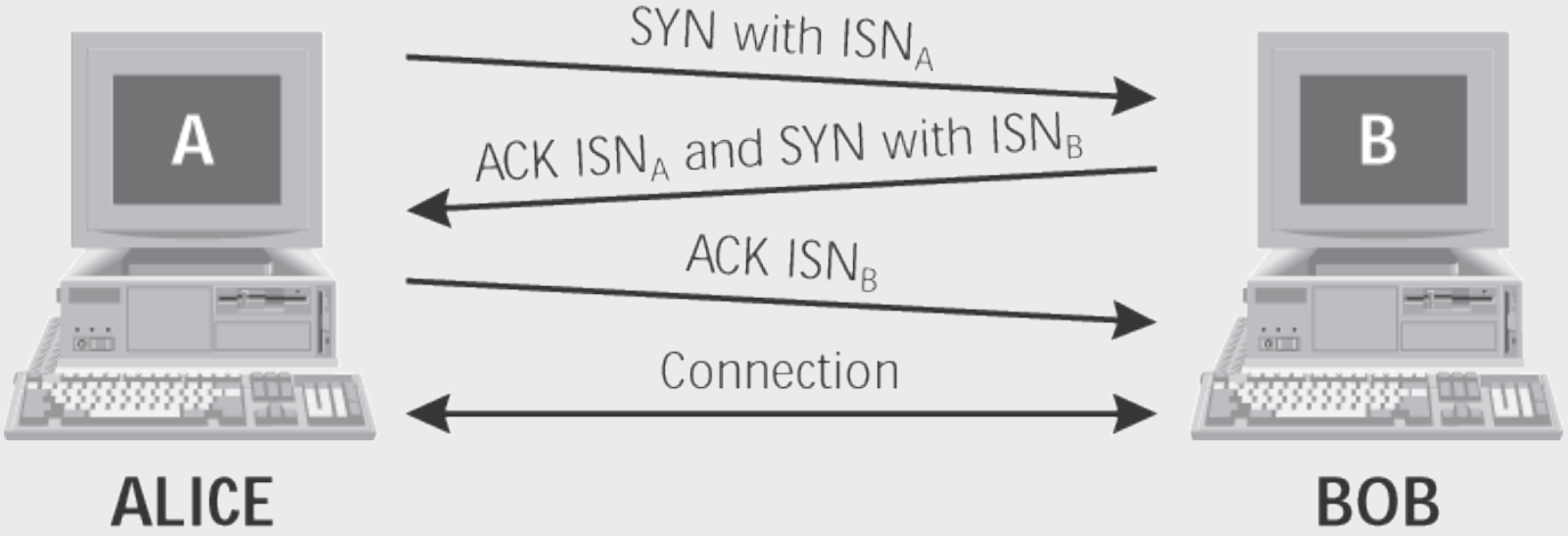
Output from: nmap -sS -O -Dantionline.com xanadu vectra playground

```
Interesting ports on vectra.yuma.net (192.168.0.5):
Port       State          Protocol   Service
13         open           tcp        daytime
21         open           tcp        ftp
22         open           tcp        ssh
23         open           tcp        telnet
37         open           tcp        time
79         open           tcp        finger
111        open           tcp        sunrpc
113        open           tcp        auth
513        open           tcp        login
514        open           tcp        shell

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=14943 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Interesting ports on playground.yuma.net (192.168.0.1):
Port       State          Protocol   Service
```

Figure 6.6 Nmapfe: A nice GUI for Nmap

Scan Types supported by Nmap

- TCP Connect (-sT)
  - Attempts to completes 3-way handshake with each scanned port
  - Sends SYN and waits for ACK before sending ACK
  - Tears down connection using FIN packets
  - If target port is closed, sender will received either no response, a RESET packet , or an ICMP Port Unreachable packet.
  - Not stealthy



Scan Types supported by Nmap (cont.)

- TCP SYN (-sS)
  - Only sends the initial SYN and waits for ACK to detect open port.
  - SYN scans stop two-thirds of the way through the 3-way handshake
  - Aka half-open scan
  - Attacker sends a RESET after receiving a SYN-ACK response
  - A true connection is never established
  - If target port is closed, destination will send a RESET or nothing.
  - Faster and stealthier than Connect scans
  - SYN flood may cause accidental denial-of-service attack if target is slow

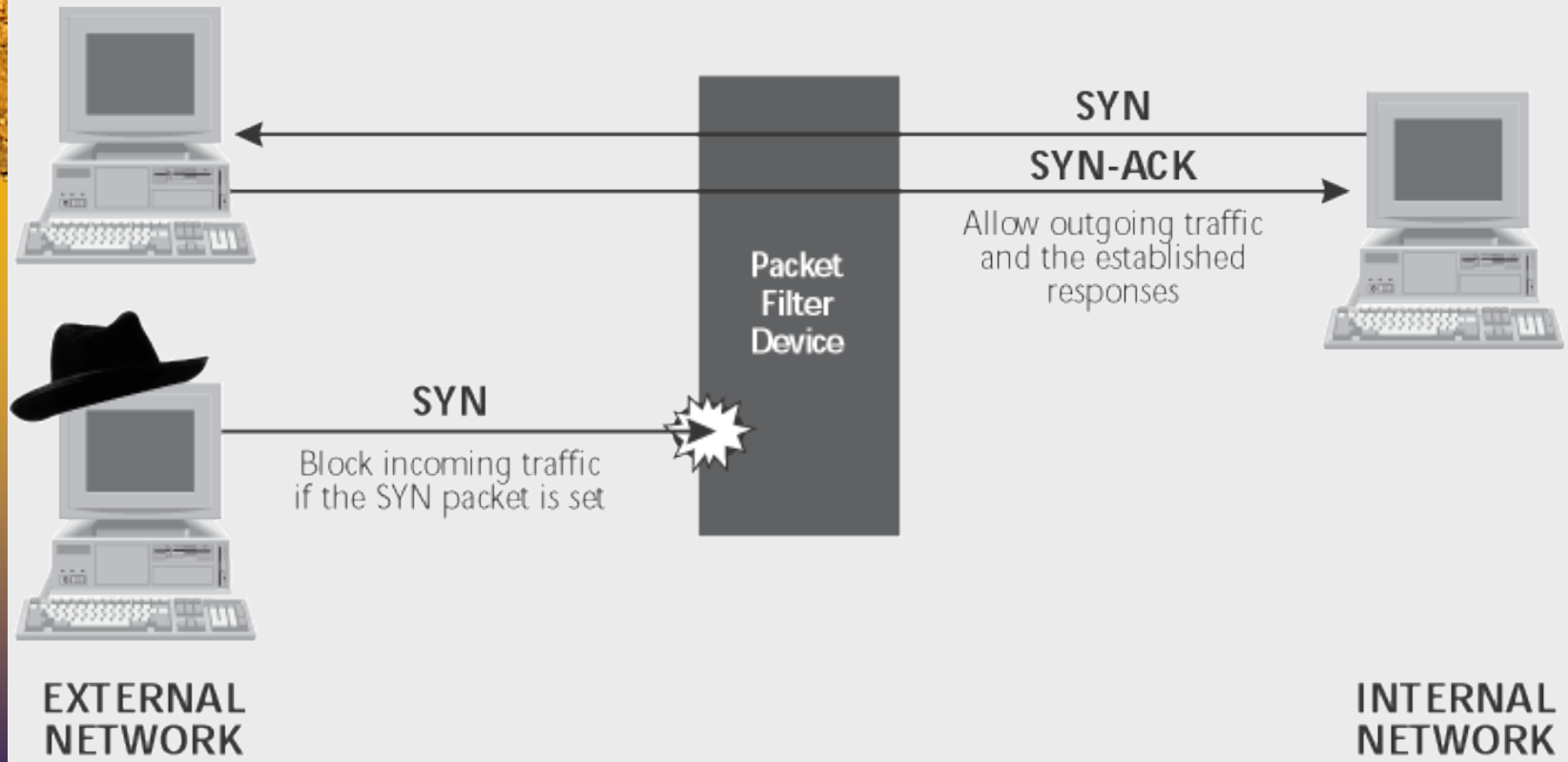
Scan Types supported by Nmap (cont.)

- TCP FIN (-sF)
  - Sends a TCP FIN to each port. A RESET indicates that the port is closed, while no response may mean that the port is open
- TCP Xmas Tree (-sX)
  - Sends a packet with FIN, URG, and PUSH code bits set. A RESET indicates that the port is closed, while no response may mean that the port is open
- Null (-sN)
  - Sends packets with no code bits set. A RESET indicates that the port is closed, while no response may mean that the port is open.

Note: Microsoft systems don't follow the RFCs regarding when to send a RESET if a FIN, Xmas Tree, or Null packet comes in. These scan types useful for other platforms

Scan Types supported by Nmap (cont.)

- TCP ACK (-sA)
  - Sends a packet with the ACK code bit set to each target port.
  - Allows attacker to get past some packet filtering devices



- TCP ACK (-sA)
  - Allows attacker to determine what kind of established connections a firewall or router will allow into a network by determining which ports through a firewall allow established connection responses
  - If no response or an ICMP Port Unreachable message is returned, Nmap will label the target port as “filtered”, meaning that a packet filter is blocking the response

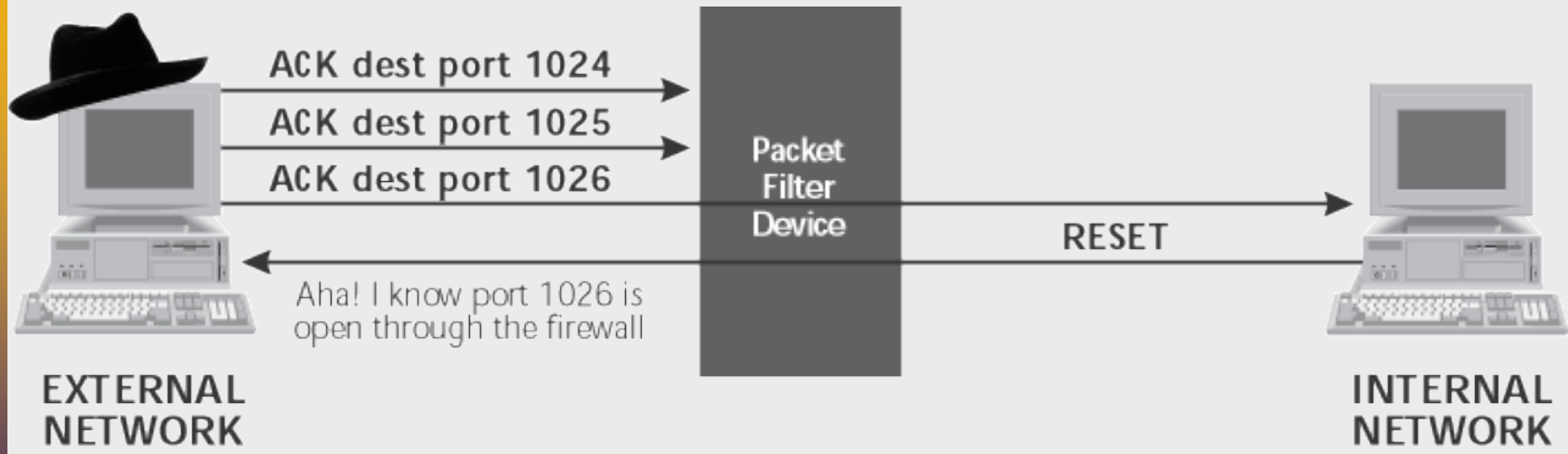
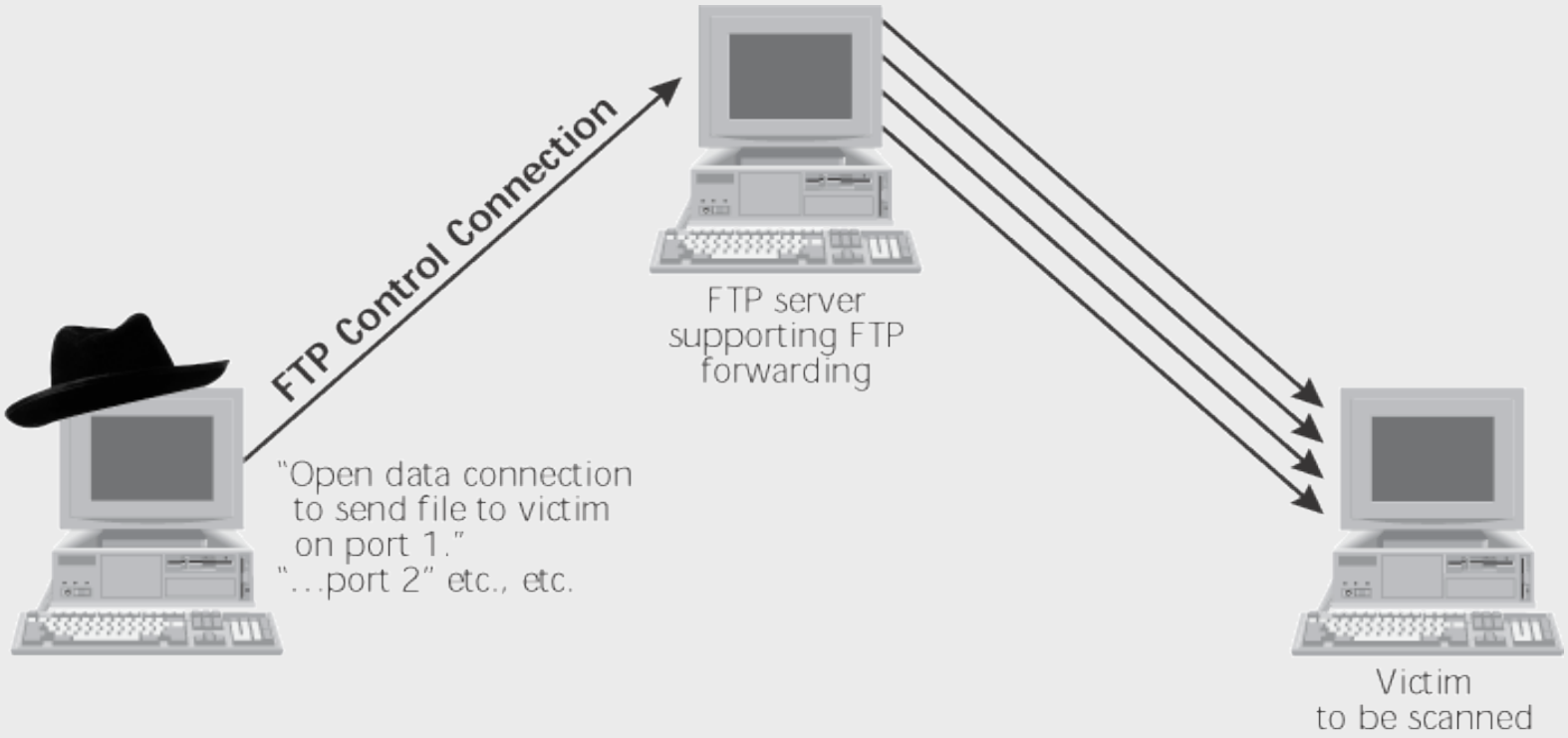


Figure 6.9 ACK scanning

Scan Types supported by Nmap (cont.)

- Window (-sW)
  - Similar to ACK scan, but focuses on the TCP Window size to see if ports are open or closed on a variety of operating systems
- FTP Bounce (-b)
  - Bounces a TCP scan off of an FTP server, hiding originator of the scan.
  - Checking FTP servers for bounce capability at http://www.cert.org/advisories/CA-1997-27.html

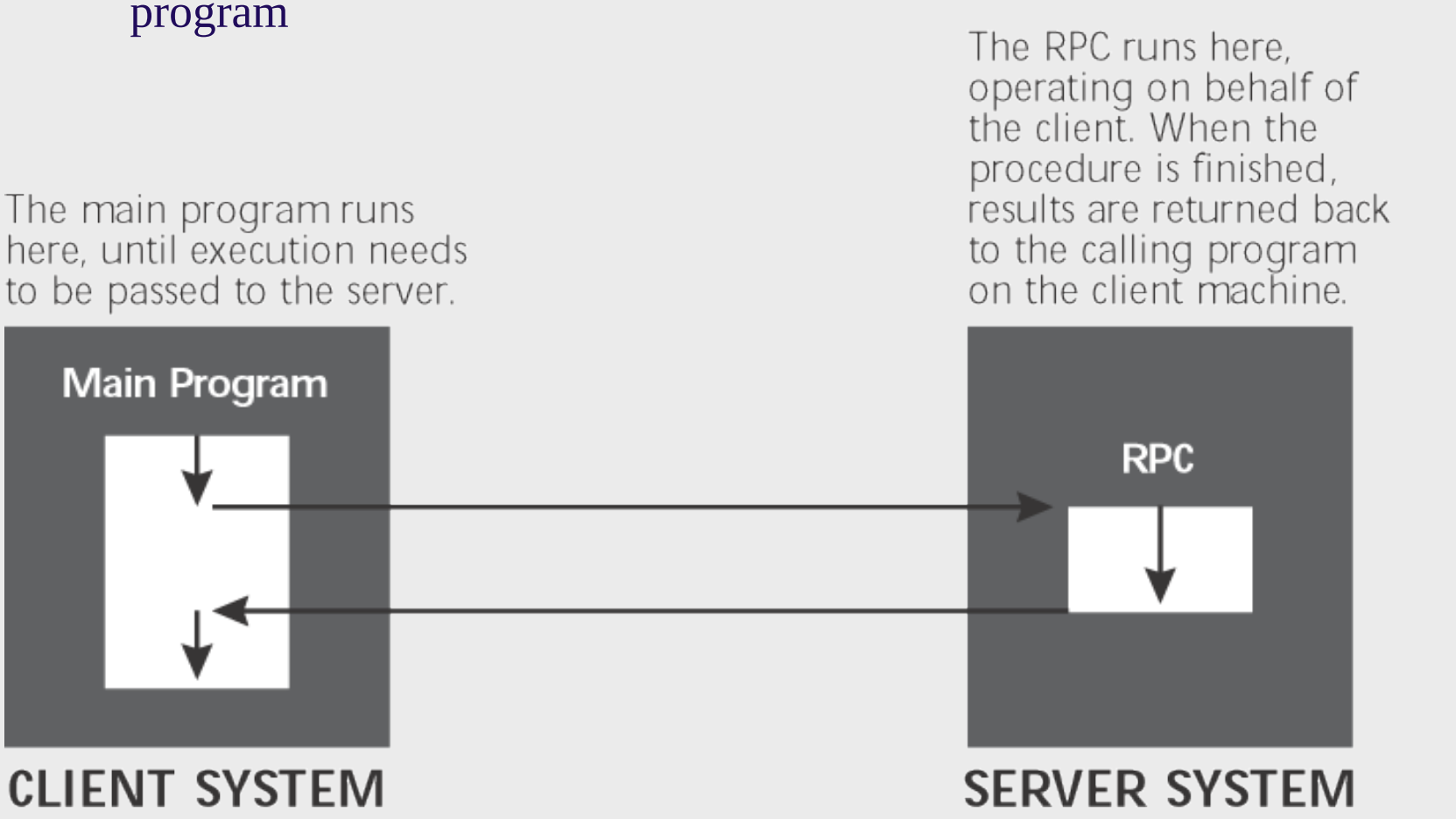


Scan Types supported by Nmap (cont.)

- UDP Scanning (-U)
  - Sends a UDP packet to target ports to determine if a UDP service is listening
  - If the target system returns an ICMP Port Unreachable message, the target port is closed. Otherwise, the target port is assumed to be open.
  - Unreliable since there may be false positives
  - Client program of discovered open port is used to verify service
- Ping (-sP)
  - Sends ICMP echo request packets to every machine on the target network, allowing for locating live hosts. This isn't port scanning; it's network mapping.
  - Can use TCP packets instead of ICMP to conduct Ping sweep

Scan Types supported by Nmap (cont.)

- RPC Scanning (-sR)
  - Scans RPC services using all discovered open TCP/UDP ports on the target to send RPC NULL commands. Tries to determine if an RPC program is listening at the port and identifies type of RPC program



Setting Source Ports for a Successful Scan

- Choose specific source ports to increase the chance that the packets will be admitted into the target network
- Using source port of 25 or 80 together with an ACK scan will make the traffic look like responses to Web traffic or outgoing email
- Using TCP source port 20 will look like incoming FTP data connection
- Using UDP source port of 53 will look like DNS responses

Using Decoys

- Nmap allows attacker to specify decoy source addresses to use during scan
- Packets containing attacker's actual address are interleaved with decoy packets

TCP Stack Fingerprinting

- Used to determining operating system of target
- Nmap sends various abnormal packets
  - NULL packet to open port
  - SYN/FIN/URG/PSH packet to open port
  - SYN packet to closed port
  - ACK packet to closed port
  - FIN/PSH/URG packet to closed port
  - UDP packet to closed port
- Nmap sends series of SYN packets to determine predictability of Initial Sequence Number
- Nmap compares responses against database describing how various systems respond to illegal code bit combinations and sequence number prediction check

Nmap timing options

- Paranoid
  - Send one packet every 5 minutes
- Sneaky
  - Send one packet every 15 seconds
- Polite
  - Send one packet every 0.4 seconds
- Normal
  - Send packets as quickly as possible without missing target ports
- Aggressive
  - wait no more than 1.25 seconds for any response
- Insane
  - wait no more than 0.3 seconds for any response
  - Prone to traffic loss

Defenses against Port Scanning

- Unix systems
  - remove all unneeded services in /etc/inetd.conf
  - Remove unneeded services in /etc/rc*.d
- Windows systems
  - uninstall unneeded services or shut them off in the services control panel
- Scan your own systems before the attackers do
- Use stateful packet filter or proxy-based firewall
  - blocks ACK scans
  - Blocks FTP data source port scans

Firewalk

- Tool which allows attacker to determine firewall filter rules
- sends packets through a packet filter device to determine which ports are open *through* it
- Identifies TCP and UDP ports that firewall allows new connection initiations
- Available at http://www.packetfactory.net/Projects/Firewalk/firewalk-final.html

Firewalk Network Discovery Phase

- Requires the attacker to specify IP address of the packet-filtering device and IP address of destination machine
- Sends packets with incrementally higher TTL values until ICMP Time Exceed message is received from packet-filtering device

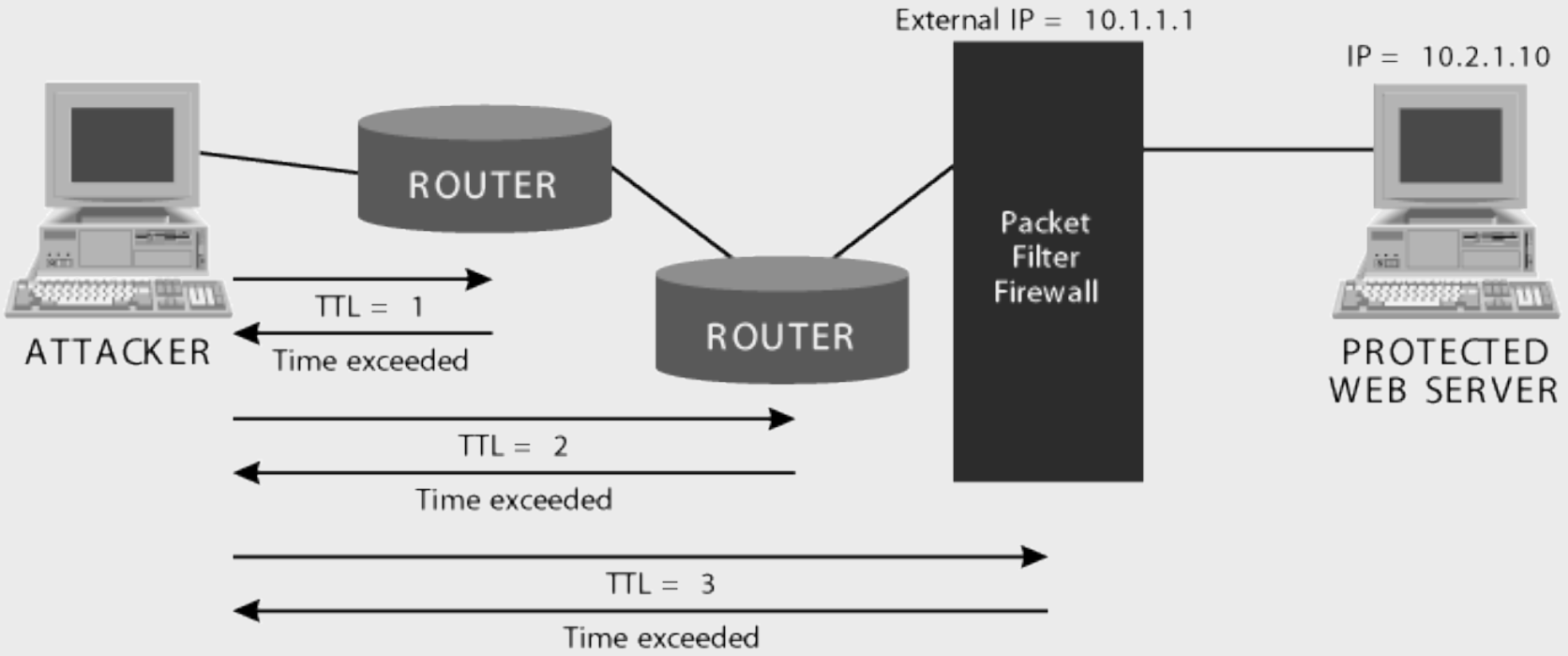


Figure 6.14 Firewalk network discovery phase counts the number of hops to the firewall

Firewalk Scanning Phase

- Firewalk generates a series of packets with TTL set to one greater than the hop count to the packet filtering device
- Packets contain incrementing destination TCP and UDP port numbers
- An ICMP Time Exceeded response means that the port is open through the firewall
- If nothing or ICMP Port Unreachable comes back, the port is probably filtered by the firewall
- Works well against traditional and stateful packet filters
- Does not work against proxy-based firewalls since proxies do not forward packets

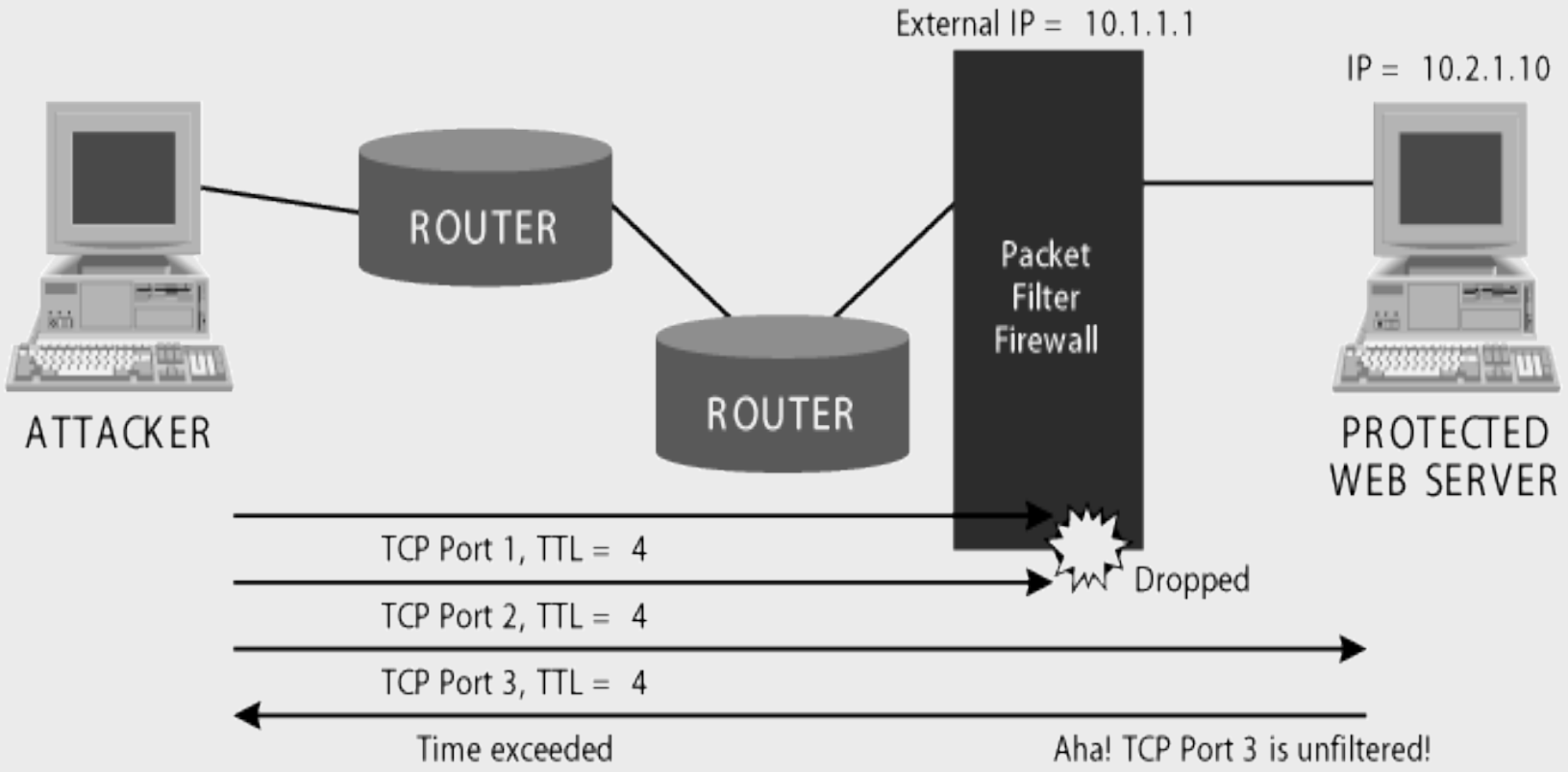


Figure 6.15 Firewalk scanning phase determines open ports through the firewall

Firewalk Defenses

- Configure firewall to pass a minimum set of ports
- Accept the fact that an attacker can determine your firewall rules
- Filter out ICMP Time Exceeded messages leaving your network
  - Side effect of crippling traceroute
- Replace traditional and stateful packet filters with proxy-based firewalls

Vulnerability Scanning Tool

- Checks for the following types of vulnerabilities
  - Common configuration errors
  - Default configuration weaknesses
  - Well-known system vulnerabilities

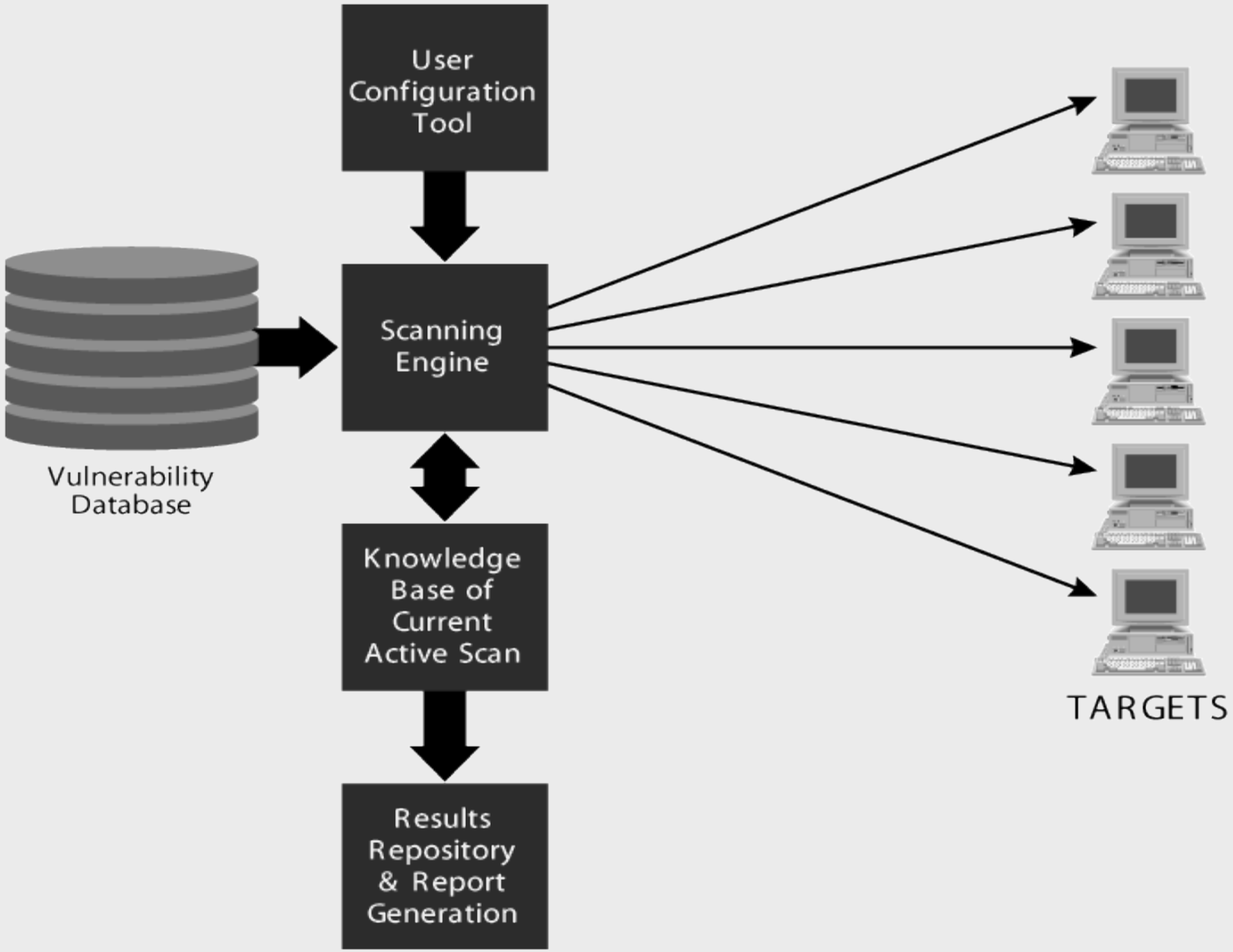


Figure 6.16 Components of a vulnerability scanner

Free Vulnerability Scanners

- SARA http://www-arc.com/sara
- SAINT http://www.wwdsi.com/saint
- VLAD http://razor.bindview.com/tools
- Nessus http://www.nessus.org

Commercial Vulnerability Scanners

- Network Associates' CyberCop Scanner http://www.pgp.com/products/cybercop-scanner/default.asp
- ISS's Internet Scanner http://www.iss.net
- Cisco's Secure Scanner http://www.cisco.com/warp/public/cc/pc/sqsw/nesn
- Axents NetRecon http://www.axent.com
- eEye's Retina Scanner http://www.eeye.com

Nessus

- Free
- Source code available for review
- Support for new vulnerability checks
- You can write your own vulnerability checks in C or in Nessus Attack-Scripting Language(NASL)

Nessus Plug-Ins

- Small modular programs to check for a specific vulnerability
- Categories of plug-ins
  - Finger abuses
  - Windows
  - Backdoors
  - Gain a shell remotely
  - CGI abuses
  - General
  - Remote file access
  - RPC
  - Firewalls
  - FTP
  - SMTP problems
  - Useless services
  - Gain root remotely
  - NIS
  - Denial-of-Service
  - Miscellaneous

Nessus Architecture

- Nessus server includes a vulnerability database (set of plug-ins), a knowledge base of the current active scan, and a scanning engine
- Supports strong authentication for the client-to-server commumication via public key encryption
- Nessus server runs on Unix platforms (Solaris, Linux, FreeBSD)
- Nessus client runs on Linux, Solaris, FreeBSD, Windows9x, Windows NT/2000, and any Java-enabled browser (eg. Macintosh with Netscape)

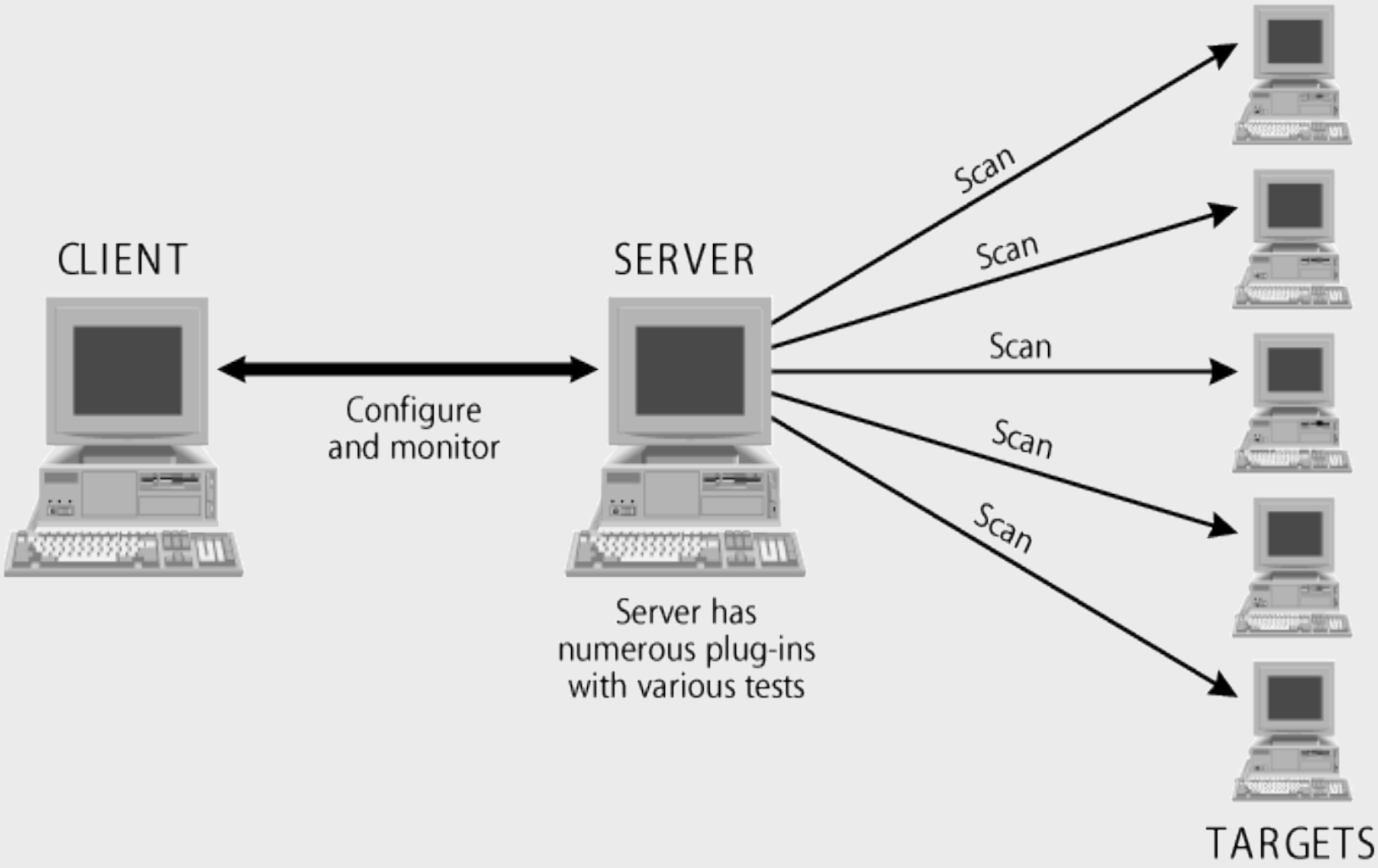


Figure 6.17 The Nessus architecture

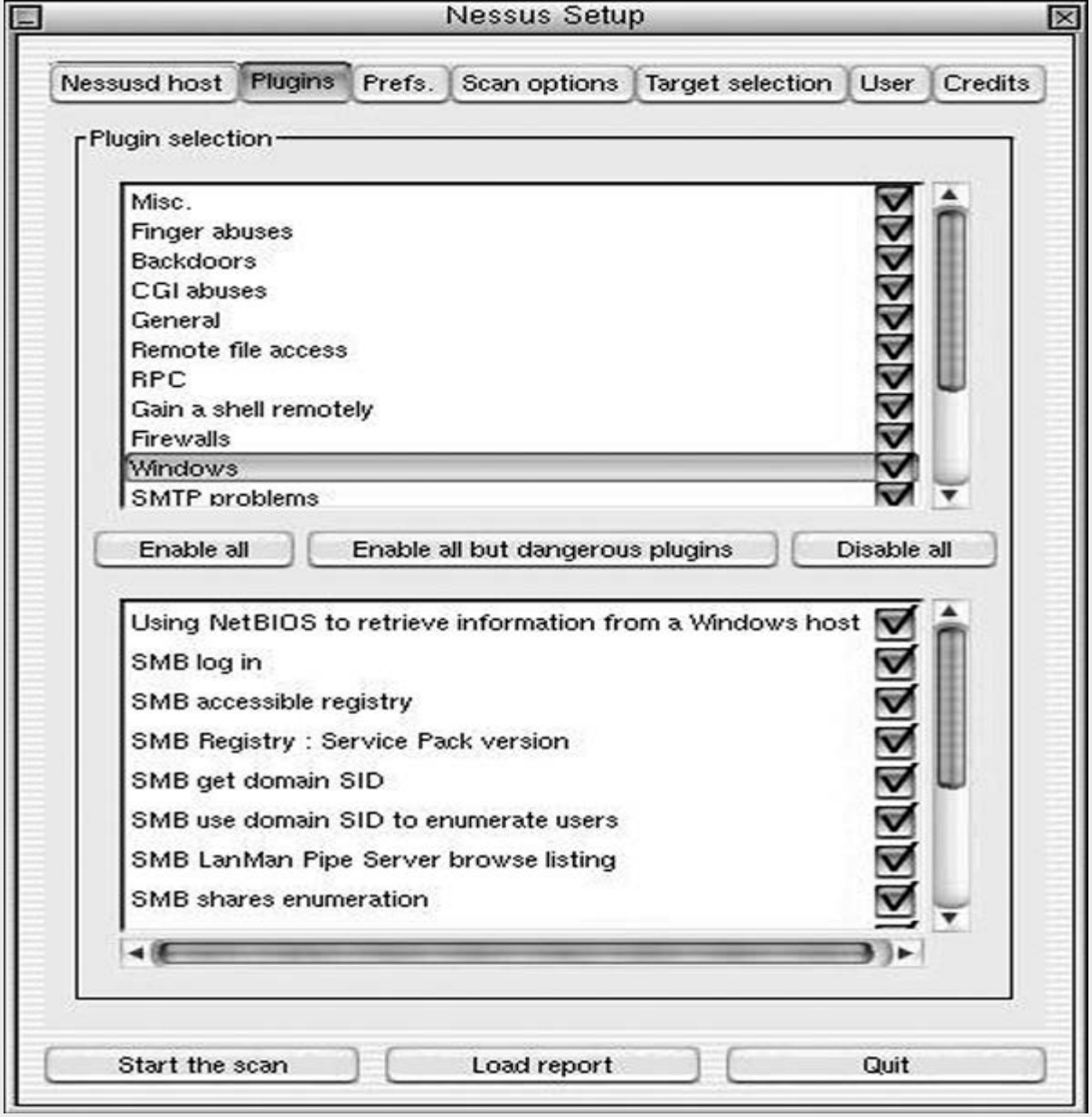


Figure 6.18 The Nessus GUI supports the selection of various plug-ins

Nessus Vulnerability Scan Report

- Used by attackers to find exploit code via search engines and attacker-friendly web sites

Vulnerability Scanning Defenses

- Scan your own network using latest vulnerability database
  - Do not use dangerous plug-ins against production servers
- Close all unused ports
- Apply patches to your systems
- Have policy and practices for building and maintaining secure systems

Network-based Intrusion Detection Systems

- Network-based IDSs have a database of attack signatures used to match against network traffic
- When an attack is detected, an administrator can be notified via email or pager

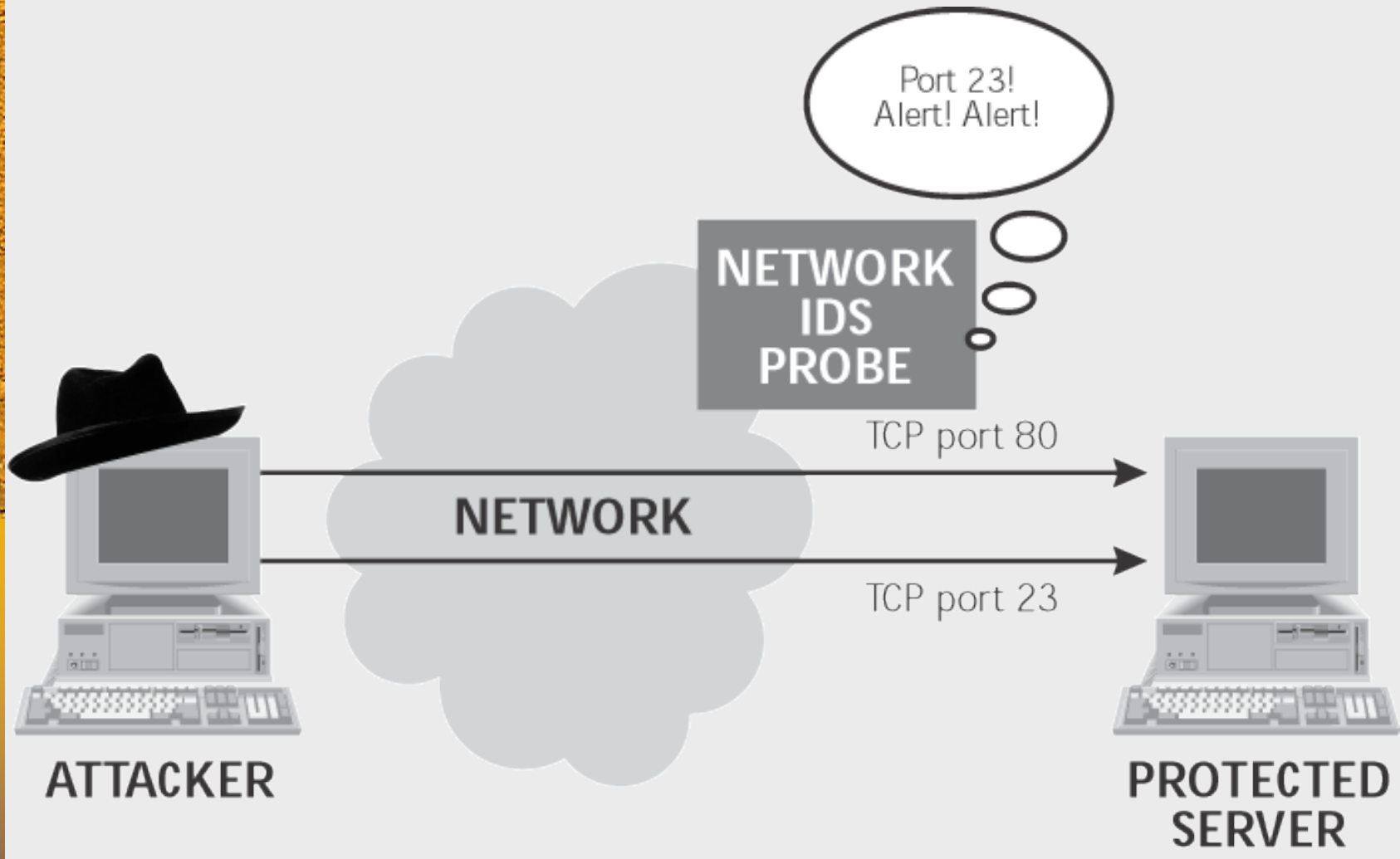


Figure 6.19 A network-based intrusion detection system configured to detect telnet access to a server

Evading Network-Based Intrusion Detection Systems

- Modify appearance of traffic so it does not match the signature
- Change the context

IDS Evasion at the Network Level

- Use IP fragments on IDSs that cannot perform packet reassembly
- Send a flood of fragments to saturate IDS prior to attacking targets
- Fragment the packets in unexpected ways

Tiny Fragment Attack

- Create an initial fragment that is very small
- Packet is sliced in the middle of the TCP header

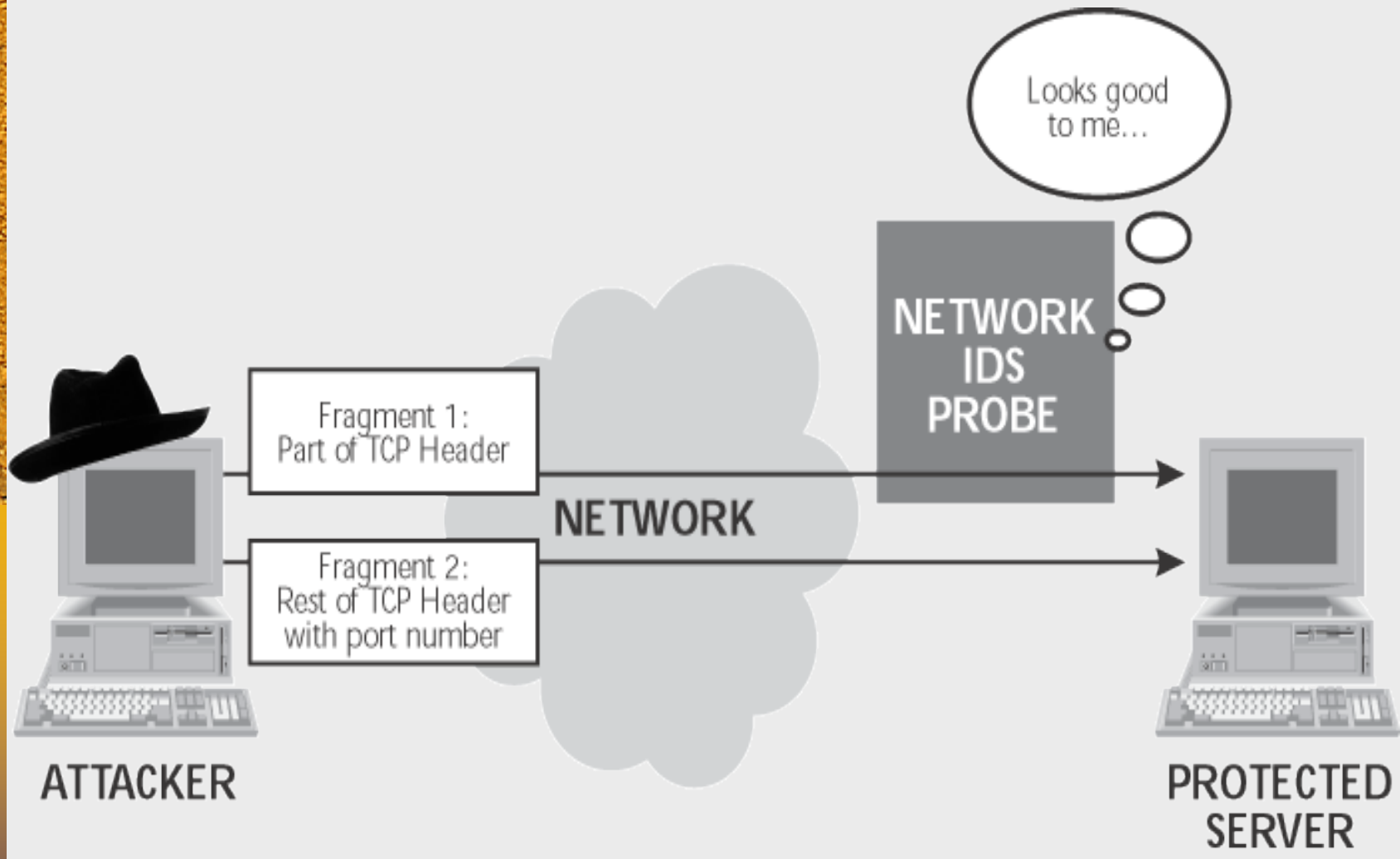


Figure 6.20 The tiny fragment attack

Fragment Overlap Attack

- Manipulates the fragment offset field of the IP header
- Each IP packet is fragmented into to packets
- First fragment contains TCP port number of a harmless service not closely monitored
- Second fragment has an offset value so small that the fragments overlap during reassembly

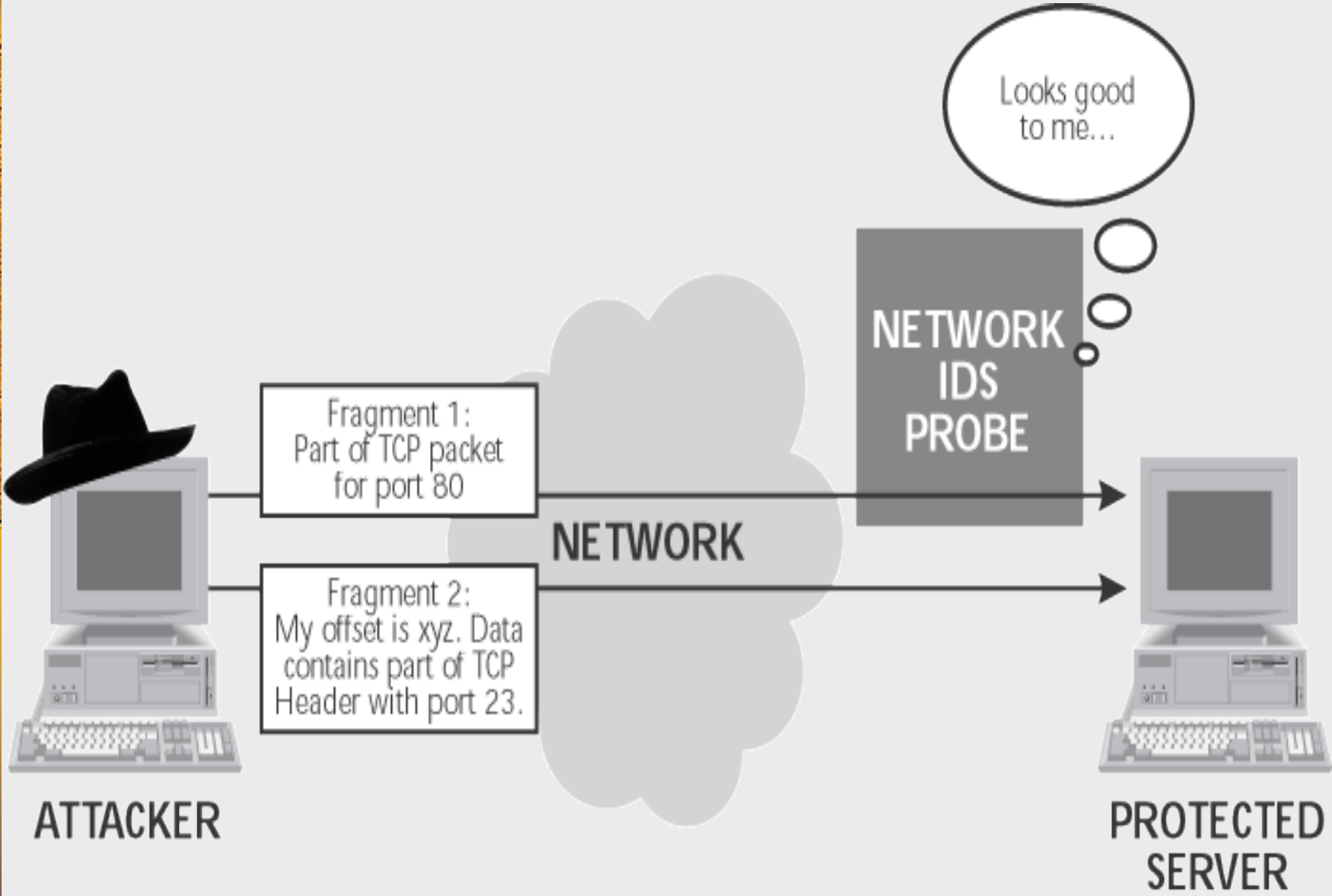


Figure 6.21 A fragment overlap attack

Fragmentation Attacks using FragRouter

- FragRouter
  http://www.anzen.com/research/nidsbench
- Runs on BSD, Linux, and Solaris
- A router that fragments all packets in various ways
- Works in combination with other attack tools

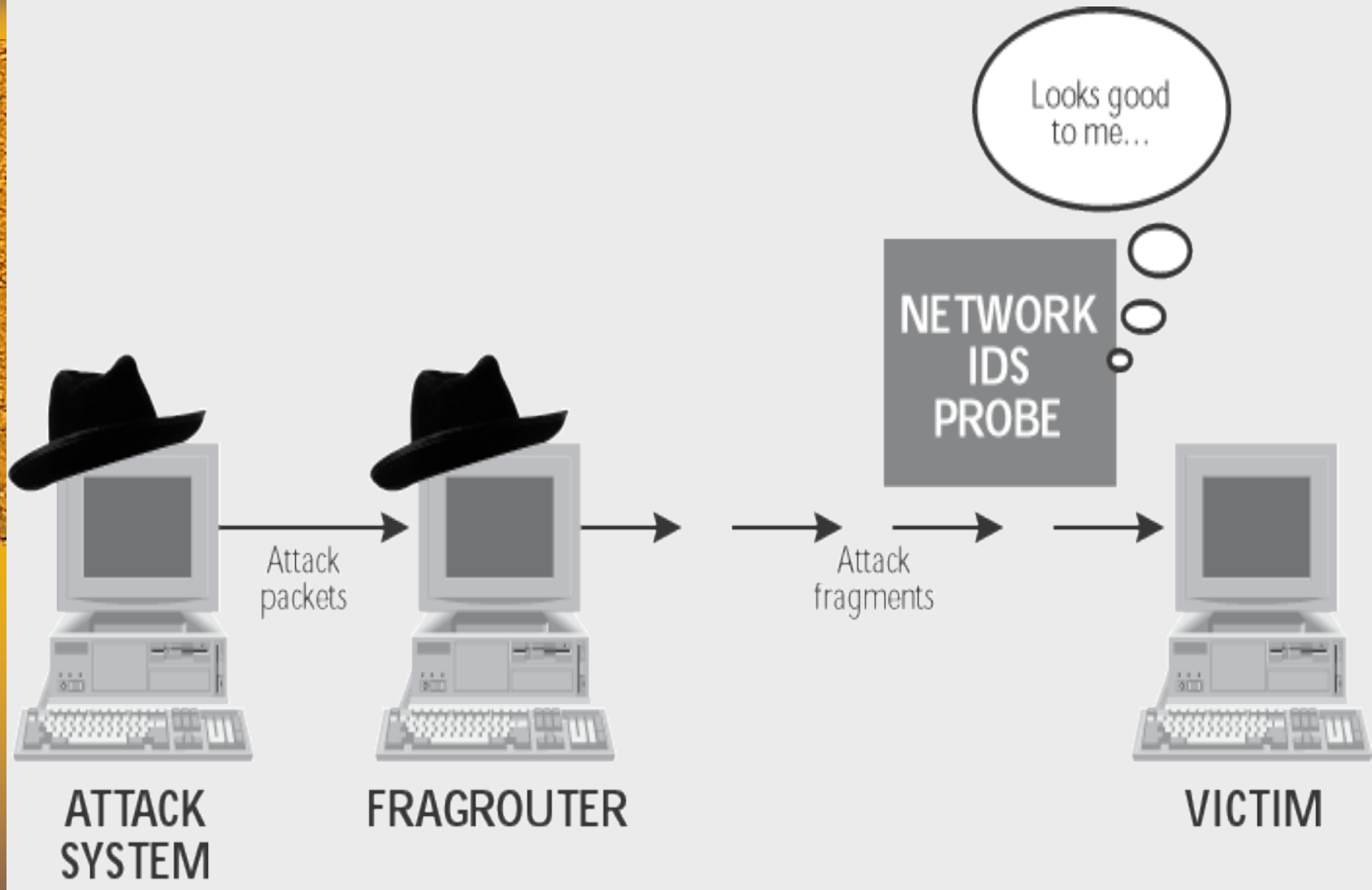


Figure 6.22 Using FragRouter to evade IDS detection

Whisker

- Whisker http://www.wiretrip.net/rfp
- Scanning tool that looks for vulnerable CGI scripts on Web servers
- Evades network-based IDS detection at Application Level by subtly changing the format of the CGI requests
- Manipulates the request so that they do not match the IDS signatures exactly

Whisker's IDS Evasion Tactics

- URL Encoding with unicode equivalent
- /./ directory insertion
- Premature URL ending
- Long URL
- Fake parameter
- Using Tab in lieu of space separation
- Case sensitivity
- Windows delimiter
- Null method
- Session splicing

IDS Evasion Defenses

- Keep attack signatures on IDS systems up-to-date
- Use both network-based and host-based IDS
- Use host-based IDS agent on sensitive Web, DNS, and mail servers

NETWORK-BASED IDS

HOST-BASED IDS

Figure 6.23 Host-based IDS versus network-based IDS