

---

# Network Mapper and Vulnerability Scanning



# Avviso

---

- Per la legge italiana questi strumenti sono equivalenti a strumenti per lo scasso
- Possono essere posseduti solo da chi ha un ruolo professionale che lo giustifichi
- Possono essere usati solo sui nodi della propria rete per scoprire errori di configurazione



# Scanning

---

- Può essere eseguito sia dall'attaccante che dal difensore
- L'attaccante lo esegue per raccogliere informazioni sul sistema per analizzarlo e scoprirne le vulnerabilità
- Il difensore lo esegue per capire cosa attaccante può scoprire e quindi cosa può fare



# What Can We Scan For

---

- Modems (and other telephone devices)
- Live Hosts
- TCP ports
- UDP ports
- Promiscuous NICs



# Modems

---

- Repeatedly dial phone numbers looking for a modem to answer or other things
  - War Dialers – used to find modems
  - Demon Dialers – once a modem is found repeatedly dial it and guess passwords
- Other things
  - Free phone calls – if the phone answers and gives a dial tone the number will let you dial another number, some companies do this so that roaming employees can dial into the company or into a company owned 800 number



# 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

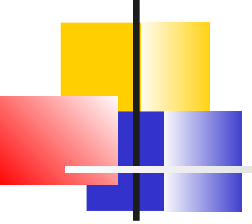
# Live Hosts



---

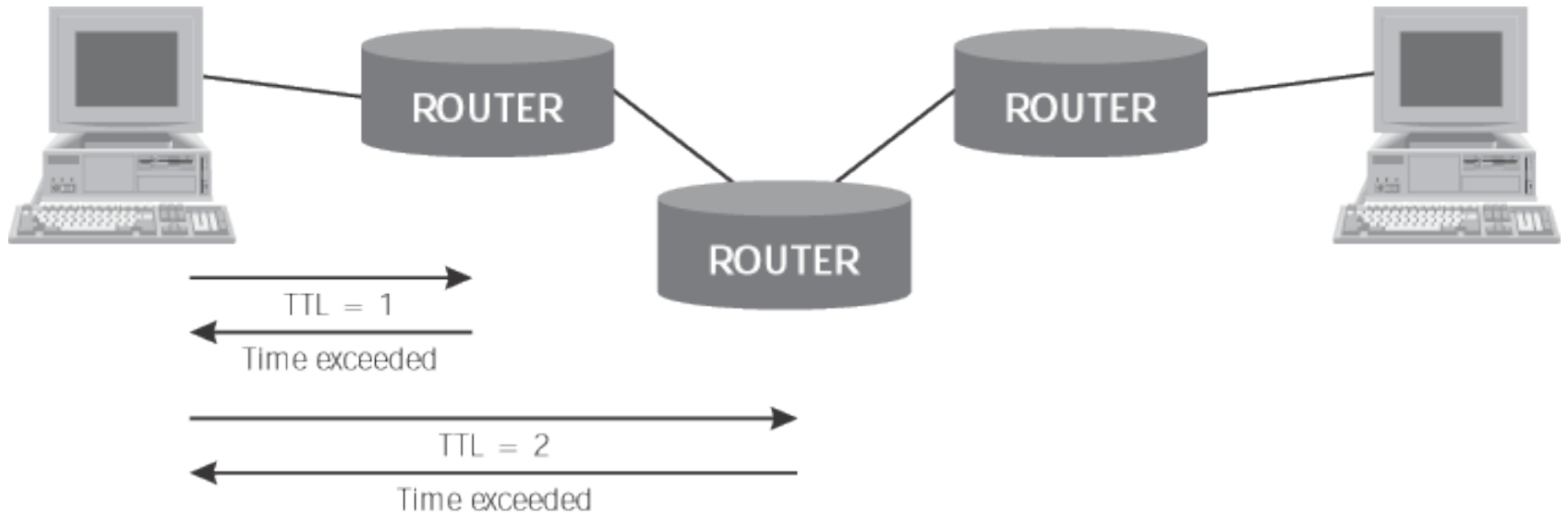
- Try pinging (ICMP Echo request) all hosts on a particular subnet to see who replies
  - No reply indicates host is not live
  - Incoming ICMP messages are blocked
- It's a good idea to block incoming ICMP messages at the firewall
- If no reply a hacker would try connecting to a commonly open port (TCP port 80) or sending a UDP packet to a commonly open port.
- In java (which doesn't do ICMP) send a ping using JNI to execute the ping command as an OS command line command.

# 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



# discover path from source to destination



Traceroute

# Windows NT tracert output

```
Command Prompt
D:\> tracert 10.15.15.1

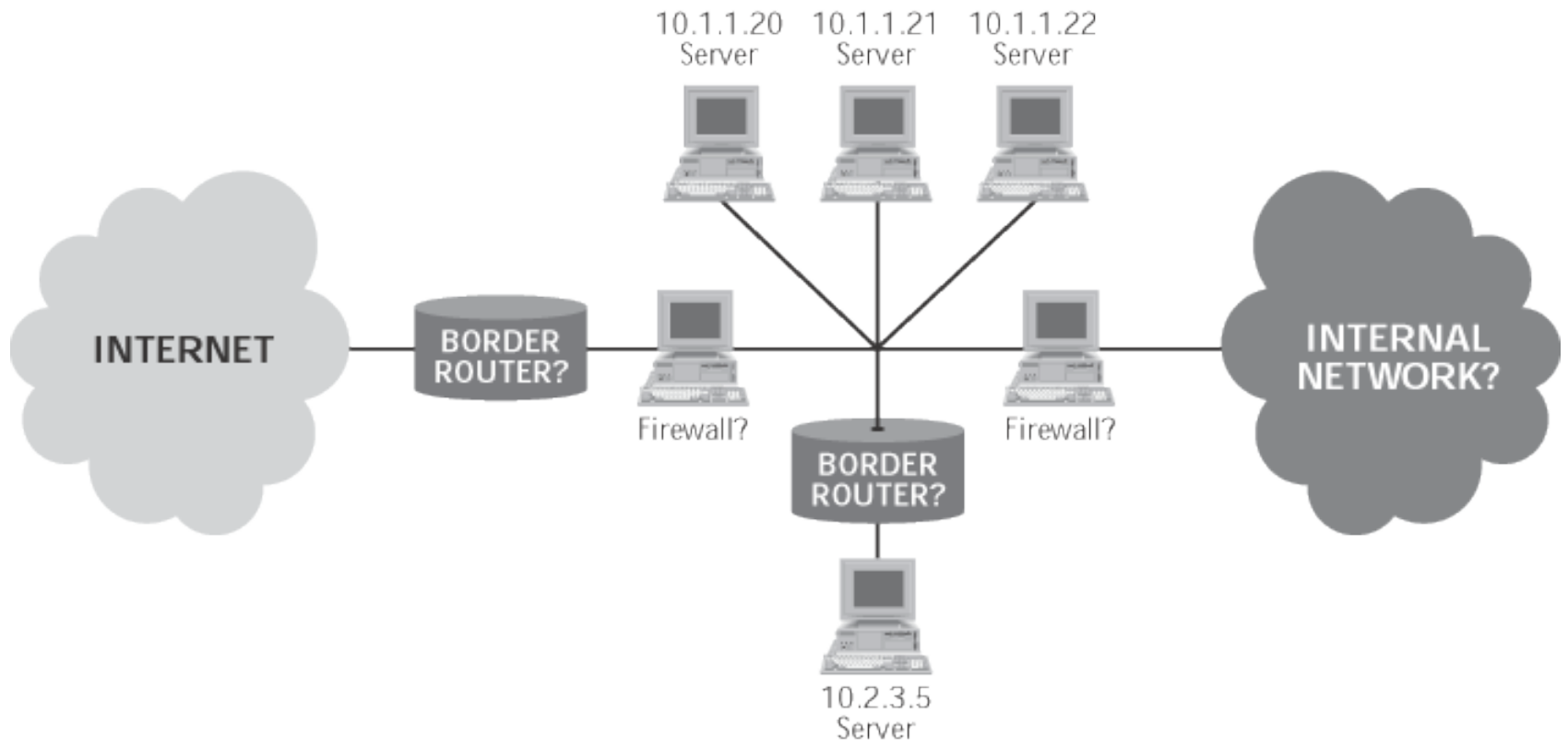
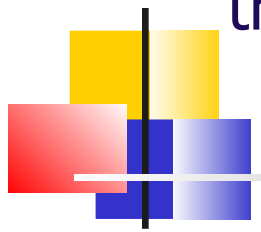
Tracing route to 10.15.15.1 over a maximum of 30 hops:

  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

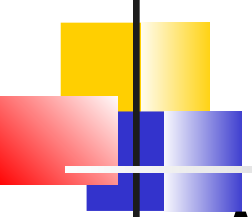
Trace complete.

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

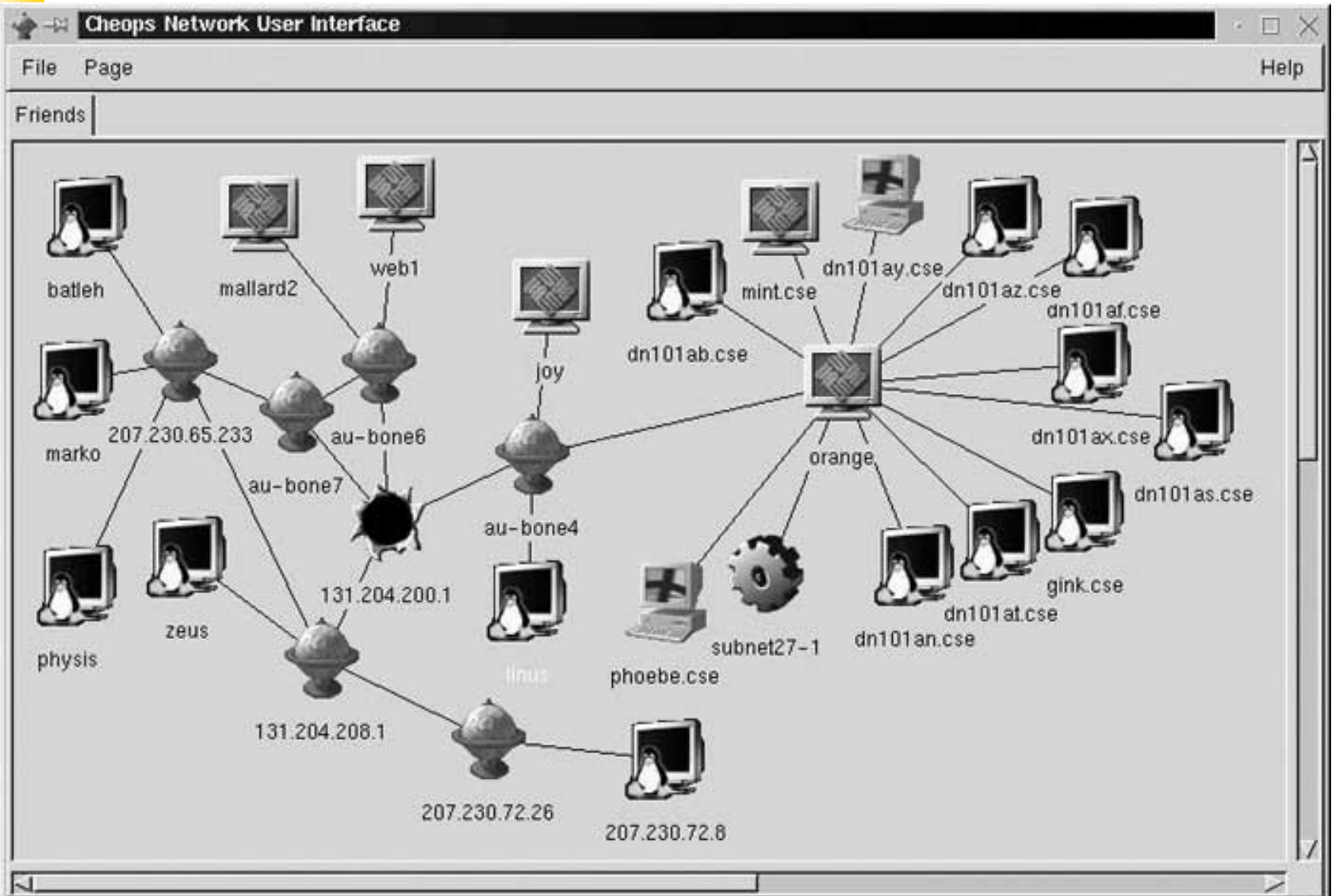
# Network diagram created by attacker using ping and traceroute



# Cheops

- 
- 
- A nifty network mapper tool
  - Runs on Linux
  - Generates network topology by using ping sweeps and traceroute
  - Supports remote operating system identification using TCP Stack Fingerprinting

# The Cheops display



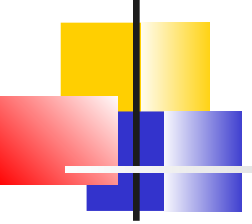


# Defenses against Network Mapping

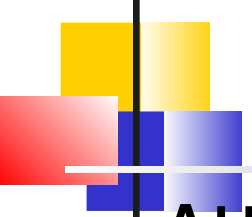
---

- 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

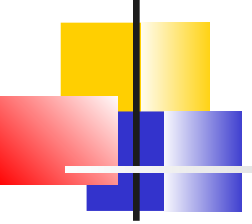
- 
- 
- Used to find open ports
  - Free port scanning tools
    - Nmap
    - Strobe
    - Ultrascan

# Port scanning

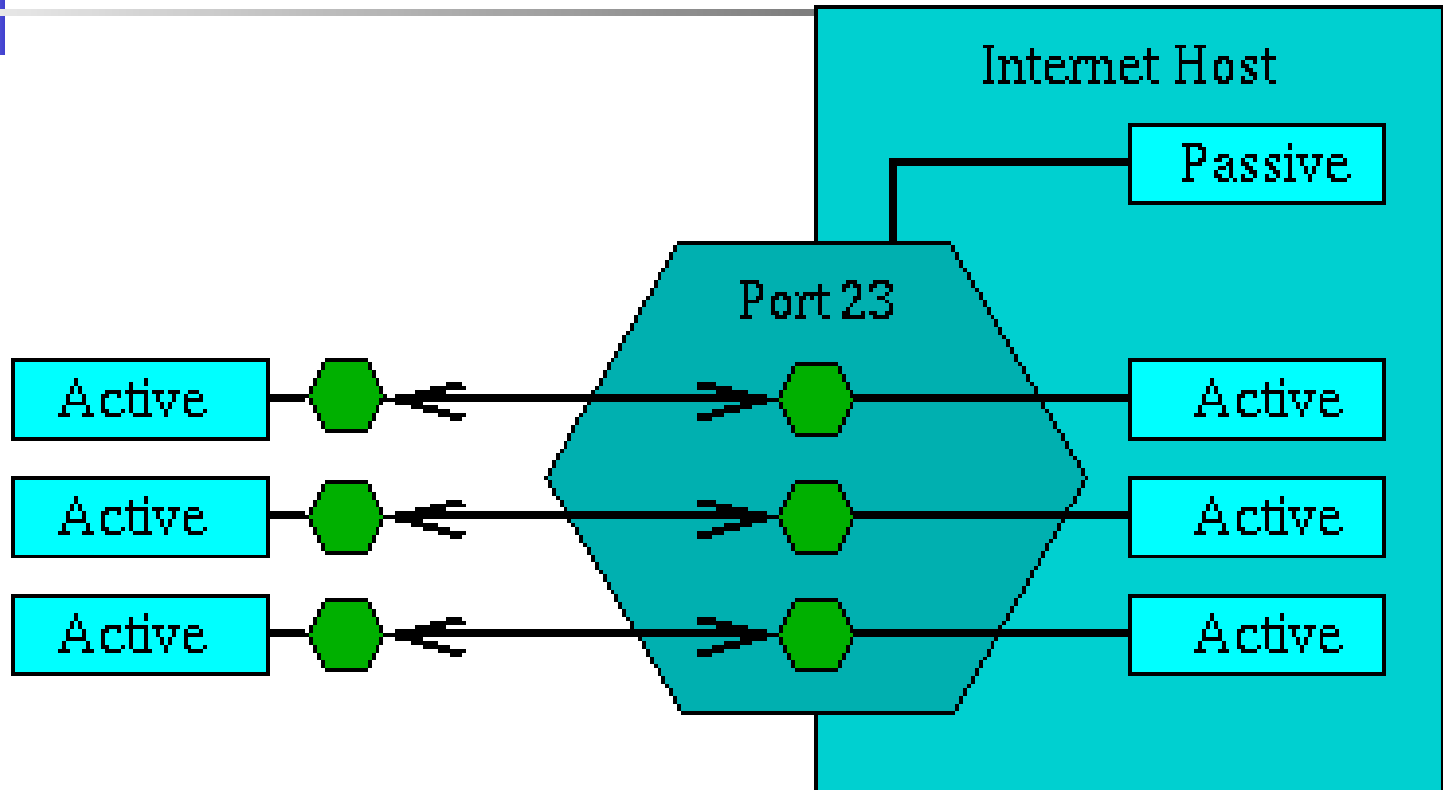
- 
- 
- Attackers wish to discover services they can break into.
  - Security audit: Why are certain ports open?
  - sending a packet to each port, one at a time.
    - Based on the type of response, an attacker knows if the port is used.
    - The used ports can be probed further for weakness.

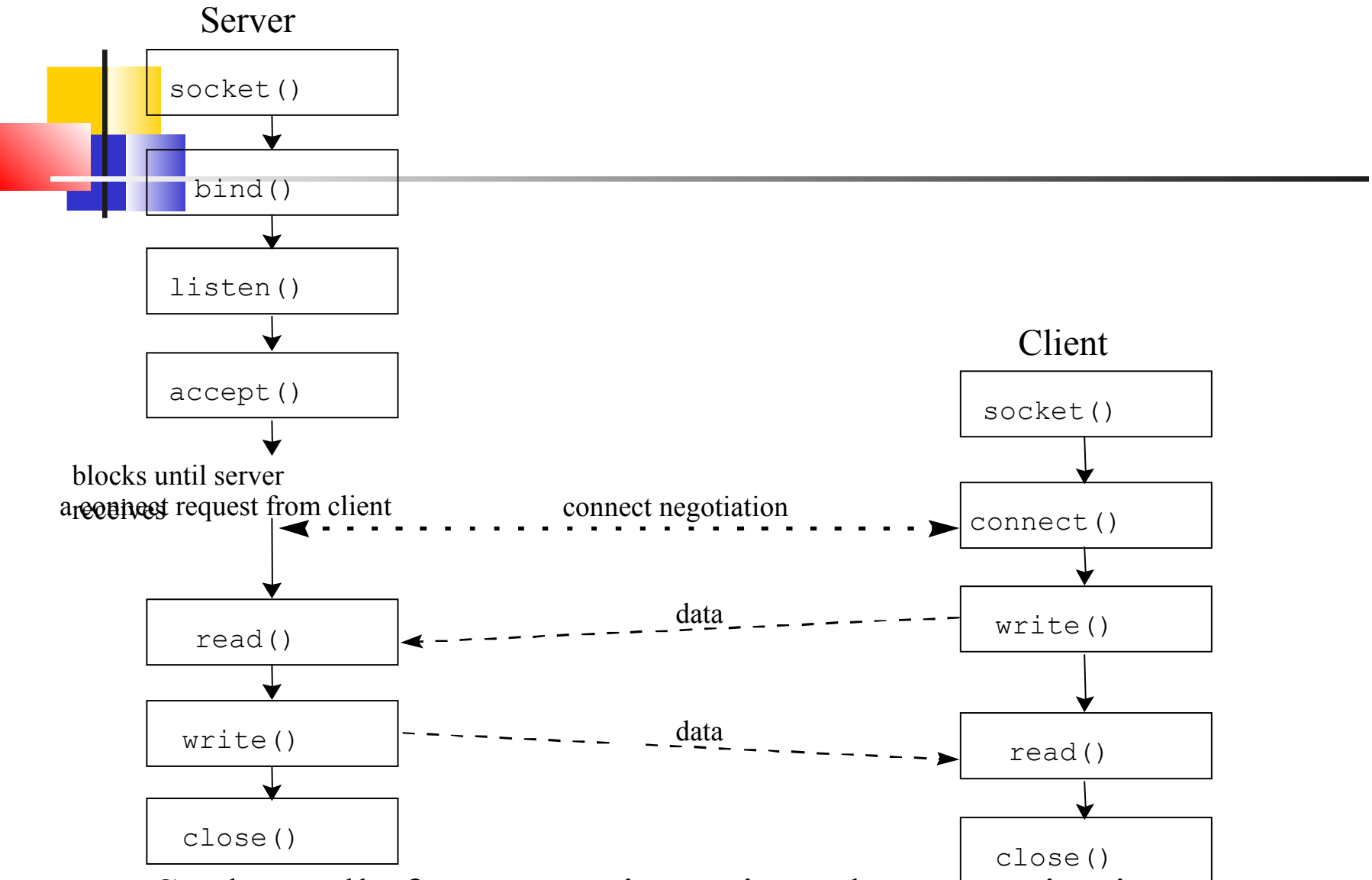


# Port Numbers

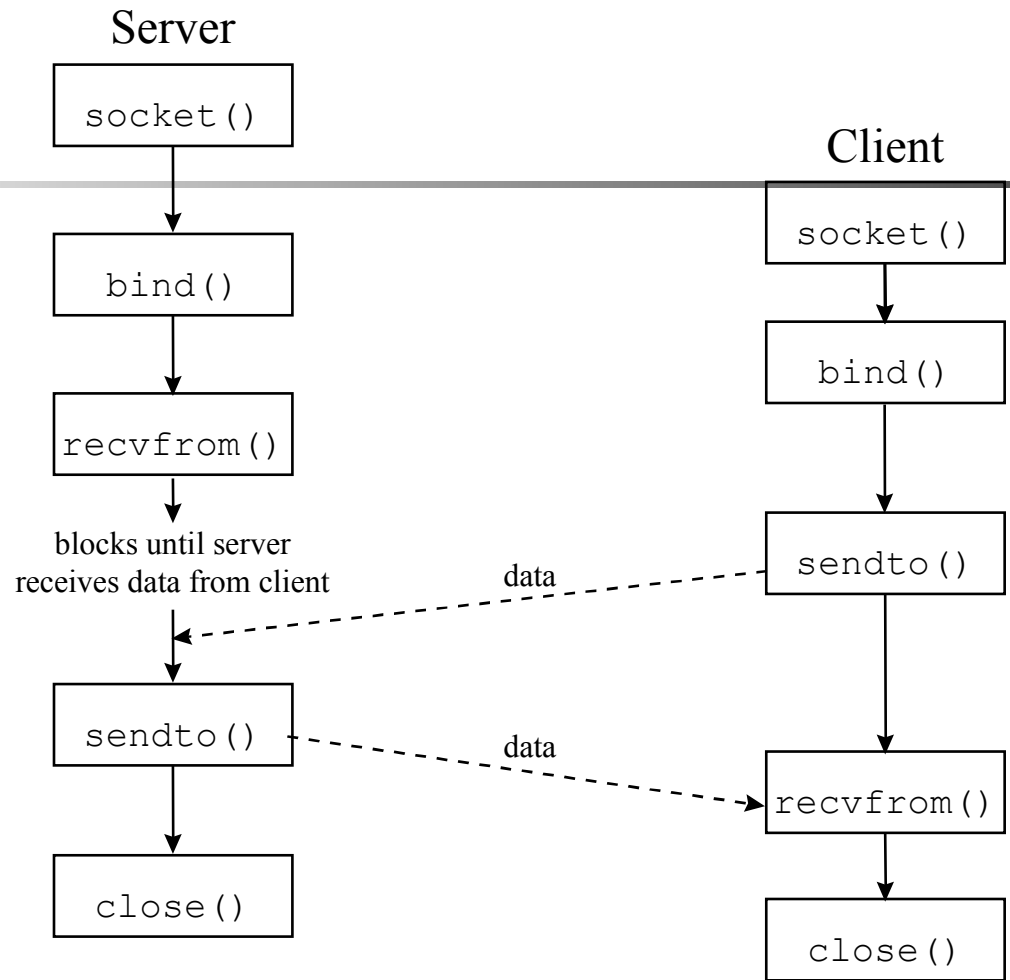
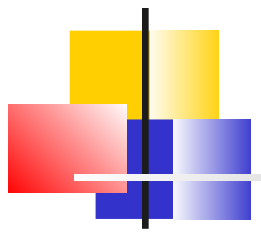
- 
- 
- An abstraction of the OS + Net Stds
  - Part of UDP and TCP packets
    - UDP and TCP port numbers are disjoint
    - Typical to use the same port number for both UDP and TCP service
    - E.g., 80/TCP and 80/UDP for www
  - 16-bit unsigned integer
  - Well Known Ports (0 .. 1023)
  - Registered Ports (1024 .. 49151)
  - Dynamic and/or Private Ports (49152 .. 65535).
  - [www.iana.orghttp://assignments/ port-numbers](http://www.iana.org/http://assignments/port-numbers)

# Sockets





Socket calls for connection-oriented communication



Socket calls for connectionless communication

# Well Known: 0 - 1023



---

- Only root-privileged programs are allowed to open these ports.
- Examples
  - ftp-data 20/udp
  - ftp 21/tcp
  - ssh 22/tcp
  - telnet 23/tcp
  - Time 37/tcp
  - Time 37/udp
  - Whois 43/tcp
  - Imap 143/tcp



# Registered: 1024 ..49151

---

- Ordinary programs/users can use these
- shockwave2 1257/tcp Shockwave 2  
shockwave2 1257/udp Shockwave 2
- x11 6000-6063/tcp X Window System x11  
6000-6063/udp X Window System



Dynamic/Private: 49152 .. 65535

---

- Ordinary programs can use these

# State of a Port



- Open

- A service process is listening at the port.
- The OS receives packets arriving at this port and passes the messages to the service process.
- If the OS receives a SYN at an open port, this is the first packet of the three way handshake.

- Closed

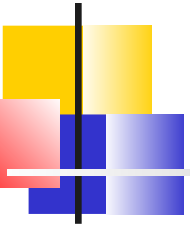
- No process is listening at the port. If the OS receives a SYN at a closed port, an RST is sent.

- Filtered

- A packet filter is listening at the port DOS DOS DOS :-)

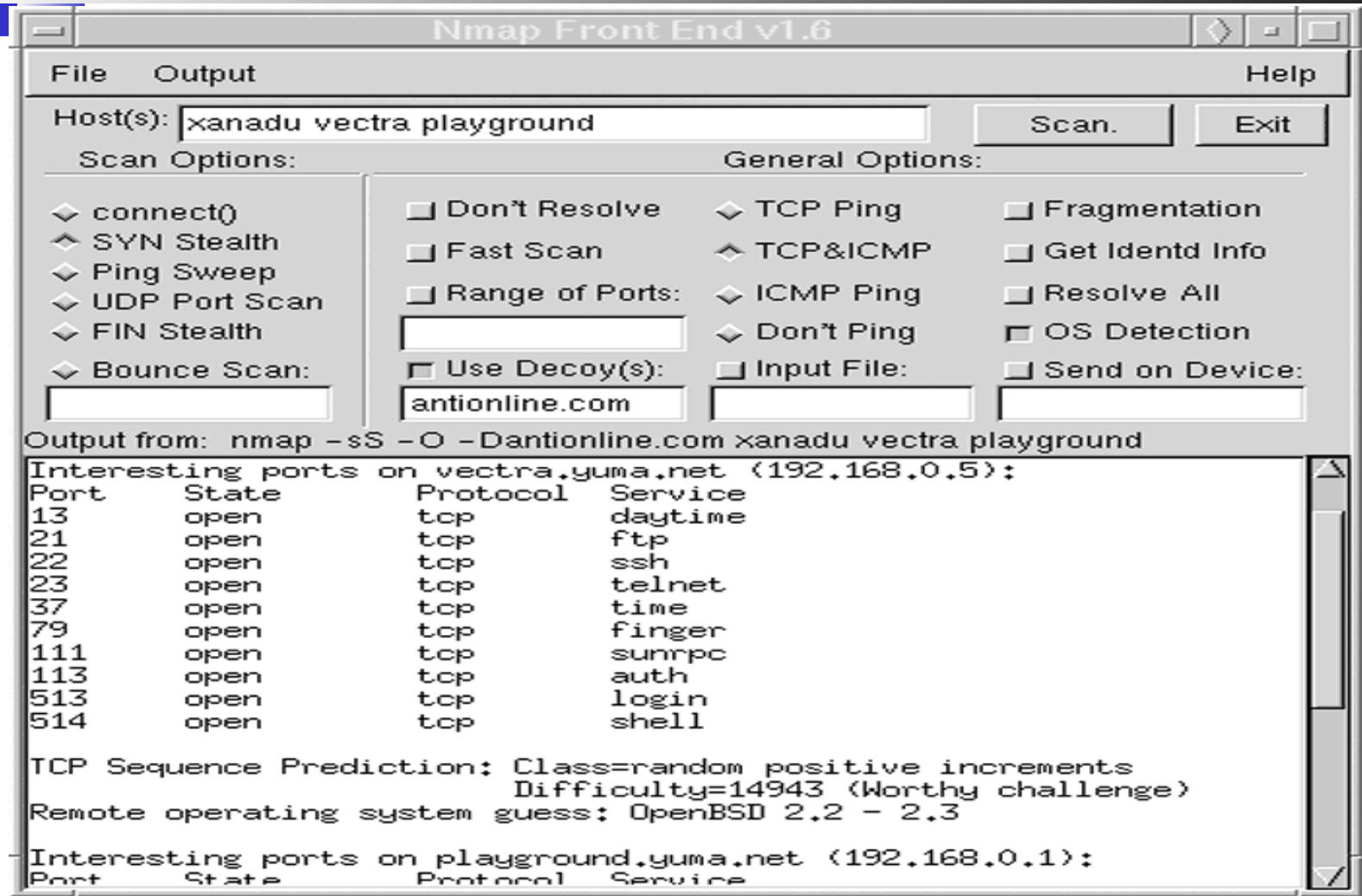


# Nmap



- 
- Full-featured port scanning tool
  - Unix version
  - Windows NT version

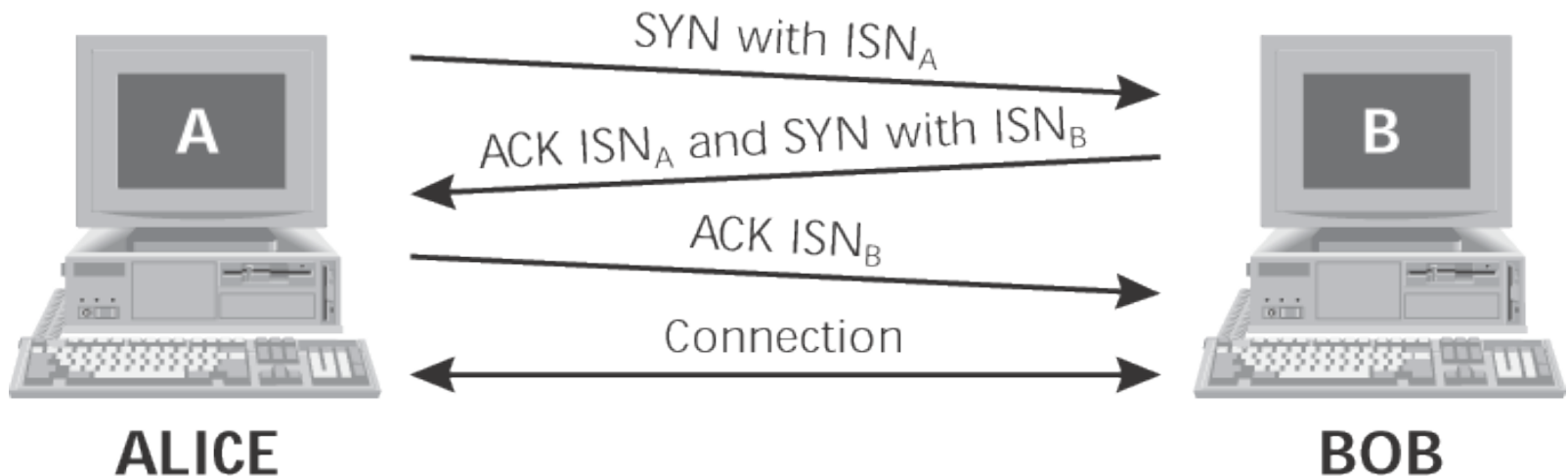
# Nmapfe: A nice GUI for Nmap



# Scan Types supported by Nmap

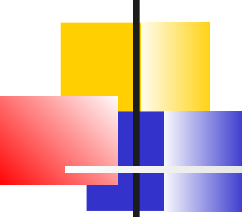
## ◆ TCP Connect (-sT)

- Attempts to complete 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 receive either no response, a RESET packet, or an ICMP Port Unreachable packet.
- Not stealthy



# Scan Types supported by Nmap

## (cont.)

- 
- 
- TCP SYN (-sS)
    - 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
    - It may result in a denial-of-service attack with slow target

# Scan Types supported by Nmap

## (cont.)

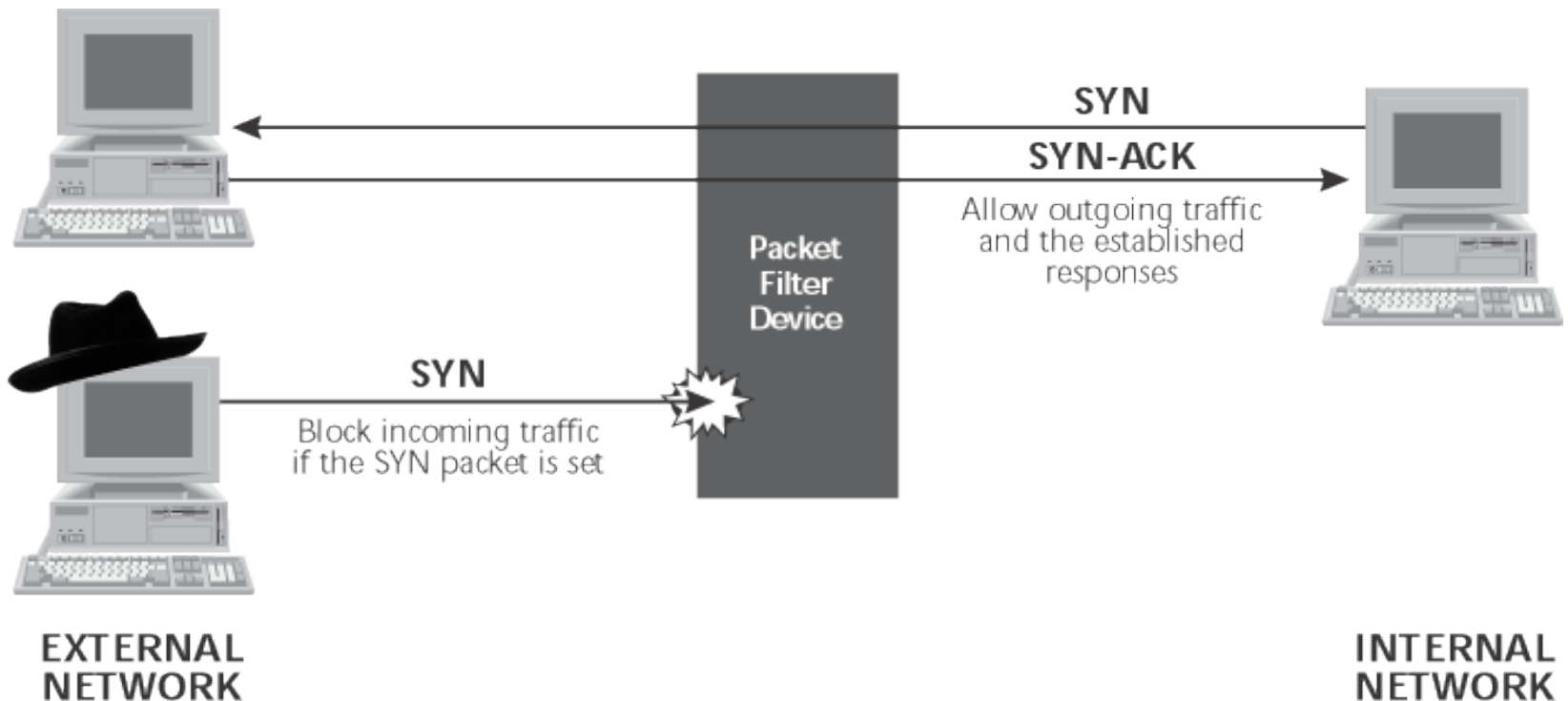
---

- 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.

# Scan Types supported by Nmap (cont.)

## ◆ TCP ACK (-sA)

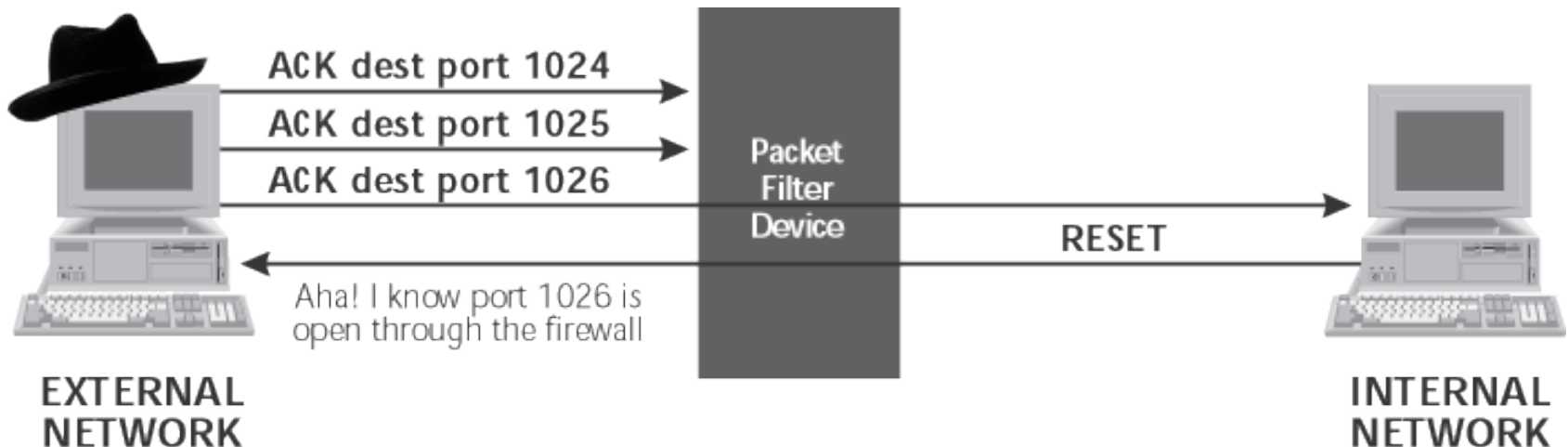
- Sends a packet with the ACK code bit set to each target port.
- Allows attacker to get past some packet filtering devices



# ACK scanning

## ◆ 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



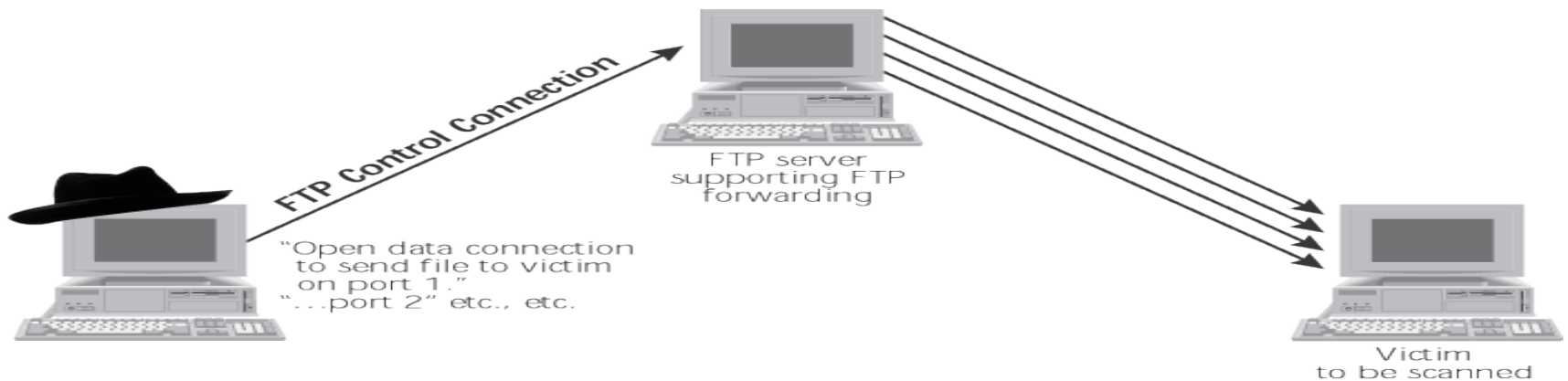
# Scan Types supported by Nmap (cont.)

## ◆ 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)

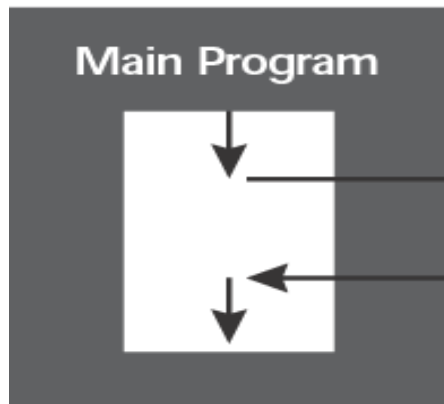
- Sends ICMP echo request packets to every machine on the target network, allowing for locating live hosts. This isn't port scanning; it's network mapping.
- Can use TCP packets instead of ICMP to conduct Ping sweep

# Scan Types supported by Nmap (cont.)

## ◆ RPC Scanning (-sR)

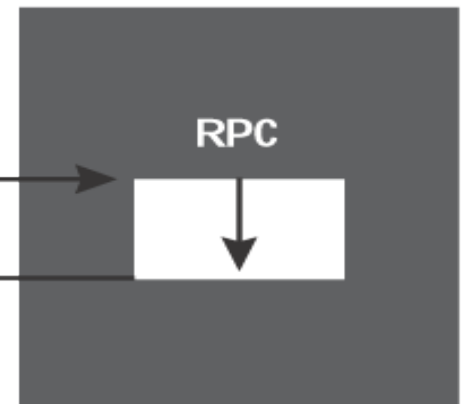
- Scans RPC services using all discovered open TCP/UDP ports on the target to send RPC NULL commands. Tries to determine if an RPC program is listening at the port and identifies type of RPC program

The main program runs here, until execution needs to be passed to the server.



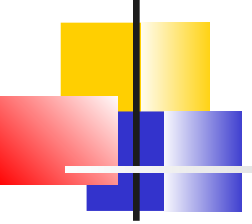
**CLIENT SYSTEM**

The RPC runs here, operating on behalf of the client. When the procedure is finished, results are returned back to the calling program on the client machine.

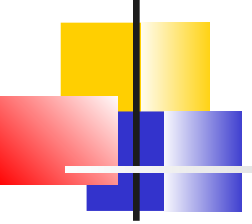


**SERVER SYSTEM**

## 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

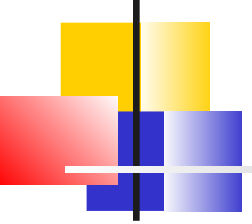


# TCP Stack Fingerprinting

---

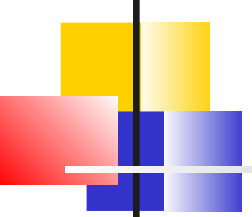
- To determine target OS, Nmap sends various abnormal packets
  - NULL packet to open port
  - SYN/FIN/URG/PSH packet to open port
  - SYN packet to closed port
  - ACK packet to closed port
  - FIN/PSH/URG packet to closed port
  - UDP packet to closed port
  - series of SYN packets to determine predictability of Initial Sequence Number
- Nmap compares responses against database describing systems response and sequence number prediction check

# Nmap timing options

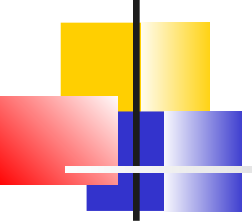
- 
- 
- Paranoid = Send one packet every 5 minutes
  - Sneaky = Send one packet every 15 seconds
  - Polite = Send one packet every 0.4 seconds
  - Normal = Send packets ASAP without missing target ports
  - Aggressive = wait no more than 1.25 seconds for any response
  - Insane = wait no more than 0.3 seconds for any response

Prone to traffic loss

# Defenses against Port Scanning

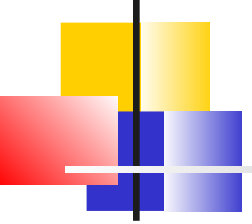
- 
- 
- Unix systems
    - remove all unneeded services in `/etc/inetd.conf`
    - Remove unneeded services in `/etc/rc*.d`
  - Windows systems
    - uninstall unneeded services or shut them off in the services control panel
  - Scan your own systems before the attackers do
  - Use stateful packet filter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

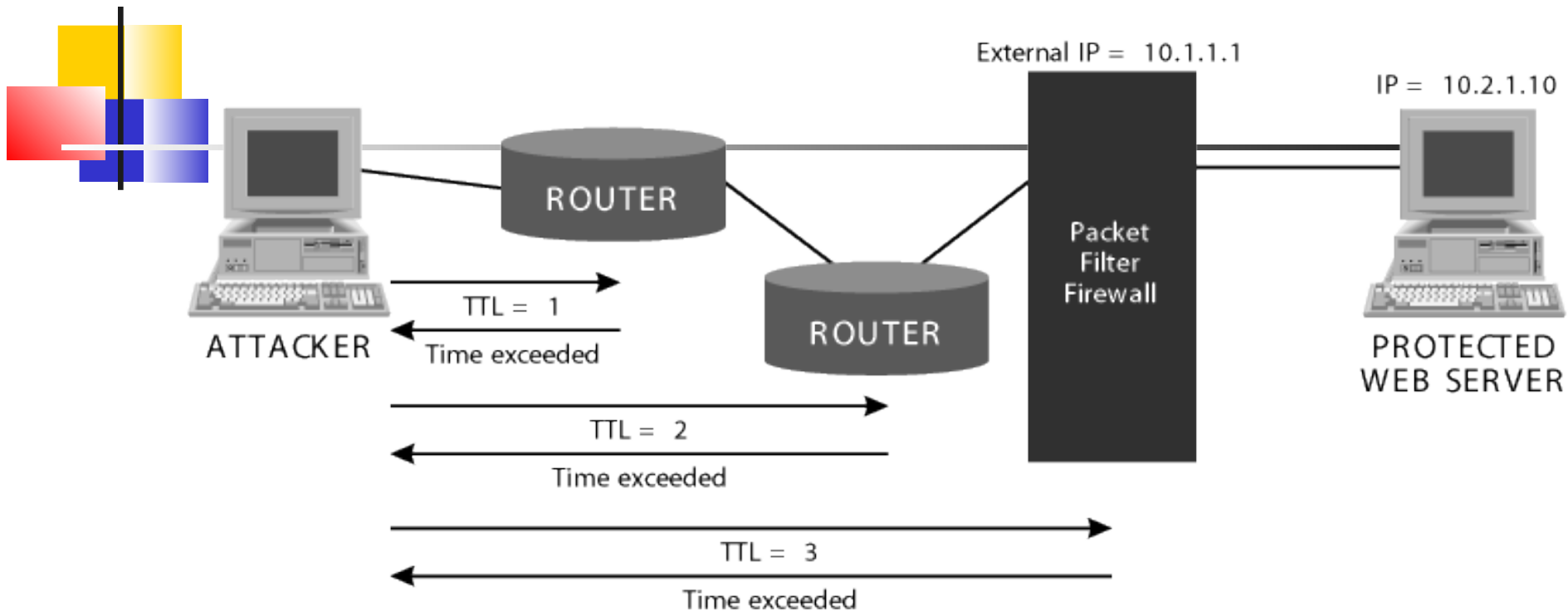
# Firewalk

- 
- 
- Tool which allows attacker to determine packet filter rules
  - sends packets through a packet filter device to determine which ports are open *through* it
  - Identifies TCP and UDP ports that filter allows new connection initiations



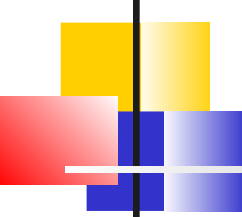
# Firewalk Network Discovery Phase

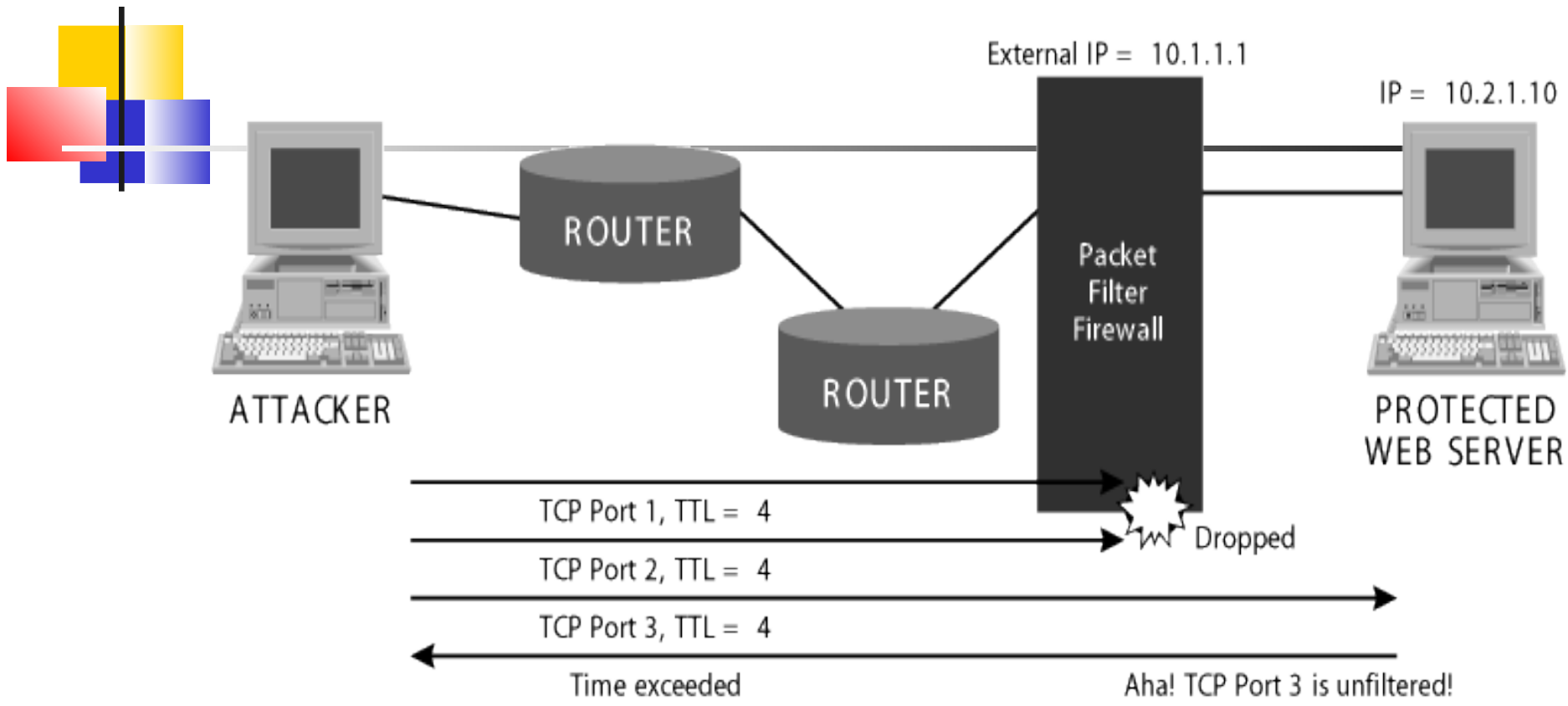
- 
- 
- Requires the attacker to specify IP address of the packet-filtering device and IP address of destination machine
  - Sends packets with incrementally higher TTL values until ICMP Time Exceed message is received from packet-filtering device



Firewalk network discovery phase counts the number of hops to the packet filter firewall

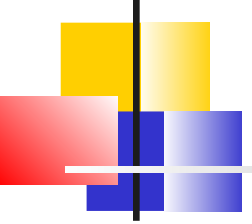
# Firewalk Scanning Phase

- 
- 
- It generates 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



Firewalk scanning phase determines open ports through the packet filter firewall

# Firewalk Defenses

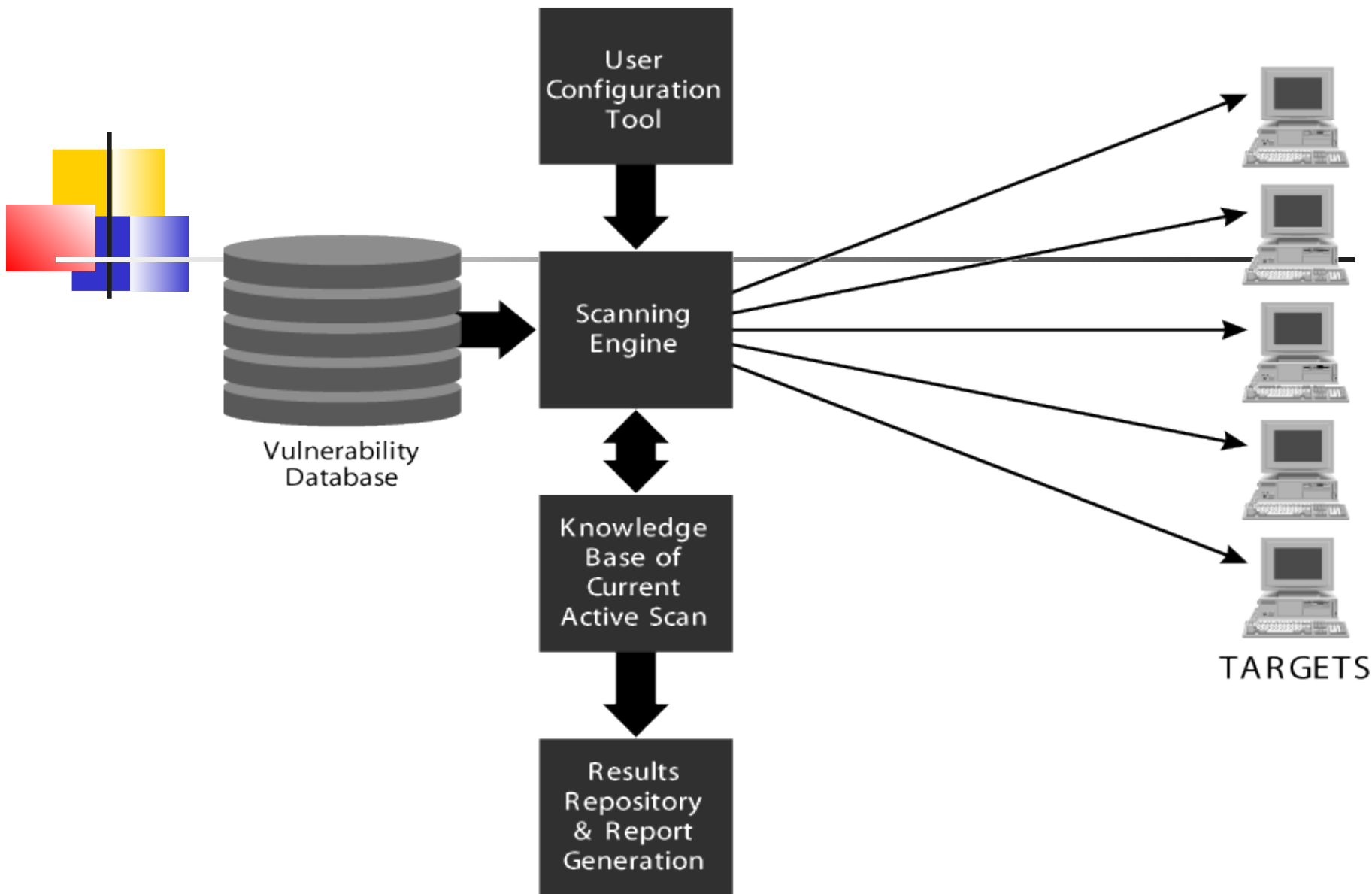
- 
- 
- Configure firewall to pass a minimum set of ports
  - Accept the fact that an attacker can determine your packet filter rules
  - Filter out ICMP Time Exceeded messages leaving your network
    - Side effect of crippling traceroute
  - Replace traditional and stateful packet filters with proxy-based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



# Vulnerability Scanning Tool

---

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



Components of a vulnerability scanner



# Free Vulnerability Scanners

---

- SARA
- SAINT
- VLAD
- Nessus



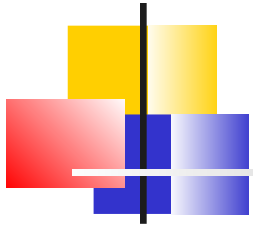


# Nessus

---

- 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
  - Backdoor
  - CGI abuses
  - Remote file access
  - Firewalls
  - SMTP problems
  - Gain root remotely
  - Denial-of-Service
  - Windows
  - Gain a shell remotely
  - General
  - RPC
  - FTP
  - Useless services
  - NIS
  - Miscellaneous

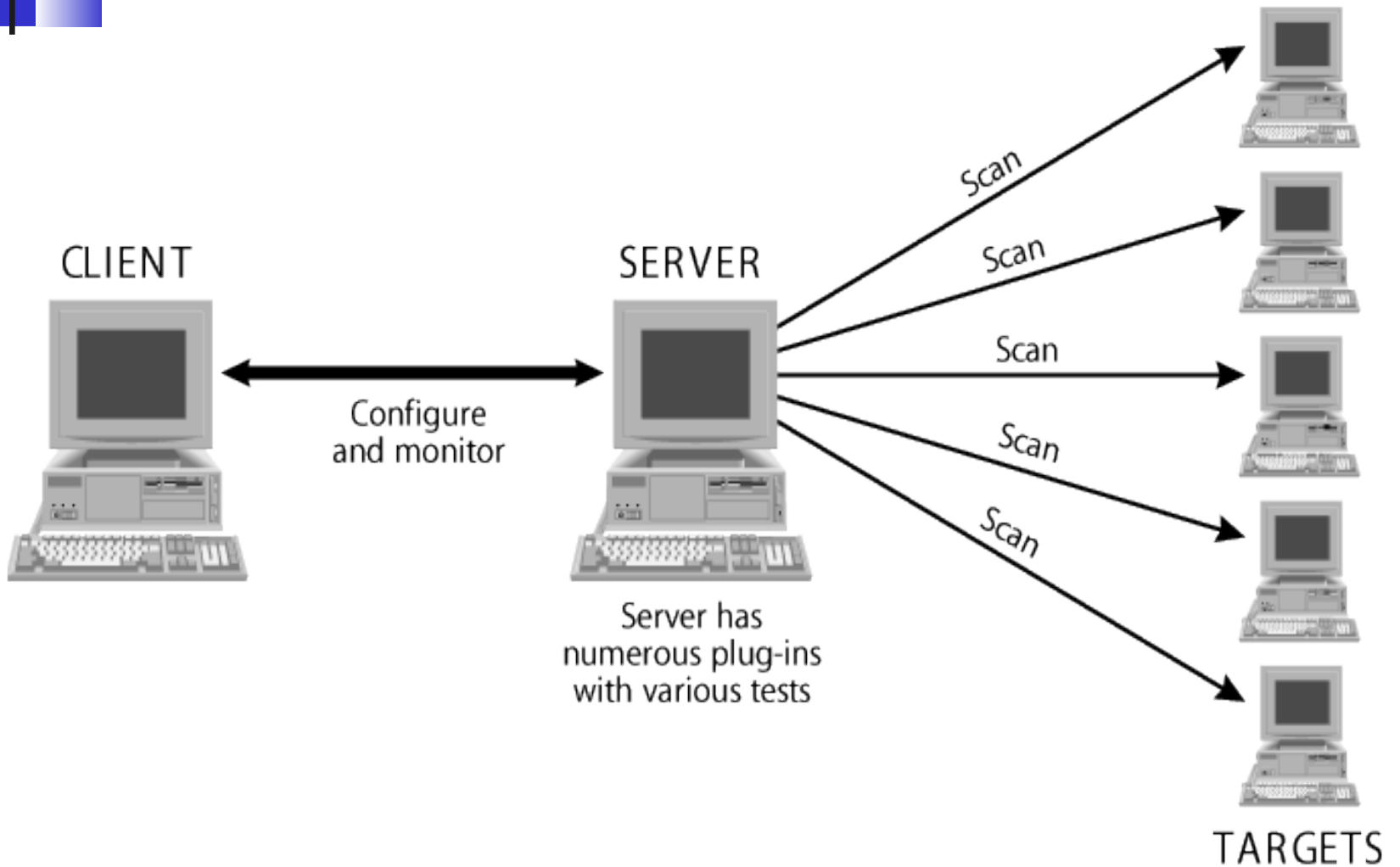


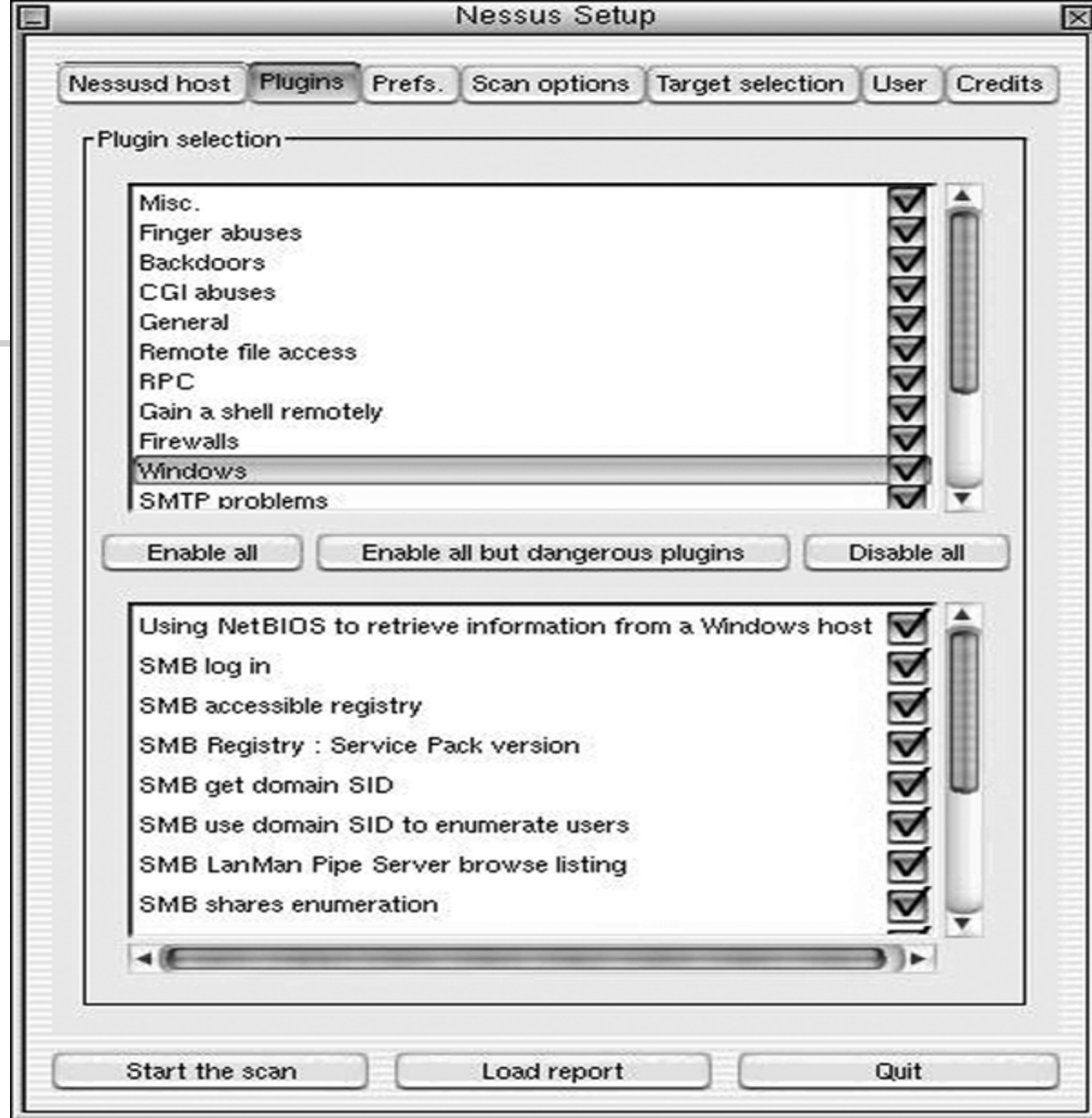
# Nessus Architecture

---

- 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 communication 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)

# The Nessus architecture





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