



"If I had six hours to chop down a tree, I'd spend the first four hours sharpening the axe."  
- Abraham Lincoln

## Topics

Hardening Via Scripts

Cisco ACLs

Infrastructure Security

Media Security

## In the News



### Seoul blocks access to 31 North Web sites

**November 19, 2004** — The Ministry of Information and Communication said yesterday that it has blocked access to 31 Internet sites operated by North Korea, or sites containing what South Korea considers "pro-North Korea" propaganda. The National Intelligence Service and the National Police Agency asked the information ministry to block the sites; the ministry took action on Nov. 12, the ministry's spokesman said. The Web sites include the site of the Korea Central News Agency, the North's state-run wire news service, and that of Kim Il Sung Open University, a distance learning program operated by the communist state to spread the country's founding juche, or self-reliance, ideology. The action was based on the National Security Law, which bars the spread of materials praising North Korea and its leaders.

## In the News

**CNN.com** MEMBER SERVICES  
**TECHNOLOGY**  
**Gates world's most spammed person**  
Receives 4 million emails per day, most of it spam  
Thursday, November 18, 2004 Posted: 5:10 PM EST (GMT)

**SINGAPORE (AP)** — Forget trying to flood Bill Gates' e-mail inbox with junk.

The Microsoft Corp. chairman receives 4 million e-mails a day, but practically an entire department at the company he founded is dedicated to ensuring that nothing unwanted gets into his inbox, the company's chief executive said Thursday.

"There are two people who probably are the number one spam recipients in the world," Steve Ballmer said.

"Bill Gates (is first) because he is Bill Gates. Bill literally receives four million pieces of e-mail per day, most of it spam."

Ballmer said Microsoft has special technology that just filters spam intended for Gates.

"Literally there's a whole department almost that takes care of it," he said.

Microsoft has a department set up to filter spam intended for Gates, Microsoft's chief executive says.

**Popular Spam Filter**  
Free Trial, easy and reliable Anti Spam program - Stop Spam Now.  
[www.spilinks.com](http://www.spilinks.com)

**Spam Inspector... Stop Spam**  
Spam Inspector's award winning spam protection for Outlook, Outlook

## "Cool" Security Story

Pirated programs accounted for 55% of software used in Korea in 2003, substantially higher than the world average of 38%

After a year-long crackdown, the Korea Software Property Council (SPC) found 858 companies used illegal software, costing domestic developers 9 billion won.

## The Results

Despite crackdowns, the rate of piracy increased from 45% to 55%

Most copied: Microsoft, Haansoft and Ahn's Anti-Virus Lab.

They plan to make a film with CEOs of software companies encouraging consumers to use legal products.

## In the News - November 19, 2004

The Broward School District paid \$5 million to provide the \$1,200 Apple laptops to four schools, including Miramar High School. The goal was to see whether student performance improves with daily access to a computer.

Video: Stolen Laptops

## In the News

**SOPHOS** anti-virus, anti-spam and email policy for business  
Home Contact English Deutsch Español Français Italiano 日本語  
Home Virus info Articles

29 October 2004

**Bagle-AU worm disables Windows XP SP2 firewall, reports Sophos**

Experts at Sophos have warned users that the new W32/Bagle-AU worm attempts to disable security software on infected Windows PCs.

"By turning off firewall protection and other security software the author of the latest incarnation of the Bagle worm is opening up computers to attack," said Graham Cluley, senior technology consultant for Sophos. "Increasingly virus writers are aiming to take over innocent peoples' computers in order to steal, spam or launch denial of service attacks."

Sophos notes that the W32/Bagle-AU worm is capable of turning off the firewall built into Microsoft's recent Windows XP Service Pack 2 update.

"Just because you are running the latest version of Windows XP you shouldn't think you are necessarily protected from this worm," continued Cluley. "If you launch it on a PC running Windows XP SP2 it can turn off your firewall opening the door to hackers and other internet attacks."

**Firewall**  
OFF

The Bagle-AU worm can disable security applications, including the firewall built into Windows XP Service Pack 2.

## Hardware Firewalls not Perfect Either

### Cisco IOS DHCP Packet Handling Denial of Service Vulnerability

**Secunia Advisory:** SA13148  
**Release Date:** 2004-11-11

**Critical:** ■ ■ ■ ■  
**Less critical**  
**Impact:** DoS  
**Where:** From local network  
**Solution Status:** Vendor Patch

**OS:**  
[Cisco IOS 12.x](#)  
[Cisco IOS R12.x](#)  
[Cisco ONS 15000 Series](#)

Select a product and view a complete list of all Patched/Unpatched Secunia advisories affecting it.

**Description:**  
A vulnerability has been reported in Cisco IOS, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the processing of DHCP packets. This can be exploited to block the input queue on an interface by sending some specially crafted DHCP packets to a vulnerable device.

Successful exploitation requires that the DHCP server or relay agent is enabled (default setting), but not necessarily configured.

**In the News - January 26, 2010****BlueCross BlueShield of Tennessee****Breach is Proving to be Costly**

A security breach at BlueCross BlueShield of Tennessee has already cost the company more than US \$7 million. Last October, 57 hard drives were stolen from an abandoned office. The company is likely to have to spend considerably more money to determine exactly what information the drives contained and provide identity fraud protection for consumers. As many as 500,000 people are believed to be affected by the breach. The stolen drives were waiting to be sent back to the manufacturer for disposal.

**In the News - January 20, 2010****People Leaving USB Drives in Clothing****Pockets, Say Cleaners**

A UK survey found that 4,500 USB drives have been found in people's clothing pockets when they were taken to dry cleaners. That number is half what it was a year earlier, but this could be explained by a shift to users downloading data to smartphones and netbooks as opposed to increased vigilance about data security. USB drive security was in the news recently when several manufacturers acknowledged a vulnerability in the access control mechanism of their devices.

**In the News - Feb 20, 2010****Spying school update: turned on webcams****42 times, FBI isn't sure that's legal**

Remember the Pennsylvania school district that was accused of remotely flipping on the webcams of students' laptops? As if the civil suit filed on behalf of those students wasn't going to be enough trouble for the Lower Merion representatives, now it seems the FBI wants to know just what's going on, launching an investigation into the practice. For its part the district said that it remotely activated the cams 42 times, and that it only did so with the bestest of intentions: when trying to locate a missing laptop. It would also like to point out that only two employees had the power to flip the switch, and that they only captured images -- never sound.

# Security Demo

## Automated Hardening

**Hardening with Syskey**

Start Windows 2000 server on Vmware  
 Revert the Image  
 Start / Run / syskey  
 Encryption Enabled - Click Update  
 Password Startup  
 A password to boot windows  
 System Generated Password  
 Store Startup key on Floppy Disk  
 Floppy is required to boot system  
 Store Startup key Locally  
 Restart Windows

**Hardening using a Template**

Start Windows 2000 server on Wmware  
 Revert the Image  
 Start / Run / mmc  
 Console / Add/Remove Snap-in... Add  
 Security Configuration and Analysis  
 Security Templates  
 Expand Security Templates  
 Select Templates

**Analyzing**

Right-Click Security Configuration...  
 Open Database  
 C:\winnt\security\database  
 Make copy of file  
 Select copy  
 Right-Click Security Configuration...  
 Import Template  
 Select any  
 Right-Click Security Configuration...  
 Analyze Computer Now  
 Expand Setting

**Hardening**

Right-Click Security Configuration...  
 Configure Computer Now  
 Right-Click Security Configuration...  
 View Log File  
 Right-Click Security Configuration...  
 Export  
 Start / Programs / Admin Tools / Local  
 Security Policy  
 Right-Security Settings / Import

**IIS Lockdown Tool**

Install iislockd.exe  
 Next / Agree / Next  
 Select Template, View Template  
 Remove Unselected Services  
 Disable Scripts  
 Additional Security  
 URL Scan  
 Apply Settings  
 View Log

# In Class

## Cisco ACL

### Router Access Control Lists

Packet Inspections

Access Control Lists (ACL)

Example: Since telnet transmits in cleartext, let's disable it

```
access-list 101 deny any any eq 23
```

### ACL Fundamentals

Standard ACL (1-99)

```
access-list number {permit | deny} source-address
```

Extended ACL (100-199)

```
access-list number {permit | deny} protocol source-address [port] destination-address [port]
```

### Access List Examples

Allow established TCP sessions everywhere

```
access-list 101 permit tcp any any established
```

Allow Telnet to Server3 from anyone

```
access-list 101 permit tcp any host 206.195.2.3 eq 23
```

Allow pc2 to ftp to ftp1

```
access-list 101 permit tcp host 206.195.1.2 host 206.195.4.1 eq 21
```

```
access-list 102 permit tcp host 206.195.4.1 eq 20 host 206.195.1.2
```

### Notes

ANY

Same as 0.0.0.0 255.255.255.255

Established

TCP packet with ACK flag

Single Host

host 206.195.2.3

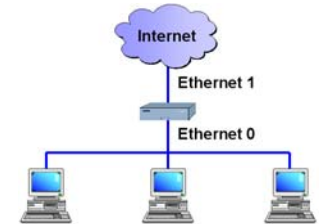
206.195.2.3 0.0.0.0

Range of Address

206.195.2.0 0.0.0.255

Default Deny All

### Example



```
access-list 101 permit tcp any any established
access-list 101 permit tcp any 206.195.0.0 0.0.255.255 eq 23
access-list 102 permit tcp any any established
access-list 102 permit tcp 206.195.0.0 0.0.255.255 any eq 23
interface Ethernet1
ip access-group 101 in
ip access-group 102 out
```

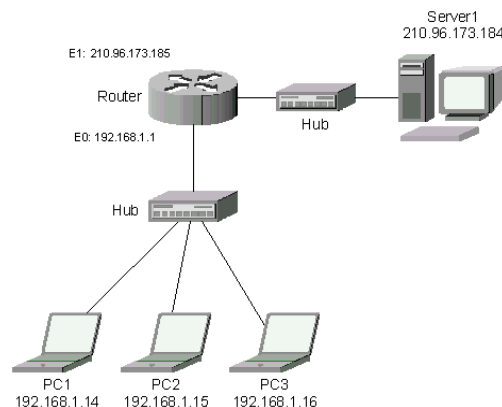
### ACL Configuration Worksheet

Rule	ACL #	Permit or Deny	Protocol	Source IP	Source Port	Destination IP	Destination Port	Other

Create one for Each Interface

Use in a spreadsheet

### The Network



### In Class

Write the ACLs for the following rules

Allow PC1 to telnet to router

Allow PC1 to SSH to Server1

Allow all PCs to access web

Allow all systems to ping

# Security+

## Domain 3: Infrastructure Security

### Switches

- Operate at Level 2 of OSI
- Routes via MAC address
- Eliminates Packet Collisions
- Reduces sniffing

### Switch Features

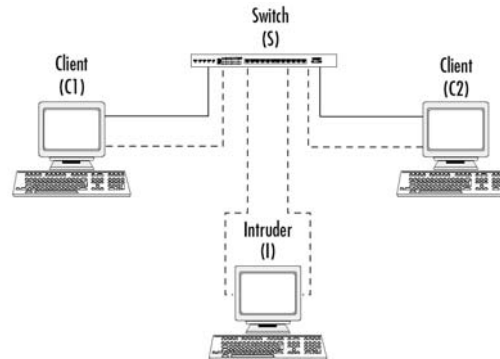
- Administrator Access
- SPAN
  - Switches Port Analyzer
  - Copies all data to specific port
  - Used for troubleshooting
- VLANs
  - Virtual Local Area Networks

### ARP spoofing

Address resolution protocol

- Intruder sends ARP packet to C1 with C2 IP's and Intruder MAC
- Intruder sends ARP packet to C2 with C1 IP's and Intruder MAC
- C1 and C2 communicate via Intruder

### Switch MITM Attack



### Modems

- Potential backdoor into system
- Remote Access Servers
- Who is allowed to have access
- War dialers

### RAS

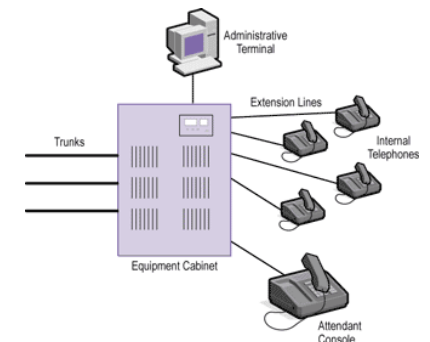
- Remote Access Service
- Access network from home/road
- Authentication
  - CHAP, PAP, EAP...
- Caller ID / Mandatory Call Back

### Securing RAS

- Use most secure authentication client supports
- Encrypt Communications
- Block unnecessary protocols
- Separate logins / different names

### Telcom / PBX

Private Branch Exchange



## PBX Issues

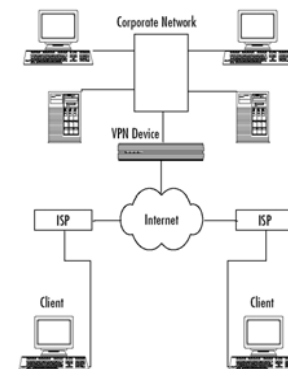
- Remote Maintenance  
Disable until needed
- Passwords on Mailboxes
- Call forwarding
- Phreakers

## Virtual Private Networks

- Remote access to private LAN
- Heavy Encryption
- Types
  - Remote access VPN
  - Site-to-site intranet-based VPN
  - Site-to-site extranet-based VPN

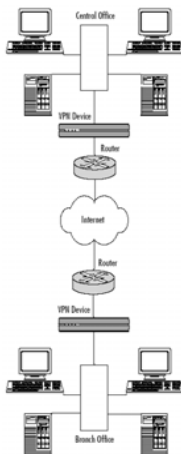
## Remote access VPN

Individual Users



## Site-to-site VPN

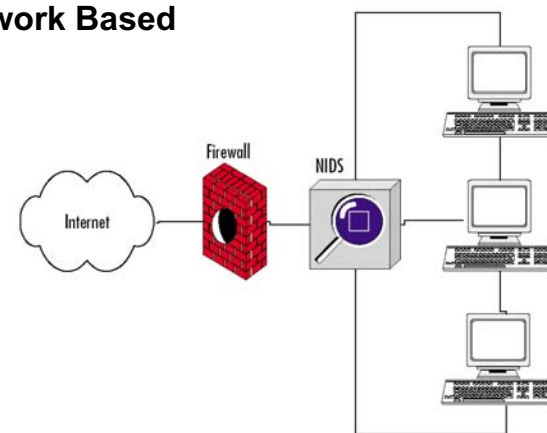
- Intranet  
Same Company
- Extranet  
Business to Business



## IDS - Intrusion Detection Systems

- Burglar Alarm for your system
- False Positives
- Keep it up to date
- Host based / Network based
- Can perform corrective actions  
Locking account, blocking ports

## Network Based

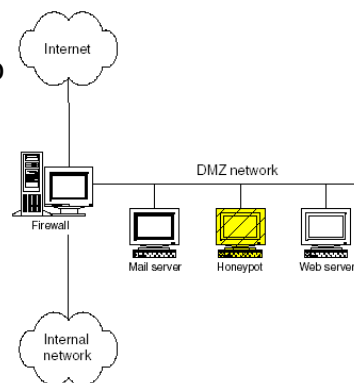


## Honeypots

- Fake Systems
- Designed to lure hackers
- Keep them away from real systems
- Monitor them, learn their techniques

## Honeypot

Firewall setup to redirect attacks to honeypot system.



## Workstations / Servers

- Keep patches up to date  
Test first!
- Close unneeded protocols/ports
- Activate auditing  
Limit User Activities / Access
- Enable Security Options  
NTFS / FAT, etc...

**Mobile Devices**

Lots of data, wide open

Theft

Password Protection

Hard Drive, BIOS, OS

Encryption

**Media Security**

Cables

Disks

Tapes

CDRs

Hard Drives

Flashcards

Smartcards

**Cables**

Coax

Christmas Tree Problem

Terminators

UTP/STP

Open ports

UTP: EMI / RFI

**Cables**

Fiber

Most Secure

Longer Runs

No EMI / RFI

Difficult to tap

Plenum

Flame resistant shielding

Used inside walls/floors/ceiling

**Media**

More storage, smaller size

Encryption

Password Protected

Disable access to media

End of this Lesson