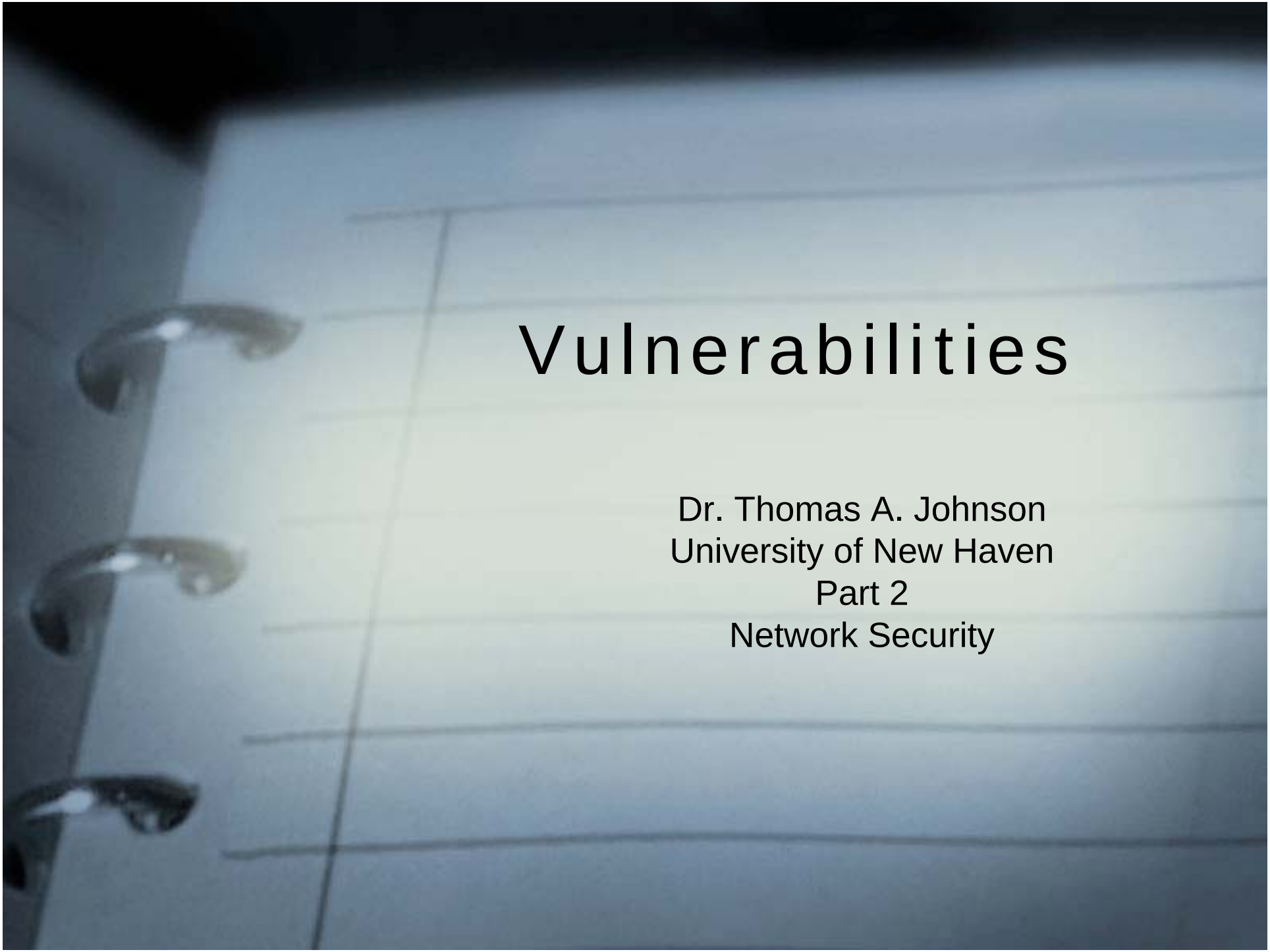
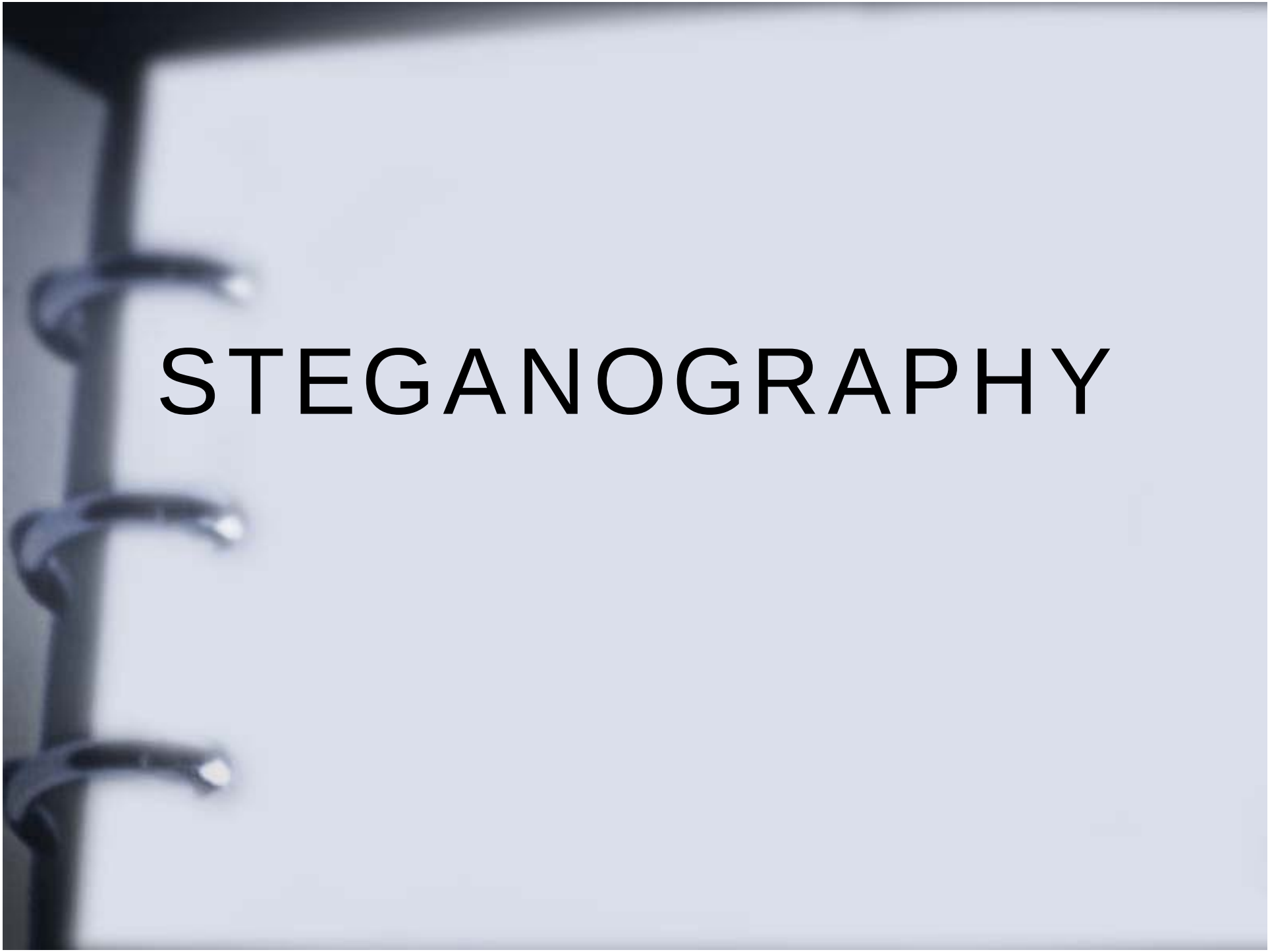


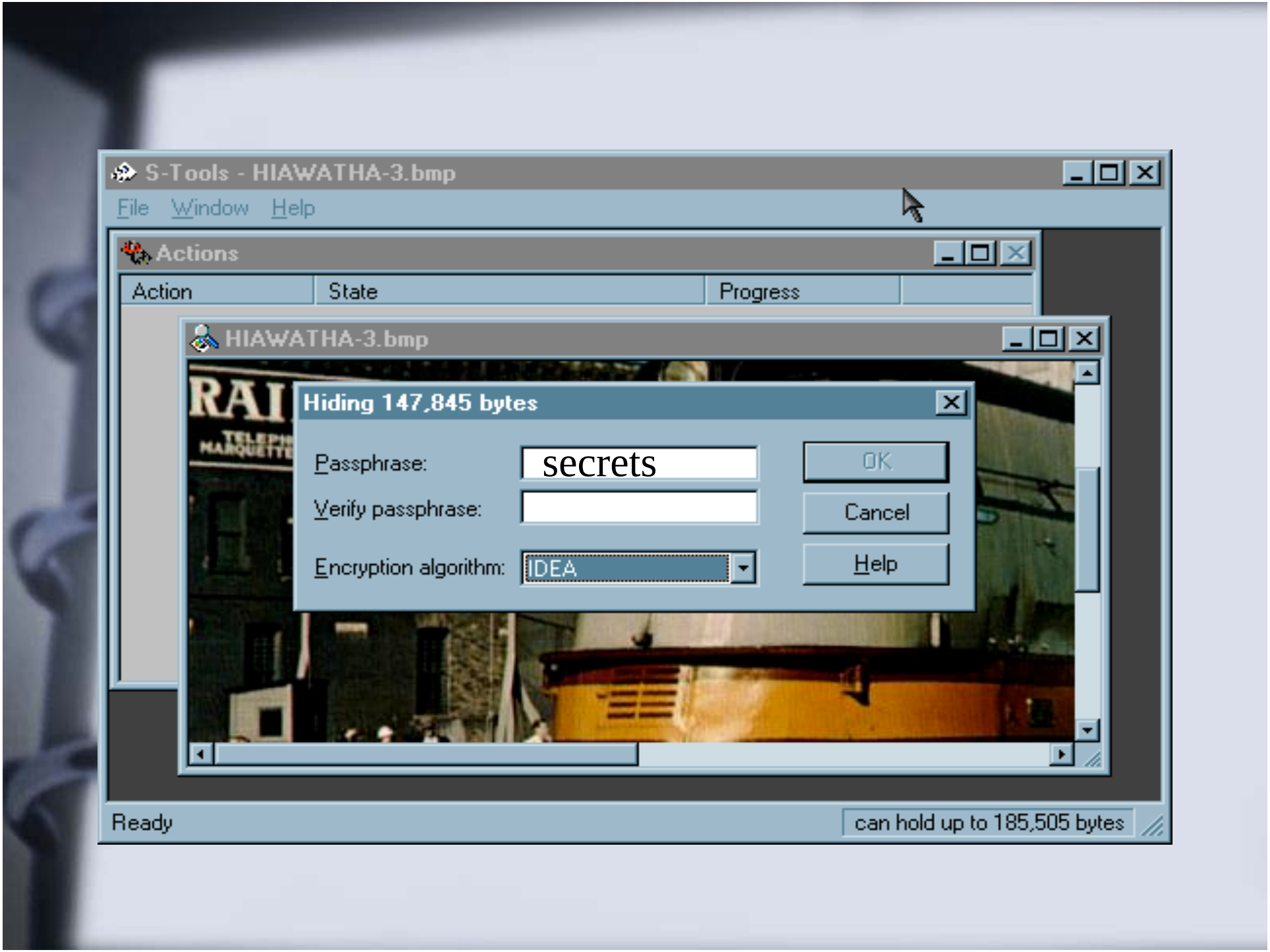
Vulnerabilities

Dr. Thomas A. Johnson
University of New Haven
Part 2
Network Security


STEGANOGRAPHY

- To hide in plain sight
- Today's electronic microdot
- Uses BMP, GIF or WAV files


S-Tools - HIAWATHA-3.bmp
S-tools v.4
File Window Help
Actions
Action
State
Progress
HIAWATHA-3.bmp
RAILWAY EXPRE
TELEPHONE MARQUETTE 5870 MILWAUKEE
3
1450Kb
Ready
can hold up to 185,505 bytes


S-Tools - HIAWATHA-3.bmp
File Window Help
Actions
Action
State
Progress
HIAWATHA-3.bmp
Hiding 147,845 bytes
Passphrase:
secrets
Verify passphrase:
Encryption algorithm:
IDEA
OK
Cancel
Help
Ready
can hold up to 185,505 bytes


S-Tools - hidden data
File Window Help
Actions
Action
State
Progress
HIAWATHA-3.bmp
hidden data
RAILWAY EXPRE
MILWAUKEE
Ready
can hold up to 185,505 bytes

Hidden Message

Steganography

- Container can be
  - Bitmap, GIF, WAV file
- Message can be
  - image, sound, text, spreadsheet, etc…
- Can be an image on the Corporation Website
  - why worry about sneaking out a document?
- Can be guarded with a pass phrase and encrypted
  - you can download it and still not see the message


IP Address
Internet Protocol

IP Addresses

- What is the difference between an internet and a physical network?
  - Network depends upon infrastructure
  - an internet is a ‘logical’ network / extended network constructed from software overlays on top of existing computer systems / networks

IP Addresses

- Uniformity in addressing allows messaging between systems despite the differences in structures
- Each host is assigned a 32 bit address (4bytes) known as an Internet Protocol Address (IP Address)
- Host must know destination address to send message to

IP Address Hierarchy

- IP divided into prefix and suffix
  - prefix physical network of computer
  - suffix individual host on that network
- prefixes must be unique on a global basis
  - suffixes unique only to that particular network

IP Classes

- The first 4 bits of the IP address determine which class it belongs to
  - values 0 - 7 class A
  - values 8 - 11 class B
  - values 12-13 class C
  - value 14 class D
  - value 15 class E

IP Classes

- Classes A, B, C are '*primary classes*'
  - used for host addresses
    - A prefix / suffix boundary between bytes 1 & 2
    - B prefix / suffix boundary between bytes 2 & 3
    - C prefix / suffix boundary between bytes 3 & 4
- Class D
  - multicasting (set of hosts)
- Class E
  - reserved for future use

Dotted Decimal Notation

- Octets represented as 4 decimal values
  - 10000001 00110100 00000110 00000000
    - 129.52.6.0
  - 0.0.0.0 thru 255.255.255.255 range
- Classes (first octet range)
  - A0 - 127
  - B 128 - 191
  - C 192 - 223
  - D 224 - 239
  - E 240 - 255

Hosts accommodated in Classes

- **A** 128 networks 16,777,216
- **B** 16384 networks 65,536
- **C** 2097152 networks 256

- IANA (Internet Assigned Number Authority) assigns numbers to ensure uniqueness

Special Addresses

- Never assigned to hosts
  - Host address zero reserved to denote network
    - 128.211.0.0 class B prefix 128.211
    - should not appear as normally as destination address in packet

Special Addresses

Prefix	Suffix	Type	Reason
Zeros	Zeros	This host	Boot process
Network	Zeros	Network	Identify network
Network	Ones	broadcast	On that net
Ones	Ones	Broadcast	Local net
127	*	Loopback	Testing

Special Addresses

- Pools of IP addresses reserved on local networks
  - not in use on Internet
    - 10.0.0.0 thru 10.255.255.255
    - 172.16.0.0 thru 172.31.255.255
    - 192.168.0.0 thru 192.168.255.255
  - for use behind firewall or proxy
    - LAT (Local Address Table) shows these as belonging to internal network

BSD

- Variation of Unix (Berkeley) used all 0’s as a broadcast instead of all 1’s
  - some Unix ‘flavors’ are based on BSD

Addresses

- Routers are assigned IP addresses (at least two)
  - each IP contains prefix ID'ing physical network
- Examples of connecting networks
  - Ethernet 131.108.0.0
    - router 131.108.99.5 / 233.240.129.2
  - Token Ring 233.240.129.0
    - router 233.240.129.17 / 78.0.0.17
  - WAN 78.0.0.0

Multihomed Hosts

- Host connected to multiple networks
  - multiple IP addresses assigned
  - redundancy

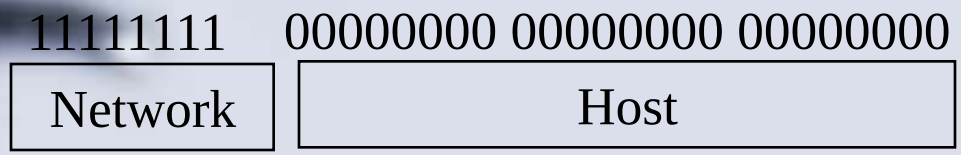
Subnet masking

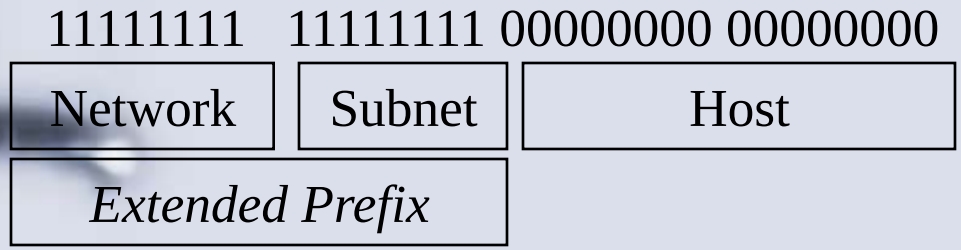
- Method to logically divide a network
  - mixed topologies (TR & Ethernet)
  - control traffic congestion (bandwidth intensive applications)
  - reducing number of InterNic addresses required

Subnet Masking

- How many segments does network need addresses for? (physical segment separated by routing device)
- Future requirements?
- Number of hosts on the largest segment?
- Future host on a given segment?

Class A subnet





Masking

- Used to determine if host and destination on the same physical network by performing the AND with subnet mask
  - results of ANDing the same? Same network
- IP 172.16.2.4
- Mask 255.255.0.0

10101100 00010000 00000010 00000100
11111111 11111111 00000000 00000000
10101100 00010000 00000000 00000000

IP 172.16.3.5

Mask 255.255.0.0

10101100 00010000 00000011 00000101
11111111 11111111 00000000 00000000
10101100 00010000 00000000 00000000

Subnet Mask Problems

- Cannot communicate with remote hosts
- Cannot communicate with a local host (time out type messages)
- Local host believed to be remote

IPv6

- 128 bit addressing (compared to 32 bit)
- IP Header changes
  - removal of old IPv4 header information
  - forwarding info, option fields length information, future capability for option fields
  - flow control for QOS
  - security (authentication of src & dest); encryption


DNS
Domain Name Services


ICMP

ICMP

- Internet Control Message Protocol
  - IP uses ICMP to send an error message
  - ICMP uses IP to get across the network
  - 5 Error messages
  - 4 Info messages

ICMP error messages

- Source Quench
  - Tell the sender to slow down transmission
- Time Exceeded
  - TTL reaches zero (0)
  - reassembly timer on receiver expires
- Destination Unreachable
  - host cannot be reached.. Or network cannot be reached
- Redirected
  - Change in routing
- Fragmentation required
  - “Don’t fragment” bit is set in header; message can’t get across due to MTU size

ICMP info messages

- Echo Request / Reply
- Address Mask Request / Reply
  - host boots and broadcasts AMR; routers send back reply w/ 32 bit subnet mask for that network

ICMP

- Encapsulation
  - ICMP and header bundled into IP packet
  - IP header and data (which is the ICMP datagram) bundled into frame
  - Frame and Frame header sent across the physical network
- Replies know where to go back since source address is part of the IP header
- no priority is assigned to ICMP traffic
- ICMP message has an error? No ICMP error message generated for this error...

PING

- Echo request reply
  - sees if a host is “reachable”
- TTL used (contained in header)
  - router checks sum
  - count decrements by one at each router
  - checksum generated and message forwarded
  - TTL 0?
    - Discard the message

Traceroute

- UDP used to send messages
- TTL is increase by one on successive messages until a host is reached
- UDP attempts to “talk” with an non-existent application on a remote host
  - either returns with ‘non-existent host’ or ‘time expired’ message

Path MTU discovery

- Messages of decreasing size sent across with the “don’t frag” bit set
  - if MTU too small, ICMP reply of “Frag Req’d” is returned
    - “feedback” mechanism

ICMP Message Types

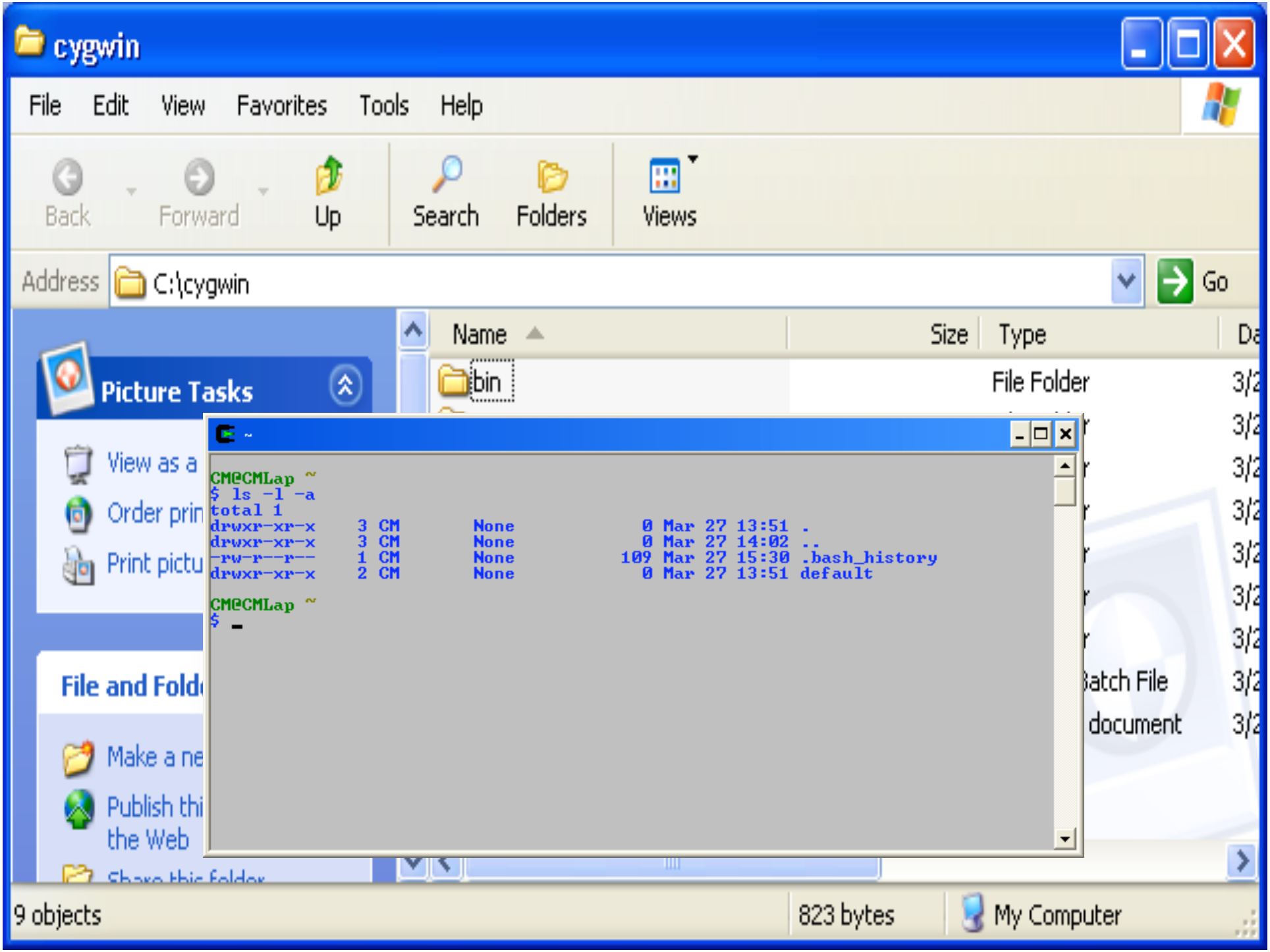
- 0 Echo Reply
- 3 Destination Unreachable
- 4 Source Quench
- 5 Redirect
- 8 Echo
- 9 Router Advertisement
- 11 Time Exceeded
- 30 Traceroute

CYGWIN

- Linux style ‘shell’ operating under a Windows environment
  - Get the feel for Linux

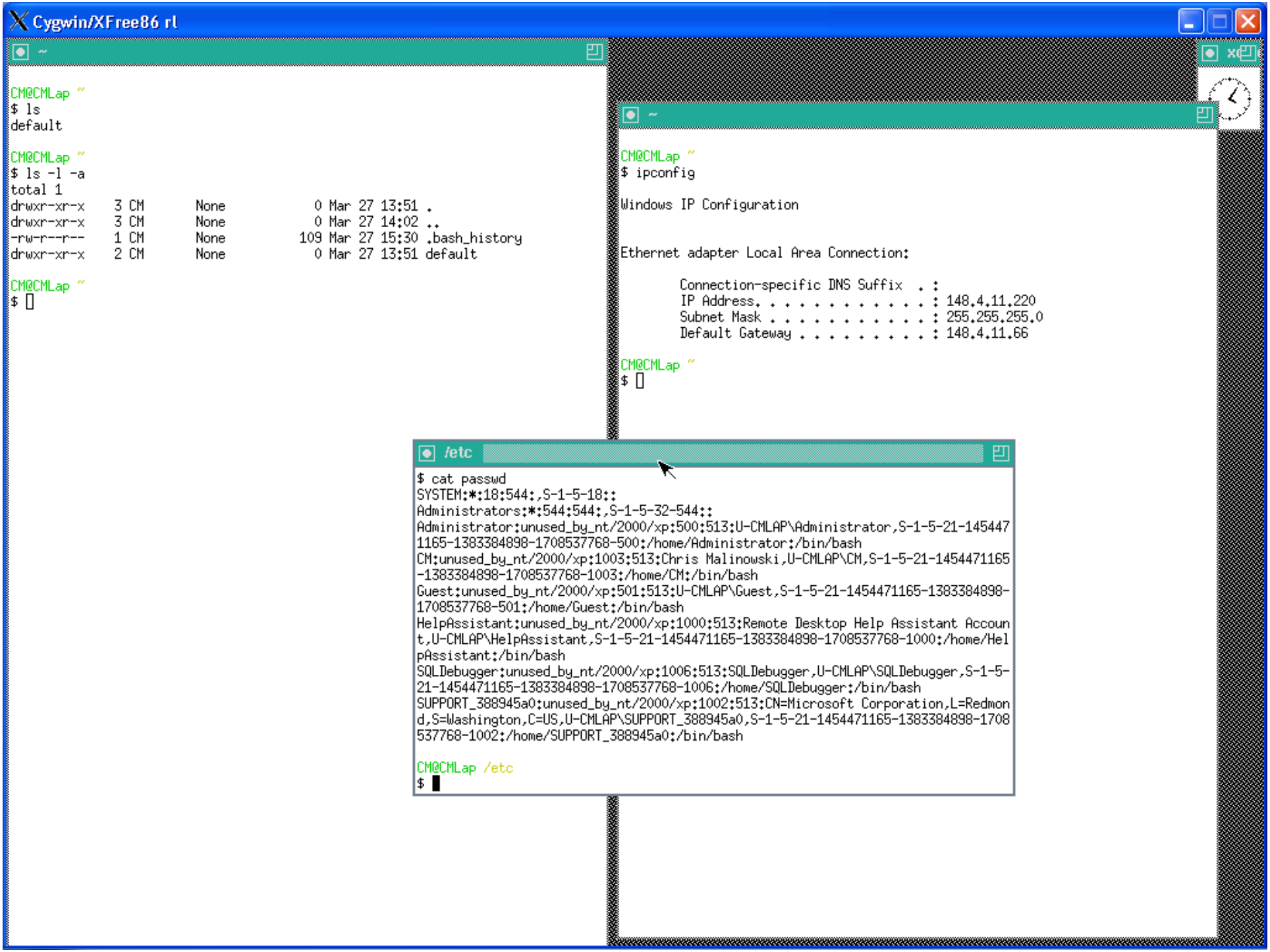
Cygwin (GNU + Cygnus + Windows)

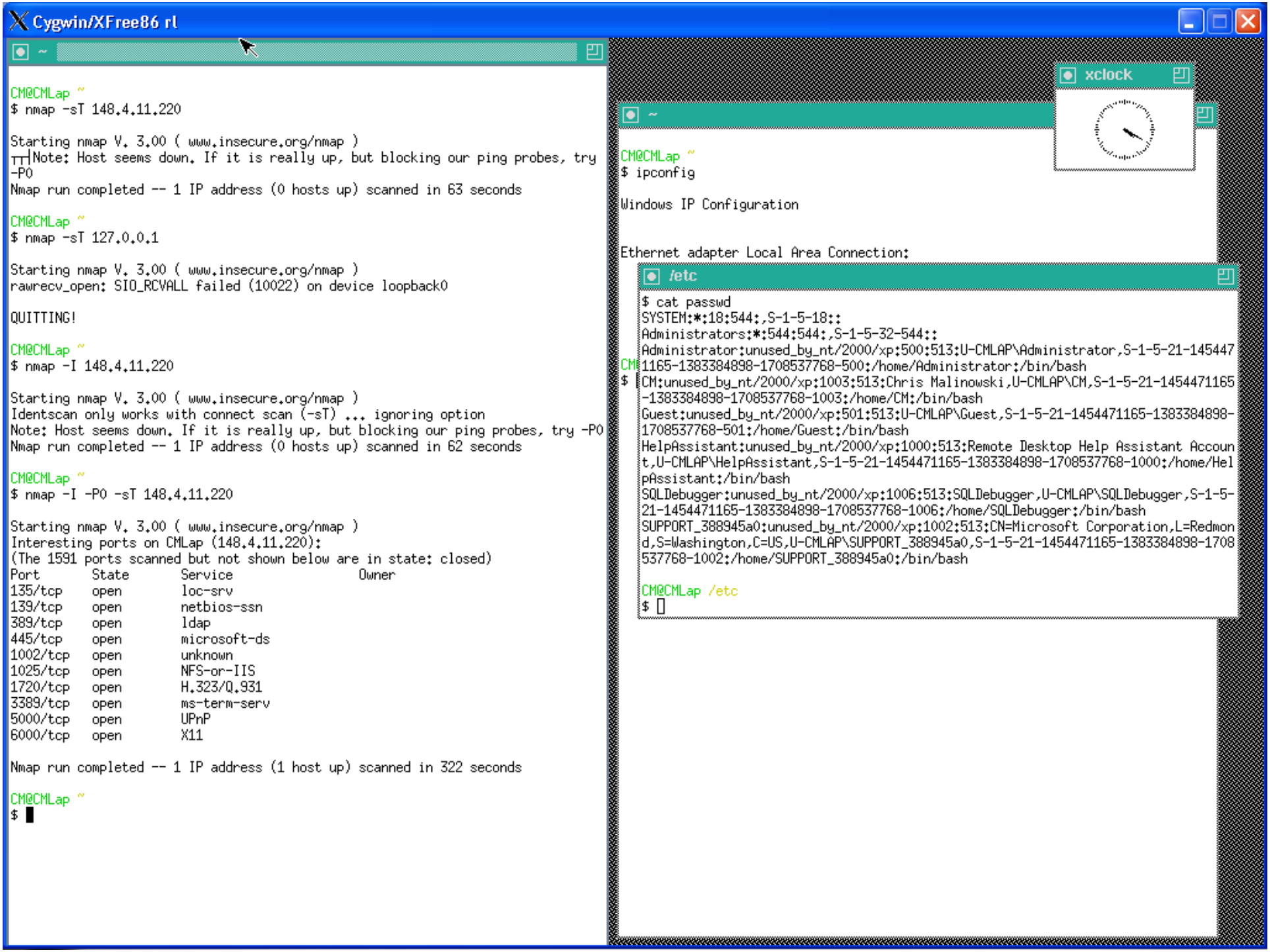
- Allows the user (via *cygwin1.dll API*) to display a Unix “bash shell” feel
  - user can still execute Windows instructions from within
- packages can be selected
  - you can d’load source as well
  - user can get Xfree86 library and run X-Windows
- grep, nmap, perl,


cygwin
File Edit View Favorites Tools Help
Back Forward Up Search Folders Views
Address C:\cygwin
Go
Picture Tasks
View as a
Order prin
Print pictu
File and Fold
Make a ne
Publish thi
the Web
Name Size Type
bin File Folder
~
CM@CMLap ~
$ ls -l -a
total 1
drwxr-xr-x 3 CM None 0 Mar 27 13:51 .
drwxr-xr-x 3 CM None 0 Mar 27 14:02 ..
-rw-r--r-- 1 CM None 109 Mar 27 15:30 .bash_history
drwxr-xr-x 2 CM None 0 Mar 27 13:51 default
CM@CMLap ~
$
Batch File
document
9 objects
823 bytes
My Computer

Window C / C++ development

- Installing GCC, GDB, make, Binutils
  - ***FREE*** Windows C/ C++ development platform
    - (not a pretty, but….)


Cygwin/XFree86 rl
~
CM@CMLap ~
$ ls
default
CM@CMLap ~
$ ls -l -a
total 1
drwxr-xr-x 3 CM None 0 Mar 27 13:51 .
drwxr-xr-x 3 CM None 0 Mar 27 14:02 ..
-rw-r--r-- 1 CM None 109 Mar 27 15:30 .bash_history
drwxr-xr-x 2 CM None 0 Mar 27 13:51 default
CM@CMLap ~
$
~
CM@CMLap ~
$ ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 148.4.11.220
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 148.4.11.66
CM@CMLap ~
$
/etc
$ cat passwd
SYSTEM:*:18:544:,S-1-5-18::
Administrators:*:544:544:,S-1-5-32-544::
Administrator:unused_by_nt/2000/xp:500:513:U-CMLAP\Administrator,S-1-5-21-1454471165-1383384898-1708537768-500:/home/Administrator:/bin/bash
CM:unused_by_nt/2000/xp:1003:513:Chris Malinowski,U-CMLAP\CM,S-1-5-21-1454471165-1383384898-1708537768-1003:/home/CM:/bin/bash
Guest:unused_by_nt/2000/xp:501:513:U-CMLAP\Guest,S-1-5-21-1454471165-1383384898-1708537768-501:/home/Guest:/bin/bash
HelpAssistant:unused_by_nt/2000/xp:1000:513:Remote Desktop Help Assistant Account,U-CMLAP\HelpAssistant,S-1-5-21-1454471165-1383384898-1708537768-1000:/home/HelpAssistant:/bin/bash
SQLDebugger:unused_by_nt/2000/xp:1006:513:SQLDebugger,U-CMLAP\SQLDebugger,S-1-5-21-1454471165-1383384898-1708537768-1006:/home/SQLDebugger:/bin/bash
SUPPORT_388945a0:unused_by_nt/2000/xp:1002:513:CN=Microsoft Corporation,L=Redmond,S=Washington,C=US,U-CMLAP\SUPPORT_388945a0,S-1-5-21-1454471165-1383384898-1708537768-1002:/home/SUPPORT_388945a0:/bin/bash
CM@CMLap /etc
$


Cygwin/XFree86 rl
~
CM@CMLap ~
$ nmap -sT 148.4.11.220
Starting nmap V. 3.00 (www.insecure.org/nmap)
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 63 seconds
CM@CMLap ~
$ nmap -sT 127.0.0.1
Starting nmap V. 3.00 (www.insecure.org/nmap)
rawrecv_open: SIO_RCVALL failed (10022) on device loopback0
QUITTING!
CM@CMLap ~
$ nmap -I 148.4.11.220
Starting nmap V. 3.00 (www.insecure.org/nmap)
Identscan only works with connect scan (-sT) ... ignoring option
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 62 seconds
CM@CMLap ~
$ nmap -I -P0 -sT 148.4.11.220
Starting nmap V. 3.00 (www.insecure.org/nmap)
Interesting ports on CMLap (148.4.11.220):
(The 1591 ports scanned but not shown below are in state: closed)
Port State Service Owner
135/tcp open loc-srv
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
1002/tcp open unknown
1025/tcp open NFS-or-IIS
1720/tcp open H.323/Q.931
3389/tcp open ms-term-serv
5000/tcp open UPnP
6000/tcp open X11
Nmap run completed -- 1 IP address (1 host up) scanned in 322 seconds
CM@CMLap ~
$
xclock
~
CM@CMLap ~
$ ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
/etc
$ cat passwd
SYSTEM:*:18:544:,S-1-5-18::
Administrators:*:544:544:,S-1-5-32-544::
Administrator:unused_by_nt/2000/xp:500:513:U-CMLAP\Administrator,S-1-5-21-145447
1165-1383384898-1708537768-500:/home/Administrator:/bin/bash
CM:unused_by_nt/2000/xp:1003:513:Chris Malinowski,U-CMLAP\CM,S-1-5-21-1454471165
-1383384898-1708537768-1003:/home/CM:/bin/bash
Guest:unused_by_nt/2000/xp:501:513:U-CMLAP\Guest,S-1-5-21-1454471165-1383384898-
1708537768-501:/home/Guest:/bin/bash
HelpAssistant:unused_by_nt/2000/xp:1000:513:Remote Desktop Help Assistant Accoun
t,U-CMLAP\HelpAssistant,S-1-5-21-1454471165-1383384898-1708537768-1000:/home/Hel
pAssistant:/bin/bash
SQLDebugger:unused_by_nt/2000/xp:1006:513:SQLDebugger,U-CMLAP\SQLDebugger,S-1-5-
21-1454471165-1383384898-1708537768-1006:/home/SQLDebugger:/bin/bash
SUPPORT_388945a0:unused_by_nt/2000/xp:1002:513:CN=Microsoft Corporation,L=Redmon
d,S=Washington,C=US,U-CMLAP\SUPPORT_388945a0,S-1-5-21-1454471165-1383384898-1708
537768-1002:/home/SUPPORT_388945a0:/bin/bash
CM@CMLap /etc
$


Discovery Methods

Discovery / enumeration

- Pinging
  - ICMP packets returned might “fingerprint” the OS of the target system
- Email
  - trace headers
- Instant messaging
  - IRC
    - finger
    - whois
    - DCC (direct IP-IP)
      - netstat

Other applications

- Utilize another feature of application which allows for direct point-to-point
- ICQ
  - can simply netstat
- MSN messenger
  - built in file transfer
    - then netstat

Netstat

- netstat –r
  - shows routing information on local
- netstat –a
  - all open connctions
- other options
  - -n numerical format of IP and port
  - -e Ethernet stats
  - -s per protocol stats
  - -p *protocol* TCP, UDP or IP
  - *interval* in seconds; CTRL+C to stop (windows)

Netstat

- states
  - Established
  - TIME_WAIT
  - FIN-WAIT_2
  - SYN
- Port numbers
  - RFC 1700 lists assigned port numbers

Netstat

- Privileged (well-known) ports
  - 0-1023
- Registered
  - 1024 – 49151 used by applications
- Dynamic / Private
  - 49152 – 65535
    - rarely used… many Trojans use this range

Firewalls

- Personal
  - Black Ice Defender
  - Zone Alarm
  - McAfee Guardian

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\CM>nmap -g67 -P0 -p130-140 -sU 127.0.0.1

Starting nmap V. 3.00 ( www.insecure.org/nmap )
rawrecv_open: SIO_RCVALL failed (10022) on device loopback0

QUITTING!

C:\Documents and Settings\CM>nmap -g67 -P0 -p130-140 -sU 148.8.11.220

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (148.8.11.220):
Port        State        Service
130/udp     open         cisco-fna
131/udp     open         cisco-tna
132/udp     open         cisco-sys
133/udp     open         statsrv
134/udp     open         ingres-net
135/udp     open         loc-srv
136/udp     open         profile
137/udp     open         netbios-ns
138/udp     open         netbios-dgm
139/udp     open         netbios-ssn
140/udp     open         emfis-data

Nmap run completed -- 1 IP address (1 host up) scanned in 38 seconds

C:\Documents and Settings\CM>^O
```

Proxy Server

- Wingate
- Squid

Wingate

- Uses port 23
- SOCKS on 1080
- IRC on 6667

Wingate

- TELNET on 23
  - used for intercommunicating between hosts behind the proxy
  - no password required
    - ANYONE can Telnet in!!!
    - can use this to hide ID from target

Scanner 1.01 Rate it!

Software :: System :: Administration :: Monitoring 7 Votes | Rate It!

Network Port Scanner

Updated by Omer S.
Fancy on Saturday, March 23rd 2002.

A small yet fast network port scanner with wingate detection.
Licence : GPL

Version : 1.01 [Stable] 0.50 [Development]

Email me on New Release. Update

Ice POLL

There is nothing more useful than...

- PDAs
- Notebooks
- Tablet PC
- Wearable computers
- Paper & Pen

Vote !

NewsLetter

Your Email
Subscribe

Walk Leaders

SCREEM 0.7.0
program designed to allow fast creation and maintenance of websites
baudline 0.95
real-time signal analysis tool and offline time-frequency browser.
MySQL 4.1.0
SQL (Structured Query Language) database server.
Gaim 0.61
clone of AOL Instant messenger
eXtace 1.7.8
Gnome Audio

Wingate

- Connect to Port 23

  WingateBox>

  telnet real_target_system_IP:23

Wingate

- Once connected, issue commands to target
- “BOUNCE” attack
- no record, unless the Wingate box records it
  - can “bounce” from proxy to proxy

Wingate Host

- SOCKS and IRC
  - can also be leveraged for BOUNCE attacks

Wingate

- Countermeasures
  - disable access to ports from outside hosts

Squid

- Use *ipchains* to set up a *transparent proxy*
  - redirects request to another port *on the same machine*
  - appears that connection is direct

HTML

- HTML exploit

```
<html>
<body>
<script>
    var ip = new java.net.InetAddressgetLocalHost();
    var ipStr = new java.lang.String(ip);
    document.writeln(ipStr.subsrting(ipStr.indexOf("/")
        +1));
    </script>
    </body>
    </html>
```

- Additional information can be obtained
  - OS, browser information, ISP, country, screen resolution, etc

Countermeasures

- Proxy server
  - hides IP information
  - hides other information as well
- Anonymizers
  - hide IP
  - don’t necessarily hide other information

Port scanning

- TCP connect
- TCP SYN
- SYN/ACK
- TCP FIN
- TCP NULL
- TCP XMAS tree

TCP connect

- Detected
- Difficult to counter
  - might be legitimate request to connect to server
  - monitor packets
    - stateful filters

SYN Scans

- “half connect” scanning
  - netstat –a
    - shows state of “SYN_RECEIVED” on multiple ports
- not stealthy
- blockable
- target replies either with
  - SYN/ACK
    - listening
  - RST/ACT
    - no service on that port

SYN/ACK

- sent to:
  - closed port
    - RST reply
  - open port
    - typically no reply
- No reply
  - also possible due to firewall interception

TCP FIN

- Open port
  - should not respond to FIN
- no service or closed port
  - UDP
    - ICMP
  - TCP
    - RST packet sent back
- some operating systems send RST as response to FIN on open port
  - possible method of fingerprinting

TCP Null

- packet with NO flags set
- target baffled
  - open port?
    - responds with error message
    - could discard packet
  - closed port?
    - RST response

TCP XMAS tree

- ALL the flags are set
- port open?
  - error message response
  - or discard of packet by target
- port closed?
  - RST response

ACK Scanning

- TTL < RST packets received earlier
  - port is open and listening
- window's size > 0
  - port is open and listening

UDP scanning

- closed port
  - ICMP error message response

FTP Bounce Port Scan

- connect to FTP of host
  - from there
    - connect to *any port of any system including target*
- PORT command
  - used to open connection between client and server
  - once connection established, PORT to another host
    - if the bounce server can see it, *YOU* can see it
      - even if you don't normally have rights to it!

FTP Bounce Countermeasure

- Configure the FTP server
  - DO not allow connections with host other than client

Port Scanning

- nmap
  - OS detection
  - ping sweeps
  - mapping networks
- Strobe
  - TCP port scanner
- hping
  - custom packets (ICMP/UDP/TCP)

Scanning countermeasures

- Scanlogd
  - Unix
- BlackIce
  - Windows
- Portsentry (Abacus)
- NukeNabber
  - Windows

```
   USER    PORT    MODE    MSND*   REST    XCWD    HELP    PWD     ADAT
   PASS    LPRT    RETR    MSOM*   RNFR    LIST    NOOP    XPWD    PROT
   ACCT*   LPSV    STOR    MSAM*   RNTO    NLST    MKD     CDUP    PBSZ
   SMNT*   PASV    APPE    MRSQ*   ABOR    SITE    XMKD    XCUP    CCC
   REIN    TYPE    MLFL*   MRCP*   DELE    SYST    RMD     STOU    SIZE
   QUIT    STRU    MAIL*   ALLO    CWD     STAT    XRMD    AUTH    MDTM
214 Direct comments to ftp-bugs@phoenix.
ftp> literal stat
211-phoenix FTP server status:
     Version 4.1 Thu Sep 12 23:46:23 CDT 2002
     Connected to 148.4.11.220 (::ffff:148.4.11.220)
     Logged in as cmalinow

     No data connection

211 End of Status
ftp> literal syst
215 UNIX Type: L8 Version: BSD-44
ftp> _
```

IDENT (port 113)

- owner information
- OS information
- DISABLE this service

ICMP

- Echo Request / Echo Reply
  - host alive
  - fingerprint OS
- Timestamp request
  - determine target's time
    - target alive?
- Address Mask Request
  - Subnet address

Sniffers

- tcpdump
- Ethereal
- etherpeek
- Dsniff

Sniffers

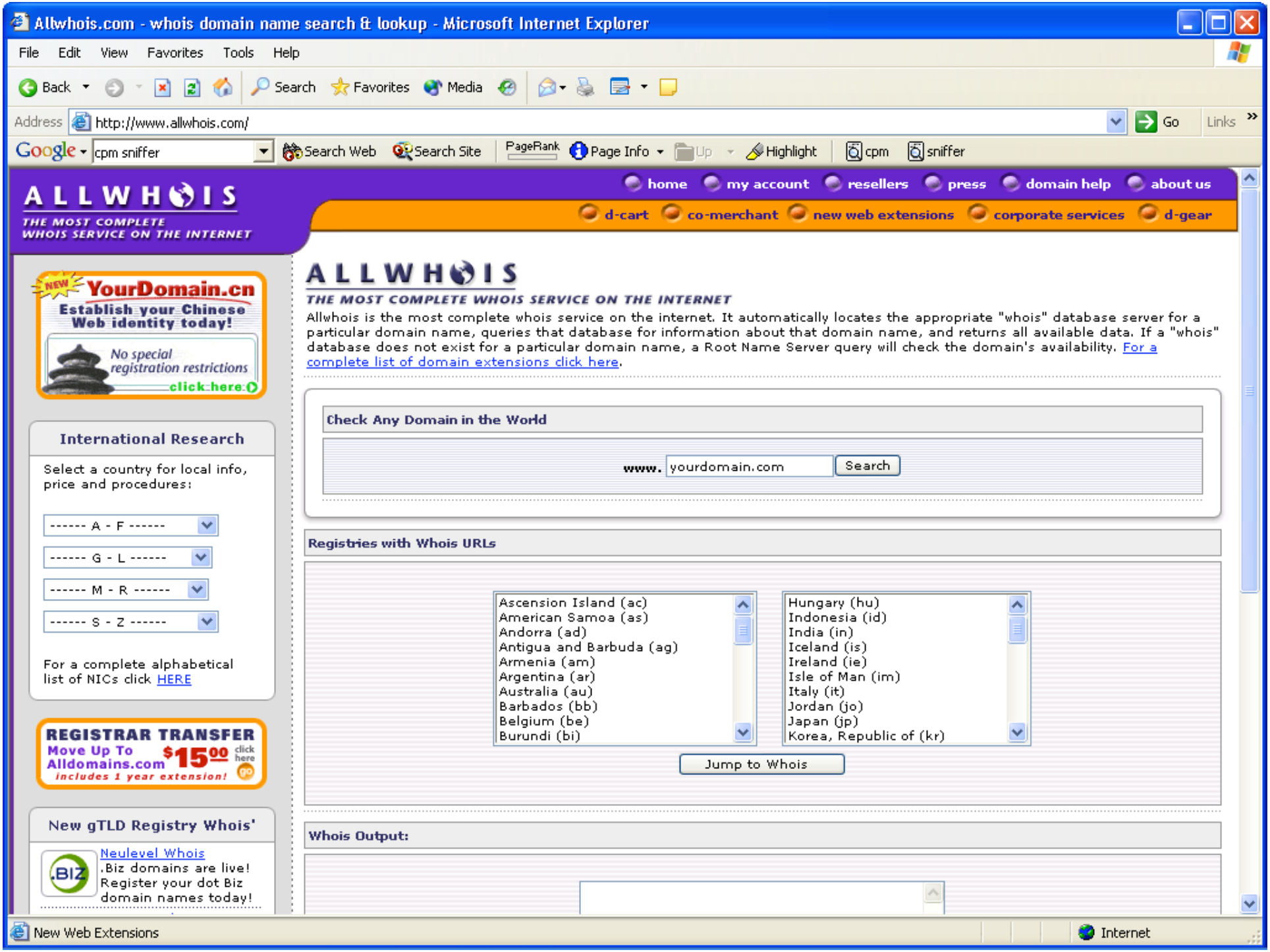
- Countermeasures
  - NIC in promiscuous mode indicates sniffer
    - “cpm” utility determines if NIC in that mode
  - sniffer might be in task list / process list
  - log file
    - hidden directories
  - AntiSniff
    - L0phtCrack
      - network based sniffer detection
  - infrastructure
    - switched network
    - encryption

Routing Tables

- Why bother
  - indicates entry and exit mechanisms
  - attack points
- Netstat –rn
  - on Unix
    - indicates if it’s a router, a gateway, a host, or redirected
    - also indicates number of users
    - packets using that node

nslookup

- performs reverse lookup for IP
- Sam Spade
  - Windows based application


Allwhois.com - whois domain name search & lookup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.allwhois.com/
Go Links
Google cpm sniffer
Search Web Search Site PageRank Page Info Up Highlight cpm sniffer
ALLWHOIS
THE MOST COMPLETE WHOIS SERVICE ON THE INTERNET
home my account resellers press domain help about us
d-cart co-merchant new web extensions corporate services d-gear
NEW YourDomain.cn
Establish your Chinese Web identity today!
No special registration restrictions
click here
International Research
Select a country for local info, price and procedures:
------ A - F ------
------ G - L ------
------ M - R ------
------ S - Z ------
For a complete alphabetical list of NICs click HERE
REGISTRAR TRANSFER
Move Up To Alldomains.com $15.00 click here
includes 1 year extension!
New gTLD Registry Whois'
Neulevel Whois
.BIZ domains are live! Register your dot Biz domain names today!
ALLWHOIS
THE MOST COMPLETE WHOIS SERVICE ON THE INTERNET
Allwhois is the most complete whois service on the internet. It automatically locates the appropriate "whois" database server for a particular domain name, queries that database for information about that domain name, and returns all available data. If a "whois" database does not exist for a particular domain name, a Root Name Server query will check the domain's availability. For a complete list of domain extensions click here.
Check Any Domain in the World
www. yourdomain.com Search
Registries with Whois URLs
Ascension Island (ac)
American Samoa (as)
Andorra (ad)
Antigua and Barbuda (ag)
Armenia (am)
Argentina (ar)
Australia (au)
Barbados (bb)
Belgium (be)
Burundi (bi)
Hungary (hu)
Indonesia (id)
India (in)
Iceland (is)
Ireland (ie)
Isle of Man (im)
Italy (it)
Jordan (jo)
Japan (jp)
Korea, Republic of (kr)
Jump to Whois
Whois Output:
New Web Extensions
Internet


Attacks

Ping Of Death

- ping –l *(length) hostname*
  - using the “l” option, send a packet in excess of 64K
  - might hang system / crash it

Teardrop

- Fragmentation attack
- overlapping fragments

SYN flooding

- overwhelm host with connection attempts without the subsequent connection
- source IP in packet is invalid
- indicated by the SYN_RECEIVED in netstat
  - half open connection
- Countermeasures
  - reduce timeout time
  - increase connection requests
  - patches
  - firewalls

LAND attack

- like Syn, except the IP address and the Port number are the same as the target
  - infinite loop
- Firewall
  - outgoing packets having destination IP the same as the local IP address

Smurf attack

- Brute force
  - forces a condition where a target responds back to IP on same network
    - floods the network

UDP Flood attack

- Chargen or echo service attack
  - loop between two or more services producing output
- Disable services unless / until required

DDoS

- Trinoo
- ‘zombie’ machines

Modem Disconnect

- use the *echo* command
  - generate control characters for the escape sequence
  - issue the “hangup” command
- *ATH0 attack*
  - target allows ICMP echo packets
  - target uses a modem
  - need capability of spoofing packets
    - unless you don’t care if they know..
- modem can be set to ignore the control sequence and treat it as data
  - depends on modem

IP Spoofing

- Convince target that *source IP* is not you
- difficult to spoof from Windows system
- Sys admin can protect against it

IP Spoofing

- Responses to “you” never reach you since it’s a faked IP address
  - “blind” attack
- The “fake” IP receives the response
  - possible the REAL guy responds back
- Spoofed IP must exist
  - not respond back the packets sent to it from target
- Trust relationship

IP Spoofing

- Sequence numbers
  - upon boot
    - ISN (initial sequence number issued)
      - 1
    - updated by 128,000 every second
    - with each connection
      - incremented by 64000
    - ISN incremented by 1 after certain packets issued
      - SYN, FIN,
- Acknowledgement number
  - the number the system expects to receive next
  - serves to acknowledge receipt of packets with lower sequence numbers
- Spoofing takes advantage of predictability of sequence number generation
  - session hijack
  - trust relationship
    - expected sequence number and IP address.. it MUST be the proper host

IP Spoofing

- Locate trusted system
- disable that system
  - so it won't respond back to spoofed packets
  - DOS attack
- hijack the session
  - obtain ISN
    - send several packets to determine timing of ISN generation
    - note sequence numbers
    - calculation can take into account the round-trip-time
      - (propagation delay)
- after attack
  - send FIN

IP Spoofing

- Examine trust relationships
  - consider authentication, ACL as user based rather than system (IP) based
- Firewalls
  - incoming packets having internal IPs
  - outgoing packets having external IPs
- encryption
- random ISNs

TCP wrappers

- Access Control Rules
  - which systems allowed access to which services
- TCP wrappers
  - log clients using those services
    - time
    - purpose
  - booby trapping

TCP Wrappers & Services

- /etc/services
  - defines
    - services
    - port numbers
  - used by inetd
- /etc/inetd.conf
  - names of services
  - daemon/program associated with service

TCP Wrappers & Services

- incoming request for port xx
- inetd then:
  - looked up in /etc/services
  - then looks up daemon in inted.conf

TCP Wrappers

- interposed between inetd and the actual daemon / programs initiated by inetd
- access allowed based on IP source information
- request is logged

TCP Wrappers

- uses
  - /etc/hosts.allow
  - /etc/hosts.deny
- allows checked first
- then deny
- if no match (or both empty) then access allowed

/etc/hosts.deny

- deny telnet and ftp

  in.telnetd in.ftpd : xyz.badsite.net .badsite.com

  – denies services to xyz.badsite.net and entire badsite.com domain

  ALL: xyz.badsite.net .badsite.com

  – Wildcards
    - ALL
    - UNKNOWN unresolved by DNS
    - KNOWN
    - PARANOID names doesn’t match IP

  in.telnetd : ALL EXCEPT mysite.net


Authentication
qou vadis?

Kerberos

- Doesn’t prevent / assumes
  - Password guessing or cracking
  - assumes physical security of hosts
  - DoS attacks
  - assumes hosts synchronized time-wise
  - AS must be secure

CHAP

- Challenge Handshake Authentication Protocol
  - used over PPP
  - Challenge and response between server and client
    - done at Network Layer
    - 1) Use CHAP?
    - 2) Response: Yes
    - 3) Send Challenge
    - 4) Respond
    - 5) Indicate success / failure
      - terminate session
    - 6) Randomly periodic challenges
      - should change and not be the same

CHAP

- Problems:
  - passwords should not be the same in both directions
    - Replays
  - not all implementations terminate the session
    - allow access to some of the Network Layer protocols
      - possible to update passworkds

Digital Certificates

- email
- e-commerce
- transfer of electronic funds

- Combined with digital signatures and encryption
  - 3rd party to qualify individuals / organizations as trusted certificates

Security Tokens

- Assigned to a specific user by a specific administrator
  - small, carry-around devices
  - may be “binary”
    - device
    - password or pass phrase possessed by the user
- Lose the token, lose the access….

Passive Tokens

- Storage device for ‘base keys’
  - notches on device matched on receiver
  - magnetic strip
    - ATM cards
  - optical bar code
- Magnetic strips easily copied
  - usually may require a PIN
- ESN digitally encoded on cell phone
  - identifies the phone and is associated with a phone number (ie, account)
    - ESN is broadcast
      - read at access points such as traffic thoroughfares
      - encoded into other cell phones

Active Tokens

- Actively creates a ‘base key’
  - one-time password
  - encrypted form of base key
- ‘smart cards’
  - IC containing memory / processor
    - contact or contact-less
  - can double as:
    - employee ID
    - credit card
    - card-key
  - can also store personal information, biometric information, PKI, digital certificates, etcetera
- PCMCIA
- USB tokens

One-time Passwords

- limited duration
- once used, invalidated
- generated:
  - counter-based
    - combines a counter with the ‘secret password’
  - clock-based
    - requires synchronization with a server’s clock
- Susceptible to attacks
  - IP address theft, man-in-the-middle, redirection (phone)

Biometrics

- Information provided is particular to the owner that doesn't change over time
- Types:
  - Physical
    - fingerprint
    - features
    - hand geometry
    - retinal
    - iris
  - Behavioral
    - written signature
    - voice

Biometrics

- Needs to be initially scanned or ‘registered’
  - Digitized
  - Repository (centralized, localized, portable)
  - server, smart card
- Scan upon access request
  - comparison of data and grant / deny access
- Maintain record of scan and result

Biometrics

- False positives (improper authentication)
  - due to relaxing of standards in comparison
- False negatives (improper denial)
  - measurements changed from initial scanning
    - facial features
      - weight gain, or other pathology
    - retinal scan
      - change in blood vessels (pregnancy, etc)
  - improper measurement
    - equipment faulty / improperly cared for
    - background noise (voice scans)

Biometric problems

- Device used to scan / measure may be cumbersome or not portable enough
- Social issues
  - Fingerprint scanning and privacy issues
- Inability of system to cope with changes from initial scan registered
  - due to changes in principal or equipment
- Security of repository containing registered scan
- Security of the channel over which the transaction occurs
- Ability to fool the system
  - fingerprints “lifted” and duplicated in gelatin can fool the system

Multi-factor Authentication

- Factors:
  - known to principal
    - password
  - ownership by principal
    - smart card
  - property of principal
    - biometric
- Use *at least ONE* of each factor to verify identity


Exploits
Port Vulnerabilities

Sources:

- Hack Attacks Revealed
  - John Chirillo


Exploits
“Normal” services
available

Ports

- TCP and UDP
  - associated with an application or process with is “listening” or “waiting to speak”
  - the application / process is the requestor of
    - a) port number
    - b) the protocol

Port 7 / TCP

- Echo
  - ICMP packet
  - Ping of Deatch
    - send an oversize packet
    - buffer overrun
      - packet processed incorrectly
      - system reset / halt
  - Ping flooding

Port 11 / TCP

- Systat
  - can reveal information on operating system of host

Port 15 / TCP

- Netstat
  - connection information
  - subsystem information
    - protocols
    - addresses
    - connected sockets
    - MTU sizes

Port 19 / TCP

- chargen
  - can be used to generate characters
  - output can be redirected to a telnet connection
    - for example DNS (port 53)
      - can blow up DNS services

Port 20 & 21 / TCP

- ftp
  - 20 data
  - 21 ftp control connection

Port 23 / TCP

- telnet
  - terminal emulation for issuing console commands
  - allows access to host

Port 25 / TCP

- SMTP
  - mail bombing, spamming, DoS attacks

Port 43 / UDP & TCP

- whois
  - runs on central machines
  - network-wide directory services
    - discover

Port 53 / UDP & TCP

- domain
  - name associated with IP address(es)
    - lookups performed
  - DNS spoofing
  - DoS

Port 67 / UDP

- bootp
  - diskless workstation discover its own IP
    - buffer overflow

Port 69 / UDP

- tftp
  - used to load files into various devices
    - switches, routers
  - doesn’t have the complexity of ftp
  - fits into ROM
  - designed for bootstrap process
    - no username / password required
  - able to retrieve sensitive files
    - /etc/passwd

Port 79 / TCP

- finger
  - used in discovery
    - social engineering

Port 80 / TCP

- http
  - web hacks

Port 109 & 110 / TCP

- pop2, pop3
  - pop2
    - requires smtp server daemon
  - pop3
  - server can reveal information by telneting in

Port 111, 135 / TCP & UDP

- 111 Portmap
  - converts RPC into port numbers
    - knows every registered port on host
    - knows programs available on ports
  - 135 Loc-serv
    - NT's version of portmap
      - NIS domain name might be discoverable
        - » possible to get copy of password file if NIS domain known

Port 137 UDP, 138 UDP, 139 / TCP & UDP

- nbname, nbdatagram, nbsession
  - Wins / Netbios name service
    - lack of authentication
  - nbname
    - broadcast resolution
  - nbdatagram
    - broadcast discovery
  - nbsession
    - point-to-point communications

Port 144 / TCP

- news
  - Network extensible Window System
    - (Sun Unix)
    - PostScript window system interpreter
      - extensions for drawing on screen
      - handles input events

Port 161 & 162 / UDP

- snmp, snmp-trap
  - directs network traffic
    - PDUs (protocol data unit) sent to nework devices (agents)
    - information stored in Management Information Bases
      - MIBs
    - data returned to snmp requestors

Port 512 / TCP

- exec
  - for ‘rexec’
    - X-windows client might be running
    - capture / display window
    - interject keystroke events
  - target also accepts telnets to port 6000?
    - possibly DoS attack target

Port 513, 514 / TCP

- login & shell
  - privileged ports
  - used for address spoofing
  - 514 also used for *rsh*
  - together might indicate X-Windows daemon

Port 514 / UDP

- syslog
  - DoS attack

Port 517 & 518 / UDP

- talk, ntalk
  - text conversations with another station

Port 520 / UDP

- route
  - RIP communicates with this port
  - target discovery

Port 540 / TCP

- uucp
  - Unix-to-Unix copy protocol
    - transfer of files
    - transmittal of commands

Port 543, 544, 750 / TCP

- klogin, kshell, kerberos
  - subject to attacks
    - DoSS
    - overruns
    - spoofs
    - masked sessions
    - ticket hijacking


Exploits
subverted ports

Port 21, 5400 - 5402

- Back Construction, Blade Runner, Fore, FTP Torjan, Invisible FTP, Larva, WebEx, WinCrash
  - possible to include server and client versions of program
  - often registry entry can be found under the “CurrentVersion\Run

Port 23

- TTS
  - Tiny Telnet Server
    - runs in ‘stealth’ mode

Port 25, 110

- Can be a screen display or joke
- used to get system passwords, spam, keystroke capture, backdoor entry
- Ajan, Antigen, Email Password Sender, Haebu Coceda, Happy 99, Kuang2, ProMail Trojan, Shtrilitz, Stealth, Tapiras, Terminator, WinPC, WinSpy

Port 31, 456, 3129, 40421-40426

- Agent 31, Hackers Paradise, Masters Paradise
  - remote administration
    - application redirect
    - file manipulation
    - Registry manipulation

Port 41, 999, 2140, 3150, 6670-6771-60000

- Deep Throat
  - stealth FTP file servers
  - screen capture and viewing
  - password theft
  - reboot
  - open web browser
  - process control

Port 59

- DMSetup
  - mIRC chat client
    - corrupts startup files and mIRC settings
    - passes itself to communicator

Port 79, 5321

- Firehotker
  - Firehotker Backdoorz
    - file “server.exe”

Port 80

- Executor
  - command execution
    - system files and settings
    - sexec.exe
      - under \CurrentVersion\Run Executer1=“c”\windows\sexec.exe”

Port 113

- Kazimas
  - IRC worm
    - mIRC channels
      - file.. milbug_a.exe
      - in
        - \windows\kazimas.exe
        - \windows\system\psys.exe
        - \icqpatch.exe
        - \mirc\download\mirc60.exe
        - \mirc\logs\logging.exe
        - \mirc\sounds\player.exe
        - \games\spider.exe
        - \windows\freemem.exe

Port 119

- Happy 99
  - fireworks display
    - passwords, spamming, DoS and backdoor

Port 121

- JammerKillah
  - Trojan
    - autodetect BO and NB
    - puts in BO server

Port 541, 1045

- Rasmin
  - Lies dormant for wakeup..
    - rasmin.exe
    - wspool.exe
    - winsrvc.exe
    - inipx.exe
    - upgrade.exe


Security Port Scanner, Trojan Port List: Rasmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.glocksoft.com/trojan_list/Rasmin.htm
Go Links
Google rasmin trojan
Search Web Search Site PageRank Page Info Up Highlight rasmin trojan
G-Lock Software
Home Products Forums FAQ Downloads Registration
... \ Port Scanner \ Trojans Port List \ Rasmin
Name: Rasmin
Aliases: WSpool,
Ports: 531, 1045
Files: Wspool.exe - 59,904 bytes Winipx.exe - 59,904 bytes Winsrvc.exe - 59,904 bytes Upgrade.exe - 59,904 bytes Rasmin.exe - 58,368 bytes Rasmin.exe - 59,904 bytes Rasmin.lgc -
Created: Jan 1999
Requires: N/A
Actions: Destructive trojan
Rasmin uses up all the memory and the infected computer crashes regularly.
Versions: N/A
Registers: HLM\Software\Microsoft\ Windows\CurrentVersion\RunServices\
Notes: Works on Windows 95 and 98.
Country: N/A
Program: Written in Visual C++.
Using the Process Monitor from AATools, you will see whether any foreign programs are running on your computer. If you find some unwanted program, you can terminate it by clicking the 'Terminate Process' button on the Toolbar. Using the AATools Network Monitor, you can see what ports are in use on your local PC for connection with remote systems (LAN/Internet). On Windows NT/2000/XP the Network Monitor will display you the services that are active on the ports, and map the ports to their respective applications. If you register port probes
Advanced Administrative Tools
Port Scanner
Proxy Analyzer
Trace Route
Email Verifier
Links Analyzer
Whois
Network Monitor
Process Monitor
System Info
Resource Viewer
Registry Cleaner
Services
Registration
Affiliate
Support
Contact us
Info
Trojans Port List
Privacy Statement
Add to Favorites
Internet

Port 555, 9989

- Ini-Killer, NeTAdmin, phAse Zero, Stealth Spy
  - Trojan
  - Phase zero
    - A simple trojan written in 1998. It's distinguishing feature is that that the *server* can easily act as a remote FTP *client*. This allows a hacker to easily transfer files with an FTP server without exposing his/her IP address

Port 666

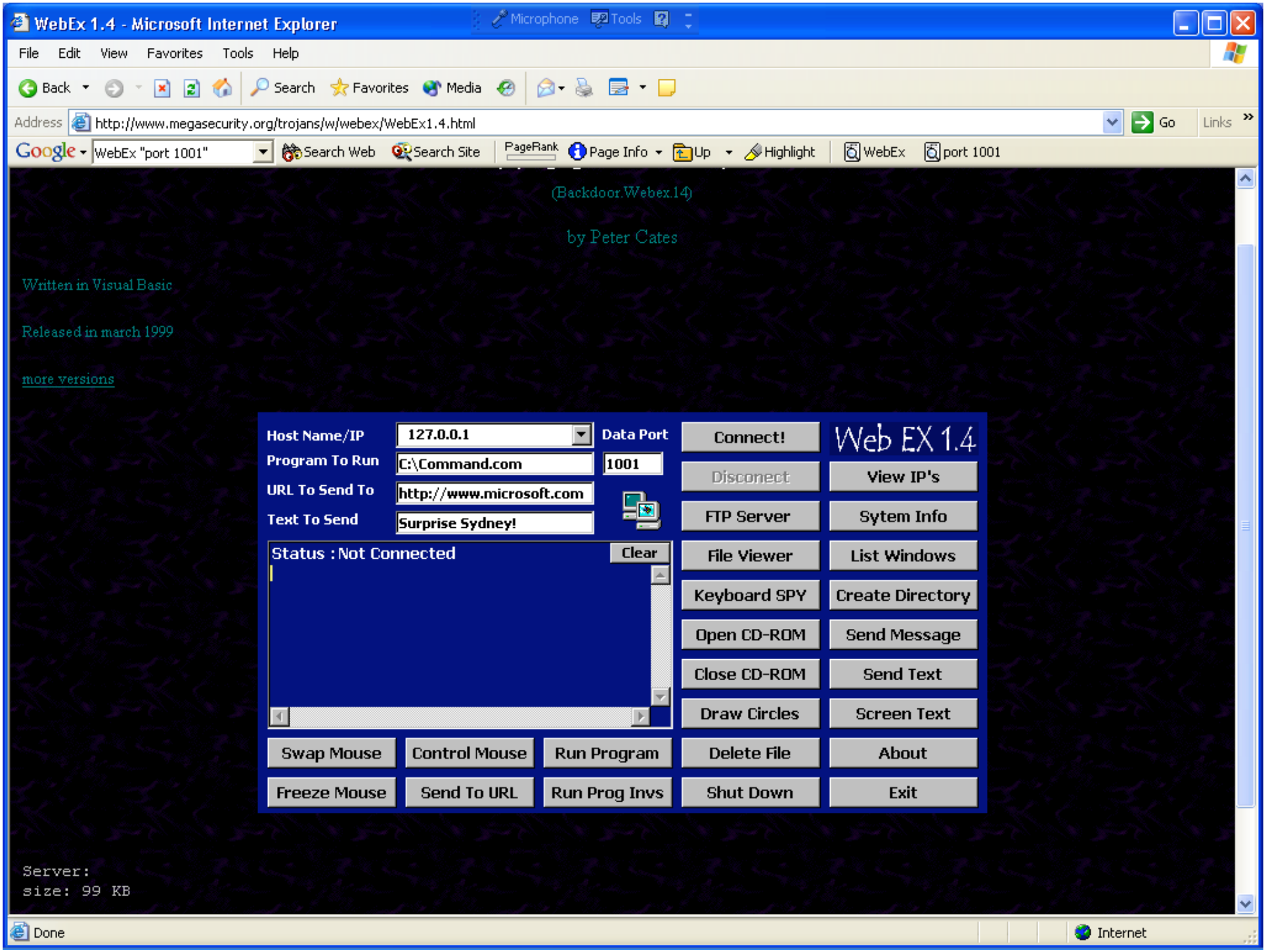
- Attack FTP, Back Construction, Cain & Abel, Satanz Backdoor, ServeU, Shadow Phyre
  - Cain
    - steal passwords
  - AttackFTP, Abel
    - stealth FTP
  - Satanz Backdoor, ServeU, Shadow Phyre
    - remote access

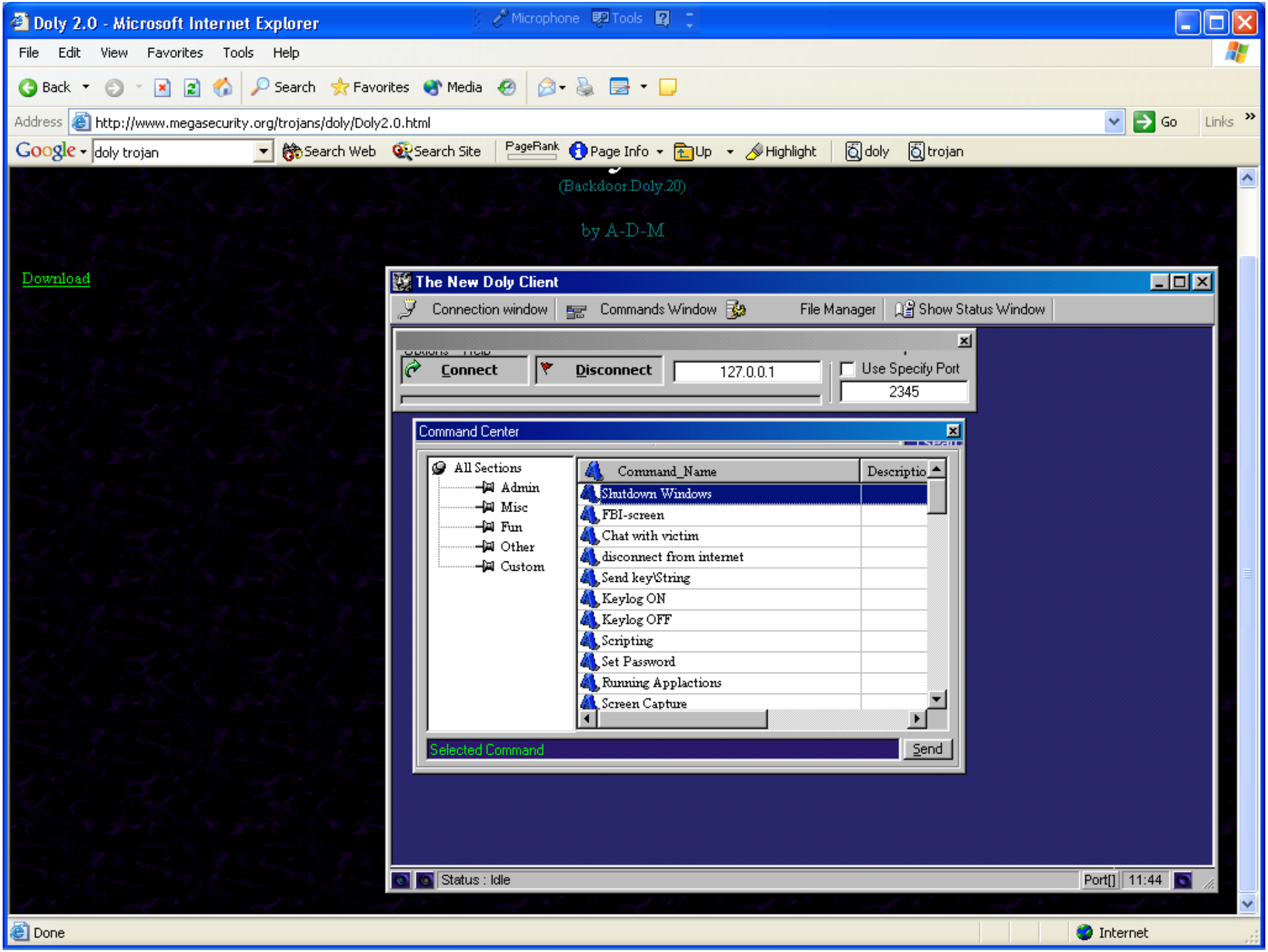
****

Apparently, the Trojan starts an FTP daemon that listens for connections on port 999. The default directory for this FTP server is C:\TEMP and there's no need for username or password - any username/password pair will gain entry.
As we previously described, the Trojan gives remote access to the victim's machine. One of the 'features' this Trojan give to the attacker, is the ability to format the victim's hard-drive. This is accomplished by running the following command:
echo,y,|,format,c:\",>,c:\autoexec.bat
This command adds a line to the autoexec.bat, instructing it to run an unconditional format the next time the computer starts.
Narr0w also found the complete list of servers that the Trojan tries to connect to:
irc.stealth.net, www.rootshell.com, irc.webbernet.net, irc.stealth.net,
ircnet.sprynet.org, irc.webbernet.net, irc.univ-lyon.fr,
ircnet.sprynet.com, irc.rus.uni-stuttgart.de, irc.rus.uni-stuttgart.de,
eu.ircnet.org, us.ircnet.org, irc.mmm.com.hk,
web.im.tut.fi,
irc.univ-lyon1.fr, 206.252.192.20 (irc.stealth.net).

After connecting to an IRC server, the Trojan uses one of the following nicknames:
USIL55, GUERIN, Entel, Procergs6, Rich0433, Niels, SII78, KTE-MP63, Usil94,
CCG67, Usil5, PROCERGS, Authorized, Jorge, Suporte88.
A private message is sent to the nickname scroll and scroll1. The message looks like this:
Privmsg scroll Online! I am ... , I use ... , my CPU is a ...
Privmsg scroll1 Online! I am ... , I use ... , my CPU is a ...

... One of the 'features' this Trojan give to the attacker, is the ability to format the victim's hard-drive. This is accomplished by running the following command:
echo,y,|,format,c:\",>,c:\autoexec.bat
This command adds a line to the autoexec.bat, instructing it to run an unconditional format the next time the computer starts.


WebEx 1.4 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.megasecurity.org/trojans/w/webex/WebEx1.4.html
Go Links
Google WebEx "port 1001" Search Web Search Site PageRank Page Info Up Highlight WebEx port 1001
(Backdoor.Webex.14)
by Peter Cates
Written in Visual Basic
Released in march 1999
more versions
Host Name/IP 127.0.0.1
Data Port
Program To Run C:\Command.com
1001
URL To Send To http://www.microsoft.com
Text To Send Surprise Sydney!
Status : Not Connected
Clear
Connect!
Web EX 1.4
Disconect
View IP's
FTP Server
Sytem Info
File Viewer
List Windows
Keyboard SPY
Create Directory
Open CD-ROM
Send Message
Close CD-ROM
Send Text
Draw Circles
Screen Text
Swap Mouse
Control Mouse
Run Program
Delete File
About
Freeze Mouse
Send To URL
Run Prog Invs
Shut Down
Exit
Server:
size: 99 KB
Done
Internet


Doly 2.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.megasecurity.org/trojans/doly/Doly2.0.html
Go Links
Google doly trojan
Search Web Search Site PageRank Page Info Up Highlight doly trojan
(Backdoor.Doly.20)
by A-D-M
Download
The New Doly Client
Connection window
Commands Window
File Manager
Show Status Window
Connect
Disconnect
127.0.0.1
Use Specify Port
2345
Command Center
All Sections
Admin
Misc
Fun
Other
Custom
Command_Name
Descriptio
Shutdown Windows
FBI-screen
Chat with victim
disconnect from internet
Send key\String
Keylog ON
Keylog OFF
Scripting
Set Password
Running Applactions
Screen Capture
Selected Command
Send
Status : Idle
Port[]
11:44
Done
Internet

Port 1024

- NetSpy
  - file access
  - change directories
  - enable server control
  - system information
  - messaging
  - stealth execution of command

Port 1243, 6776

- BackDoor-G, SubSeven, SubSevenApocalypse

- \windows\nodll.exe
- \windows\server.exe or kernel16.dl or window.exe
- \windows\system\watching.dll or lmdrk_33.dll

Virus-Trojan.WinCrash.103 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

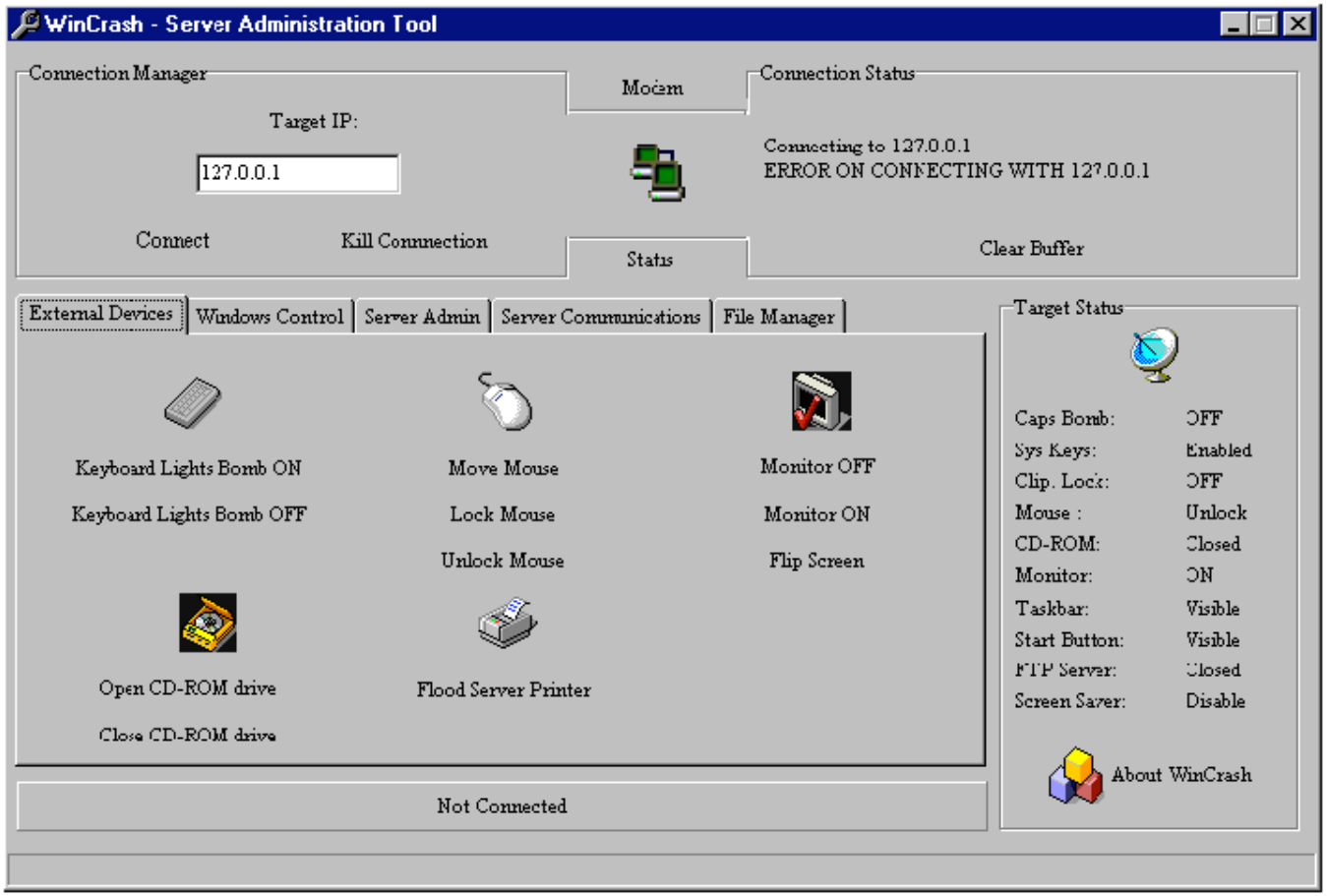
Back Search Favorites Media

Address http://www.ntsecurity.net/Panda/Index.cfm?FuseAction=Virus&VirusID=621

Google wincrash Search Web Search Site PageRank Page Info Up Highlight wincrash

Find next occurrence of 'wincrash' in current document

The client section of the Trojan is the one installed in the infected computer via a tool designed for this purpose. This consis
display with different sections within which it is possible to use the services offered by the server. Its aspect is as shown in the
figure below and each of the services shown is explained in the text that follows.



Each of the services offered is offered and accessible via four tabs, each of them being the following:

- **External Devices**

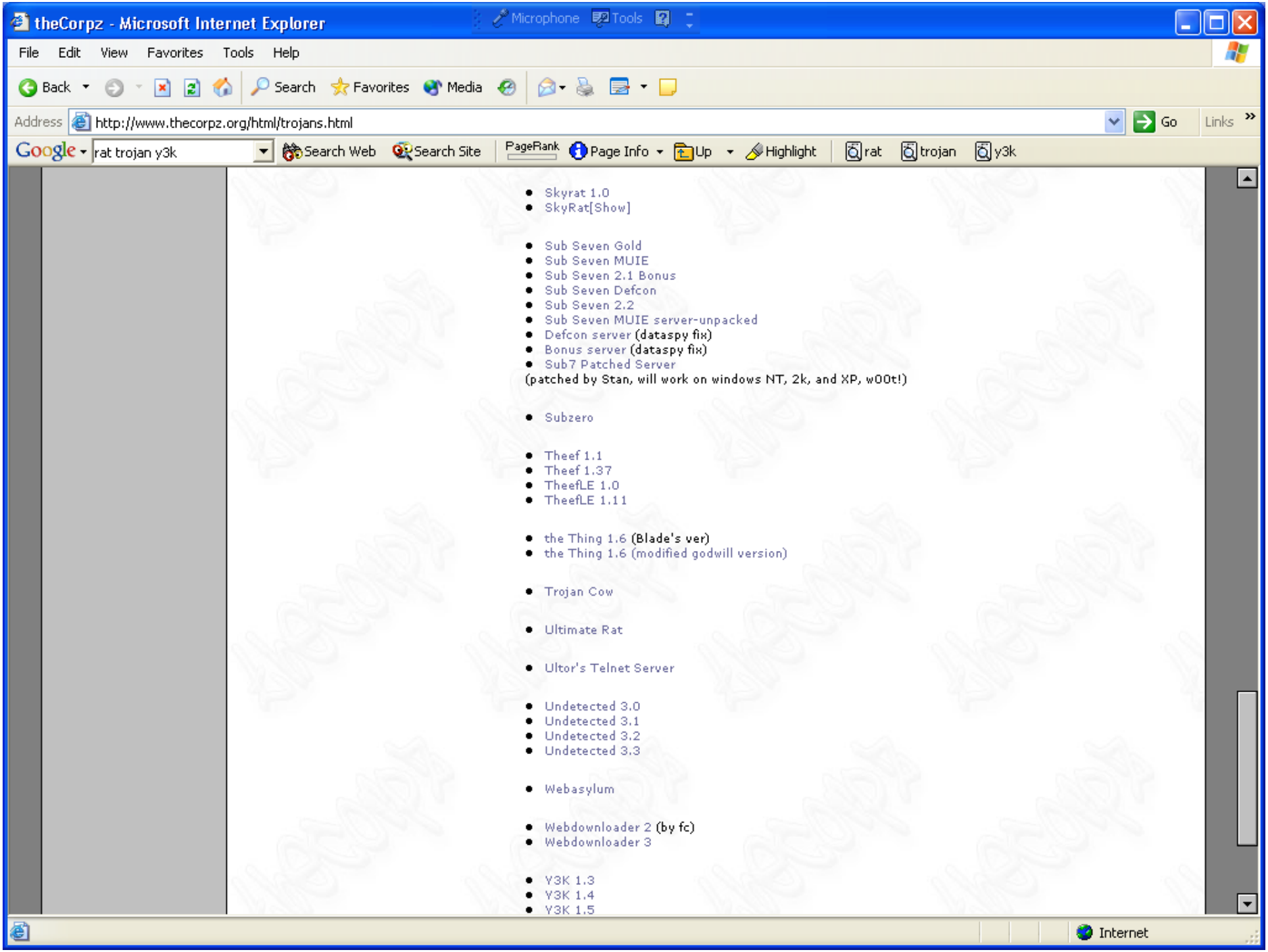
Done Internet

Port 2989

- RAT
  - Trojan designed to trash hard drives

5880, 5882, 5882 (UDP), 5888, 5888 (UDP), 5889 (ports can be hanged)

- **Actions:**
  - Remote Access / ICQ Trojan / IP sniffer / AIM Trojan / MSN Trojan
  - Includes an ICQ IP sniffer and may send a notification to the hacker's UIN. The server may be configured in many ways using combinations of some 40 features. It can stop local use of the Trojan, so nobody will be able use the client on the same machine as the server. As it is possible to alter the various registrations in the Registry, manual removal instruction may not be totally reliable.


theCorpz - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.thecorpz.org/html/trojans.html
Go Links
Google rat trojan y3k
Search Web Search Site PageRank Page Info Up Highlight rat trojan y3k
Skyrat 1.0
SkyRat[Show]
Sub Seven Gold
Sub Seven MUIE
Sub Seven 2.1 Bonus
Sub Seven Defcon
Sub Seven 2.2
Sub Seven MUIE server-unpacked
Defcon server (dataspy fix)
Bonus server (dataspy fix)
Sub7 Patched Server
(patched by Stan, will work on windows NT, 2k, and XP, w00t!)
Subzero
Theef 1.1
Theef 1.37
TheefLE 1.0
TheefLE 1.11
the Thing 1.6 (Blade's ver)
the Thing 1.6 (modified godwill version)
Trojan Cow
Ultimate Rat
Ultor's Telnet Server
Undetected 3.0
Undetected 3.1
Undetected 3.2
Undetected 3.3
Webasylum
Webdownloader 2 (by fc)
Webdownloader 3
Y3K 1.3
Y3K 1.4
Y3K 1.5
Internet


Sniffer Demo