Ethical Hacking:

The Value of Controlled Penetration Tests

Dr. Bruce V. Hartley, CISSP

Privisec, Inc.

August 6 , 2003

bhartley@privisec.com

719.651.6651

Session Overview

- Session Introduction
- Ethical Hacking
  - Taking a Look at the Environment
  - The Process, Tools, and Techniques
    - Internal Penetration Tests
    - External Penetration Tests
  - Some Real-Life Case Studies
- Conclusions

Before We Get Started

- My Background:
  - In The IT Field for 22 Years – Security for About 16
  - Currently President & CEO of Privisec, Inc.
  - Previously President and CEO of PoliVec, Inc.
  - Before That, SVP and CTO of Trident Data Systems
  - Academic Credentials:
    - Doctorate in Computer Science From Colorado Technical University, Masters and Bachelors Degrees in Computers as Well…So I'm a Geek…And, Remember: Geek is Sheik!
    - CISSP Since Forever as Well
  - Other Information:
    - Technical Editor for Business Security Advisor Magazine, Formally Internet Security Advisor Magazine
    - Numerous Publications, Conferences, etc.

Ethical Hacking:

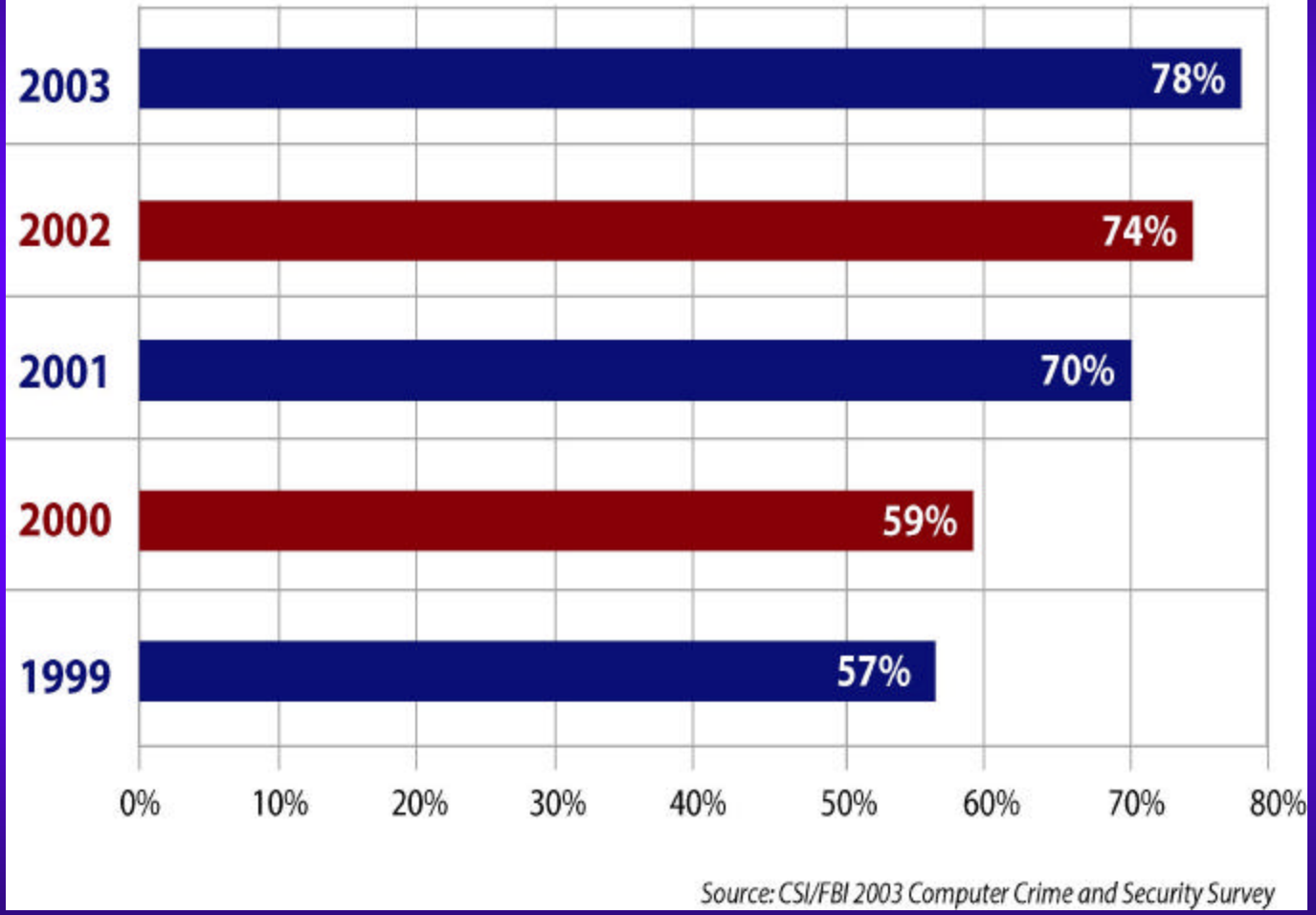
An Assessment Mechanism

Why Penetration Testing?

- Taking a Look at the Environment
- Penetration Testing – Benefits
- Taking a Look at the Process
- Real-Life Case Studies – Proof!

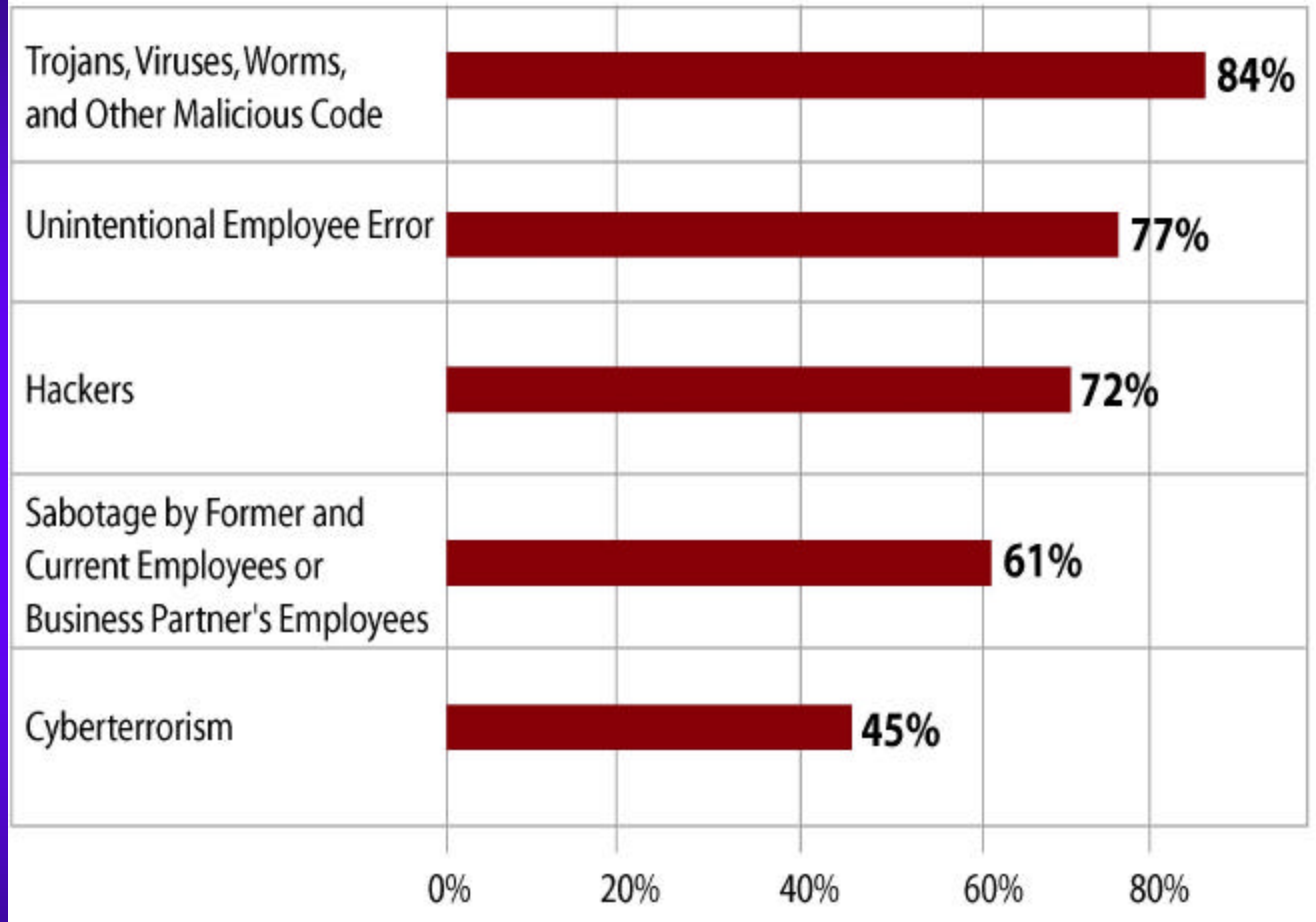
NET INTRUSIONS

% of organizations saying the internet is a "Frequent" point of cyberattacks.



Source: CSI/FBI 2003 Computer Crime and Security Survey

What are the Top Five Threats to Enterprise Network Security?



Source: 2003 InfoWorld Security Survey

Look At The Environment

- We Now Have Open Discussions on The Internet Concerning:
  - Vulnerabilities
  - Exploits and Attacks
  - Bugs and Faults
- Newer and More Sophisticated Attacks
- Newer and More Sophisticated Hacker Tools
- Attack Scripts and Penetration Tools Available to Anyone on the Internet

Look At The Environment

- Recent Google Search Results:
  - Hacker 12,500,000 Hits
  - Hacker Tools 757,000 Hits
  - Hacker Exploits 103,000 Hits
  - NT Exploits 99,000 Hits
  - Unix Exploits 139,000 Hits
  - Computer Vulnerabilities 403,000 Hits
  - Hacking NT 292,000 Hits
  - Hacking Windows 2000 271,000 Hits
  - Hacking Unix 390,000 Hits
  - Hacking Linux 1,290,000 Hits

Ethical Hacking - Benefits

- Penetration Tests are Designed to Identify Vulnerabilities Before They are Exploited
- Provides a Solid Understanding of What is Visible and Possibly Vulnerable
- Preventative Measure – Can be Very Effective
- Should Include a Remediation Phase
  - Correct Identified Vulnerabilities and Exposures

Ethical Hacking - Rationale

- Vulnerabilities and Exploits are Always Changing
  - Unless This is Your Business, Its Hard to Keep Up
  - Need to Perform on a Recurring Basis
- Hacking Tools and Methods Can Cause Damage IF Used Incorrectly
  - Some Exploits are Passive, Some are Not!
  - Some Exploits are Destructive, Some are Not!
- A Well Defined Process, Attack Methodology, and a Set of Tools are Required

Penetration Testing - General

- Can Consider Both Internal and External Assessments
- Internal: Goal is to Gain "Unauthorized Access to Data/Information"
  - Ultimate Goal is to Gain Administrator, System, or Root Access From the Inside (Depending on Platform)
  - Usually Begin With Just a Network Connection
  - May Require a Standard, Non-privileged Account (User)

Penetration Testing - Internal

- Start by Sniffing Network
  - Try to Obtain Userid and Password Combos
  - Common Tools
    - Snort (Unix/Linux and Windows)
    - WinSniff (Windows)
- Scan Internal Network (Port Scan)
  - Discover Active IPs and Devices
  - Gain Info About System Types and OSs
  - Common Tools
    - Nmap (Unix/Linux and Windows)
    - SuperScan (Windows)

Penetration Testing - Internal

- Check for Systems Running snmp With Exploitable Community Strings
  - Looking for ‘Public’, ‘Private’ or Other Common Words
  - Common Tools
    - SolarWinds (Windows)
    - SNScan (Windows)
- Launch Vulnerability Scanners to Identify Vulnerabilities to Exploit
  - Nessus, Nikto, Whisker, Brute Forcer Tools, Etc.

Penetration Testing - Internal

- Once Any Level of Access is Gained, Try and Obtain Privileged Access
  - Grab Password Files and Crack Passwords
    - Pwdump3 and pwdump3e
    - SAM Grab
    - L0phtCrack
    - John-the-Ripper
- Run More Sophisticated Exploits Against Vulnerable Services, Applications, Etc.

Penetration Testing – External

- External – Both Dial-Up and Internet
- Goal – Get Privileged Access
- Starts With Enumeration of the Target Network and/or Systems
- External Scan of Assets/Devices, Possibly More Enumeration
- Once Devices are Identified, Determine Type of Platform, Services, Versions, Etc.
- Hypothesize Potential Vulnerabilities and Prioritize Based on Likelihood of Success
- Attack in Prioritized Order

Penetration Testing – Tools

- Relies on Numerous Tools:
  - Port Scanners
  - Demon Dialers
  - Vulnerability Scanners
  - Password Grabbers and Crackers
  - Vulnerability and Exploit Databases
  - Default Password Databases
  - Other Resources
    - Experience and the Good Old Internet!

Penetration Testing – The Process

- The Vulnerability Assessment Process:
  - Gather Information
  - Scan IP Addresses
  - Determine Service Versions
  - Assemble Target List
  - Gather and Test Exploits (Yes, Test Them First!)
  - Run Exploits Against Live Targets
  - Assess Results
  - Interactive Access on Host(s)
  - Root/Admin Access on Host(s)
  - Repeat Until No More Targets Available or Desired Results are Achieved

Preparatory Work

- Things You Need Before Starting the Test
  - Authority to Perform Test
    - **This must be in writing!**
  - A Specific Set of Ground Rules That Should Answer at Least the Following Questions
    - Is this test covert or overt?
    - Are there any “off-limits” systems or networks?
    - Who is our trusted POC?
    - Is there a specific target (system, type of information, etc) of this test?

Gathering Information

- The First Thing You Want to Know is What IP Address Range(s) are Owned and/or Used by the Target Organization
- Start With a whois Lookup
  - American Registry for Internet Numbers (ARIN) whois http://whois.arin.net/whois/index.html
  - Network Solutions whois http://www.networksolutions.com/cgi-bin/whois/whois/
  - European information is at the RIPE NCC http://www.ripe.net/perl/whois
  - Asian information is at the Asia Pacific Network Information Center http://www.apnic.net/

Gathering Information

- Other Sources of Information:
  - IP address of Webserver(s), Mail Server(s), DNS Server(s)
  - Go Back to whois and Verify Who Owns Those IP Addresses and the Network Space That Contains Those IP Addresses
  - IP Addresses of Other Organizations That May Have Been Purchased by the Primary Organization
  - SamSpade.Org!
- Verify All IP Addresses and Ranges With Trusted POC Before Proceeding!

Scanning IP Addresses

- Intent: To Discover What Network Ports (Services) are Open
- Tool of Choice: nmap, by Fyodor Available at: http://www.insecure.org/nmap/
  - Written for Unix/Linux Systems
  - Freely available
  - Ported to Windows NT/2000 by eEye Digital Security http://www.eeye.com/html/Research/Tools/nmapnt.html
  - Provides Many Features
    - Multiple different scanning methods
    - Operating System detection
    - Ping sweeps
    - Changeable scan speed
    - Multiple logging formats

Scanning IP Addresses

- If You Are Scanning From a Windows NT/2000 System, Your Options are:
  - Use nmapNT from eEye
    - Requires installation of a libpcap network driver
    - More difficult to use, specifically wrt selecting network interfaces
  - Use SuperScan from Foundstone
    - GUI interface
    - Lots of options
  - Use fscan from Foundstone
    - Command-line tool (very useful in some instances)
    - Lots of options

Scanning IP Addresses

- Both Unix/Linux and Windows Versions of nmap have a Graphical Front-End Available (nmapfe)
- Same Options Available Via the GUI – Easy to Use

Scanning IP Addresses

- SNMP Scanning
  - Usually can be Performed Quickly
  - A Default SNMP Server can Yield **Reams** of Useful Information
    - Default community strings (passwords) are ‘public’ and ‘private’
  - Tools
    - SNScan From Foundstone
    - Solarwinds Network Management and Discovery Tools (for Windows)
      - SNMP sweep
    - ucd-snmp/net-snmp for Unix
      - snmpstatus
      - snmpwalk

Scanning IP Addresses

- Web Server Scanning
  - Whisker by Rain Forest Puppy http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=1
    - Perl script that probes web servers for
      - Version information
      - Executable subdirectories
      - Potentially vulnerable executable scripts or programs
    - Basic use: *perl whisker.pl -v -h hostname | tee filename*
      - Many advanced features available
  - Nikto
    - HTTPS-only web servers can be scanned with stunnel (http://www.stunnel.org/) + Whisker or Nikto
      - *stunnel -c -d localhost:80 -r hostname:443*
      - *perl whisker.pl -v -h localhost | tee filename*

Determining Service Versions

- Each Open TCP Port Likely Provides a Network Service
- Well-Known Port Numbers are Normally Used to Provide Well-Known Services
  - e.g. TCP port 23 is expected to be a telnet daemon
  - Reference http://www.iana.org/assignments/port-numbers
- Many Well-Known Services Will Provide Version Numbers With Very Little Prodding

Vulnerability Assessment Tools

- Once Target List is Identified, Can Run Vulnerability Scanner to Attempt to Identify and Possibly Exploit Known Vulnerabilities
  - CERT and CIAC Advisories
  - Vendor Advisories and Warnings
  - Other Public Sources (Bugtraq)

Vulnerability Assessment Tools

- Once Target List is Identified, Can Run Vulnerability Scanner to Attempt to Identify Vulnerabilities
- Some Common Tools:
  - Nessus (Unix/Linux)
  - SNScan (Windows)
  - Nikto (Unix/Linux)
  - Whisker (Unix/Linux)
  - SMB Brute Forcer (Windows)

Assembling The Target List

- Assemble a Comprehensive List of Open Ports and Known Service Versions
- Examine List for Likely Vulnerable Versions of Software, e.g.
  - wu-ftpd versions older than 2.6.1
  - bind (DNS) servers older than 8.2.3
  - Any IIS web server
- For Web Servers, Examine the Results of Whisker or Nikto Scans for Potentially Vulnerable Scripts or Programs
- Pick the Top Five Most Likely Exploitable Hosts/Services

Gathering and Testing Exploits

- Exploit Code Should **Never** be Run Against a Live Target Without Prior Testing Against a Test System
- Exploits Can be Very Dangerous!
- If You Haven't Tested it Don't Run It!!!
- Behavior May Not be as Expected or Desired

Gathering and Testing Exploits

- Minimal Criteria for Exploit to be Worth Testing
  - Exploit Must Match Both
    - Target operating system
    - Target service version number
- Need to Assemble or Have Access to Test System(s) That Matches Configuration of Target
- Exploits Have Many Potential Results
  - Read any File on the Target System
  - Modify any File on the Target System
  - Allow Non-interactive Execution of Commands
  - Allow Interactive Access to Remote System as an Unprivileged User (Unprivileged Shell or Command-level Access)
  - Allow Interactive Access to Remote System as a Root, Admin, or Other Privileged User (Privileged Shell or Command-level Access)

Gathering and Testing Exploits

- Sources for Exploits
  - SecurityFocus vulnerability database http://www.securityfocus.com/vdb/
  - http://www.hack.co.za/
  - Fyodor's exploit world http://www.insecure.org/sploits.html
  - Packetstorm security http://packetstorm.securify.com/
  - Shaedow's exploit library http://www.reject.org/shaedow/exploits/index.html
  - Technotronic http://www.technotronic.com/
  - Securiteam's exploit archive http://www.securiteam.com/exploits/archive.html
  - Johnny's exploit index http://www.martnet.com/~johnny/exploits/

Gathering and Testing Exploits

- Once a Candidate Exploit is Located
  - Compile the Code on an Appropriate Platform
  - Test it Against Test System
  - Assess Results
    - Exploit Failed
      - Move on to the next candidate
    - Exploit Succeeded
      - What did it give us?
      - What can we do with that elevated access?

Running Exploits Against Live Targets

- Set All the Pieces Up
  - Attacking System
  - Any Required Network Listeners, etc
- Type the Commands to be Executed Into a Text Editor
- Triple Check the Commands, Especially IP Addresses!
  - Recommend Two-person Teams, Each Double-checking the Other's Work
- Recommend Simultaneous use of a Sniffer to Monitor all Relevant Network Traffic
- When Prepared to Execute, Copy and Paste the Commands into the Execution Window
- Hope it Works!

Assessing Results

- If Exploit Fails, Attempt to Determine Why
  - Exploit was Supposed to Open a Command Shell on a High-numbered Port, but Port was Unavailable for Connection Attempt
    - Potentially blocked by a firewall
  - Examine Sniffer Logs for Clues
- Unfortunately, it is Often Very Difficult to Determine the Cause of a Failed Exploit Attempt
- Move on to the Next Candidate Exploit

Assessing Results

- If Exploit Succeeded
  - Assess Level of Access Currently Obtained
  - Reprioritize Target List for Next Exploit Attempt
- First-Level Goal Should be any Sort of Interactive Access to the Remote System
- Second-Level Goal Should be root or Admin-Level Interactive Access on Remote System

Interactive Access on Host(s)

- Once Interactive Access is Obtained, Local Exploits Can Be Run
  - These are Much More Prevalent Than Remote Exploits
  - Much Easier to Obtain Root or Admin-level Privileges
- Even With Unprivileged Interactive Access, Many Useful Steps Can be Taken
  - Determine Available Network Interfaces and Settings
    - Is this system behind a network address translator?
    - Is this system on a DMZ or an internal network?
  - Perform Port Scans From This System Against Others on its Local Network (nmap, SuperScan, or fscan)
  - Be Very Careful to Avoid all GUI or Windowing Commands, Especially on Windows Systems

Interactive Access on Host(s)

- Privileged Command Access Leads to Many Further Options
  - Start up a network sniffer on each interface
    - Winsniff for Windows NT/2000 http://winsniff.hypermart.net/
    - Dsniff or Snort for unix systems http://www.monkey.org/~dugsong/dsniff/
  - Look for trust relationships between this host and others
  - Obtain encrypted passwords or password hashes and begin cracking passwords
    - On unix: /etc/passwd, /etc/shadow, or other appropriate location
    - On windows: pwdump or pwdump2
  - If the objective is a specific piece or type of information, check the system for that information

Interactive Access on Host(s)

- As Each New Piece of Information is Obtained, Re-prioritize the Target List and Take Action Appropriately
- Continue Until All Objectives are Accomplished, or No Further Access Can be Obtained

Some Real-life Case Studies:

Recent Penetrations

Example Penetrations

- Five Examples From the Multiple Industries
- All Penetrations 100% Successful
  - Gained “Unauthorized” Privileged Access
  - Access Undetected by Systems Personnel
- All Penetrations Were Preventable – Known Vulnerabilities or Poorly Configured Systems

Example Penetrations

Industry	Type of Attack	Penetration Method	Level of Access	Vulnerability	Firewall Installed
Airline	Netware and Dial-up Connections	Dial-in – Used remote control program to connect to a Novell client machine without any authentication. Client had an active session on a network server. Using a Novell default account gained full system privileges.	Complete system access to entire Network: File Servers, Mail Servers, Applications Servers, Database Servers, and Personal Workstations.	Dial-in	Yes. Commercial firewall installed on a Windows NT Server.
Multimedia Entertainment	UNIX and Dial-up Connections	Dial-in – Exploited a known vulnerability on a UNIX host via modem connection – gained root access.	Complete system access to entire network.	Vulnerability on a UNIX host via modem connection	Yes. Commercial firewall installed on a UNIX Server.
Newspaper	Intranet Vulnerability	Internet – Exploited a known vulnerability in NFS and gained root access on WWW (UNIX) server. Gained access to internal network due to poor host security (trust relationships) on WWW server.	Complete system access to WWW servers, DNS Servers, Mail Servers, File/Print Servers, and publishing systems.	Vulnerability in NFS	Yes. Commercial firewall installed on a UNIX Server.

More Penetrations

Industry	Type of Attack	Penetration Method	Level of Access	Vulnerability	Firewall Installed
Financial	NFS Vulnerability	Dial-in – Exploited a known vulnerability in sendmail to gain access to an Intranet server (UNIX). Gained access from Intranet server to internal network due to trust relationships. Exploited a known vulnerability in NFS on a VMS host to gain additional full system access.	Complete system access to Intranet and internal (trusted) network.	NFS	Yes. Commercial firewall installed on a UNIX Server.
Publishing	NIS Vulnerability	Internet and Dial-in - Exploited a known vulnerability on an exposed UNIX server to gain access via Internet. Penetrated a client PC running Windows 95 via modem access using remote control software, and a UNIX host via a terminal program and a default account. Gained root access by exploiting a known vulnerability.	Complete system access to internal networks.	Vulnerability on an exposed UNIX server to gain access via internet.	Yes. Commercial firewall installed on a UNIX Server.

Penetration Tests: Lessons

- In Each Case, the Penetration Could Have Been Prevented IF:
  - A Comprehensive Security Policy had Been Implemented Across the Enterprise
  - Good Systems Administration Practices Were Utilized
  - A More Proactive Security Process was in Place
    - Security Audits and/or Assessments
    - Investment in Security Assessment Technology
    - Better User Security Education and Awareness
    - Minimal Incident Response Capability

Conclusions

- Penetration Testing Can Be Used to Significantly Improve Your Security Posture
- A Reasonably Secure Infrastructure is Achievable
  - Must View Security as a Process, Not a Project
  - Embrace Technology and Use it!
  - Be Consistent Throughout the Enterprise
  - Consider the Entire Business Process, Not Just the Transaction Component
- Think About Security From an Enabling Standpoint vs. an Inhibitor
- Be Proactive…Don't Wait for a Security Problem

My Contact Information

Dr. Bruce V. Hartley, CISSP
President & CEO
Privisec, Inc.

719.651.6651 (Phone)
719.495.8532 (Fax)
bhartley@privisec.com
www.privisec.com