DC Phone Home

Defcon, Las Vegas 2002
<table>
<thead>
<tr>
<th>Chris Davis, CISSP</th>
<th>Aaron Higbee, CISSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>RedSiren</td>
<td>Foundstone</td>
</tr>
<tr>
<td>Reston, VA</td>
<td>Washington DC</td>
</tr>
</tbody>
</table>
Overview

- 180-Degree Hacking
  - Phone Home
- Developed Platforms
  - Sega Dreamcast
  - Compaq iPAQ
  - x86 Bootable CD
- Demonstrations
- Remedies
This Presentation
Sega Dreamcast Distribution
iPAQ Distribution
x86 Bootable CD-Rom
Assumptions

- Linux
- General Computer Architecture
- TCP/IP
- General Information Security Concepts
- Firewalls / NAT / Private Addressing
- VPN’s
- Proxies
- Common haxOr toolz
Conventional Enterprise Security

- Firewall
- Network Address Translation
- Private Addressing – RFC1918
- DMZ
Higher End Enterprise Security

- IDS (managed?)
- VPNs, Remote Access
  - Strong Authentication
- Proxies, URL filtering
- Content-checking (email virus)
- Security Personnel
- Security Consulting
Hard Crunchy Outside

Soft CHEWY Center
The Problem

- Networks go both ways: in and out
- The focus is on perimeter network security instead of the data contained within
- Even hackers are focused on the perimeter instead of the data
  - Apache
  - OpenSSH
Firewalls

What *can* they do?

- Enforcing inbound connection policies
- DMZ
- NAT
- Authentication
- VPN Gateways for remote users
- Restricting *some* outbound traffic
Proxies

- Used to enhance network performance
- Limited content-checking features
- Mostly have to allow outbound tcp/80
  - Soap
  - DAV
  - HTTP-U
  - 30+ in development
Network Intrusion Detection

Exists to help identify and respond to hack attempts in a timely manner

- Mostly focused on listening for incoming attacks
- Signature-based detection
  - Must be aware of particular attack to identify it
  - Anomaly protocol detection only detects anomalies
    - WTF is that!?
The Soft Chewy Center

- Outbound connections are believed to be initiated by employees
- Companies need their employees to use the Internet
- Physical security is ‘good enough’
- Outside = Bad, Inside = Good
The “Computer” Concept

- Fits on a desk or in your lap
- Runs Windows

Wrong!

- A “Computer” is a general purpose architecture
  - Tivo
  - Cell Phones
  - Printers
  - Cable Boxes
  - Printers
  - Copiers
  - Game Consoles
  - Vending Machines
180-Degree Hacking

- Why hack the network? Bring it home!
- Based on the following principles
  - FIREWALLS ARE POINTLESS
  - Delivery
    - Physical access
    - Zero-day sploit
  - The Internet
  - Stupid user tricks
Firewalls Are Worthless

- In 180-degree hacking, firewalls are transparent
  - Data is tunneled through an authorized protocol or via encrypted transport
  - Firewalls are two-way
  - They can’t block ALL traffic
Physical Access

- Physical access is trivial to obtain (seriously)
- Especially for short periods of time [5 min]
- Creativity and planning is the only limiting factor
Super Stealth Method
The Smoke Screen
Piggy Back
0-day sploit

- Same-ole Same-ole
- Boring
- Anybody, and Everybody
  - Apache
  - Openssh
- BNC and dDoS... is the best you can do!? Get Creative!
180-Degree Hacking: Post-Delivery

- Discover network
- Enumerate outbound traffic
- Phone Home
180-Degree Hacking: Similar Concepts

- P2P File-sharing
  - WinMX
  - Bearshare
- Chat Appz
  - Aim
- Remote Desktops
  - GoToMyPC.com
180-Degree Hacking: Network Discovery

- Network Auto-Configuration DHCP
- Enumerate Allowed Outbound Traffic
- Write Results To /dcph_info.txt
- Ports: 80, 443, u53, ICMP, Etc...
180-Degree Hacking: Analysis

Analyze dcph_info.txt

- 80 open?
- 443 open?
- 53 open?
- ICMP open?

Start VTun

Start VTun

Start cIPe

Start icmp tunnel

Yes - No

Goto Proxy Finder
180-Degree Hacking: Proxy Finder

Proxy Finder

Zone Transfer DNS

Reverse Lookup Range

Grep proxy, pxy squid

Http-tunnel

Sad face
180-Degree Hacking: Delivery Types

- Drop-n-go hardware
  - SEGA Dreamcast
  - Compaq iPAQ
- Software
  - Bootable x86 CD-Rom
- Remote Exploit
  - duh
Why the hell did we pick a Dreamcast!?

- Innocuous: doesn’t it just play games?
- Cheap: under $100 for everything
- 10/100 Ethernet: made just for hacking
- Powerful processor
- Rumors of a Linux port
- Crazy Taxi got boring
Dreamcast Architecture

- Hitachi SH4 Core Processor @200MHz
- 16MB RAM
- CD-ROM
- 10/100 RTL-8931 Ethernet
- Keyboard (pretty useful)
Dreamcast Development

- Building the distro
  - RPMs from www.sh-linux.org
  - X-Compile Toolchain
  - Kernel patching and compiling
    - Experimental support in recent 2.4 kernels
  - Linux development waning since DC was discontinued
- Compiling Toolz
  - Limited RAM prevents native compilation
Compaq iHACK Architecture

- Compaq iPAQ 3765
- StrongARM 206MHz core processor
- 64MB RAM
- 32MB Flash ROM
- Dual-Slot PCMCIA Expansion Pack
- USB/Serial Interface
- 10/100 Ethernet and 802.11b capable
Compaq iHACK Development

Linux Support

- ARM proc support in kernel since 2.2.x
- Large group of Linux developers
  - [www.handhelds.org](http://www.handhelds.org)
- Functional distribution available
  - Used Familiar v0.5.2
- Native compiler
  - Independent development platform
x86 Bootable CD

- **Trinux**
  - Supports many types of hardware
  - Runs on virtually any PC
  - 20meg ISO
  - Kernel 2.4.5
  - Easily modified
Toolz

- **Network Autoconfig**
  - DHCP
- **Scanning**
  - netcat
  - nmap
- **Sniffing**
  - PHoss
  - ngrep
  - tcpdump
- **Tunneling**
  - VTun
  - CIPE
  - httptunnel
  - icmptunnel
  - stunnel
  - ppp
  - ssh
Common Tools

- host
- nslookup
- shell scripting
- sed
- cut
- tr
Phoning Home Simplified

- Delivery
- Booting
- Network autoconfiguration
- Network discovery
- Enumeration
- Tunneling
Demos

Enough chit-chat! Let’s see it work!
Demo Summary

Network Diagram:
- Workstation 10.x.x.50
- Proxy Server
- Internal 10.x.x.x
- Swiss Cheese Firewall
- Router External 63.x.x.x
- Internet
- Home 24.x.x.x
- Dreamcast 10.x.x.99 v192.168.1.1

Pinging 10.x.x.30 with 30 bytes of data:
Reply from 10.x.x.30: bytes=32 time<10ms TTL=44
Reply from 10.x.x.30: bytes=32 time<10ms TTL=44
Reply from 10.x.x.30: bytes=32 time<10ms TTL=44
Reply from 10.x.x.30: bytes=32 time<10ms TTL=44

DC Phone Home
VPN
How is this stopped?

- To sum it up: constriction, not prevention.
  - Limited egress paths
    - As many proxies as possible
      - HTTP
      - DNS
      - Email
  - Full-mesh intranet VPN topology
    - Authentication between all endpoints, including gateways
    - Only prevents drop-n-go hardware

- **Switch Port Security**
  - Pre-registration of MAC addresses

- **Superfine Granular IDS**
  - Protocols must adhere to strict specifications
  - Protocol-analyzing proxies
    - Can deconstruct sessions to detect misuse

- **Wireless Jamming**
  - Prevents rouge Access-Points
Covert channels will ALWAYS be possible
Smaller devices make detection and removal more difficult
Targeted attacks are based on research of your organization
Like most information security, the only true protection is the air-gap
Links

http://www.dcphonehome.com
http://trinux.sourceforge.net
http://www.sh-linux.org
http://sites.inka.de/sites/bigred/devel/cipe.html
http://www.phenoelit.de
http://vtun.sourceforge.net
http://www.nocrew.org/software/httptunnel.html
http://www.detached.net/icmptunnel/
http://www.stunnel.org
http://www.buildinglinuxvpns.net
http://www.foundstone.com
http://www.redsiren.com
http://www.realultimatepower.net