

# Basics of Home Internet Security

- Dick Bonneville, CISSP
- Director of Network Services / Security Services
- PC Solutions, Inc

# Understanding Data Security

- The Seven Layer OSI Model
- IP Protocol Suite
- IP Packet Construction
- Nuances of various flags and fields within the packet and how they change as we move through the various protocols within the IP suite
- Just kidding

# What is Data Security?

- Data Confidentiality
- Data Availability
- Data Integrity

# Components of Security

- Firewalls
- WAPs
- Modems
- Password Strength
- Spyware / Viruses / Trojans
- Unnecessary services running on the computer
- Physical Security
- Social Engineering

# Firewalls

- Firewalls are an important part of security, but they are not a “be all and end all”
- Many low cost hardware solutions available
- They are frequently configured incorrectly
- Routers are not firewalls
- You can get ZoneAlarm from [www.zonealarm.com](http://www.zonealarm.com)

# WAPs (Wireless Access Point)

- WAPs are frequently incorrectly configured using no encryption
- More homes are going wireless
- “War Driving” is becoming more and more common

# Password Strength

- Most people use insecure passwords
- Passwords are often on a post-it note attached to the computer
- Dictionary and brute force attacks
- Many people use passwords that never expire
- Use a “Pass phrase”
- Trdiayw,aslcntb,ab1t

# Spyware / Viruses / Trojans

- These range from annoying to devastating
- Nimda / Code Red showed that antivirus software is not always effective

# GoToMyPC.com

- GoToMyPC.com is representative of a new breed of security problems
- They travel over port 80 or 443 effectively bypassing the firewall
- You are effectively creating a WAN with an unknown company

# Gator.com

- Gator.com is Spyware
- Gator sends a report in real time to gator.com on every web site you visit
- Targeted marketing

# Unnecessary Services

- Check your PC for unnecessary services (web server, ftp, telnet) and disable them
- Don't share your drive – People on cable systems can sometimes click on “Network Neighborhood” and see their neighbors files

# Physical Security

- Anyone who can touch a machine can own it
- Know who's using your machine, and make sure you trust them (The neighbors kid may be an up and coming hacker, and he may decide to practice on your machine)

# Technical hacks vs. Social Engineering

- Technical hacks take advantage of an operating system or application vulnerability i.e. buffer overflow attacks
- Social Engineering is form of “con” that utilizes technical and non-technical means to get to your computer.
- Most hackers use a combination the two

# Social Engineering

- Hackers use a number of techniques to get people to give them information
  - ◆ “Selling the Boat” to get names and determine logins or to use in further penetration
  - ◆ “I can’t get in” calls to the help desk to get password reset
- People have a natural tendency to be helpful and trusting – Hackers love helpful people

# Methods of Social Engineering

- Posing as a direct employee
- Posing as a vendor employee
- Posing as someone in authority
- Posing as a new employee requesting help
- Posing as a vendor manufacture to offer a system patch or update

# Methods of Social Engineering (Cont.)

- Send free software for for the victim to install
- Using false pop up windows asking user to log on again
- Capturing victim keystrokes
- Using insider lingo to establish trust.
- Sending a virus or Trojan Horse as a email attachment
- DNS poisoning to hijack a web site
- Offering something for free to get you to create a user name / password on a malicious website

# Social Engineering – Case Study

- This an actual attack by John Ceraolo, CISSP

# The Sting

- Call to the receptionist “I need to send a resume.”
- “But I’ve been out of work for 6 months”
- Bob Smith is the IS Manager

# The Sting (Cont)

- Call the computer room
- “Hello, this is Bill Johnson”
- Click
- One of the operators is Bill Johnson

# The Sting (Cont)

- Next, he called up later in the day, and said "I'm Ralph from Digital Equipment Corporation, I was talking to Dave Smith, and I need the password to 'Root,' and Bob, Bill's manager said..."
- "Okay," said his unwitting victim, "let me get that for you." Boom!
- Ten to 15 minutes of work, and he was into the system, with 'Root.'

# The Sting (Cont)

- Using 'Root', he went through the system and found out all kinds of information about other systems including their locations
- Next, he called up another site.
- "There's a patch in VMS 5.1 that I need to apply, and..." He mentioned Bob's name again, and got into that system too. Now he had two 'Root' passwords, plus the dial up numbers

# The Sting (Cont)

- Two days later, he called another site at 5:00 p.m. The guy who answered the phone wanted to go home – Same conversation - Guess what?
- That makes three 'Root' passwords

# The Sting (Cont)

- The tactic didn't work at the fourth location, but if at first you don't succeed....
- he tried the third shift. He called up at 4:30 a.m. He said "I need to get on your 'Root' account". He mentioned a couple of names.
- That makes four 'Root' passwords

# The Sting (Cont)

- In his defiance, he turned off auditing, created backdoors, sent an e-mail message to the VP of Technical Services and stayed logged on until 7:30 a.m. No one detected him.

# The Sting (Cont)

- The Network was secure, technically, but the human factor was ignored
- Could you, your co-workers, your spouse or your kids be fooled?

# Social Engineering against home users

- “Please review this document and return it to me”
- “Visit this website and you could win...”
- “In order to visit this website you must register”
- “Check out this screensaver”

# Nigerian email scam

- Official sounding person needs to get money out of Nigeria
- Of course, you need to send money for permits and to bribe officials
- Eventually you go to Nigeria, where customs is expecting you and you are waved through
- At least one person has been killed in this scam

# Peer to Peer file sharing programs

- Examples are KaZaa, Gnutella, Morpheus
- These programs are used to share files, usually music and video
- These programs have security holes which could allow a hacker to access your personal files
- There are liability issues – you are often serving up copyrighted content

# Sub 7

- Sub 7 is one of a plethora of programs which, once run on your system, allow access through a backdoor
- AD-Aware is a Spyware checking and removal tool available at [www.lavasoftusa.com](http://www.lavasoftusa.com)

# Conclusion

- Always know the source of any file you open or execute on your computer or program you install
- Run up to date anti-virus software
- Use a firewall
- Periodically check your computer for Spyware
- Be wary of anyone asking for your password or other information
- Use secure pass phrases
- Patch your computer regularly
- If you run xp, patch it tonight