Chapter 3

REAL THREATS THAT IMPACT SECURITY

INTRODUCTION

The Internet provides a wonderful means of exchanging information, but no one wants sensitive information on their computers to be stolen or destroyed. Hackers and worms are constantly on the lookout for computers with security vulnerabilities connected to the Internet. Unfortunately, whether it's due to a lack of knowledge, tight budget, or sheer laziness, too many of you don't protect your own data [1].

COMMON HACKER EXPLOITS

Once a hacker finds a computer with open ports they probe further to see if the software behind each open port contains buffer overflows, outdated software or misconfigurations. If a hacker finds one of these vulnerabilities they may attack your computer. Here is a partial list of the things a hacker could do to your computer if it has vulnerabilities:

1. View Your Passwords
2. Watch Everything You Do
3. Install a Zombie
4. Copy Files From Your Hard Drive
5. Copy Files To Your Hard Drive [1]

View Your Passwords

If a hacker has access to your computer they may have access to files stored on your computer where passwords are kept. Sometimes passwords are stored in normal text and sometimes they are encrypted. Either way, a hacker can probably crack the passwords you use on your system so they can continue to access your computer [1].

If you access your enterprise's network from home then this becomes especially dangerous. The passwords you type to access your enterprise's network may be stored on your home PC. A hacker may be able to break into your enterprise's network because your home PC was not secure [1].

Watch Everything You Do

If a hacker installs remote control software then you are no longer safe. Remote control software allows a hacker to view everything on your computer as you do. If you view your personal banking information on your computer then so does the hacker. Also, remote control software allows a hacker to record keystrokes typed into your computer. So your passwords are no longer safe and should be changed [1].

Install A Zombie

Zombie software allows a hacker to make your computer attack other computers on the Internet. Once Zombie software is installed on your computer you will not know it is running. If Zombie software were installed on your computer right now you could be attacking the website of a large enterprise. The enterprise will trace the attack back to your computer and you will plead ignorance. In European countries you are now liable for damages to others if a hacker is using your computer for attack purposes [1].

Copy Files From Your Hard Drive

If you have network shares set to READ for the group EVERYONE then a hacker may be able to copy your data. If you have personal accounting data or confidential files on your computer then a hacker may have already copied that data. Accounting software, word processing, spreadsheet, and most applications don't use good password encryption schemes. Most passwords for these applications can be cracked easily [1].

Copy Files To Your Hard Drive

If you have network shares set to READ/WRITE for the group EVERYONE then a hacker may be able to copy files to your computer. Why is that a problem? This is how hackers install remote control software. Or they may decide to copy viruses to your computer, or ruin the configuration of your computer, or store pornographic material for later browsing or whatever [1].

VULNERABILITY DETECTION

What makes a computer vulnerable to hackers and worms? Whenever a computer starts a program that program uses a port. Each port has a number from 0 to 65,535. For example,