Conducting Network Penetration and Espionage in a Global Environment

Bruce Middleton
# Contents

Preface ......................................................................................................................... xi
About the Author ......................................................................................................... xiii

1 What You Need to Know First .................................................................................. 1
   MATLAB® and SimuLink (MathSoft.com) ............................................................. 9
   Recommended Defensive Measures ...................................................................... 11
   Google News Groups ............................................................................................ 14
   Typical PT Process ............................................................................................... 17
   Recommended Books/Classes .............................................................................. 18
   Last But Not Least—A Pet Peeve ....................................................................... 21
   Training .................................................................................................................. 23
   Minimal Paperwork ............................................................................................. 23

2 Attack from Christmas Island ................................................................................ 25

3 Indirect Target Information Acquisition (ITIA) ...................................................... 43
   Shodan .................................................................................................................. 64
   Using Google to Obtain Information .................................................................. 65
   TheHarvester ........................................................................................................ 72
   Nslookup ............................................................................................................... 73
   Dig ......................................................................................................................... 73
   Dnsenum .............................................................................................................. 74
   Dnswalk ............................................................................................................... 75
   Dnsrecon ............................................................................................................. 75
   Fierce ..................................................................................................................... 76
   Smtp-user-enum .................................................................................................. 76
   Dnsmap ................................................................................................................ 76
   Dmitry .................................................................................................................. 77
   Itrace ..................................................................................................................... 77
   Tcptraceroute ....................................................................................................... 78
   Tctrace ............................................................................................................... 78
   Goorecon ............................................................................................................. 78

BUY Conducting Network Penetration and Espionage in a Global Environment
http://www.crcpress.com/product/isbn/9781482206470
Snmpenum ................................................................................................79
Snmpwalk ................................................................................................79
Snmpcheck ..........................................................................................79

4 Direct Target Information Acquisition (DTIA) .....................................81
   Target Discovery ................................................................................81
      Ping .............................................................................................81
      #ping -c 2 <target> .....................................................................81
      #ping -c 3 -s 1000 IP .................................................................82
      Fping .........................................................................................82
      Genlist .......................................................................................82
      Hping .........................................................................................83
      Nbtscan .....................................................................................83
      Nping .........................................................................................83
      Onesixtyone ..............................................................................84
      P0f ..............................................................................................84
      Xprobe2 ....................................................................................85

   Enumerating Target .........................................................................86

Some Miscellaneous Items to Keep in Mind (Refer to as Needed) ...........87
   Start Networks ..............................................................................87
   Create Videos ..............................................................................87
   Whois xumpidhns.it.cx .................................................................89
   Whois 95.141.28.91 .................................................................90
   Whois nucebeb.changeip.name .......................................................90
   Whois 64.120.252.74 .................................................................90
   Netcraft ......................................................................................91
   Host .............................................................................................95
   DNS Tools (More) ........................................................................95
   Nslookup .....................................................................................96

5 Nmap ..............................................................................................97
   Nmap -T0 -O -sTV -vv -p -PN IP ....................................................106
   Nmap -O -sSV -v -p -PN IP ..............................................................108
      -p 80 IP ......................................................................................110
   Nmap -A -vvv -p -PN -iL IPlist.txt ..............................................110
   Nmap -f -f -vvv -p -PN IP ..............................................................111
   Nmap -sP -PA IP.0/24 ....................................................................111
   Nmap -sS -sU -p U:53,T:22,134-139 IP ..........................................112
   Nmap -O -sUV -vvv -p -PN IP ......................................................113
   Nmap -O -sXV -vvv -p -PN IP ......................................................113
   Nmap -O -sNV -vvv -p -PN IP ......................................................113

BUY Conducting Network Penetration and Espionage in a Global Environment
http://www.crcpress.com/product/isbn/9781482206470
Nmap -mtu 16 -vvv -p- -PN IP ................................................................. 113
Nmap -SM -vvv -p- -PN IP ................................................................. 114
Nmap -sC -p- -PN IP ................................................................. 114
Nmap -p 139,445 IP ................................................................. 114
Nmap -scanflags PSH -p- -PN IP ................................................................. 114
Nmap -scanflags PSH -p135 IP ................................................................. 114
Nmap -scanflags SYN -p135 IP ................................................................. 115
Nmap -sA -scanflags PSH -p- -PN IP ................................................................. 115
Nmap -sP IP.0/24 -oA Results ................................................................. 115
Nmap -sP -PA -oN Results IP.0/24 ................................................................. 115
Nmap -n -sP 192.168.4.1-20 ................................................................. 115
Nmap -sP -oG Results IP.0/24 ................................................................. 115
Nmap -sA -sP 192.168.0.0/16 10.0.0.0/8 ................................................................. 116
Nmap -sP -PN -PS -reason IP ................................................................. 116
Nmap -sL IP.1-255 ................................................................. 116
Nmap -sS -sV -O -v IP ................................................................. 116
Nmap -T0 -vv -b FTP_IP TARGET_IP -oA Results ................................................................. 117
Nmap -sF -PN -p22 IP ................................................................. 117
Nmap -sU -p0-65535 IP ................................................................. 117
Nmap -sU -v -p 1-65535 IP ................................................................. 117
Nmap -sU -p 161 ................................................................. 117
Nmap -sU -T5 -p 69, 123, 161, 1985 IP ................................................................. 117
Nmap -PP -PM IP ................................................................. 118
  Nmap -sO IP ................................................................. 120
  Nmap -O IP ................................................................. 121
  Nmap -sV IP ................................................................. 122

6 MATLAB, Simulink, and R ................................................................. 149

7 Metasploit Pro ................................................................. 161
  Now Verify Database Connectivity with Metasploit ................................................................. 203
  Perform an Nmap Scan within Metasploit ................................................................. 203
  Using Auxiliary Modules in Metasploit ................................................................. 203
  Using Metasploit to Exploit ................................................................. 204
    No Options to Set ................................................................. 204
    See Lots of Them ................................................................. 204
    Did We Obtain a Command Shell? ................................................................. 204
    See the Active Driver, such as postgresql ................................................................. 204
  If You Get an Error While Connecting to the DB ................................................................. 205
  Using the DB to Store Pen Test Results ................................................................. 205
  Analyzing Stored Results of DB ................................................................. 205
  Unfiltered Port ................................................................. 206
Using Metasploit Auxiliary Module for Scans ........................................ 206
  Use ................................................................................................ 206
  Set ................................................................................................... 206
  Run ............................................................................................... 206
To Make the Scan Faster across Multiple Devices .................................. 207
Target Services Scanning with Auxiliary Modules .................................. 207
Vulnerability Scan with Metasploit Using Nessus .................................. 207
Scanning with Nexpose within Metasploit: ......................................... 208
Note about Exploit-db ................................................................. 209
Some Metasploit Exploit Commands ................................................. 209
Microsoft Exploit ............................................................................ 209
Exploiting a Windows 2003 Server ................................................. 210
Exploiting Windows 7/Server 2008 R2 SMB Client ............................ 210
Exploiting Linux Ubuntu System .................................................... 210
Client Side Exploitation and A/V Bypass ........................................ 210
Msfpayload Can Be Used to Generate Binary and Shellcode ............... 211
To Set Up a Listener for the Reverse Connection ................................ 211
Run Some Linux PPC Payloads against the FSB. ............................... 211
Generate Shellcode in C .................................................................. 211
Meterpreter Commands ................................................................... 212
Executive Summary ........................................................................ 216
Detailed Findings ............................................................................ 217
  Tools Utilized .............................................................................. 217
Recommendations to Resolve Issues ................................................. 240

8 China, Syria, and the American Intelligence Community ................... 241
  The Burning ................................................................................... 245
  China ............................................................................................... 246
  Syria ............................................................................................... 248

9 Building a Penetration Testing Lab .................................................. 253

10 Vendor Default Passwords and Default Unix Ports ....................... 259

11 Oldies but Goodies If You Have Physical Access ............................. 331
  SafeBack ........................................................................................ 331
    New Technologies, Inc. ............................................................... 331
  GetTime ....................................................................................... 334
    New Technologies, Inc. ............................................................... 334
  FileList and FileCnvrt and Excel ................................................. 334
    New Technologies, Inc. ............................................................... 334
  GetFree ....................................................................................... 336
    New Technologies, Inc. ............................................................... 336
  Swap Files and GetSwap .............................................................. 336

BUY Conducting Network Penetration and Espionage in a Global Environment
http://www.crcpress.com/product/isbn/9781482206470
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Technologies, Inc. ................................................................. 336</td>
</tr>
<tr>
<td>General Information ......................................................................... 338</td>
</tr>
<tr>
<td>GetSlack .......................................................................................... 339</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 339</td>
</tr>
<tr>
<td>Temporary Files ................................................................................ 339</td>
</tr>
<tr>
<td>Filter_I ............................................................................................. 340</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 340</td>
</tr>
<tr>
<td>Filter ................................................................................................ 340</td>
</tr>
<tr>
<td>Intel .................................................................................................. 341</td>
</tr>
<tr>
<td>Names ............................................................................................... 342</td>
</tr>
<tr>
<td>Words .............................................................................................. 342</td>
</tr>
<tr>
<td>Keyword Generation ........................................................................... 343</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 343</td>
</tr>
<tr>
<td>TextSearch Plus ................................................................................ 345</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 345</td>
</tr>
<tr>
<td>Crcmd5 .............................................................................................. 348</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 348</td>
</tr>
<tr>
<td>DiskSig .............................................................................................. 349</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 349</td>
</tr>
<tr>
<td>Doc .................................................................................................... 349</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 349</td>
</tr>
<tr>
<td>Mcrypt ............................................................................................... 350</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 350</td>
</tr>
<tr>
<td>Micro-Zap .......................................................................................... 353</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 353</td>
</tr>
<tr>
<td>Map .................................................................................................... 354</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 354</td>
</tr>
<tr>
<td>M-Sweep ............................................................................................ 354</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 354</td>
</tr>
<tr>
<td>Net Threat Analyzer ......................................................................... 357</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 357</td>
</tr>
<tr>
<td>AnaDisk ............................................................................................... 358</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 358</td>
</tr>
<tr>
<td>Seized ............................................................................................... 359</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 359</td>
</tr>
<tr>
<td>Scrub ................................................................................................. 360</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 360</td>
</tr>
<tr>
<td>Spaces .............................................................................................. 361</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 361</td>
</tr>
<tr>
<td>NTFS FileList .................................................................................... 361</td>
</tr>
<tr>
<td>New Technologies, Inc. ................................................................. 361</td>
</tr>
<tr>
<td>Example ............................................................................................. 362</td>
</tr>
<tr>
<td>General Information ......................................................................... 362</td>
</tr>
</tbody>
</table>
Contents

NTFS GetFree .................................................................362
  New Technologies, Inc. ...............................................362
  Example ........................................................................362
  General Information .................................................363
NTFS GetSlack ..............................................................363
  New Technologies, Inc. ...............................................363
  Example ........................................................................363
  General Information .................................................363
NTFS VIEW .................................................................364
  New Technologies, Inc. ...............................................364
  Example ........................................................................364
NTFS Check .................................................................364
  New Technologies, Inc. ...............................................364
  Example ........................................................................364
NTIcopy .................................................................365
  New Technologies, Inc. ...............................................365
Disk Search 32 .............................................................366
  New Technologies, Inc. ...............................................366
  Example ........................................................................367

12 Order of Operations for Your Tools ...............................369
  Reconnaissance .........................................................369
  Enumeration ............................................................409
  Exploitation .............................................................422
  Wireless Networks ....................................................429
  VOIP Networks .........................................................429
  Reporting ....................................................................430
  Scripting/Programming/Debugging .........................430

13 Using Your iPhone as a Network Scanner .......................431
  IP Scanner ...............................................................431
  NetPro .........................................................................452
  WiFi Scanner ..........................................................475
  iNet .............................................................................479
  Net Detective ............................................................484
  Net Swiss Army Knife .............................................505
  Ping Analyzer ............................................................532
  WiFi Net Info ...........................................................536
  TraceRoute ...............................................................538
  PortScan .................................................................543
  Net Utility .................................................................551
  zTools .........................................................................554

Index .............................................................................565
Preface

The past 40 years have seen a phenomenal growth in the area of data communications, to say the least. During the Vietnam War, one of my duty stations was on an island in the China Sea. I was part of a signal intelligence group, intercepting and decoding wartime communications traffic. We did our best to decode and analyze the information we intercepted, but there were many times when we required the help of a high-end (at that time) mainframe computer system. Did we have a communications network in place to just upload the data to the mainframe, let it do the processing, and then download it back to us? Not a chance! We had to take the large magnetic tapes, give them to the pilots on the SR-71 Blackbird, and fly them to the United States for processing on the mainframe computer system. Once the results were obtained, we would receive a telephone call informing us of any critical information that was found. It’s hard to believe now that 40 years ago that’s the way things were done.

Fast-forward to today. Now we have data networks in place that allow us to transmit information to and from virtually any location on Earth (and even in outer space to a degree) in a timely and efficient manner. But what did this tremendous enhancement in communications technology bring us? Another place for criminal activity to take place. Who are these criminals in cyberspace? You could start with organized crime, such as the Mafia and others. What is their major focus here? Financial activity, of course. They have found a new way to “mismanage” the financial resources (among other things) of others. We also have foreign espionage activities making good use of our enhanced communications systems. They routinely break into government, military, and commercial computer networked systems and steal trade secrets, new designs, new formulas, and so on. Even the data on your home computer are not safe. If you bring your work home or handle your finances on your computer system, both your personal data and your employer’s data could easily be at risk. I could go on, but I’m sure you get the picture.

Why is it like this? Why can’t we make these communications systems fully secure? Think about it. Banks and homes and businesses have been in existence as far back as we can remember. Despite all the security precautions put in place for banks, homes, aircraft, and businesses, we haven’t been able to fully secure them.
There are still bank robberies, aircraft hijackings, businesses, and homes being broken into. Almost nothing in the physical world is really secure. If someone wants to focus on and target something, more than likely he or she will obtain what he or she wants (if he or she has the time, patience, and other sufficient resources behind him or her). We shouldn’t expect it to be any different in cyberspace. Just like in the physical world, where we have to be constantly alert and on guard against attacks on our government, military, corporations, and homes, in cyberspace we have to be even more alert. Why? Because now people can come into your homes, your businesses, and your secured government and military bases without being physically seen. They can wreak havoc, change your formulas, change your designs, alter your financial data, and obtain copies of documents—all without you ever knowing they were there.

Where does this bring us? This brings us to the fact that we need to keep doing the same things we have been doing for many years in the realm of physical security. Do not let your guard down. But it also means that we must continue to enhance our security in the cyber realm. Many excellent products (hardware and software) have been developed to protect our data communications systems. These products must be further enhanced. Numerous new and enhanced laws over the past 35 years have provided law enforcement with more teeth to take a bite out of cybercrime and cyber espionage. What is also needed are those who know how to test the security of computer networks via an art termed “penetration testing.” Just as we have tested the physical security of banks and other institutions for thousands of years, we must test the security of our computer networks. That is what this book is about—testing the security of computer networks—coupled with discussions pertaining to ongoing global cyber espionage via the same tools used for testing the security of computer networks globally.

Bruce Middleton, CISSP, CEH, PMP, BSEET, MBA

University of Houston Alumni (Go Cougars!)

Bruce@SecurityRefuge.com

MATLAB and Simulink are registered trademarks of The MathWorks, Inc.

For product information, please contact:

The MathWorks, Inc.
3 Apple Hill Drive
Natick, MA 01760-2098 USA
Tel: 508 647 7000
Fax: 508-647-7001
E-mail: info@mathworks.com
Web: www.mathworks.com

BUY Conducting Network Penetration and Espionage in a Global Environment
http://www.crcpress.com/product/isbn/9781482206470
About the Author

Bruce Middleton, CISSP, CEH, MBA, PMP, President and CEO of Security Refuge LLC (SecurityRefuge.com), is a graduate of the University of Houston (BSEET—Go Cougars!) and has been involved with the security of electronic communications systems since 1972, when he enlisted in the military (U.S. Army Security Agency [ASA]) during the Vietnam conflict and worked overseas in the field for NSA. Since that time he has worked with various government, military, and commercial entities such as NASA (Space Station Freedom communications systems design team), CIA, DISA (Defense Information Systems Agency), The White House, NAVSEA (Naval Sea Systems Command), and Boeing (ground station-to-aircraft communications systems). While employed at various Fortune 500 companies, Bruce has held positions in engineering, management, and executive management (CIO). Mr. Middleton has been the keynote speaker at select national and international industry events and a trusted advisor in both the government and commercial sectors. He has written multiple books, e-books, and magazine articles in the fields of communications security, cybercrime, and computer network penetration.
Chapter 1
What You Need to Know First

Whatever you do, don’t skip this first chapter. It contains the background you need in order to properly utilize and understand the rest of this book. Also, keep in mind that although there are many things in here that a beginner can use, this is not being written as a beginner’s book for penetration testing. A number of items throughout the book assume that the user has the experience to recognize what is going on, how to modify something to work for your environment, and so on. So don’t expect to see everything step-by-step, and don’t expect to see explanations for everything I do. There are other books on the market that beginners can use for steps and explanations. At times it may seem to you that certain items are out of order, or what the heck is he talking about here, or really? Stay with me anyway. Read through the book in order the first time, start to finish; after another read or two things will fall all the more into place. I’ve lived or worked in a number of countries while serving in the military, working for the intelligence community (IC), and just as a tourist, and I’ve learned something from all of them, both culturally and technically. A list of such countries would be:

- China
- Vietnam
- Syria
- Thailand
- Turkey
- Japan
- Canada
- Mexico
- Iceland
- Czech Republic
- Switzerland
- Egypt
- Guam
I’m going to mention a few things now, but I’m going to repeat this later on in the book as a reminder. Do not just jump in and begin using tools trying to hack into a system somewhere. That’s what impatient losers do (it’s also done by those who have already had the recon work done for them by someone else). You need to spend as much time as necessary learning all you can about your target without your target knowing that you are researching them. Also remember—and this applies to those whose assignment includes seeking to bypass the network defense team—that when doing recon, no matter which tool and which site you are visiting to learn information, you must keep your MAC address, IP address, and physical location a secret. That means either disguising each of those in some way, shape, or form, or using a totally different computer system and more than one geographical location for your endeavors. You could also be part of a team in which each of you agrees on who will do what from dispersed geographical locations. Never discuss your plans via any type of electronic means if you are up against a tough adversary—only together, in person, in whispers (and never travel to meet each other in a way that can track all of you as to being together at any one time). Patience and perseverance are your biggest allies. Keep all this in mind during other steps of the pen test process where it makes sense to do so. Impatience and poor planning will be your downfall. One more thing: Don’t do any pen test work (if you need or want to remain hidden from a powerful adversary) using modern operating systems, including both Microsoft Windows and various flavors of modern Unix/Linux. Using operating systems that were in existence prior to 1999 is fine, and if you must use email communications, there are a few anonymous ones out there, but the best route to keep your communications private is to use the email application that came with Unix prior to 1999 in conjunction with a compromised or unsecured message transfer agent (MTA). I recommend against encrypting your email communications because that just calls attention to you and raises a red flag. Instead, in your in-person meetings agree on common words or sentences used in everyday life that mean something special to your group and use those. Also, remember that the hardware you are using can be vulnerable to detection due to some extra electronics now embedded in laptops and desktops. Either build your own system from scratch or use laptops or desktops built prior to 1999. And one last thing—again, depending on just how private your penetration test needs to be—if you are up against a tough adversary, then before doing any pen testing, wipe (not just format, but wipe) your hard drive and reinstall your operating system from scratch. Do not update your operating system with any service packs, antivirus software, etc.; that will be a mistake—you want the operating system you are running to be as bare bones as possible. As soon as you do that, make a list of any and all services running on your computer and absolutely know what each one is for. You want to keep those services as stripped down as possible and check them hourly to be sure you recognize each and every one. And don’t just rely on the names of the services. Know their MD5 checksum, file size, or whatever it is that allows you to know that you have not been fooled into loading a Trojaned service. Before each pen test be sure to wipe your drive and reload your operating
system from scratch, and even if you are not pen testing, I still recommend having an image of your drive that you trust, and subsequently on a monthly basis wipe your hard drive and reload that trusted image of your operating system. The recommendations I’ve just mentioned depend on just how much you value your privacy and how powerful your adversary is.

I keep my focus on three areas: cyberforensics, reverse engineering, and penetration testing. My training in reverse engineering came from Sandia Labs out in New Mexico—the instructor was working on his doctorate, and he was outstanding. These three all play very closely together. For example, in the past I’ve done work for agencies within the federal government to develop penetration testing tool sets that “hide” themselves and what they do from standard forensic tools on the commercial market today. I’ve also worked with penetration testing (PT) tool developers by performing forensics examinations on their practice targets, letting them know what I found, and going back and forth like that until either no trace or a very minimal trace of the tool and its activities are found. This allows our cyber soldiers and others within the U.S. government (USG) to use PT tools on targets that significantly minimizes or eliminates altogether their footprint into the targeted systems.

Someone may wonder, Why does a hacker need an MBA? Good question. It’s because years back I was frustrated in a number of meetings because I was given business reasons that I did not understand as to why we could or could not do something. I didn’t understand the lingo, nor did I understand the financials, risk management, and so on. So I moved forward on an MBA. It took me 3 years to acquire it, but it has been one of the best educational investments I have ever made. I highly recommend this education. Now when I believe something needs to be done, I can explain the situation to the business personnel who control the budgetary spending in a way that makes business sense to them.

I have been working with computers for nearly 45 years. I’m one of those guys who could easily just go back to the 1950s and 1960s and live in that world. I remember the red boxes and the blue boxes and so on. Using sound waves/varying frequencies to hack into systems—not thought about much now, but still valuable.

I inadvertently found myself on my first computer in 1970, using punched cards and setting toggle switches just to boot the computer that was taller than me; I couldn’t get my arms around it and I could never have picked it up. I was in high school and I thought the class was on electronics, but instead it turned out to be a data processing class for those who wanted to begin learning how to work in a bank that was moving toward automated data processing (ADP). I found that data processing didn’t interest me, but the classes did whet my appetite to learn more about how computers worked.

In 1972 I joined the Army during the Vietnam conflict. I was in the mindset of wanting to be an Army Ranger, but when my recruiter saw my test scores he decided to turn me in a different direction. He told me that if I instead went for a certain other military occupational specialty (MOS) I would receive a “top secret” clearance. To a 17-year-old that sounded really impressive, so I said yes. So I was put
into the Army Security Agency (ASA), which had been created in the 1950s and was for all practical purposes National Security Agency’s (NSA) military branch out in the field. So during my time in the military I worked under the auspices of NSA focused on the communications systems analysis of foreign entities using NSA mainframe computer systems. Eventually in the mid-1980s ASA was folded into U.S. Army Intelligence and Security Command (INSCOM).

During the 1988–1990 time frame I was one of those chosen by NASA to be on the communications system design team for the Space Station Freedom project being run out of Huntsville, Alabama, at NASA’s Marshall Space Flight Center. Many people don’t realize just what a high-tech area Huntsville, is. It’s one of the most high-tech cities in our nation and in the world.

In the late 1990s I began working at times in the bowels of the Pentagon. I was so fortunate on 9/11. On the morning of 9/11 I was at an FBI facility briefing some agents when they started getting up and leaving the room. This was far from normal, so I began thinking, Wow, what did I say that upset them? I actually started heavily perspiring and sweat began running down my face. Then I learned that a plane had flown into the World Trade Center twin towers, and that’s what they were checking out. The full impact was not yet known, so they came back into the room and let me finish my spiel. I was now going to be late for my next appointment because they had delayed part of our meeting by walking out. I was now on my way to my next appointment—the Pentagon. I’m so glad that I was late that day; otherwise, I would have been there when the plane struck the building.

Now of course I’m not going to spend time delving into decades of computer security work on both the offensive and defensive sides of the fence, but my work has spanned the government, military, and commercial realms and includes penetration testing of military networks, insurance companies, the White House, Air Force One, utilities, manufacturing facilities, CIA headquarters, Defense Information Systems Agency (DISA), NASA, foreign entities, and other financial organizations—with a nearly 100% success rate.

Of course, if the purpose of a particular penetration test was to find vulnerabilities in our own systems, I usually then sat with the system administrators and others to ensure they knew how I compromised their systems and how to enhance their security so that it became more and more difficult to break in to their respective systems.

Around 13 years ago I thought it would be a good idea to become a private detective. Through research I learned that every state had different regulations and laws regarding this profession. I was living and working in northern Virginia in the Washington, D.C., area at the time, so I followed the Virginia process. I attended the classes, passed the exam, and became a registered PI. This enhanced my social network, and I came into contact with experts in various areas that I knew at times would be useful. That was the good part of becoming a PI. However, after a couple of years I let the PI registration lapse because I found that as a PI I came under additional scrutiny in conjunction with a number of rules, laws, and regulations that
What You Need to Know First

before I had not needed to concern myself with. For me the cons outweighed the pros, so I’m no longer a PI, but I still maintain the network contacts I made—and those are important to me.

I spent 2009–2011 working overseas in the Middle East. So what have I been doing since late 2011 upon my return from the Middle East? Still performing penetration testing on computer networks of course, but I’ve also been involved in what are termed supply chain operations concerns. In the late 1990s American companies began slowly but surely moving some or all of their manufacturing operations to China and elsewhere in the desire for enhanced profitability. Dell was one of those companies. What wasn’t foreseen at the time was that China would eventually become so technically adept that it could surreptitiously (secretly) slightly alter computer motherboard chip designs and embedded software in order to put malicious backdoors into some of the computers it manufactured and distributed to other countries, such as the United States. So without having to use any real hacking techniques, China had its “automatic in” manufactured into the products (we are talking about more than just computers here). For years now some governments have required certain hardware or software be built in to the computer for tracking purposes—it just depends on the brand you buy and where it’s coming from. To hack with these systems, you first have to disable certain hardware/software accordingly.

Another company of interest is Freescale (a Motorola spinoff), whose embedded products (microprocessors, etc.) are in the transportation sector globally, including the United States. But their chips are manufactured in China, and much of the software is written in Romania, Russia, and India. American companies are using these Freescale products without thinking about inadequate security due to supply chain concerns. Vehicles manufactured over the past several years can now be brought to a standstill electronically, and if they are using chips/software with malicious backdoors built in, then vehicles could be stopped (among other things) via commands from China over the Internet. Some of these companies are seeking to move their products into our military and intelligence community.

Using what I just said as a background, what I’ve been asked to do (and have been doing since late 2011) is perform penetration testing on the embedded systems themselves before they are allowed onto the premises of whoever ordered the systems. So I’ll take a computer motherboard or some other type of board with embedded electronics and seek to compromise it in conjunction with a search for malicious hardware or software. Quite interesting. But we really need to look at bringing our manufacturing of electronics chips and systems back into the United States for our own security.

I’m also engaged to test network security defense teams and physical security defense teams. Depending on what the agreed-upon plan is, I might begin a hack that makes near zero noise and slowly raises the intensity over time until the network security defense team is able to specifically state where I am in the network and what I’m doing. Then I work with the team to enhance their capabilities. One
Conducting Network Penetration and Espionage

trick I pull (and keep in mind that malicious hackers can pull this on you too) is to make a lot of noise in one or more sections of your network via some automated tools running, get the network security defense team to focus over there, and in reality I’m not there at all. I’m elsewhere in the network, very slowly but surely acquiring the golden goose, whatever that may be. And if there are webcams I’ve gained access to, I can actually watch the team working away from my remote location. In order to test physical security, I’m usually provided with an appropriate badge and walk around seeing what I can collect of value due to security infractions from:

- Garbage cans
- Printers
- Fax machines
- Help desk repairman for computers and phones
- Tailgating at security doorways
- Dumpster diving
- Hallway conversations that should have been taking place in a private conference room

So essentially, I’m like a fly on the wall.

As I move through this chapter, I’m going to work from both sides of the fence. I’ll discuss what you need to do if you are someone who wants to become a certified ethical hacker (CEH) or someone who wants to learn to perform penetration testing against your own network in order to enhance its security, and I’ll discuss malicious hackers themselves.

So what type of individual makes the best hacker? Those I know that are tops in this field are very detail oriented; they will find the missing comma in a 100-page document. At the same time, though, you have to be able to step way back and see the big picture. Plan to be a lifelong learner. You have to love to learn new things. You also need a physical security mentality, and you need to pursue security aggressively. You may also need to be confrontational.

- Why is that person sitting there with a laptop next to the ATM in the mall food court? And why is there a cable running from his laptop to the rear of the ATM?
- Isn’t that a little suspicious? Don’t be afraid to confront. Your company should have guidelines for this.
- You know what malicious individuals count on in situations like this? That people will notice but do nothing. Be someone who does something, who is proactive in the security realm.

It does help to be somewhat paranoid. It helps to have a naturally suspicious nature. Remember, just because you are not paranoid doesn’t mean they aren’t watching
you! You need to be meticulous, patient, and methodical. But also ready at a moment’s notice to deviate from a plan based on new information garnered.

Be research oriented and really think things through. Don’t just react—really think. I can’t emphasize that enough. Avoid knee-jerk reactions. Albert Einstein is one of my heroes, and I’d like to throw out a few quotes of his that are significant to us:

- “Thinking is the hardest work there is, which is probably the reason so few engage in it.”
- “The true sign of intelligence is not knowledge but imagination. Imagination is more important than knowledge.” And I do use my imagination on both the defensive and offensive aspects of security. I sit and visualize the packets traveling over the network, encountering various devices, how those packets will be handled at each device, what could possibly go wrong, how someone could intercept those packets, and so on.
- “A man should look for what is, and not for what he thinks should be.” That’s a word of warning for all of us. If you focus your thoughts on what you think should be happening, then there is a good chance you’ll miss out on what’s really happening. It’s very important to keep an open, imaginative mind.

If you decide you want to be a CEH, then you need to work with your personality. You have to decide whether to be a generalist or a specialist (expertise in one to three items). If you decide to be a generalist, then you must build a network of experts and be a very quick learner on the fly. Over the past 40+ years I’ve seen quite a bit, so I know something about many things, which makes me a generalist. I think in the world as it is today, most people are better off being an expert in one or two things and backing that up with a solid network of other experts. Still, though, generalists who understand the entire system to some degree are also needed, and it’s best if you have one in your network. Nowadays a generalist is harder to find.

- What are your gifts? Your natural talents? Know them and use them to be successful. Don’t try to be something or work in a way that’s not you.
- I know one guy who for the past 15 years has made a great living totally focused on Apple computers. He travels globally for any work involving forensics analysis of or penetration of Apple computers. He is the expert—the go-to guy.

Putting classified tools aside here, I begin my penetration testing engagements with the use of standard commercial tools. However, as I move forward, depending on the targets and goals, I move to the use of my own personal tool set. Why? Because I want absolute control over what the tool is doing, and I want to know that I really know what the tool is doing. I don’t have that same comfort level with commercial tools I buy off the shelf. Unless I take the time to thoroughly analyze them (and I don’t have that kind of time for the most part), I really don’t know what else that commercial tool is doing on the backend, under the covers.

BUY Conducting Network Penetration and Espionage in a Global Environment
http://www.crcpress.com/product/isbn/9781482206470
And when I develop tools, I don’t use languages that have a lot of overhead to them. For example, for tool development I don’t use languages such as C#.net, Ada, Java, or C++. I don’t use object-oriented programming; it’s just too much overhead. It takes me 20 lines just to say hello—a little exaggeration perhaps, but there is just too much going on “under the covers” for me to feel comfortable. Languages like this just make me feel bloated.

What do I use? My favorites are Python, PERL, Assembly, Bash shell, Ruby, and C. I want absolute control over my programs, and I want to know exactly what they are doing at all times—and these languages give me that control with minimal overhead. I also make use of Window’s PowerShell at times. If someone forced me to choose one and only one language for pen testing software development, it would be Python.

My operating system of choice? A stripped-down version of some flavor of Unix, especially when it’s warfare of some type. As I stated before, I spent 2009–2011 working overseas in the Middle East. At various times when I was engaged in real-time cyber warfare I could just feel the opponent’s frustration when they tried useless attacks one after the other because my system was so stripped down. It was fixed to do exactly what I needed it to do and nothing more. When I had the opportunity, I also Wiresharked all incoming traffic for analysis later. You can keep yourself high on the learning curve doing things like that. I also Wiresharked the entire 2012 Superbowl since it was being broadcast over the Internet and millions were tied in via very specific ports globally. I made the assumption that various entities would perform some malicious activities. Sure enough, analysis of the pcap file had shown that my assumptions were correct.

Another nice tool to use is BusyBox, but keep in mind that there are some entities that like to add a little bit of malicious flavor to certain items within BusyBox. This is a multicall binary that combines many common Unix utilities into a single executable. Its nickname is the Swiss Army Knife of embedded Linux. The utilities are far smaller with minimal options. It can be difficult to hack into a BusyBox setup.

As long as I’m hyping on the software, I might as well elaborate more on something I mentioned to a degree earlier in this chapter. If you want to keep your pen testing private/secret, you also have to carefully consider the computer hardware you are using. Our government in the United States (and governments in various other countries too) has required, under the auspices of security against terrorism, various additions to the computer hardware you are using for electronic tracking purposes. So if you want to be sure to avoid such problems, avoid using any laptop/desktop manufactured after 2003. If you feel this is important to you, then pick up older laptops at garage sales, Craigslist, flea markets, foreign countries using older technology, and so on. The same applies to the software you are using. Again, if your privacy is important to you, then avoid using any operating system on the Microsoft Windows side of the fence beyond Microsoft XP, and don’t move past Service
What You Need to Know First

Pack 1. This also applies to other operating systems such as Linux, antivirus software, and other similar items. If privacy is important, then do not use the “latest and the greatest”—this applies to routers and other items too—and keep your systems off the Internet except when they must be. Use air gap security, meaning you keep your Ethernet cables unplugged except when you have to have them plugged in, and you keep your devices unplugged (laptops, desktops, switches, routers, etc.) except when you are actually using them. And I hate to break it to you, but I’m also talking about your cabled televisions, radios, and various other devices. Neighborhood area networks (NANs) are another invasion to your privacy from some utility companies that come right to your home in the name of security and administrative ease for monitoring/controlling the electricity coming into your homes. If you have some of the newer (and coming down the pike) refrigerators, stoves, and other appliances, these NANs can put them on the Internet and they can be hacked. Newer cars are in the same boat, with on-board electronic devices that can be hacked via the Internet, mobile phones and laptops, and so on. And last but not least, your mobile phones are at the same risk level. There are various things you can do to protect yourself against snooping, but I can’t go into all of that here. One of the best things to do is to let the snoops think that you don’t know what they are doing, but at the same time, when they tunnel into you, you automatically tunnel back into them without their knowing about it. I teach classes on these things, and I also build custom laptops for those who have privacy concerns; it just depends on what you feel you need to do. I also advise avoiding the use of wireless networks for anything you are doing if you are concerned about privacy. If you really want to use one, go ahead, but only have it on when you need it; otherwise, unplug it from the back of the unit. Keep in mind that some items have built-in batteries that keep certain electronics running even if you unplug them from the wall. In those cases remove the battery (or batteries). If you can’t easily remove the battery, then put the device in a Faraday bag (and test that bag—some are more dependable than others). If privacy invasion is not an issue for you, then don’t worry about it and proceed as you always have.

MATLAB® and SimuLink (MathSoft.com)

Mathematics is very important. Don’t just think about software tools. Remember that the software you see on the monitor is just for your human eyes and mind to be able to somewhat interpret what’s happening (or going to happen). Don’t get lost in the software. The software may be your gateway, but it’s not your be all and end all. The only thing going down that Ethernet cable (or other type of cable or wireless), coming out of (or into) your computer system, is electrical signals, and all of those electrical signals can be formulized mathematically. The closer to the real source you can get, the better off you are when it comes to really understanding what’s going on.
Conducting Network Penetration and Espionage

At NSA the science of physics is utilized. For example, electron microscopes are used to examine hard drives for hidden data, and they have the top mathematicians in all the world.

So what can you use?

MATLAB and SimuLink are just the tools to help you do that. SimuLink can be used to simulate the actions occurring in any type of communications network, and it can be used in conjunction with MATLAB to look at your network communications from a mathematical perspective. Also keep in mind that you can write C programs that interface directly with these tools.

Interestingly, I’m finding that older tools from the 1980s and 1990s are now once again working on newer systems. It’s like some computer designers are so focused on protecting themselves from current high-profile threats that they’ve forgotten all about older attack vectors. In fact, their protection solutions are the very thing that’s opening the doors for older “forgotten” tools to successfully attack the newer systems. And other times, just a slight variation on the old tool works wonders.

Statistics also comes into play in the information security arena. An excellent tool for statistical analysis on the fly is R. I use it more for determining the best tool or approach to use in a given situation. I usually use it in an automated fashion, built in to one of the various scripts I’ve built and used over the years.

If you want to be a high-end penetration tester, then you should be able to write quick and dirty programs on the fly in your language of choice, such as Python. So many programmers nowadays depend on looking at someone else’s code, and then looking at a programmer’s reference manual for that language, and subsequently modifying the code to do whatever it is they now want it to do. But you shouldn’t stop there. Whether you are involved on the offensive or defensive side of information security, you should be able to write short programs on the fly on an as-needed basis. Most of the programs I need to write on the fly are 100 lines or less.

Remember: Don’t fall into the trap of using only commercially available automated tools. They are a good place to start, and they will serve you well both offensively and defensively from a “normal hacker encounter” perspective. But you are up against much more than that. For some adversaries they are just a minor annoyance.

Who are your adversaries? There was a time when hackers consisted mainly of curious individuals seeking to learn or seeking to make a name for themselves among their peers. That is no longer true and hasn’t been for a while. Nowadays your adversaries could be state-sponsored entities from Russia, China, India, or elsewhere. They could be making their living by working for organized crime networks. They may have come across one of the websites out there that lists exactly what they are looking for from company X, and it’s even stated how much money they will pay for each individual item. Your adversary could also be just the type of individual we first discussed—just curious and trying to learn and looking to make a name for himself or herself among his or her peers.
The late 1990s began the era of more understanding and involvement of federal law enforcement authorities. I once was part of a team that was investigating a security breach at an Air Force facility. During the interview process one of the network administrators talked about seeing a mouse pointer move by itself on one of his systems. He thought that the system just had a malfunction, rebooted it, and left for the day. What he really had was a hacker on his system who eventually compromised other systems, using the one as a jump-off point to other local systems. Again, have a security mindset. Obviously this network administrator did not. If he would have had a security mindset, his response to seeing the moving mouse would have been quite different and would have saved a lot of time, money, and trouble. Your mindset determines how you think about and how you react to some event in your network environment.

As stated earlier, some utility companies are now using computer networks all the way to your house and linking them to what they call smart meters. I'll touch on this once more here, but in essence this subject could easily be a book all by itself. You and your neighbors are in what they call a neighborhood area network (NAN). More and more your power, television, refrigerator, and stove are being tied to these networks. Hackers could shut off your power or turn off your refrigerator or television from any country in the world that has sufficient Internet access. What if they turn on your stove and you are not home? What if they access your thermostat and shoot the temperature up to 90 degrees during wintertime and you've left the house for a week? Who is responsible for the electric or gas bill if this happens? And this is more trouble on the horizon—these systems are susceptible to a variety of attacks:

- Buffer overflows
- State machine flaws
- Bus sniffing
- Clock speed
- Power glitches
- Differential power analysis

Do you know we have had hospital disasters due to remote access to building power, lights, elevators, etc.? Several years ago there was a teenage boy just playing around and he didn't know he was in a hospital. He shut power off on a section of the hospital, the backup failed, and a patient died due to machine failure. One company that is manufacturing and pushing this technology is ZigBee. Go ahead and Google it.

**Recommended Defensive Measures**

I know it's more of a burden from a financial, administrative, and training (FAT) perspective, but I do recommend that you have a variety of equipment on your network, like I have done. You do hackers a great service by using all the same types of firewalls, all the same types of routers, all the same types of desktop computers,
all the same web browsers, and so on. Once they see one of your firewalls, they make the assumption that all your firewalls are of this type and proceed accordingly. If they are correct, then their job is all the easier to accomplish. If they begin to run into two or three different types of routers, firewalls, desktop computers, operating systems, web browsers, and so on, then this frustrates them, confuses any manual or automated attacks they launch, and they just go looking for easier targets and greener pastures. That’s good for you and bad for someone else. So if you have the financial resources to do so, then you should diversify the network hardware/software you purchase.

And here is another recommendation that you may not want to hear, but if you want to take another major step forward in securing your network (and I’m talking about both your home computers and the ones where you work), then use only cabled networks—no wireless.

- Keep in mind that for some computers you buy (desktops, laptops, servers, etc.), you will have to physically open them up and make a couple of cuts to disable the wireless. If you don’t do that, then for some systems the wireless capability can be remotely activated even if you have disabled it via software on the computer itself.
- Speakers can be microphones via remote control, and webcams that you own can begin watching you without your knowing it. The same goes for mobile phones.

And for those cables, be sure to label them in a way you understand so that you can walk into a wiring closet and know exactly where each and every cable should be. Don’t have a rat’s nest wiring closet—that only invites trouble. Be sure to keep those wiring closets locked and secured from above and below (flooring/ceiling tiles).

Here are some more recommendations that are not administratively friendly, but from a security perspective are very helpful both at your home and in your work environment. Remember, someone, somewhere, is running hacking tools at all hours every day, some manually and some in an automated fashion. You can do the following to all the more enhance your security. Again, don’t get lost in the “automation jungle” and think that you are not technically savvy just because you choose to do some things manually. For instance:

- Sneakernet is just fine. It can both save you money and increase the security of various systems. Every system you use does not have to be on your network. If it’s a highly critical system that would seriously impact your business if compromised, then take it off the network and let it be a stand-alone system in a secured room. Then just use secured and controlled USB sticks or DVDs for input/output access. Additionally, you get the benefit of more exercise. Standing up and walking around once in a while is better for your health than sitting all day. So what if you have to leave your desk, go to another secured room, sit down at the stand-alone system, and get your work done in a secure fashion?
Figure out which systems don’t need to be up and running 24/7, and either power them down (including unplugging the power cord from the back of the system—remove batteries if necessary) or unplug their network cables from your network when they are not in use or when you leave at night. It’s like having a moat around the castle, but in this case the moat is the air gap you create. At my office everyone knows that if you are not using the Internet, then you unplug the router (unplug from the back of the router, not the on/off switch), and if you are not using a particular computer but someone else is still on the Internet using that router, then you unplug the network cable from the back of the computer you were using—and no wireless is permitted.

- Do you leave your car turned on 24/7? No, because you are wasting fuel, putting wear and tear on the engine belts, and someone might steal it.
- Do you leave your house unlocked 24/7? No, because you are concerned that someone might come in and steal from you.
- Then why leave such a valuable commodity as your critical network systems up and running 24/7 on a network that others could possibly enter without your knowledge?
  - Your business secrets walk out the door and you don’t even know it.
  - Never in our past history have we trusted something that we can’t even see. We only “see” what our software allows us to see, for example, like using Wireshark to watch network traffic. If there is a protocol running on the wire that Wireshark is not programmed to see, then you won’t see it and you’ll think it’s not even there.

I’m sure some will not like the security suggestions I’ve made, but I’m recommending these things for your own good. Nowadays security is not a luxury; it’s a necessity. Nefarious personnel are seeking to use your systems on a 24/7 basis as both a hiding place and a gateway to other, more lucrative targets, be they military sites, government sites, hospitals, factories, utility companies, SCADA systems, ATM machines, and so on. Be part of the solution, not part of the problem. Also, being privacy oriented does help you to have a mindset that helps you to behave in a more secure manner.

When your HR department is posting new jobs on the Internet, such as on Monster or on your own website, they need to be careful about what they put in those advertisements. Yes, on the one hand, the individuals seeking a new position need to know to some degree what you are looking for. On the other hand, when hackers choose a company (or companies) to focus on, they use the job postings to learn what systems you have in house, be it operating systems, types of routers, types of firewalls, and so on. At other times a new exploit has come out against system X, and they want to find some companies with that system, so they just run a keyword search on Monster (for instance) to find out all companies using system X and then move forward on their attacks. You need to minimize or generalize as much as possible the type of computer network technology you are using. If you receive a resume of interest, then you can always provide additional details via a phone call.
Misinformation can be your friend. At various sites throughout the Internet universe put information about your network systems that is not true. Obviously on some sites critical to your business you want the right information out there, but there are a number of sites hackers like to visit in order to find out more about your systems. Misinformation there can pay you a bonus security-wise. Hackers will use that information thinking it is legit. This approach costs you little but frustrates the automated attacks hackers launch in an effort to research what network components you have so they can launch the appropriate attacks. This will frustrate many and cause them to move on to other targets of opportunity.

Google News Groups

Millions of people use them, and just like Vegas, what you put there stays there. If you are a network admin and you go out asking for help about hardware X or software Y, then keep in mind that malicious individuals also see that information. This may be a quick and easy approach to problem solving, but since it’s all very public, you are telling a vast number of people globally details about your own network or about embedded systems you are working on—details that may compromise the security of your network or the device you are intending to manufacture. One or more individuals within your corporation should spend time performing some automated searches pertaining to what may be out there about you and your personnel. Then get it cleaned up if need be.

Google news groups are one place that you could lay out some misinformation. For example, your system administrators could get on there on an irregular basis and begin asking questions about specific hardware/software that you don’t really have. But when a hacker sees that, he or she will think that you may well have those systems in house and begin preparing to move against your network based on that incorrect information. That’s the kind of misinformation I’m referring to.

Be careful what you put on your corporate website. And remember that just because you make a change and republish, that information that you sought to change or eliminate is still out there available to others globally via the Wayback Machine, a site that has archived websites for nearly 20 years.

Do you have Voice over Internet Protocol (VOIP) phones in your lobby? Be sure they are properly locked down and secured (including locking the phone cable to the phone so it is difficult to move the cable from the phone to a laptop). I know they are nice to have both administratively and financially, but I don’t recommend them from a security viewpoint. Many a time when I’m engaged to do either physical security walk-throughs or penetration testing of a network, it’s been the VOIP phones in the lobby that have been my gateway to some part of the corporate network. I’ve found that the best times to try that route into the network are:
When you are out at a restaurant or café, be aware of your surroundings and who is listening to your conversations. Don’t broadcast corporate plans, network information, phone numbers of individuals or departments, and so on.

In cities across the world (including the United States, of course) hacker meetings occur on a weekly or monthly basis. Find out where they are meeting (many times it’s at a coffeehouse or mall) and sit close by (or join the group). Listen to what they say. It could be something pertinent to your organization.

Another thing you have to watch out for is unexpected software built in to the operating systems or applications that you purchase and install yourself, whether it be on computer systems or your mobile phones. You should read with care those long boring licensing agreements that almost no one reads. Some of them have one or two sentences that specifically state that you agree to “something extra” in the software. They get by with this because they know most buyers of the software don’t read the agreements, so if something went to court, they feel protected. And it’s not just the software you install that you have to watch out for. There could be other low-level software built in to the motherboard electronics and elsewhere doing things that you just don’t know or expect.

Keep in mind that a “secure” virtual private network (VPN) tunnel is in effect a two-way street. You can get yourself an unwelcome visitor when your adversary is backed by major billion dollar organizations and other resources.

If you need to keep a system up and running on the network for some reason but you don’t need to keep its data on the system, then don’t. Keep the data on an external drive when you need access to it, and then disconnect that drive when you don’t need it and place it in a secure location. We operate this way at my office.

Keep backups offline and not touchable by the network until you actually need them. Then take what you need from a secured area, load a copy of the backup (to keep your offline backup pure and malware free), and then destroy that backup copy (wipe, magnet) to keep your backups malware free.

For critical storage areas and server/system rooms, require both a physical key lock and the electronic keypad. If there is an electronic keypad only, then someone with appropriate knowledge could bypass it without your being aware of it. Adding an additional physical key lock helps to further enhance security. Also, keep in
mind that (and this is happening now) adversaries, if they can’t hack into your network in a designated amount of time—and they really want your data, then they will mask themselves, break into your facility, and carry your computer out the door. If it’s a small facility, then they can grab your systems pretty quickly. If it’s a medium to large facility and they are successful, then most likely they have had some insider assistance. Keep that in mind.

Laptops should be physically cabled to desks with either a key lock (preferred) or a combination lock so they can’t just walk off. Desktop and server covers should be hardware locked so that no one can just open up a system, remove the hard drive, and walk out with it (or copy it and bring it back without your knowledge). Keep all keys and combinations properly secured.

If you are not using an Ethernet jack or phone line, then turn it off so it can’t be utilized by anyone just walking into the room. Don’t let vendors come in to your facility with their laptops and just jack into your network in a conference room. You have no idea what’s running on their laptops. I’ve encountered vendors in the past who are running scanners in the background while jacked into the network of the client they are visiting. If it works for you, make each Ethernet jack only respond to particular medium access control (MAC) addresses and then reject anything else.

Have keyed lockers outside conference rooms to hold cell phones if you are concerned about others (such as visitors) recording the meeting on their cell phone or leaving a phone line open so someone else can listen in.

I built my first computer from scratch somewhere in the 1985-to-1987 time frame. It was built around a Zilog Z80 microprocessor. I remember that time well because the new Air Force One was sitting on the flight line at Boeing flight test in the Seattle area at the time undergoing various tests. When I say “from scratch,” I mean from scratch. I smile when I hear many people nowadays say they build their own computers. What they really mean is they bought a case, a motherboard, a power supply, some memory, hard drives, etc., and put them all together and then loaded Windows, Unix, or some other operating system. To me, from scratch means you design and build your own motherboard and write your own bare-bones operating system that does exactly what you need and no more. I build these once in a while for customers who need them, so if you need one let me know, but I can tell you it takes time and it’s not cheap.

Nowadays bugs and cameras are so small that they are very easily hidden from sight. Do you know how cameras work? Do you know the physics behind the camera? If not, but you are interested, then do your research. Cameras don’t have to see you if you don’t want them to. They only work due to certain scientific principles, and if you want to take the time to protect yourself from being seen, then you can do so. If you have a concern about whether or not your conference rooms or other areas have been bugged, then I recommend you hire an expert who sweeps rooms for such items. But be sure that whomever you hire really knows what he or she is doing (i.e., does the equipment he or she is using really operate at the appropriate frequency that will detect the bugs that are operating at your premises?). Keep this
in mind when you are traveling also. Some companies and countries are known for setting up hotel rooms and even commercial aircraft seats with these little tidbits. If you find yourself wondering how a competitor obtained certain information or data, then it’s time to sweep those rooms, think about what you may have said or done in a hotel room or commercial flight, or if they have hacked into your network unknown to you. I’ve seen all of this in the past.

Think twice about holding meetings over video telecoms if the subject you’re discussing is going to air critical business information. Security can be a problem with these systems, and they are definitely hackable.

If you want to be sure no one can hack into your cell phone, then you have to both turn it off and take out the battery. Otherwise, it can be remotely accessed. Unless you really feel like you need it at night when you go to bed, turn off your cell and take out the battery. Doing so prevents automated phone hacking tools from leaving you a present during that time frame.

If you want to be sure you are not being tracked via your cell phone when traveling, then purchase a Faraday bag and drop it in there. These bags let no communications into or out of the phone. Some are better than others, so test them by calling your phone when it’s in the bag. It shouldn’t audibly ring, take messages, etc.

**Typical PT Process**

The upfront research about the target is key to a successful penetration test. I’ll learn all I can about you from various sites on the Internet, such as Google, financial news reports, your job postings (Monster, for instance), which Google Groups you use and what you said, your own corporate website, and numerous other sites on the Internet. Even though various social networks, Google, and other search engines are monitored by law enforcement and intelligence agencies globally, top-of-the-line hackers can do all this anonymously and without your knowledge.

Next, I start hanging around restaurants, cafes, the sidewalk outside your facility, and organizations your company is involved with, and I’ll listen in on conversations to see what information I can pick up that might assist me.

I’ll try to find out phone numbers within your company that I can call and use. I want to find out just how security savvy personnel are, so I’ll hit them up with various questions to see what I can learn—just how much will your people give out? A good annual or semiannual security briefing to all your employees can be invaluable, warning them as to what to watch out for.

I’ll find out all I can about you via Domain Name System (DNS) records, email addresses I find on the Internet, your IP address range, and so on. So for all public DNS records, be sure to minimize the information you put out there.

Next, I’ll actually touch your system. How quietly or severely I scan a system depends on whether or not I care if I am noticed. Now I know even more about
your network systems, such as operating system types, ports open, services running, etc. I’ll have a list of potential vulnerabilities.

Note that in this step (for the most part) I do not manually type every command. I have a large number of commands already typed into a text file and categorized and prioritized. As I move through the assignment, I just copy and paste commands. Doing it this way greatly minimizes fumbling a command due to typing errors and fat fingering. It also keeps you from forgetting command parameters, and it keeps you from making mistakes during an engagement. I’ll do some research on those potential vulnerabilities and decide which tools/techniques to use.

Now I exploit the system and do what was agreed upon for the assignment. Note that in this step (again, for the most part) I do not manually type every command. I have a large number of commands already typed into a text file and categorized and prioritized. As I move through the assignment I just copy and paste commands. As I stated earlier, doing it this way greatly minimizes fumbling a command due to typing errors and fat fingering. It also keeps you from forgetting command parameters, and it keeps you from making mistakes during an engagement.

Next, I meet with management, system administrators, and the security team to discuss how I compromised the system and what needs to be done to shore up the security of the system(s).

After each penetration test wipe your hard drive, shut down the system, and then bring it back up and lay a pristine image onto the hard drive. This both helps to protect your system (you never know what might have snuck in during a penetration test—be on the safe side) and ensures that you don’t accidentally infect a new client that’s next on your schedule.

**Recommended Books/Classes**

1. *Principles of Communications Satellites*, Gary D. Gordon and Walter L. Morgan:
   a. Highly recommended and mathematically intensive—calculus based.
   b. Many of your potential adversaries are reaching your network via satellites, and understanding this technology can be the difference between being on the winning end and being on the losing end of an attack on your network. The more you understand the communications technology you are tied to, the better you can shore up your network defenses.

2. Safari Books Online (SBO), corporate license:
   a. Enables you to search thousands of technical books online on the fly.
   b. I can travel globally without reference material as long as I have efficient Internet access to SBO.
   c. There is also Safari Books Online Mobile. I can search books on the fly right from my phone (and I can also download PDF versions of the books right to my phone or computer).
3. *Hakin 9* magazine: Comes out every 2 months. I try and read each issue cover to cover; it lets me know what others are thinking.

4. **Who is Fourier?** Transnational College of Lex:
   a. For the mathematically inclined.
   b. Does a great job in a step-by-step fashion of explaining in detail the mathematics behind modern communications systems. Knowledge of this type is a must if you desire to be on the upper cusp of the penetration testing field.

5. An excellent blend of skills if you desire to be a successful penetration tester on the high end is the addition of cyberforensics and reverse engineering. I have personally taken (and taught) these classes in the past and recommend the vendor InfoSec Institute (InfosecInstitute.com) and the classes listed below. Before taking these classes, you should pick five books on penetration testing and read through them at least once, and preferably two or three times (and practice with the authors as they lead you through various exercises). Additionally, if you take these classes, don’t be one of the lazy ones. You are in class all day from 8:00 a.m. to 5:00 p.m., and when the class is over it’s easy to just go out for supper and then head for your room and take it easy. But if you do that, then you are missing a key part of the class. Around 7:00 in the evening the optional portion of the classes begins, and usually maybe a third of the class shows up. From approximately 7:00 to 10:00 (and later) are the evening live hacking contest exercises. That’s where you can really put into practice what you’ve been learning from experts in the field—a great learning experience. Also, don’t take the classes online—take them in class, live with real people. The network you develop, along with what you hear people saying while in the class, is well worth the live class effort. You get out of something what you put into it—you come back with a number of tools that you now own and can use on your own network.
   a. Certified Information Systems Security Professional (CISSP) prep (if you don’t already have this certification)
   b. Ten-day penetration testing class
   c. Certified Penetration Tester (CPT) class
   d. Certified Ethical Hacker (CEH) class
   e. Advanced ethical hacking
   f. Web app pen testing
   g. Reverse engineering
   h. Computer forensics

6. Now feel free to take some of the online classes, especially the ones that let you practice your newfound tools/techniques against their live servers. Also make use of the live CDs/DVDs and virtual machines you can set up to practice your hacking, reverse engineering, or forensics skills.

   a. The main thing you are going to get out of this book is the proper security mindset and field experience explanations along with the

BUY Conducting Network Penetration and Espionage in a Global Environment
http://www.crcpress.com/product/isbn/9781482206470
processes/procedures. The tools could be considered out of date now since they are over 10 years old, but they all still work just fine; they are more manually intensive—and sometimes that's just what you need.

8. *Understanding Internet Protocols*, J. Mark Pullen: Includes actual exercises and software you develop along the way to enhance your knowledge in this area.

Don’t feel overwhelmed by all of these suggestions. Just start somewhere and week by week learn more and do more. Put together a plan and follow it. What should you keep up with? Do I keep up with all the latest attacks, viruses, new software, and so on? No. These can change daily. You only have so many hours in the day, and you have to spend them wisely. If you spend significant time just keeping up with the latest and greatest that comes out on a daily or weekly basis, then you won’t have time for what really matters in the long run.

What does really matter? If you are on the defensive side of the house seeking to protect your network from malicious hackers, then you need to spend plenty of time becoming intimately familiar with your own network. You need to get to know it like you know a good friend.

For example, bank tellers (and others who spend their day dealing with currency on a regular basis) at major banks (and this has been true for decades) have to be on the alert for counterfeit monies every day they work, year in and year out. So what does the bank do—spend the tellers’ time on a regular basis learning about all the different counterfeit bills in circulation, how to spot them, their nuances, techniques to produce them, and so on? No. Instead, the bank trains them to know the real thing so well that anything counterfeit just sticks out like a sore thumb to them. This has a direct application to you and your network. You should be so intimately familiar with your own network that if someone is (or has while you were sleeping) attempting to break into your network, you recognize that something is not right and you begin your investigation and either stop or mitigate the malicious activity in progress.

On the offensive side this also has application. Just like the bank tellers have become currency experts, you need to be an expert in two, maybe three, things at the most. For example, perhaps you choose to be an expert in both Python and BackTrack. For everything else you need to develop a network of experts—people who also know one or two things extremely well. It’s the “you scratch my back and I’ll scratch yours” scenario. When you need help, you contact them, and when they need your expertise, they contact you. Having a network like this is very important. No one can know everything. There is just too much out there.

What I do spend time reading each week, though, from an update perspective, are the SANS @Risk and NewsBites emails. If you have not signed up for those, then I strongly recommend that you do so. As you read these, if you see something that is directly applicable to you and your network, then Google is your friend and you can do some research. I also attend the SANS webcasts that are pertinent to me. I suggest you attend those also. Just go to SANS.org and follow the appropriate links.