Global Information Assurance Certification Paper

Joe Granja
SANS Security Essentials
GSEC Practical Assignment
Version 1.4b, Option 1
October 25, 2002

Hackers VS Burglars

Abstract

As a Security Professional, at some point in your career, you will be asked to describe what your job duties are to someone who may know very little about computers and network security. This could be a friend, a neighbor or even a business associate at your company.

It is unfortunate that Computer Security still hasn't earned the respect or received attention as a vital element of doing business today. Frequently IT personnel must justify the costs of investing in technology to safeguard networks. Unfortunately, security is an area that is being hit by budget cuts in an era that continues to show that computer threats are rising.

The goal of this paper is to draw comparisons with the hacker who breaks into a business computer network with the criminal who commits a home burglary. This will include assessing the value of what you are protecting, the steps taken to minimize the exposure of being a victim, and what you can do if you are hacked or burglarized.

Introduction

A hacker is, "a person who illegally gains access to and sometimes tampers with information in a computer system." [1] The public has had a lot more exposure to the term "hacker", thanks to the media coverage for the likes of the Melissa Virus, the Code Red Worm and the "I Love You" virus. There have even been movies on the subject like "War Games", "Hackers" and "The Net". One almost gets a sense that it is still "cool" to be hacking into a computer network and snooping around someone else's private network. The thought process and intentions of the computer hacker are varied.

Some hackers exist to help secure networks; these are called "White Hat" hackers. They break into networks to help detect security lapses and protect companies. This is contrary to the "Black Hat" hacker who has thoughts of espionage, theft, and disruption of service. Recently companies have been hiring former "hackers" to help design or test out their networks. There are not many burglars who have gone "legit", admit they were criminals and then offer their services.

This paper will focus on comparing the "black hat" hacker, who is intent on causing damage to your business, to the burglar who is looking to rob your home. The home burglar typically is targeting residences that have either made it easy to rob or have valuable items that are worth the risk of getting caught. A burglar is "a thief who enters a building with intent to steal." [2]

Both the computer hacker and the home burglar enter the premises illegally and without authorization. Their intentions may vary in terms of what they plan to do or how they gain access. The bottom line is they are there without the owner's permission. Many times it is the weakest link in the chain that provides the opportunity for the criminal hacker or burglar to take advantage of the situation.

Hacking and burglary definitions can be used in tandem; both include criminal activity that includes theft and unauthorized entry onto your property. Often this includes physical property that is stolen from work or home. Sometimes the crime is committed electronically over the Internet and the hacker steals information online.

Burglary at work occurs when someone not authorized gains access to a computer system or leaves a secure door available for a criminal to access. Burglary in the home can be someone leaving the front door open or leaving a spare key underneath the doormat.

These are crimes of opportunity. Most burglaries at work would most likely happen when offices are closed and there are less people around. Burglaries at home usually occur when people are away during the day or on vacation. Once again the home burglar does not want to get caught. They commit their crime with few people around. The hacker has the added benefit of anonymity with unlimited remote access attempts to penetrate computer systems twenty-four hours a day, seven days a week.

Assessing value

Work – For a corporation, keeping customer data from the prying eyes of a hacker is essential to maintaining a sense of trust for any company doing business on the web. Imagine the public relations nightmare to deal with if your company has just exposed all the credit card information stored on its server and it can be found floating somewhere in cyberspace.

You can put a price tag on physical equipment like servers and routers but how do you come to grips with putting a value on items like databases or customer data? What would be the financial impact if your data was lost or corrupted?

> "Fortune 1,000 companies lost more than $45 billion from the theft of proprietary information in 1999, according to a study released by the American Society for Industrial Security and consulting firm PricewaterhouseCoopers. The majority of

those hacking incidents hit tech companies, with nearly 67 individual attacks and the average theft ringing up about $15 million in losses. " [3]

What would be the long-term affect if someone broke into your systems over the weekend and sent a worm in your computer system that prevented your employees from logging on to their systems? Think of the lost productivity per hour that would cost the company. In many instances, companies are so reliant on computers that they cannot function in a paper environment. They cannot process orders or perform their daily business functions.

Home - Determining what the value of your personal belongings is a daunting task for most people. It is a lot easier to itemize the physical items like a sofa, TV, stereo, and computer. Items such as jewelry or other more personal items like family heirlooms can be considered priceless. What would you be willing to do to ensure that this is protected from theft?

Many people store their valuables in a home safe or safety deposit box at the bank. That is the same type of thinking the business owner should take when assessing the value of their company's data. Both at work and at home, there is a price to pay for security and piece of mind.

Comparisons – The value of assets for both the homeowner and business owner is relative. The dollar value of computer systems and company data will have a much higher dollar value than the goods of a typical homeowner. However, you cannot attach a price tag to the value of one's personal property. It is just as important for individuals to know that their valuables are safe and secure as it is for the business owner.

Classify Your Threats

Work – Hacker theft can be internal or external. An internal threat requires access to secure areas such as a data center and server rooms. These should be the most protected area of the building. Securing this area should entail physical security such as pass codes, key cards and surveillance equipment.

External threats are part of today's web environment. Part of every business associated with internet access has a certain level of exposure by default, since there has to be public access to certain systems that host web pages and FTP sites.

Home - "Burglary is a crime of opportunity where entry is gained due to the carelessness of homeowners. Few people bother about security until something happens to them or a neighbor. The public's complacent attitude is the burglar's best friend and your worst enemy." [4]

Most of us can relate to this last paragraph. If you have never had your home ransacked or had someone you do not know go through your personal belongings, then you cannot appreciate the sense of rage, anxiety and fear that can go through a victim's mind.

There are similarities to these types of thefts. I have met plenty of computer users who are religious about data backups AFTER they have had the unfortunate experience of having their hard disk crash and they did not have a current backup.

From Government to the Private Sector, networked computers access the internet or what some people jokingly refer to as the Wild Wild West (WWW). In cyberspace there are threats from anyone around the globe, 24/7, with more than curiosity on their minds.

Comparisons – It's safe to say there are ways to minimize your risks to computer theft or home burglary, but they require investing in the necessary protection to secure those assets. Many times being vigilant about security in your home and your workplace can decrease your chances of being a victim.

Securing the Perimeter Defenses

Work – It is essential to implement a layered defense strategy in order to minimize the potential harm an intruder can have on your business. The Department of Defense coined the term "Defense in Depth" which includes implementing hardware, software and trained personnel.

Among the hardware devices used would be Network Intrusion Detection Systems (NIDS), Routers and Firewalls. There are also many protections available in software that helps protect the privacy of your data. Encryption, VPN's, and IPSec are just a few of the technologies available. The proper use of permissions and access to networked systems is also very important in the battle against the determined hacker.

Home – Just as there is a need for security at work, there are many things we can do to help protect our home from being ransacked and vandalized.

A home alarm system would be beneficial just as a Network Intrusion Detection System would be for protection. Both provide a first warning against a potential intruder with alert warning systems and alarms that go off. Both also have false alarms and false positives in the case of IDS machines.

Your property should have a fence or wall separating it from the curbside for better protection or at least a sense of personal property versus public access. You are not in a castle; you allow visitors and people you know to come up and enter your yard. This person could be a neighbor or the UPS driver delivering a package for you. This person is a step closer to your front door, but you have no reason to believe this person is there to commit a crime. In fact, if this person were a criminal they could be staking out the

surroundings and making note of your security system. This is very similar to what a computer hacker might do.

It is also advisable to have a guard dog protecting your yard and home so that burglars are dissuaded from coming onto your property.

What if your dog is chained up? Most likely the burglar will be looking for an easy way to get into the home like an open window or garage door.

Think of your home address as an IP address on the Internet. In your neighborhood, other homes have more or less security than you do. It doesn't mean that you are more likely than they are of becoming a victim but once again you want to minimize your risk.

Posting a security warning near the front door about your alarm security can help dissuade the criminal element that may be looking for their next target. After all, they are looking for an easy target. It is good practice to post a security warning on all computer systems at work that computers may be monitored.

A neighborhood watch program is yet another deterrent of the criminal element. It's sharing information with your neighbors about potential risks in the area. People seen lurking about or "not fitting in" with the local area. In a way, the business side of computing also has its own version of the friendly neighbor who is on the internet looking to uncover inadequacies in software development that leave computer systems vulnerable. Like your friendly neighbor, they are just looking out for you. They are not getting paid to help protect you. They may just be driven by the fact they want to make sure their neighbors can live without fear of crime.

Just as a hacker would find an open port or backdoor to exploit, the home burglar is also looking for that unlocked door or open window.

Burglars kick in doors also just as a hacker would run a brute-force program to crack a password to gain network access.

What can help prevent home burglary? Put dead bolts on doors, secure windows and sliding doors, close open doors and garages when not in plain view and install an alarm system.

What can help prevent a hacker attack? Setup firewalls and routers, lockdown systems by only running services needed and removing sample applications. Patch all systems and install a network intrusion detection system (NIDS). Post a login banner for authorized use only.

Basically make it tough for the thief to break into a network or a residence. Perform your own security audit.

Comparisons – In both work and home security, it is essential to build and maintain your defenses with all your available resources. Identify areas where you may have weaknesses in your defense strategy and build up and fortify those weak areas.

How often does it occur?

Work – According to CERT, "The total number of attacks in 2001 climbed almost 160 per cent." [5] Most computer crimes go undetected and many are uncovered long after they have happened. Companies don't have the resources and are losing ground to the hacker community. Another glaring problem is that most of these cyber intrusions go unreported.

In today's business climate, it's generally not good PR if your company has just been hacked and your server's data with customer and credit card information has been compromised. It makes sense that most companies would take every precaution to make sure that a security breach is handled within their company, without any press involved.

Home – According to the National Center for Victims of Crime, there is "one burglary every 15 seconds." [6] If you live in rural regions or urban cities, there are burglars waiting for an opportunity. You must minimize your risk of being a statistic.

Comparisons – Although home burglary stills exist there has been a steady decline in the incidents of theft in this country. This is in stark contrast to the continued increase in hacker reported incidents over the past few years.

The cost of not securing networks and residences

Work – "According to the security group Attrition.org, unpatched computers led to 99 percent of the 5,823 Web site defacements last year, up 56 percent from the 3,746 Web sites defaced in 1999. [7]

"The reported damage estimate from the "LoveLetter" virus is as much as $10 Billion. The reported damage estimate from the "Melissa" virus was $385 Million. Including hard and soft dollar figures, the true cost of virus disasters is between $100,000 and $1 Million per company" [8]

A report by The Cooperative Association for Internet Data Analysis (CAIDA) found "the Code Red worm affected more than 359,000 servers in less than 14 hours." They also determined: "At the peak of the infection frenzy, more than 2,000 new hosts were infected each minute." [9]

"According to the Association of Contingency Planners, the cost for every hour of system downtime ranges from $89,000 per hour for airline reservations to $6.4 million per hour for financial institutions."[10] These are startling figures when you consider that most hacker activity goes undetected and usually is never reported.

Computer Economics estimates that viruses such as SirCam and NIMDA in 2001 cost companies around the world an estimated $13.2 Billion Dollars. [11]

Home – Burglary in your neighborhood hits a lot closer to home. Statistics show that crime happens both in urban and rural America. It is not based on race, color or gender. Many times, the thief just wants to get in and take what he or she can carry and quickly depart without incident. These crimes are similar to the hacker in that most burglars are not looking to get caught.

The profile of a home burglar is usually an adult male looking for easy cash to pay off a debt or money for drugs. The typical hacker today is barely in their teens with many who don't even have a driver's license. Hacking is also a male dominated crime. Motivation for the computer hacker varies. Hacking a business is usually motivated by a dare, or simply curiosity. In some cases, hackers may want to deface a website to make a statement or to cause a disruption in service. Still others are motivated by greed and want to collect credit card information, or acquire items by gaining control over systems.

Comparisons – As you do with your personal property when you leave your home, you always want to secure your belongings and not give the criminal an easy target. A simple routine like dead-bolt locking your front door at home or securing the data center at your business will make it that much harder for the hacker or burglar attempting to break-in.

Knowing Your Enemy

Work – Make no doubt about it, this is a war that is fought on the front lines everyday by businesses across the nation. Many have the financial strength to allocate resources and personnel to help secure their networks; but inevitably, there are no computers, networks or operating systems and are impenetrable.

> "It doesn't take a computer expert to become a hacker. There are over 30,000 hacking-oriented sites on the Internet, offering easy to use click-and-hack programs and scripts for anyone to download. These easily accessible hacking tools have opened the door for a multitude of new exploits. The motivation of the new breed of hackers appears not to be curiosity, or a hunger for knowledge, as it used to be. Instead, most of today's hackers are driven by greed, power, revenge, or some other malicious intent, treating hacking as a game or sport, employing the tools that are readily available via the Internet." [12]

Instead of locking files away in safes, valuable company information is stored and subsequently accessed in networked files throughout organizations. This means that once the hacker gains access, they can quickly determine where the valuable data is stored and attempt to transfer that data without being caught.

Your enemy can potentially be located in a remote country that does not recognize US Criminal law and can get away from prosecution.

"If scanning can be equated to a trespass of a sort, then scanning a net block for vulnerable systems should be made a crime. More correctly, it's an attempt to commit a crime."[13]

Home – Most burglars are going to "stakeout" an area prior to committing the robbery. They will look for areas that are hidden from the street, such as a backdoor or window hidden by trees.

The majority of house burglars are looking for the quick and easy grab and dash theft. If you have a lot of obstacles in the way, such as locked doors, alarm systems, guard dogs and fences, you are more likely going to scare off the casual house burglar.

The above obstacles will not deter the more skilled "cat burglar". You just better hope that it never happens to you and that you have adequate insurance to cover the burglary.

Comparisons – Most hackers today would be classified as "script kiddies" who use automated programs to scour the network for open ports to exploit. They can stakeout out thousands of computers by the time the lone house burglar has set his or her eyes on a target to rob. These young hackers are basically testing all the locks on your homes, turning the knob and essentially seeing if they can get in the door.

Tools of the Trade

Work – Hackers use packet sniffers, Trojan horses, exploits, password crackers, and social engineering.

Packet Sniffers allow someone to capture packets of data to perform diagnostics and manage network traffic as it passes over the wire. However hackers can also use them "for illicit purposes such as stealing a user's password or credit-card number." [14]

A Trojan horse is malicious software code hidden in software that is designed to penetrate firewalls and give the hacker remote access capabilities to gain access to target computers.

Exploits are publicized vulnerabilities that exist in operating systems and software code used by corporations all around the globe. If these exploits go unpatched, they leave systems connected on networks extremely vulnerable and statistically more likely to be compromised.

Password Crackers are software programs that give the hacker the ability to "crack" and uncover encrypted passwords used to login and access networks. ""The average password cracker program can guess 65,000 dictionary words per second." [15] The odds are definitely in the hackers favor at this point.

Social Engineering – refers to deception by a hacker to trick someone into revealing a password or other information that can be used to access a network. An example of this would be calling a support desk and impersonating an employee who has either forgotten his password or who needs to access the network temporarily.

Home –
The residential burglar is going to have a minimum number of tools. Maybe a lock pick, a sharp object to pry a door open or possibly a weapon, such as a knife or gun. Some thieves will wear gloves so they don't leave any fingerprints for the police when they investigate. Many times the house burglar will have a partner either working in tandem, or watching out for witnesses so they can escape.

Comparisons – The hacker's main weapon is the computer and whatever hacker software tools used to break into a network.

The home burglar will pick the lock on a door just like the hacker will break a password to get into a computer. The burglar may use other tricks, like calling the residence to see if anyone answers the phone. If someone does answer the phone, the thief may ask some probing questions to gather more information or try to impersonate a salesperson, for example.

It's quite easy to compare known exploits in the computer world with known facts about protecting your home from burglary. Statistically, it could be a matter of a few minutes before your web server is hacked with the Code Red Worm if it is not properly patched. This is like leaving your automobile in your driveway with the keys in it. Don't expect it to be there in the morning!

During the Crime or Hacking event

Work – If you detect an intrusion, there may be a couple of actions the security professional can take. The integrity of the network is the first order of business. Preventing additional systems from being compromised is essential, paramount to mitigating your exposure to additional systems on the network.

It is important for forensic analysis, to make sure that you capture the logs to disk and not reboot the computer. At this point you can disconnect the infected server from the network.

If this is a Production server, you need to bring out the latest backup tape and restore them to another system.

Home – If you are at home and catch a burglar in the act, call the police immediately and ensure that your family is safe and out of harms way. For safety reasons, you normally would not want to try and capture the intruder because of threat of physical harm that can be caused.

Comparisons – The two scenarios, burglar and a cyber-thief, require different actions. You would want to capture the hacker in progress by gathering evidence and perhaps tracking down the location and identity of the intruder.

Just like in a burglary, the thief usually doesn't intend to leave evidence, such as fingerprints at the crime scene. In the case of the computer hacker, this person would want to remain anonymous as much possible, making it harder for police to investigate and track them down. Fingerprint evidence from a hacker would be the computer logs showing unauthorized access to accounts on the network, or IP addresses from the originating computer. In the human world, the police could really use the human fingerprint as evidence to be used in catching and prosecuting the thief.

You've been hacked or robbed, what now?

Work – Company security policies and procedures are setup in the event something like this happens. In larger companies, you will have a dedicated staff of security experts who have a plan of action to first protect the company's assets. These may include physical servers, databases or other proprietary information. Smaller companies may not have the resources or funds to pay for IT staff and either have their network administrator take care of it, or outsource to a security firm to investigate, if the amount of damage justifies it.

If the hack was limited to one system and you have a reliable backup in place, you could be back online in short order. The problem is the amount of man-hours required to determine this. The last thing you want to do is reintroduce some hacker tools that are setup in your systems or load data that has been compromised.

As hacking activity increases, more resources are becoming available for reporting incidents. You can always call the local authorities, like the police, for reporting the criminal activity. Other resources include the FBI, US DOE-CIAC (Computer Incident Advisory Capability) and InfraGuard which is the FBI's online reporting website.

Home – Finding your home ransacked by a thief may be considered a homeowner's worst nightmare. If this happens to you, authorities say it is best to leave your house immediately and call the police from a neighbor's house. You want to make sure that you protect yourself in the event the thief is still in the house. Also you do not want to use the phone or touch potential evidence in the house before the police arrive to investigate. Once the police arrive, you can do a walk through your house to determine what is missing. You will also need to fill out a police report on what was taken and estimated worth.

Comparisons – If you were just hacked or just burglarized, you would want to ensure that the means of entry used was secured so that the theft would not happen again. This would include adding dead-bolt locks to doors, securing windows with locks and maybe adding an alarm system to your home. For a business, you could have multiple points of entry where you are vulnerable as well. You would want to improve security for your servers and change all your passwords into the network. If the hacker entered in through a computer exploit, you would want to make sure that all systems had the most updated patches loaded.

In both cases you would increase your security measures, since it is usually the victim of a crime that becomes the biggest proponent of good security measures only after they've been hacked or burglarized.

Incidents – What is the penalty for getting caught?

Work – Unfortunately the penalties for hacker activity is still in its infancy. There doesn't seem to be the deterrent that you might see in other crimes, such a home burglary, where the thief has a better chance of prosecution and actually doing jail time.

Below are 6 examples of hackers that have been caught:

(1) May 2002 – Melissa Virus was created by 34 year old David L. Smith of New Jersey. It caused an estimated $80M in damage. He paid a $5,000 fine, served community service and was banned from computer and Internet use. This was considered the first major email virus. [16]

(2) February 2001 – Anna Kournikova Virus was created by 20 year old Jan de Wit, a Dutch citizen. It caused a total of $166,827 in damage however this figure would be much larger had most companies reported their losses to the FBI. He was sentenced to 150 hours of community service. [17]

(3) March 2001 – Denial of Service attacks on Amazon, eBay, eTrade, CNN and Yahoo were launched by a 16 year old juvenile from Quebec Canada named "Mafia Boy". He was reported to have caused $1.7B in damage. He served 2 years detention and was fined $650. He "boasted that he will commit this kind of cyber vandalism again." [18]

(4) May 2000 - "ILOVEYOU," or Love Letter was a virus written by 23-year-old computer school dropout Onel de Guzman from Manila, Philippines. The estimated economic damage was $8.7B. He was never prosecuted since there was no existing law in his country that covered computer hacking. It was considered the “most destructive virus in history.” [19]

(5) February 1995 – Kevin Mitnick, 39 years old, hacked into corporations, telephone companies, educational institutions and Internet Service Providers. The damage was estimated to be $80M. He was labeled a “computer terrorist.” “Once held for eight months in solitary confinement because the FBI feared he could launch nuclear missiles from a prison pay phone.” [21] He was sentenced to 4 years 11 months and 6 days. He will be released on January 21, 2003. He can use a cell phone and a computer but not the Internet and must notify authorities if he leaves his residence in Southern California.

(6) November 1988 – The Robert Morris Worm was written by a 22 year old Cornell graduate whose computer code this virus was named after. He was the son of a computer expert at the National Security Agency. The self-propagating worm spread to an estimated 6,000 host machines, which at the time, was close to 10% of the total connected systems using the ARPAnet. The estimated damage was over $98M. Morris was “dismissed from Cornell, sentenced to three years' probation and fined $10,000.” [22]

Home –The type of crime, age of the person and whether or not this was a first offense are all factors that determine what punishment is given to the adult or teenager. Juvenile law tries to offer ways to rehabilitate the delinquent offender. Each state has different laws when dealing with minors. Statistically, males carry out most home burglaries and they are usually looking for quick cash to pay for their drug habits. And most burglars who are caught in possession of stolen goods or have been proven through fingerprints or video surveillance to have committed a theft, are highly likely to serve jail time for their criminal activity.

Comparisons – The penalties for criminal hacking versus home burglary are quite different. You also won’t have the publicity for a home burglary that what you would have for the hacker who brings down major Internet sites on the web. The police are more likely to catch a burglar than a hacker by the sheer fact that the Internet hacker can hide his or her identity quite easily. It is also very hard to prosecute someone who is located in a country that doesn’t follow the same laws as we do in the U.S.

Hacker vs. Burglar Conclusion

There are a few highlights to remember when comparing a hacker to a burglar.

1. It is worth the time and effort to follow Good Security Practices right from the start.

2. Safeguard your possessions in the event that a theft occurs, with a backup plan or some type of insurance policy.

3. Don't let your guard down. The threats are only going to get greater as the Internet continues to grow as a worldwide medium.

4. There needs to be more laws enacted to help catch and prosecute criminals who one day could threaten vital interests of the United States.

5. Education of the public about burglary and hacking can help safeguard homes and businesses. It has been shown to work with home burglary. We need to do the same for computer users across the nation.

6. We have learned from experience that if we work together to help stop these criminal activities, we can make our neighborhoods safer and our businesses more secure.

References

1. Merriam-Webster's Collegiate Dictionary
URL: http://www.m-w.com/home.htm + enter "hacker" to get to this URL page
http://www.m-w.com/cgi-bin/dictionary
© 2002, Merriam-Webster Incorporated.

2. Dictionary.Com, "burglary"
Source: The American Heritage Dictionary of the English Language, 4th Edition
© Houghton Mifflin Company
URL: http://www.dictionary.com/search?q=burglary
© 2002 Lexico LLC

3. Lemos, Robert, "Security Patches Aren't Being Applied"
ZDNet News, January 23, 2001
American Society for Industrial Security & PricewaterhouseCoopers
URL: http://zdnet.com.com/2100-11-527502.html?legacy=zdnn
© 2002 CNET Networks Inc.

4. McGruff, Wayne, "Practical Tips To Secure Your Home"
URL: http://www.howtoadvice.com/HomeSecurity/
© 2000 HowToAdvice.com

5. Geralds, John, "Web Attacks up 160 per cent in 2001"
URL: http://www.vnunet.com/News/1128250
© 1995-2002 VNU Business Publications Ltd.

6. Crime Statistics – National Center for Victims of Crime
URL: http://www.womensdefensecenter.com/crime.htm

7. Lemos, Robert, “Security Patches Aren’t Being Applied”
ZDNet News, January 23, 2001
URL: http://zdnet.com.com/2100-11-527502.html?legacy=zdnn
© 2002 CNET Networks Inc.

8. Geralds, John, “2000 Computer Virus Prevalence Survey”
ICSA.Net, January 14, 2002
URL: http://www.securitystats.com/reports.asp
© 2002 VNU Business Publications

9. CAIDA Analysis of Code-Red, July 14, 2002
URL: http://www.caida.org/analysis/security/code-red/

10. Shively, Geoff, “Network Insecurity”
URL: http://www.pivx.com/documents/Network_Insecurity_White%20Paper.doc

11. Computer Economics, January 2, 2002
Source: http://www.computereconomics.com/cei/press/pr92101.htm (link fails)
URL: http://www.securitystats.com/webdeface.asp
© 2000, Security Stats.Com, Inc.

12. Olsen, Jen, July 15, 2002, “The Behaviors and Tools of Today's Hackers”
September 24, 2002 ARTICLE ID: 1398
URL:
http://enterprisesecurity.symantec.com/article.cfm?articleid=1398&PID=12493901&EID=0
© 2002 Symantec Corporation

13. Leadley, Peter, “RE: Bad ISP”, SP North Syracuse
URL: http://cert.uni-stuttgart.de/archive/intrusions/2002/04/msg00347.html

14. Telecom Glossary 2k, February 28, 2001
URL: http://www.atis.org/tg2k/t1g2k.html

15. FCC Computer Security Notice
URL: http://csrc.nist.gov/fasp/FASPDocs/id-authentication/Strong-Passwords.pdf

16. Lyman, Jay, “Melissa Virus Writer Sentenced to Prison”
NewsFactor Network.Com, May 1, 2002
URL: http://www.newsfactor.com/perl/story/17551.html
© 1998-2002 Triad Commerce Group, LLC

17. White, Aoife, “Kournikova creator gets off lightly”
Network News in Prague, March 2001
URL: http://www.vnunet.com/News/1125866
© 2002 VNU Business Publications

18-19. Reuters, “Melissa virus writer is latest to be convicted”
May 1, 2002
URL: http://www.infoworld.com/articles/hn/xml/02/05/01/020501hnmelissa.xml
© 2000 Reuters Limited.

20. Reuters, “Famed hacker hawking historic laptops”
October 9, 2002
URL: http://www.cnn.com/2002/TECH/internet/10/09/hacker.mitnick.reut/
© 2002 Cable News Network LP, LLLP

21. PCWorld.Com staff, “Timeline: A 40-year history of hacking”
November 19, 2001
URL: http://www.cnn.com/2001/TECH/internet/11/19/hack.history.idg/index.html
© 2002 Cable News Network LP, LLP