HACKING

AND

ETHICAL HACKING

MIT SCHOOL OF MANAGEMENT, PUNE

COURSE: MBA SHIFT 1

SEMESTER: I

DIVISION: B

SUBJECT: INFORMATION TECHNOLOGY

ASSIGNMENT NO.: 1

TOPIC: RESEARCH PAPER

SUBMISSION DATE: 20-09-2012

SUBMITTED TO: PROF. ARCHANA SINGH

REPORT COMPILED BY:

ROLL NO.	NAME
69	ANU OM ALREJA
75	VINAYA RAIBAGKAR
83	RASIKA AHER

ABSRACT:

The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a dark side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open. Many hackers are true technology buffs who enjoy learning more about how computers work and consider computer hacking an “art” form. They often enjoy programming and have expert-level skills in one particular program. For these individuals, computer hacking is a real life application of their problem-solving skills. It’s a chance to demonstrate their abilities, not an opportunity to harm others.

Since a large number of hackers are self-taught prodigies, some corporations actually employ computer hackers as part of their technical support staff. These individuals use their skills to find flaws in the company’s security system so that they can be repaired quickly. In many cases, this type of computer hacking helps prevent identity theft and other serious computer-related crimes. Computer hacking can also lead to other constructive technological developments, since many of the skills developed from hacking apply to more mainstream pursuits. For example, former hackers Dennis Ritchie and Ken Thompson went on to create the UNIX operating system in the 1970s. This system had a huge impact on the development of Linux, a free UNIX-like operating system. Shawn Fanning, the creator of Napster, is another hacker well known for his accomplishments outside of computer hacking. In comparison to those who develop an interest in computer hacking out of simple intellectual curiosity, some hackers have less noble motives. Hackers who are out to steal internet. With these concerns and others, the ethical hacker can help.

Keywords— Ethical hacking, hacking, hackers, education and training, risk management, automated

---

INTRODUCTION

Hacker (computer security)

Hacking means finding out weaknesses in a computer or computer network, though the term can also refer to someone with an advanced understanding of computers and computer networks. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground.

History

Bruce Sterling traces part of the roots of the computer underground to the Yippies, a 1960s counterculture movement which published the Technological Assistance Program (TAP) newsletter. TAP was a phone phreaking newsletter that taught the techniques necessary for the unauthorized exploration of the phone network. Many people from the phreaking community are also active in the hacking community even today, and vice versa.

Classifications

White hat

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC-Council, also known as the International Council of Electronic Commerce Consultants has developed certifications, courseware, classes, and online training covering the diverse arena of Ethical Hacking.

Black hat

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain". Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network. They choose their targets using a two-pronged process known as the "pre-hacking stage".

Part 1: Targeting

The hacker determines what network to break into during this phase. The target may be of particular interest to the hacker, either politically or personally, or it may be picked at random. Next, they will port scan a network to determine if it is vulnerable to attacks, which is just testing all ports on a host machine for a response. Open ports—those that do respond—will allow a hacker to access the system.

Part 2: Research and Information Gathering

It is in this stage that the hacker will visit or contact the target in some way in hopes of finding out vital information that will help them access the system. The main way that hackers get desired results from this stage is from "social engineering", which will be explained below. Aside from social engineering, hackers can also use a technique called "dumpster diving". Dumpster diving is when a hacker will literally search through users' garbage in hopes of finding documents that have been thrown away, which may contain information a hacker can use directly or indirectly, to help them gain access to a network.

Part 3: Finishing the Attack

This is the stage when the hacker will invade the preliminary target that he/she was planning to attack or steal. Many "hackers" will be caught after this point, lured in or grabbed by any data also known as a honeypot (a trap set up by computer security personnel).

Grey hat

A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.

Elite hacker

A social status among hackers, elite is used to describe the most skilled. Newly discovered exploits will circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

Script kiddie

A script kiddie (or skiddie) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept—hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature).

Neophyte

A neophyte, "n00b", or "newbie" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking.

Blue hat

A blue hat hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term Blue Hat to represent a series of security briefing events.

Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

Nation state

Intelligence agencies and cyberwarfare operatives of nation states.

Organized criminal gangs

Criminal activity carried on for profit.

Bots

Automated software tools, some freeware, available for the use of any type of hacker.

Attacks

A typical approach in an attack on Internet-connected system is:

1. Network enumeration: Discovering information about the intended target.
2. Vulnerability analysis: Identifying potential ways of attack.

3. Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts.

Security exploits

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web-pages. These are very common in website/domain hacking.

Techniques

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented.)

Password cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Packet sniffer

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack (Phishing)

A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool

programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

Rootkit

A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.

Social engineering

When a Hacker, typically a black hat, is in the second stage of the targeting process, he or she will typically use some social engineering tactics to get enough information to access the network. A common practice for hackers who use this technique, is to contact the system administrator and play the role of a user who cannot get access to his or her system. Hackers who use this technique have to be quite savvy and choose the words they use carefully, in order to trick the system administrator into giving them information. In some cases only an employed help desk user will answer the phone and they are generally easy to trick. Another typical hacker approach is for the hacker to act like a very angry supervisor and when the his/her authority is questioned they will threaten the help desk user with their job. Social Engineering is very effective because users are the most vulnerable part of an organization. All the security devices and programs in the world won't keep an organization safe if an employee gives away a password. Black Hat Hackers take advantage of this fact. Social Engineering can also be broken down into four sub-groups. These are intimidation, helpfulness, technical, and name-dropping.

- *Intimidation* As stated above, with the angry supervisor, the hacker attacks the person who answers the phone with threats to their job. Many people at this point will accept that the hacker is a supervisor and give them the needed information.
- *Helpfulness* Opposite to intimidation, helpfulness is taking advantage of a person natural instinct to help someone with a problem. The hacker will not get angry instead act very distressed and concerned. The help desk is the most vulnerable to this type of Social Engineering, because they generally

have the authority to change or reset passwords which is exactly what the hacker needs.

- *Name-Dropping* Simply put, the hacker uses the names of advanced users as "key words", and gets the person who answers the phone to believe that they are part of the company because of this. Some information, like web page ownership, can be obtained easily on the web. Other information such as president and vice president names might have to be obtained via dumpster diving.
- *Technical* Using technology to get information is also a great way to get it. A hacker can send a fax or an email to a legitimate user in hopes to get a response containing vital information. Many times the hacker will act like he/she is involved with law enforcement and needs certain data for record keeping purposes or investigations.

Trojan horses

A Trojan horse is a program which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later. (The name refers to the horse from the Trojan War, with conceptually similar function of deceiving defenders into bringing an intruder inside.)

Viruses

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells.

While some are harmless or mere hoaxes most computer viruses are considered malicious.

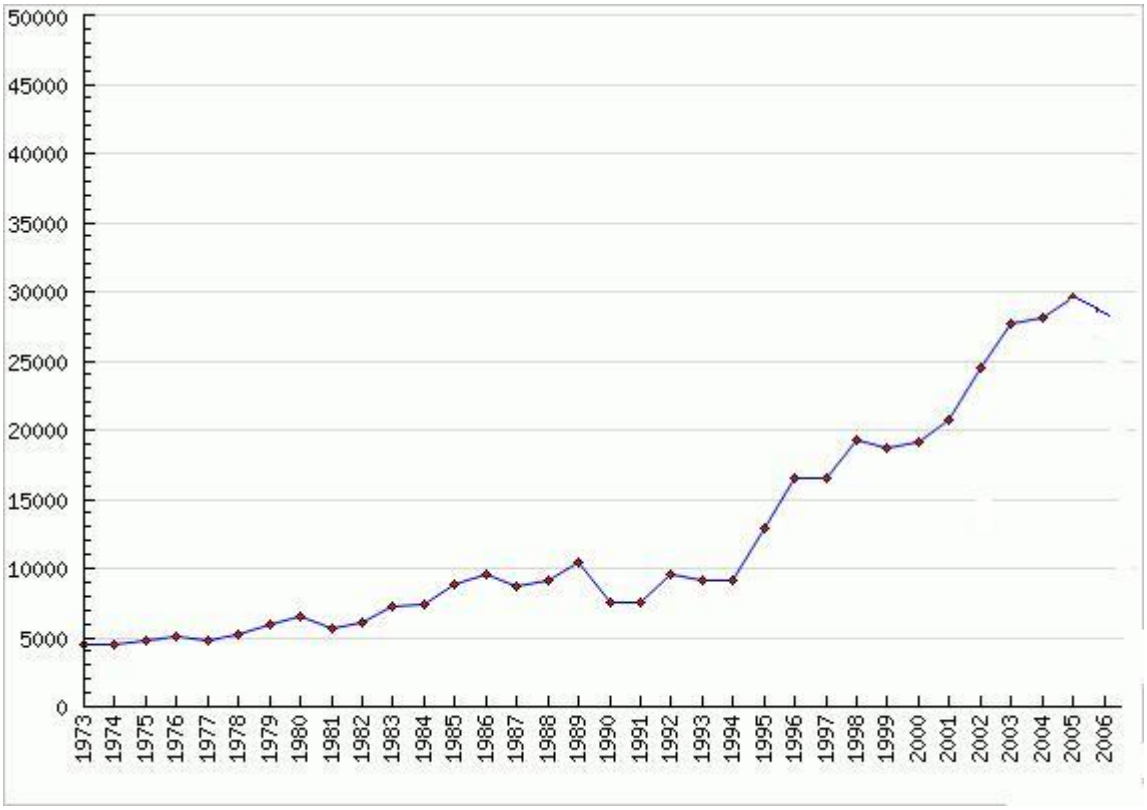
Worms

Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program. Many people conflate the terms "virus" and "worm", using them both to describe any self-propagating program.

Key loggers

A key logger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. Some key loggers uses virus-, trojan-, and rootkit-like methods to remain active and hidden. However, some key loggers are used in legitimate ways and sometimes to even enhance computer security. As an example, a business might have a key logger on a computer used at a point of sale and data collected by the key logger could be used for catching employee fraud.

GRAPH SHOWS INCREASE IN HACKING IN YEARS



Notable intruders and criminal hackers

Notable security hackers

- Eric Corley (also known as Emmanuel Goldstein) is the long standing publisher of 2600: The Hacker Quarterly. He is also the founder of the H.O.P.E. conferences. He has been part of the hacker community since the late '70s.
- Gordon Lyon, known by the handle Fyodor, authored the Nmap Security Scanner as well as many network security books and web sites. He is a founding member of the

Honeynet Project and Vice President of Computer Professionals for Social Responsibility.

- Gary McKinnon is a Scottish hacker facing extradition to the United States to face charges of perpetrating what has been described as the "biggest military computer hack of all time".[16]
- Kevin Mitnick is a computer security consultant and author, formerly the most wanted computer criminal in United States history.[17]
- Rafael Núñez aka RaFa was a notorious most wanted hacker by the FBI since 2001.
- Solar Designer is the pseudonym of the founder of the Openwall Project.
- Michał Zalewski (lcamtuf) is a prominent security researcher.
- Albert Gonzalez sentenced to 20 years in prison.

Customs

The computer underground has produced its own slang and various forms of unusual alphabet use, for example 1337speak. Political attitude usually includes views for freedom of information, freedom of speech, a right for anonymity and most have a strong opposition against copyright. Writing programs and performing other activities to support these views is referred to as hacktivism. Some go as far as seeing illegal cracking ethically justified for this goal; a common form is website defacement. The computer underground is frequently compared to the Wild West. It is common among hackers to use aliases for the purpose of concealing identity, rather than revealing their real names.

Hacker groups and conventions

The computer underground is supported by regular real-world gatherings called hacker conventions or "hacker cons". These draw many people every year including SummerCon (Summer), DEF CON, HoHoCon (Christmas), ShmooCon (February), BlackHat, AthCon, Hacker Halted, and H.O.P.E.. In the early 1980s Hacker Groups became popular, Hacker groups provided access to information and resources, and a place to learn from other members. Hackers could also gain credibility by being affiliated with an elite group.

Hacking and the media

Hacker magazines

The most notable hacker-oriented magazine publications are *Phrack*, *Hakin9* and *2600: The Hacker Quarterly*. While the information contained in hacker magazines and ezines

was often outdated, they improved the reputations of those who contributed by documenting their successes.

Non-fiction books

- *Hacking: The Art of Exploitation, Second Edition* by Jon Erickson
- *The Hacker Crackdown*
- *The Art of Intrusion* by Kevin D. Mitnick
- *The Art of Deception* by Kevin D. Mitnick
- *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker* by Kevin D. Mitnick
- *The Hacker's Handbook*
- *The Cuckoo's Egg* by Clifford Stoll
- *Underground* by Suelette Dreyfus
- *Stealing the Network: How to Own the Box, How to Own an Identity, and How to Own an Continent* by various authors

Cases:

On March 1, 2011 at Lassiter High School, two students were accused of impersonation of a staff member via cybercrime, but both claimed they were uninvolved. The offense was made a felony in the Cobb County School District two months after the impersonation had happened. Shortly afterwards, the head of the LHS School Board said "The teacher just wouldn't do this at all". The case ended on May 9, and no evidence was found. Messages can cause huge damage to an individual or business's image.

Security Systems Protective Measures Against Hackers

By G.C. Eric Brumfield

As our world heads into the next millennium, companies in every industry are becoming more computer literate. Their need for some level of sophisticated networks to keep their competitive edge is becoming greater. With every network that is installed in an organization, there is also a risk that proper security measures were overlooked or taken for granted. In these cases, companies can face a great deal of embarrassment and anxiety and even lose millions of dollars due to security breaches.

When should companies invest in security systems? When can they determine if they are at risk without one? A rule of thumb is, any company that routinely stores sensitive, confidential information that is critical to their success, or information that could cause

damage to them were it to end up in the wrong hands, should definitely look for a sound security system to protect its investment. Companies utilizing a local area network with a small number of users are at a lower risk than those that utilize a wide area network that connects to multiple sites within a city or multiple sites throughout the country.

Information equates to power and money in this day and age. The Internet is becoming one of the fastest ways to start a new business, grow an existing business or simply find needed information. Jim Reed, manager of public relations for V-One, a network security company in Germantown, Maryland, says, "It is business-to-business commerce through the Internet that is going to make the Internet even bigger than it is now. And with companies communicating with each other through the Internet, vital information is being transferred back and forth. If the information falls into the wrong hands, it could be beyond damaging."

Law offices and other industries have to deal with the power of confidentiality. As we take a closer look at how freely information is passed via our internal networks and the Internet, we must begin to recognize the importance of having an adequate network security system that will protect this information and secure the rights of confidentiality for businesses and our clients.

Proactive Measures

After accomplishing the great task of installing a network security system, there is yet another concern that demands close attention: the ability to manage network security systems effectively so that hackers do not break through security walls and create nightmares for us all. Hacker is more than just a word to many. For some it’s, a career, and for others it is like a vampire in the night waiting to suck the blood and money from the life of a company. Most organizations in business today have been the victim of hackers at one time or another. Part of the reason is that hackers come in many shapes and sizes. They can be as small and as brilliant as the adolescent genius that lives next door–the kid that spends his time solving puzzles and breaking passwords on his PC in the basement, instead of playing with the boring computer-illiterate kids in the neighbourhood. Or hackers can be as dangerous as the professionals, known as "Black Hats," computer criminals who make a living by breaking into unsuspecting computer systems and selling, destroying or manipulating data or information they poach.

How can businesses protect their investments with criminals waiting for the perfect opportunity to penetrate security systems? There are many security measures that can be taken. Some are very small steps, and others involve financial investments.

One major step that organizations can take is to eliminate use of the Internet on the job. It is common knowledge that Internet access and a modem are key sources of entry into an organization's computer system. And every organization has its workaholics–you know, people who are so dedicated to work that they have to take some of it home with them. Then they remotely access the server at the office to make modifications to their critical projects. If the fire walls of our network security systems allow people with just average computer literacy to enter, then what opportunities for intrusion exist for the "Black Hats" of the world? Just a simple password can create a virtual playground for the professional hacker.

Welcome to the world of hacker. According to the third annual "Computer Crime and Security Survey," conducted by the Computer Security Institute in San Francisco (http:www.gocsi.com), computer crime and other information security breaches are on the rise, and the cost to U.S. corporations and government agencies is growing.

The CSI report released last March noted that 64 percent of respondents reported computer security breaches within the last year. This figure is 16 percent higher than CSI's 1997 survey.

CSI also reported that, although most organizations have firewalls in place at their network perimeters, more than 70 percent had security flaws which left them vulnerable to even the most rudimentary malicious attacks.

Internal Measures

Companies must first take proactive measures from within. Initial steps should be blocking the curious onlooker or the average computer hacker. This would basically protect documents within the system from internal onlookers, but it will not protect them from that experienced hacker outside, looking in. Measures might include password protection, masking and information-change detection. Getting into the habit of changing passwords regularly is a wise thing to do.

It's recommended that companies change user passwords at least once a quarter. Masking techniques include disguising files inside the computer, or hiding ranges of information inside a file to make information appear unreadable or invisible. Change-detection techniques include audit trails such as byte count and formula difference locators. There are many security programs available in today's marketplace that address spreadsheet and word-processing techniques, operating systems security, database protection, and general safeguards and Internet security, to name just a few. Depending on your business, any one or all of these programs would benefit to the protection of data or information within your

systems. Companies that implement such internal protective measures move one step closer to preventing incidents like the Bernard Mayles case in 1991. Bernard stole drug-processing information from his then-employer pharmaceuticals giant Merck & Co, and tried to peddle it to an Eastern European company. That company's agent turned out to have a different employer: the FBI. Mayles was sentenced to nine years in prison.

Another situation that might have been avoided is the case of a retail store chain managed by Bill Kesl, director of systems integration at Datamax Systems Solutions in Boca Raton, Florida. A computer-savvy store clerk at Kesl's would log on to an electronic register and change prices so that an accomplice could buy items for next to nothing. In both cases, individuals were able to access sensitive computer information and use it for dishonest purposes, due to relaxed security parameters.

External Measures

As companies move toward decentralized networks of personal computers and away from centralized, easily protected mainframes, they become more vulnerable to hacking. In an effort to make businesses more user-friendly, we are inevitably making them more hacker-friendly as well.

The "Black Hats" of the world create varied nightmares for businesses. A hacker tampered with automaker BMW's Web site as a New Year's prank last January, taking the image of a BMW roadster tearing down the highway and transforming it into a car wreck by turning the car upside down and painting in skid marks. Later that same month, critics of Indonesia's then-President Suharto hit 15 government domains, including the site of the nation's police force, inserting their views onto the Web sites.

There is also the "denial of service" attack, in which a hacker tricks a computer so that it shuts down or is so busy with bogus requests that it can't handle legitimate ones. In March, a series of "denial of service" attacks crippled hundreds of systems, including computers owned by NASA and other government agencies, various academic institutions, Microsoft Corporation and other commercial institutions. Last year a virus shut down computers for two days at National City Corporation, a Cleveland bank. The bank spent at least $400,000 to correct the virus rewiring during the attack to activate backup computers.

In a survey conducted last year by Information Week and Ernst & Young of New York, 40 percent of respondents reported losses of up to $100,000 from macro viruses; nearly half (47 percent) reported losses of up to $100,000 due to other types of viruses.

Nick Simicich, an IBM Senior Security consultant in Boca Raton, Florida, tests social engineering methods when conducting security audits for clients. Social Engineering is a

term that commonly used by low-key hackers to describe posing as employees of a company in order to gain sensitive information. "I've gone up to a security person carrying a laptop, "Simicich says," asked him what the policy is on laptops and walked out the door." He has also gotten passwords by posing as a company computer technician: "I'll just say, 'Could you do me a favour and give me your password so I don't have to look it up?'" These are just a few of the potentially hundreds of techniques that hackers use to wreak havoc on our organizations.

One very common preventive measure that companies are using is to hire outside organizations to strengthen their network security systems. The organizations conduct a series of diagnostic tests from outside, to see how easy it is to crack the firewalls of the target organization–with the permission of the organization. This adds a new twist, paying someone to hack systems to discover the weaknesses.

One company that provides this service to all industries is IBM. Dave Gamey, of IBM Canada, is a consultant for public and private-sector organizations, including banks. Gamey is engaged in an ongoing war against computer criminals as a member of a 100-man team of "White Hats." The White Hats charge up to $40,000 to attempt to outwit their black-hatted opponents, using technologies such as Trojan horses, jails, spoofing, password guessers, war-dialers, stealth port scanners, firewalls, sniffers, daemons and finger commands. When Gamey and his team win, they can save a company embarrassment, anxiety, hours of labour costs and millions of dollars in potential losses. The $40,000 cost for this service is minimal; Gamey and his merry team of white hatters believe that they have saved millions for their clients.

Where Are We Heading

Traditionally, computer crimes have been inside jobs. But technology continues to advance, giving us all the potential to gain a competitive edge. Companies need take the proper steps to avoid internal hacking and to set security parameters, because it will become increasingly more expensive to secure data. John D. Spain, executive vice president of information technology security at Asset Management Solutions, an Atlanta-based security firm, says, "Companies need to classify their information. If you don't know what you need to protect, it's hard to protect it." We must all become more knowledgeable about common occurrences of internal and external hacking in our types of businesses, to protect our investments better in the next millennium.

Network Security Systems are a great enough problem by itself. One that has the government setting regulations on the use of information flowing through the Internet with

encryptions on it. Today our worry is the loss of great profits as a result of this hacker problem, let's hope that tomorrow our worry won't be that we will all be living in a world like the one depicted in the 1998 movie, "Enemy of the State," where the government is the real "Black Hat" to worry about.

Once we take the time and make the necessary investments to determine our security needs we will move one step closer to what we would all like to believe is "real security."**G.C. Eric Brumfield** *is president of BIT Consultants Incorporated, an IT Staffing Firm in Detroit, Michigan. He can be reached at* ***Brumfield1@aol.com***

Cyber Law of India

Cyber crime is unlawful acts wherein the computer is either a tool or a target or both. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

The Computer as a Target:

Using a computer to attack other computers. E.g. Hacking, Virus/Worm attacks, DOS attack etc.

Unauthorized access & Hacking:

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

By hacking web server taking control on another person's website called as web hijacking

Hacking & the Indian Law

According to section 66 of the IT Act -

(1)Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2)Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

News for Hacking

Get insured against hacking on Facebook, Twitter

LONDON: You may soon insure your Facebook and Twitter accounts against the nuisance of hacking as a UK-based company has launched the country's first social media insurance. The information privacy company is offering services to specifically protect against reputational damage, account jacking and ID theft, the 'Daily Mail' reported.

Hacking of users accounts on Facebook, Twitter, LinkedIn and other social media sites are quite common, where another user logs in and posts derogatory or offensive messages, and can cause huge damage to an individual or business's image.

Justin Basini, CEO of the company providing the service, ALLOW, said that insurance "perhaps wouldn't have been needed a few years ago." "That's all changed now. Every internet user faces a certain level of risk that one day a digital criminal will target them or that they will suffer damage to their reputation," Basini said.

The cover, at a cost of 3.99 pounds a month, will pay for legal advice and support if someone suffers an on-line attack and seeks some form of redress. The insurance includes the cost of disabling accounts, suppressing offensive material and stopping any legal action triggered by hacking, for example if a hacker posts illegal material under a victim's name, the paper said. It is available via the ALLOW Protect service, which also allows users to monitor how their personal data is used on-line, it added.

On-line abuse and identify theft are so common that social media users are being sold specialist insurance to help protect their reputation.

Ethical hacker

The first use of the term “ethical hackers” appears to have been in an interview with John Patrick of IBM by Gary Anthens that appeared in a June 1995 issue of *Computer World.*

An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them. Ethical hacking is also known as *penetration testing*, *intrusion testing* and *red teaming*. An ethical hacker is sometimes called a white hat (a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat).

One of the first examples of ethical hackers at work was in the 1970s, when the United States government used groups of experts called *red teams* to hack its own computer systems. According to Ed Skoudis, Vice President of Security Strategy for Predictive Systems' Global Integrity consulting practice, ethical hacking has continued to grow in an otherwise lackluster IT industry, and is becoming increasingly common outside the government and technology sectors where it began. Many large companies, such as IBM, maintain employee teams of ethical hackers.

In a similar but distinct category, a hacktivist is more of a vigilante: detecting, sometimes reporting (and sometimes exploiting) security vulnerabilities as a form of social activism.

Certified Ethical Hacker

The Certified Ethical Hacker is a professional certification provided by the International Council of E-Commerce Consultants (EC-Council.)

An ethical hacker is usually employed by an organization who trusts him or her to attempt to penetrate networks and/or computer systems, using the same methods as a hacker, for the purpose of finding and fixing computer security vulnerabilities. Unauthorized hacking (i.e., gaining access to computer systems without prior authorization from the owner) is a crime in most countries, but penetration testing done by request of the owner of the targeted system(s) or network(s) is not.

A Certified Ethical Hacker has obtained a certification in how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a hacker.
The EC-Council offers another certification, known as Certified Network Defense Architect (C|NDA). This certification is designed for United States Government Agencies, and is available only to members of selected agencies. Other than the name, the content of the course is exactly the same.

Controversy

Certain computer security professionals have objected to the term ethical hacker: "There's no such thing as an 'ethical hacker' - that's like saying 'ethical rapist' - it's a contradiction in terms." Part of the controversy may arise from the older, less stigmatized, definition of hacker, which has since become synonymous with computer criminal.

On the other hand, some companies do not seem to mind the association. According to EC-Council, there has been an increase of careers where C|EH and other ethical hacking certifications are preferred or required. Even the US government accepts this association and requires C|EH accreditation for some jobs per 8570 guidelines.

Some of the hacking concepts that ethical hackers learn to master:

- Penetration testing methodologies
- Stealthy network recon
- Passive traffic identification
- Remote root vulnerability exploitation
- Privilege escalation hacking
- IPv6 Vulnerabilities
- Remote access trojan hacking
- Running shellcode in RAM vs. on disk
- Wireless insecurity
- Breaking IP-based ACLs via spoofing
- Abusing Windows Named Pipes for Domain Impersonation
- Evidence removal and anti-forensics
- Attacking network infrastructure devices
- Hacking by brute forcing remotely

- Hiding exploit payloads in jpeg and gif image files
- Hacking Web Applications
- Breaking into databases with SQL Injection
- Cross Site Scripting hacking
- Hacking into Cisco routers
- Justifying a penetration test to management & customers
- CEH/CPT review
- Defensive techniques

Some of the hacking lab exercises performed by ethical hackers for security training experience:

- Capture the Flag hacking exercises every night !
- Abusing DNS for host identification
- Leaking system information from Unix and Windows
- Windows 2003 Server & Vista DNS Cache Poisoning Attacks
- Unix, Windows and Cisco password cracking
- Remote buffer overflow exploit lab - heap vs. stack overflows
- Attacking Kerberos Pre-Auth Hashes
- Spoofing endpoints of communication tunnels
- Impersonation of other Users- Hijacking kernel tokens
- Attacking RDP (Remote Desktop Protocol) in Windows XP, 2003 & Vista
- Remote keylogging
- Data mining authentication information from clear-text protocols
- Sniffing and hijacking SSL encrypted sessions
- Breaking wireless security via hacking
- Malicious event log editing
- Client side IE & Firefox exploits
- Tunneling through IPSec VPNs by abusing ESP
- Data retrieval with SQL Injection Hacking
- Calculating the Return on Investment (ROI) for an ethical hack

Ethical hacking as a career

Ethical hacking, also known as penetration testing, intrusion testing or red teaming is used to find loopholes in an IT system and break into it. An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. This work is ethical because it is performed to increase the safety of the computer systems, but only at the request of the company that owns the system and specifically to prevent others from attacking it. With the increasing use of the internet, it has become an essential part of IT security industry today.

Industry status

Last year ethical hacking was estimated to be a US$ 3.8 billion industry in the US alone. According to Nasscom, India will require at least 77,000 ethical hackers every year whereas we are producing only 15,000 in a year, currently. Ethical hacking is growing at a tremendous pace and offers a plethora of lucrative job opportunities.

Skillset required

First and foremost is the ability to write programmes in many programming languages like C, C++, Perl, Python, and Ruby. For those working with web applications, Microsoft .NET and PHP are vital. Knowledge of assembly language is also essential for those who want to analyse disassembled binaries. Knowledge of a variety of operating systems (Microsoft Windows, various versions of Linux, etc) is critical. Experience with various network devices, including switches, routers and firewalls is also important. An ethical hacker also should have a basic understanding of TCP/IP protocols such as SMTP, ICMP and HTTP. In addition to technical skills, an ethical hacker needs good soft skills. Perhaps the most important skill, however, is adaptability. When testing software and systems, ethical hackers never know what will come up, so the ability to be resourceful is vital.

Growth areas

The information security industry is going at a current worldwide growth rate of 21%. Frost & Sullivan have estimated that there are 2.28 million information security professionals worldwide which is expected to increase to nearly 4.2 million by 2015. The need for information security for security compliance in India is mandatory for all companies with an IT backbone. The requirement for such personnel is especially high with organisations in the IT/ITES space.

Remuneration

A fresher may work as an intern for a couple of months and can start with a minimum of Rs 2.5 lakh per annum. With one year of experience, one can expect upto Rs 4.5 lakh per annum. Those with work experience five years or more can get from 10-12 lakh per annum.

Practical use of ethical hacking

- Many large companies, such as IBM, maintain employee teams of ethical hackers.
- 'Ethical' hackers assist security agencies and finance firms to check cyber crime. One of the country's prominent ethical hackers, Sunny Vaghela has helped security agencies crack several cases using his prowess in hacking into systems. " I worked with cops and helped them trace the e-mails of people involved in the 2008 Ahmedabad blasts. I also helped solve numerous identity fraud cases," said the 22-year-old computer engineer. His technical advice was accepted and adopted by Google's social networking website Orkut in January, when he pointed out some loopholes to its administrators .
- Ashish Kaushik, who did PG diploma in ethical hacking and cyber security from Delhi, said: " I have worked as a cyber security consultant with MNCs and fivestar hotels in Delhi and Bombay. Now I am developing security softwares. There are a multitude of opportunities for ethical hackers. And for a single project, I earn three times of what one is offered in a conventional job."
- It's now one of the highest paid professions in the world. In the US, hackers are offered annual packages of over $100,000. In India, the demand for hackers, both in the private and government sector , is about 1,80,000 people a month.
- Social Networking Websites (Facebook, Twitter) have their own Hacking & Security Policies

Some of the best hackers of all time are given below:

Few of them are black hat hackers and some are white hat hackers.

.

White Hat Hackers

Hackers that use their skills for good are classified as "white hat." These white hats often work as certified "Ethical Hackers," hired by companies to test the integrity of their systems.

Stephen Wozniak: "Woz" is famous for being the "other Steve" of Apple. Wozniak, along with current Apple CEO Steve Jobs, co-founded Apple Computer. He has been awarded with the National Medal of Technology as well as honorary doctorates from Kettering University and Nova Southeastern University. Additionally, Woz was inducted into the National Inventors Hall of Fame in September 2000.

Woz got his start in hacking making blue boxes, devices that bypass telephone-switching mechanisms to make free long-distance calls. After reading an article about phone phreaking in Esquire, Wozniak called up his buddy Jobs. The pair did research on frequencies, then built and sold blue boxes to their classmates in college. Wozniak even used a blue box to call the Pope while pretending to be Henry Kissinger.

Tim Berners-Lee: Berners-Lee is famed as the inventor of the World Wide Web, the system that we use to access sites, documents and files on the Internet. He has received numerous recognitions, most notably the Millennium Technology Prize.

While a student at Oxford University, Berners-Lee was caught hacking access with a friend and subsequently banned from University computers. w3.org reports, "Whilst [at Oxford], he built his first computer with a soldering iron, TTL gates, an M6800 processor and an old television." Technological innovation seems to have run in his genes, as Berners-Lee's parents were mathematicians who worked on the Manchester Mark1, one of the earliest electronic computers.

Richard Stallman: Stallman's fame derives from the GNU Project, which he founded to develop a free operating system. Stallman, who prefers to be called rms, got his start hacking at MIT. He worked as a "staff hacker" on the Emacs project and others. He was a critic of restricted computer access in the lab. When a password system was installed, Stallman broke it down, resetting passwords to null strings, then sent users messages informing them of the removal of the password system.

Stallman's crusade for free software started with a printer. At the MIT lab, he and other hackers were allowed to modify code on printers so that they sent convenient alert messages. However, a new printer came along – one that they were not allowed to modify. It was located away from the lab and the absence of the alerts presented an inconvenience. It was at this point that he was "convinced…of the ethical need to require free software."

With this inspiration, he began work on GNU. Stallman wrote an essay, "The GNU Project," in which he recalls choosing to work on an operating system because it's a foundation, "the crucial software to use a computer." At this time, the GNU/Linux version of the operating

system uses the Linux kernel started by Torvalds. GNU is distributed under "copyleft," a method that employs copyright law to allow users to use, modify, copy and distribute the software.

Tsutomu Shimomura: Shimomura reached fame in an unfortunate manner: he was hacked by Kevin Mitnick. Following this personal attack, he made it his cause to help the FBI capture him.

Black hat hackers

Black hat hackers are those who work to exploit the computers. Some of them do it for fun and curiosity, while others are looking for personal gain.

Jonathan James: James gained notoriety when he became the first juvenile to be sent to prison for hacking. He was sentenced at 16 years old. He installed a backdoor into a Defense Threat Reduction Agency server. The DTRA is an agency of the Department of Defense charged with reducing the threat to the U.S. and its allies from nuclear, biological, chemical, conventional and special weapons. The backdoor he created enabled him to view sensitive emails and capture employee usernames and passwords. James also cracked into NASA computers, stealing software worth approximately $1.7 million. According to the Department of Justice, "The software supported the International Space Station's physical environment, including control of the temperature and humidity within the living space." NASA was forced to shut down its computer systems, ultimately racking up a $41,000 cost.

Adrian Lamo: Lamo's claim to fame is his break-ins at major organizations like The New York Times and Microsoft. His hits include Yahoo!, Bank of America, Citigroup and Cingular. When he broke into The New York Times' intranet, things got serious. He added himself to a list of experts and viewed personal information on contributors, including Social Security numbers. Lamo also hacked into The Times' LexisNexis account to research high-profile subject matter.

For his intrusion at The New York Times, Lamo was ordered to pay approximately $65,000 in restitution.

Lamo is currently working as an award-winning journalist and public speaker.

Kevin Mitnick: The Department of Justice describes him as "the most wanted computer criminal in United States history. He started out exploiting the Los Angeles bus punch card

system to get free rides. Then, like Apple co-founder Steve Wozniak, dabbled in phone phreaking. Although there were numerous offenses, Mitnick was ultimately convicted for breaking into the Digital Equipment Corporation's computer network and stealing software.
Today, Mitnick has been able to move past his role as a black hat hacker and become a productive member of society. He served five years, about 8 months of it in solitary confinement, and is now a computer security consultant, author and speaker.

Robert Tappan Morris: Morris, son of former National Security Agency scientist Robert Morris, is known as the creator of the Morris Worm,the first computer worm to be unleashed on the Internet. As a result of this crime, he was the first person prosecuted under the 1986 Computer Fraud and Abuse Act.
Morris is currently working as a tenured professor at the MIT Computer Science and Artificial Intelligence Laboratory. He principally researches computer network architectures including distributed hash tables such as Chord and wireless mesh networks such as Roofnet.

CONCLUSION

Hackers will always find ways of getting into systems. The bottom-line is we are losing the war. Businesses must be able to defend themselves to prevent the loss of money, technology, and secrets. Technology has advanced in leaps and bounds beyond our current laws. As new laws are explored, old ones amended, and solutions sought, let's think outside the box and give the good guys the advantage, or at least a fighting chance. Until then, let's stop automatically assuming we are not allowed to defend ourselves. We can and the law allows it. We just need to be very careful and methodical about it, and not harm our neighbour or trample on his privacy rights. Not vigilantism, but clear, forward, out-of-the-box thinking, and analysis to put us back in the game.

REFERENCES

http://www.cyberlawsindia.net/
http://dict.mizoram.gov.in/uploads/attachments/cyber_crime/hacking-indian-laws.pdf
http://en.wikipedia.org/wiki/Hacker_(computer_security)
http://timesofindia.indiatimes.com/tech/social-media/Get-insured-against-hacking-on-Facebook-Twitter/articleshow/16448687.cms
http://searchsecurity.techtarget.com/definition/ethical-hacker

http://en.wikipedia.org/wiki/Certified_Ethical_Hacker
http://www.ethicalhacking.com/
http://articles.timesofindia.indiatimes.com/2012-05-14/job-trends/31700173_1_ethical-hacker-malicious-hacker-information-security
http://articles.economictimes.indiatimes.com/2010-05-16/news/27630802_1_ethical-hackers-professional-hacker-cyber-security
http://www.i3indya.com/workshop/information-security/ethical-hacking-cyber-security-workshop-details.html
http://www.research.ibm.com/antivirus/SciPapers.htm

- *Hacking: The Art of Exploitation, Second Edition* by Jon Erickson
- *The Hacker Crackdown*
- *The Art of Intrusion* by Kevin D. Mitnick
- *The Art of Deception* by Kevin D. Mitnick
- *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker* by Kevin D. Mitnick
- E. S. Raymond, *The New Hacker's Dictionary*, MIT Press,Cambridge, MA (1991)