International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

ETHICAL HACKING: TYPES OF ETHICAL HACKERS

V.Chandrika

Lecturer, Dept of Computer Science, KBN College, Vijayawada, Andhra Pradesh, India

vutukurichandrika@gmail.com

***Abstract*— 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. 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 Internet. This paper explores the ethics behind ethical hacking and whether there are problems that lie with this new field of work.**

I. INTRODUCTION

More and more organisations are being targeted in cyber-attacks, and they must get to know their enemy if they are to protect vital networks. Meet the professional, ethical hacker.

Nasty, evil, devious, manipulative: adjectives commonly planted in front of the term 'hacker'. But stick the word 'ethical' in front of it, and you may just have struck on a useful concept. Of course, 'ethical hacker' sounds like an oxymoron: how can such a disruptive, destructive coder ever lay claim to a code of ethics?

With the rise of cyber-crime, ethical hacking has become a powerful strategy in the fight against online threats. In general terms, ethical hackers are authorised to break into supposedly 'secure' computer systems without malicious intent, but with the aim of discovering vulnerabilities in order to bring about improved protection.

Sometimes the local IT managers or security officers in an organisation will be informed that such an attack – usually called a 'penetration test' – is to take place, and may even be looking over the hacker's shoulder; but often they are not, and knowledge of an attack is confined to very senior personnel, sometimes even just two or three board members. Some ethical hackers work for consultants; others are salaried staffers, who conduct a scheduled programme of hacks on a regular basis.

A number of specialism's exist within the general discipline of ethical hacking; for this reason it is impossible to group all 'hackers' into a comprehensive category. An ethical hacker, also referred to as a 'white-hat' hacker or 'sneaker', is someone who hacks with no malicious intent and is assisting companies to help secure their systems. However, a 'black-hat' hacker is the opposite and will use his or her skills to commit cybercrimes, typically to make a profit. In between are hackers known as 'grey-hat' hackers, who will search for vulnerable systems and inform the company but will hack without permission?

With the growth of the Internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being hacked. At the same time, the potential customers of these services are worried about main-taining control of personal information that varies from credit card numbers to social security numbers and home addresses.

II. HACKER HISTORY

In 1974, the Multics (Multiplexed Information and Computing service) operating systems were then renowned as the most secure OS available. The United States Air Force organised an 'ethical' vulnerability analysis to test the Multics OS and found that, though the systems were better than other conventional ones, they still had vulnerabilities in hardware and software security.

As companies begin to employ ethical hackers, the need for IT specialists with accredited skills is growing, but ethical hackers require support too. Shortly after the 11 September 2001 terrorist attacks on the World Trade Center, Jay Bavisi and Haja Mohideen co-founded the International Council of Electronic Commerce Consultants (EC-Council), a professional body that aims to assist individuals in gaining information security and e-business skills.

Government institutions have recognised the benefits in using ethical hackers; the problem is where to find them. In 2011, UK intelligence agency GCHQ launched 'Can You Crack It?', an online code-breaking challenge in the aim to recruit 'self-taught' hackers to become the next generation of cyber security specialists. Early in 2012 GCHQ also unveiled a cyber-incident response (CIR) pilot scheme. This initiative launched by the agency's Communications-Electronics Security Group (CESG) and the Centre for Protection of National Infrastructure (CPNI), will provide a range of support from tactical, technical mitigation advice to guidance on the use of counter-measures to improve the quality of security within the public sector and critical national infrastructure organisations.

At present, data-intelligence provider BAE Systems Detica and security providers Cassidian, Context IS, and Mandiant have been selected by CESG and CPNI to work in partnership to provide support. A GCHQ spokesperson revealed both GCHQ and CPNI have not incurred any additional costs in establishing the scheme, but in line with other certification schemes they will charge an annual certification fee when the CIR scheme is launched in 2013.

"We certify 'ethical hacking' companies ourselves to undertake penetration testing of government IT systems, and work with industry schemes CREST and TIGER in setting the right standards for these companies to work to," adds a GCHQ spokesperson.

How ethical is 'ethical'?

Even though more enterprises are actively recruiting ethical hackers, for some there remains a hesitation when it comes from letting a licensed attacker loose on corporate information systems. According to the report 'When is a Hacker an "Ethical Hacker" – He's NOT' by AlienVault's research engineer Conrad Constantine, an 'ethical' hacker simply does not exist, and it is the contradictory job title that is the problem.

"The term 'ethical' is unnecessary – it is not logical to refer to a hacker as an 'ethical hacker' because they have moved over from the 'dark side' into 'the light'," Constantine argues. "The reason companies want to employ a hacker is not because they know the 'rules' to hacking, but because of the very fact that they do not play by the rules."

Constantine adds: "Some hackers would argue that they're not criminals, but activists. Others would say that they're just rebellious in the way they think about technology and have a duty to highlight an organisation's poor security. My personal view is that we need people who are willing to stand up and challenge authority – in so doing, does that then make them ethical? I don't see why it should, it is still hacking – end of argument."

Supporting this, Faronics project management vice president Dmitry Shesterin asks: "Have you ever heard of an ethical hacker that has started off as an ethical hacker? I have not."

"Experts do not typically adhere to textbook coding practices, and can uncover problems, vulnerabilities, or business practices of varying shades of 'ethical' – something they were not supposed to uncover," adds Shesterin. "So the concern often remains, how ethical is an ethical hacker?"

III. TEN TYPES OF CYBER HACKER

The basic definition for a hacker is someone who breaks into computer networks or personal computer systems either for a challenge or to gain profit.

These days the computer news media uses the terms hacker and cybercriminal more or less interchangeably. That can be misleading. While their meanings overlap, they are not exactly the same thing in all contexts.

A cybercriminal is just what the name implies, a person who uses computer technology to commit a crime for which that person can be prosecuted. The crime usually involves illegally gaining access to one or more computer systems to steal information, take them offline or both, either for malicious purposes or financial gain. Breaking into computer systems involves hacking, so a cybercriminal can be considered a type of hacker.But there are hackers who do this sort of thing legally, so you can't always associate a hacker or hacking with criminal activity.

White-hat

A 'white-hat' hacker, also referred to as an ethical hacker, is someone who has non-malicious intent whenever breaking into security systems. The majority of white-hat hackers are security experts, and will often work with a company to legally detect and improve security weaknesses.

A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them.

White hat hackers are usually seen as hackers who use their skills to benefit society. They may be reformed black hat hackers or they may simply be well-versed in the methods and techniques used by hackers. An organization can hire these consultants to do tests and implement best practices that make them less vulnerable to malicious hacking attempts in the future.For the most part, the term is synonymous with "ethical hacker." The term comes from old Western movies where the cliché was for the "good guy" to wear a white cowboy hat. Of course, the "bad guys" always seemed to wear a black hat.

Black-hat

A 'black-hat' hacker, also known as a 'cracker', is someone who hacks with malicious intent and without authorisation. Typically the hacker wants to prove his or her hacking abilities and will commit a range of cybercrimes, such as identity theft, credit card fraud and piracy.A black hat hacker is an individual with extensive computer knowledge whose purpose is to breach or bypass internet security.

Black hat hackers are also known as crackers or dark-side hackers. The general view is that, while hackers build things, crackers break things. They are computer security hackers that break into computers and networks or also create computer viruses. The term "black hat" comes from old westerns where the bad guys usually wore black hats and the good guys wore white ones. White hat hackers also identify security weaknesses; but, instead of performing malicious attacks and theft, they expose the security flaw in such a way as to alert the owner that there is a breach so they can fix it before a black hat hacker can take advantage of it. Though they often start out as black hat hackers, white hat hackers sometimes are paid consultants or actual employees of a company that needs its systems protected.

In the security industry, the distinction is made between white hat and black hat hackers. Organizations hire white hat hackers – sometimes referred to as ethical hackers - to probe and break into their computer systems to determine the extent to which these systems are secure and make recommendations to improve security. They frequently make full disclosures of their findings so the greater security community can benefit from the information they collect. White hat hackers' activities are legal since they sanctioned by their clients.

Black hat hackers, on the other hand, are cybercriminals whose intent is entirely malicious. Without invitation, they plunder computer systems for their own gain at considerable expense to their victims.

There was a time when black hat hackers were referred to as crackers because their computer break-ins were analogous to safe cracking by bank thieves. But I haven't seen the term cracker used in quite some time, so it seems to have gone out of fashion.Even the term black hat can be a little misleading. There is an important series of conventions called Black Hat that is attended by security experts and students – many of them white hat hackers – to learn about the latest trends and tools in the computer security industry.

Grey-hat

Like the colour suggests a 'grey-hat' hacker is somewhere between white-hat and black-hat hackers, as he or she exhibits traits from both. For instance, a grey-hat hacker will roam the Internet in search of vulnerable systems; like the white-hat hacker, the targeted company will be informed of any weaknesses and will repair it, but like the black-hat hacker the grey-hat hacker is hacking without permission.

Gray hat describes a cracker (or, if you prefer, hacker) who exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners.To a certain extent, hacktivists blur the distinction between white hat and black hat hackers. They often get involved in illegal activities but, as we've seen with Anonymous, for causes that can in some cases can be considered just. I would put hacktivists in another category of hacker known as grey hat.

The term grey hat was coined by the hacker group L0pht back in 1998. It was originally used to describe hackers who report the vulnerabilities they find to the organizations whose computers security they breach. Later in 2002, the Anti-Sec community used the term to describe people that work in the security community during the day and work as black hat hackers on off hours.

Since 2002 grey hat has taken on diverse meanings. The Electronic Frontier Foundation, a non-profit digital rights advocacy group, defined grey hats as ethical hackers who inadvertently or intentionally violate the law to research and improve security. It is this definition that I think best applies to hacktivists, except that they are not so much interested in improving security as they are in advancing their political causes.

Blue Hat

External computer security consulting firms are employed to bug-test a system prior to its launch, looking for weak links which can then be closed. Blue Hat is also associated with an annual security conference held by Microsoft where Microsoft engineers and hackers can openly communicate.

A blue hat hacker is someone outside computer security consulting firms who bug tests a system prior to its launch, looking for exploits so they can be closed. Blue Hat Hacker also refers to the security professional invited by Microsoft to find vulnerabilities in Windows. The term has also been associated with th annual security conference by Microsoft, the unofficial name coming from the blue color associated with Microsoft employee badges.

Elite hacker

These types of hackers have a reputation for being the 'best in the business' and are considered as the innovators and experts. Elite hackers used an invented language called 'Leetspeak' to conceal their sites from search engines. The language meant some letters in a word were replaced by a numerical likeness or other letters that sounded similar.

Hacker is a term commonly used to refer to an individual who secretly gains access into systems and networks for the purpose of earning money. Some, however, practice the creative art of hacking for the reason that they get a certain level of enthusiasm from the test that they are being put into. During the early years, hackers were considered to be as computer underground. The culture only progressed through time and is now regarded as an open community.

Elite hacker is the name utilized by the community with the aim of identifying those individuals who are deemed to be as

experts in their line of work. These people are actually on the "cutting edge" of both the computer and network industry.

Hacktivist

Someone who hacks into a computer network, for a politically or socially motivated purpose. The controversial word can be constructed as cyber terrorism as this type of hacking can lead to non-violent to violent activities. The word was first coined in 1996 by the Cult of the Dead Cow organisation.

During the last several years a new class of hacker has emerged, the so-called hacktivist, who engages in hacking of computer networks and systems as a form of protest. You've probably heard about the group known as Anonymous, a collective of clandestine – and yes, anonymous – hackers who have taken down and infiltrated computer systems belonging to companies and governments with whom they have political disagreements.

Hacktivism does not fit neatly into either white hat or black hat categories. Unlike either their white hat or black hat counterparts, hacktivists are motivated by politics not profit. They find themselves at ideological odds with many organizations and feel justified in their computer attacks against them.

However, depending on whether or not you agree with a given hacktivist group's point of view, you could see hacktivists as either white hats or black hats. In October, 2011, Anonymous took down 40 child pornography websites and publicly revealed the names of over 1500 people who frequented those sites.

But the group also attacked computers belonging to the Bay Area Rapid Transit (BART) and leaked personal information of over 2000 BART users on the Internet. This was done in retaliation for BART officials shutting off cell phone service to prevent people from communicating to coordinate a protest against a police shooting on a BART train. Whether or not Anonymous agrees with BART's actions is not really the important thing. The group took action against BART without due process and leaked personal information of BART users who were unlucky enough to get caught in the crossfire of this feud.

Amateur hac

Amateur hacker who follows directions and uses scripts and shell codes from other hackers and uses them without fully understanding each step performed. The insecure nature of wireless security has been highlighted by a global demonstration illustrating the ease with which such networks can be accessed.

Amateur wireless LAN sniffers detected hundreds and potentially thousands of insecure business and home industry-standard wireless LANs in North America and Europe during the past week, in an electronic scavenger hunt dubbed the "Worldwide Wardrive".Security analysts and wireless LAN industry executives said the results of the week-long Worldwide Wardrive indicate that many wireless LAN users still fail to use the most elementary form of security to protect their systems.

The Worldwide Wardrive was an exercise in detecting wireless LANs using free software called NetStumbler. While the demonstration was conducted by people who describe themselves as hobbyists, analysts warned that malevolent hackers and industrial or foreign espionage agents could easily exploit the holes found. According to analysts, home users had the least secure wireless LANs but the hobbyists also detected hundreds of potentially vulnerable corporate or government networks. Part of the problem concerns the Service Set Identifier (SSID), an identifier of up to 32 characters continuously transmitted by an 802.11b or Wi-Fi access point device.

Brian Grimm, a spokesman for the Wireless Ethernet Compatibility Alliance, a wireless LAN industry trade group said: "Everyone should turn off their SSIDs." If it is switched on a hacker can very easily detect the presence of a wireless LAN. Grimm said enterprises should beef up their security with virtual private networks and filtering of Media Access Control (MAC) addresses. Each piece of hardware on a network has a unique MAC address, and filtering these addresses reduces the possibility of a hacker mapping and penetrating a network. The large number of insecure LANs detected during Worldwide Wardrive week should serve as a wake-up call to corporate IT departments, said Chris Kozup, an analyst at Meta. "The enterprise needs to be taking a more activist approach to wireless LAN security," he said.

Spy hackers

Corporations hire hackers to infiltrate the competition and steal trade secrets. They may hack in from the outside or gain employment in order to act as a mole. Spy hackers may use similar tactics as hacktivists, but their only agenda is to serve their client's goals and get paid.Online shopping, online banking and general storage of personal information on personal computers have made consumers more vulnerable to identity theft than ever before. You now have to worry about hackers, spyware, and Trojan horse programs. With the right software, hackers can crack your login information including usernames and passwords. With this information, they can access your bank accounts, credit card accounts and other types of accounts.

Spyware and Trojan horse programs can be even more dangerous. They are both forms of malicious software also called malware. Spyware is software that is installed on your computer either directly or inadvertently. It runs in the background of your computer and secretly monitors different programs. It can be used to monitor your keystrokes, for example, and steal your login information to different sites. It can also monitor your Internet activity--which pages you visit, what things you buy, etc. Some parents use spyware to monitor their child's computer usage. It is more deviously and illegally used by con artists looking to steal identities.

A Trojan horse program is similar to spyware except that it is packaged as another program. These programs are much like the ancient story of Troy where the Greeks presented the Trojans with a large wooden horse as a peace offering. While the city slept, Greek soldiers emerged from the horse and attacked. A Trojan horse computer program also masquerades as something innocuous like a computer game. When you download it from the Internet, you also unwittingly download the malware. This program creates what is known as a "backdoor" to your computer, which thieves can use to obtain your sensitive information. Additional sinister uses of Trojan horses can be to spy on you through your microphone and web cam (if you have one), use your email to send spam messages and use your computer to store or traffic illegal files like child pornography.

These programs that infect your computer can be there for ages without you even knowing. The best programs are designed to operate stealthily behind the scenes. In some cases, you may notice your application running slowly or unexpectedly quitting. Few people will attribute such problems to malware, however. The most effective way to defend your computer against malware is with a good firewall application. Firewalls are programs that serve as a barrier between your computer and outside networks. They restrict unauthorized users from accessing your network.

Cyber terrorists

These hackers, generally motivated by religious or political beliefs, attempt to create fear and chaos by disrupting critical infrastructures. Cyber terrorists are by far the most dangerous, with a wide range of skills and goals. Cyber Terrorists' ultimate motivation is to spread fear, terror and commit murder. According to the U.S. Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. Cyberterrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

Cyberterrorism is a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any instances of cyberterrorism.

Cyberterrorism can be also defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives.Objectives may be political or ideological since this is a form of terrorism.There is much concern from government and media sources about potential damages that could be caused by cyberterrorism, and this has prompted official responses from government agencies.

Mobile hackers

These days individuals store everything on their mobile phones, from personal information such as contact numbers and addresses to credit card details. For these reasons mobile phones are increasingly becoming attractive to hackers-on-the-hoof, either by hacking faulty mobile chips or point-to-point wireless networks, such as Bluetooth. Mobile hacking is the remote, unauthorized access and manipulation of another person's mobile phone. This type of unethical mobile hacking is typically accomplished through the exploitation of defects or glitches in mobile chips or wireless devices such as Bluetooth. For the most part, mobile hacking is used to make phone calls for free or to gather personal information such as addresses and phone numbers.

To hack an electronic device is to devise or modify a computer program skillfully. Hacking involves the skillful manipulation of existing rules to accomplish results typically unanticipated by the original programmer. According to "PC Magazine," to hack a computer-based appliance such as a mobile phone is to enhance or modify a devise that's "not at all user programmable." Phone hacking is a term used to describe the practice of accessing the voicemail messages of a mobile phone without the consent of the phone's owner.

In the UK phone hacking came to prominence during the scandals in which it was alleged (and in some cases proved in court) that newspapers were involved in the accessing of mobile phone voicemail messages of the British Royal Family, other public figures, and members of the public.

Fixed line phone hacking can also mean intercepting telephone calls to listen to the call in progress. This can be done by placing a recorder on the physical telephone line, or by placing a recorder or short range transmitter in the telephone handpiece.intercepting mobile telephone calls to listen to the call in progress taking covert control of the mobile phone to receive copies of text messages and other activity, and to remotely listen to activity around the phone.This is done by installing software on the phone to provide the functionality that is remotely accessed. The phone user is not aware of the operation of the software. Information is sent using the phone data capability and is not readily identifiable from the phone bill.

There are also flaws in the implementation of the GSM encryption algorithm which allow passive interception. The equipment needed can be built from freely available parts and designs are available on the internet. Mobile operators are updating the encryption software to overcome this flaw but it has yet to be updated by all operators. Another approach is called bluesnarfing, which is unauthorized access to a phone via Bluetooth. This can only be done by someone close to the mobile phone due to the short range of bluetooth. Guarding against unauthorised voicemail access. Security of any device is a compromise between ease of use and security. Generally the easier to use then the less secure. Many electronic devices, such as mobile phones, the ease of use is a prime

consideration. Security is an 'inconvenience' that the user does not want.

The consequence of this is that the devices and services can often easily be hacked. If you want high security expect to have some inconvenience. Until such times as we are all 'chipped' at birth, as many pet dogs are, we will have to put up with the inconvenience of passwords and authentication devices if you want good security.

The password is the weakness in the security of voicemail systems. Mobile phones allow access to voicemail messages via a fixed line telephone, requiring the entry of a Personal Identification Number (PIN) to listen to the messages. Many mobile phones are supplied with a factory default PIN which not all voicemail systems force to be changed on first use. These default numbers are available on the internet. You MUST always change the default PIN / password. Research has shown that the most common PIN numbers are "1234" and "0000". Year of birth, graduation, marriage, birth of child are also common. These are all numbers that are easy to guess if someone knows some background information about you.

IV. CONCLUSION

From a practical standpoint the security problem will remain as long as manufacturers remain com-mitted to current system architectures, produced without a requirement for security. As long as there is support for ad hoc and security pack-ages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of a computer system security, proper security will not be a reality. Regular auditing, vigilant intrusion detection, good system administration practice, and computer security awareness are all essential parts of an organization's security efforts. A single failure in any of these areas could very well expose an organization to cyber-vandalism, embarrassment, loss of revenue or mind share, or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place.

V. REFERENCES

[1] H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.

[2] Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002.

[3] Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375-379, 2002.

[4] B. Reto, "Ethical Hacking", in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24, 2002.

[5] B. Kevin, "Hacking for dummies", 2nd edition, 408 pages, Oct 2006.

[6] D. Manthan "Hacking for beginners", 254 pages, 2010.

[7] my.safaribooksonline.com/.../introduction-to-ethical-hacking-ethics-legality.

[8] J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.

[9] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , "Ethical Hacking " , International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.

[10] media.techtarget.com/search Networking- Introduction to ethical hacking-Tech Target.