WE DONOT FORGIVE,WE DONOT FORGET,WE ARE HACKERS-HEROS OF COMPUTER REVOLUTION…KEEP CALM AND EXPECT US

Divya Peddapalyam[1], Dr.Satya Narayana chowdhary[2], Chaya Devi[3]
[1]Msc.Biotechnology,Garden City University, Bengaluru, Karnataka,India
[2]M.Tech;PhD;Computer Science, Passion for code-(Director);Hyderabad, Telangana,India
[3]Msc.Computer Science; Passion for code-(Faculty)Hyderabad; Telangana;India

Abstract- ***The incidences of computer hacking have increased dramatically over the years. Indeed, the current federal laws, including the Computer Fraud and Abuse Act, have done very little to deter potential computer hackers. This article finds that only a small percentage of computer hackers are ever caught and prosecuted. The biggest problem is that most victimized companies regrettably choose to hide the problem from the public due in part to negative publicity concerns. As a result, this article proposes that a mandatory reporting requirement imposed by Congress, which forces companies to disclose intrusions, will be salient to the problem of computer hacking in several regards. First, individuals who are affected by the intrusions will receive advance warning that their personal information was stolen by hackers. This will allow these affected individuals to take precautions in securing their identities. Secondly, the mandatory reportings will assist law enforcement in investigating and prosecuting a greater percentage of computer hackers. As more prosecutions of computer hackers are publicized, this should reduce the future incidences of computer hackings. Moreover, on July 1, 2003, California became the first state to enact a reporting requirement for computer hackings. This could provoke other states to pass similar reporting requirements. Because computer hacking is a national (and international) problem, Congress needs to consider enacting a reporting requirement before an untenable piecemeal state-by-state solution occurs.On the whole this review explains the seven documentation parts of our work entitled "Hacking Issues". Documentation proceeded by Ms.Divya Peddapalyam, Dr.Satya Narayana Chowdhary and Mr.Chaya Devi.Along with these we used some google links to increase the content of the paper.***

Keywords- computer, hacking, hacker, intrusion, software security, cybercrime, identity theft

I. INTRODUCTION

Computer hackings have grown at an alarming rate and the effects are widespread and costly. Each year hackers steal millions of dollars worth of proprietary information from companies and organizations. A survey by the Computer Security Institute indicated that for the year 2002, theft of proprietary information by hackers cost companies and organizations over $70 million. The cost to insure against these hackers is staggering— the market for hacker insurance is expected to increase from $100 million in 2003 to $900 million by 2005.In addition, hackers can cause severe damage to computer systems by altering or deleting data files and disabling software. In addition to proprietary information, hackers also steal personal information from these organizations and corporations including their customers' credit card numbers, account numbers, and social security numbers. For example, in 2000, hackers stole 55,000 credit card numbers from creditcards.com and 300,000 credit card numbers from CDUniverse.com.The theft of personal information such as credit card numbers raises serious concerns relating to both identity theft and privacy. Even more disconcerting than the theft of proprietary and personal information is the fact that most companies and organizations are not reporting hacking incidents to law enforcement.

II. DISCUSSION

According to surveys from 1999 to 2003, only about 30% of hacking intrusions are ever reported. Further, Internet technology presents high hurdles for law enforcement to trace the hacking intrusions back to the hacker. This means that the vast majority of hackers have very little chance of being caught and prosecuted.Because tackling the area of computer hacking requires an understanding of the technical issues involved, an Appendix is included, which will introduce the numerous tools that hackers use to accomplish their intrusive hacking attacks. Knowledge of this is necessary to appreciate the applicability of the current laws to these tools. Some readers may find it helpful to reference the Appendix before beginning Part II of the paper, which covers the scope of several federal laws commonly used against hackers.Part III of the paper will evaluate the technical, societal, and legal failures that result in hackers not being caught or prosecuted.

Against this background, Part IV of this paper proposes a national reporting requirement to tackle the problem of computer intrusions with respect to the computer networks of organizations and corporations. The term "hacker" has a dual usage in the computer industry today. Originally, the term was defined as: "A person who enjoys learning the details of computer systems and how to stretch their capabilities-as opposed to most users of computers, who prefer to learn only the minimum amount necessary. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming". This complimentary description was often extended to the verb form "hacking," which was used to describe the rapid crafting of a new program or the making of changes to existing, usually complicated software. Because of the increasing popularity of computers and their continued high cost, access to them was usually restricted. When refused access to the computers, some users would challenge the access controls that had been put in place. They would steal passwords or account numbers by looking over someone's shoulder, explore the system for bugs that might get them past the rules, or even take control of the whole system. They would do these things in order to be able to run the programs of their choice, or just to change the limitations under which their programs were running. Initially these computer intrusions were fairly benign, with the most damage being the theft of computer time. Other times, these recreations would take the form of practical jokes. However, these intrusions did not stay benign for long. Occasionally the less talented, or less careful, intruders would accidentally bring down a system or damage its files, and the system administrators would have to restart it or make repairs. Other times, when these intruders were again denied access once their activities were discovered, they would react with purposefully destructive actions. When the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage inflicted, it became "news" and the news media picked up on the story. Instead of using the more accurate term of "computer criminal," the media began using the term "hacker" to describe individuals who break into computers for fun, revenge, or profit. Since calling someone a "hacker" was originally meant as a compliment, computer security professionals prefer to use the term "cracker" or "intruder" for those hackers who turn to the dark side of hacking. For clarity, we will use the explicit terms "ethical hacker" and "criminal hacker" for the rest of this paper.The national reporting requirement framework will propose one set of reporting requirements when privacy is at stake and another set of reporting requirements aimed at deterring property damage by hackers. Part V will then illustrate how such a framework for a national reporting requirement could help bridge the current technical, societal, and legal shortcomings discussed in Part III and thus reduce the number of computer intrusions in business and organizational computer networks as a whole. Finally, Part VI anticipates and responds to several major arguments against a reporting requirement.

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 maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses. In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. This scheme is similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "tiger teams" or "ethical hackers" would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them. This method of evaluating the security of a system has been in use from the early days of computers. In one early ethical hack, the United States Air Force conducted a "security evaluation" of the Multics operating systems for "potential use as a two-level (secret/top secret) system." Their evaluation found that while Multics was "significantly better than other conventional systems," it also had " … vulnerabilities in hardware security, software security, and procedural security" that could be uncovered with "a relatively low level of effort." The authors performed their tests under a guideline of realism, so that their results would accurately represent the kinds of access that an intruder could potentially achieve. They performed tests that were simple information-gathering exercises, as well as other tests that were outright attacks upon the system that might damage its integrity. Clearly, their audience wanted to know both results. There are several other now unclassified reports that describe ethical hacking activities within the U.S. military. With the growth of computer networking, and of the Internet in particular, computer and network vulnerability studies began to appear outside of the military establishment. Most notable of these was the work by Farmer and Venema, which was originally posted to Usenet in December of 1993. They discussed publicly, perhaps for the first time, this idea of using the techniques of the hacker to assess the security of a system. With the goal of raising the overall level of security on the

Internet and intranets, they proceeded to describe how they were able to gather enough information about their targets to have been able to compromise security if they had chosen to do so. They provided several specific examples of how this information could be gathered and exploited to gain control of the target, and how such an attack could be prevented. Farmer and Venema elected to share their report freely on the Internet in order that everyone could read and learn from it. However, they realized that the testing at which they had become so adept might be too complex, time-consuming, or just too boring for the typical system administrator to perform on a regular basis. For this reason, they gathered up all the tools that they had used during their work, packaged them in a single, easy-to-use application, and gave it away to anyone who chose to download it. Their program, called Security Analysis Tool for Auditing Networks, or SATAN, was met with a great amount of media attention around the world. Most of this early attention was negative, because the tool's capabilities were misunderstood. The tool was not an automated hacker program that would bore into systems and steal their secrets. Rather, the tool performed an audit that both identified the vulnerabilities of a system and provided advice on how to eliminate them. Just as banks have regular audits of their accounts and procedures, computer systems also need regular checking. The SATAN tool provided that auditing capability, but it went one step further: it also advised the user on how to correct the problems it discovered. The tool did not tell the user how the vulnerability might be exploited, because there would be no useful point in doing so.

While there is also the problem of hacking into personal computers, this paper does not intend to address that problem. However, as will be discussed in Part III of the paper, many hackers take control of personal computers for the purpose of launching hacking attacks on corporate computers. Accordingly, it is conceivable that reducing the number of corporate and organizational hacking intrusions will result in a proportionate decline in the number of personal computers attacked. This section covers the federal approaches applicable to computer crimes that may be relevant to the problem of computer hacking. The author realizes that some states may have their own laws tailored toward various computer crimes, like the variations of the proposed Federal Computer Systems Protection Act. Further, many practitioners have been creative in applying common law approaches along with other state laws (such as trade secrets law) to the area of cybercrime. However, because of the numerous jurisdictional limitations of state laws and because computer hacking is not limited by state borders, this paper focuses on the two main federal laws relevant to computer hacking—the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. The Electronic Communications Privacy Act of 1986 ("ECPA") was Congress's patchwork attempt to fit new crimes into the existing laws.Title I of the ECPA amended the Federal Wiretap Act, 18 U.S.C. §§ 2510 et al., to include not only wire or oral communications, but also electronic communications. Title II of the ECPA created the Stored Communications Act. The coverage of both the Federal Wiretap Act and the Stored Communications Act is described below. Title I of the ECPA amended the Federal Wiretap Act to cover not only wire and oral communications, but also electronic communications. The current version of the Wiretap Act prohibits intentionally intercepting (or endeavoring to intercept) any wire, oral, or electronic communication. In addition, the Wiretap Act punishes disclosing or using the contents of any wire, oral, or electronic communication with knowledge that the information was obtained through the prohibited interception of a wire, oral, or electronic communication.

A large blow to the effectiveness of the Wiretap Act against computer hackers was the judicially-interpreted requirement of an "acquisition contemporaneous with transmission." This means that hackers that obtain information through their intrusive attacks do not violate the Wiretap Act unless they capture the information while it is being transmitted from one computer to another. Presumably, the Wiretap Act applies to hackers who install network packet sniffers ("sniffers") to intercept real-time communications. This is because sniffers capture network data packets while they are in transmission, and thus the acquisitions of the data packets by the sniffers are contemporaneous with their transmission from one computer to another. Unfortunately, the case law is absolutely devoid of examples of prosecutions in such cases. The Stored Communications Act ("SCA") was created by Title II of the ECPA. Title U.S.C. § 2701(a) of the SCA punishes "whoever— intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to wire or electronic communication

attack is an "electronic communication service." An electronic communication service is defined as "any service which provides to users thereof the ability to send or receive wire communications." An email server would clearly fit this definition as would Internet Service Providers. However, courts have determined that personal computers are not electronic communication services within the purview of the SCA. Unfortunately, this means that if the hacker breaks into a computer that is not a qualifying electronic communication service, then the SCA does not apply. This limitation has curbed the effectiveness of the SCA against computer hackers. Title 18 U.S.C. § 1030, otherwise known as the Computer Fraud and Abuse Act ("CFAA"), is currently the most targeted and comprehensive federal law directed towards computer-related criminal conduct. The premise behind the enactment of the CFAA was to "deter and punish those who intentionally access computer files and systems without authority and cause harm." The CFAAcontains seven substantive provisions. Each of the seven provisions will be introduced according to its statutory order.First, section 1030(a)(1) prohibits knowingly accessing a computer without authorization or exceeding authorization, thereby obtaining and subsequently transferring classified government information.Next, section 1030(a)(2), which is highly applicable to intrusive computer hackers, proscribes intentionally accessing a computer without authorization or exceeding authorization and obtaining information from a financial institution, any department or agency of the United States, or any protected computer involved in interstate or foreign communication.Section 1030(a)(3) makes it a crime to intentionally, without authorization, access a nonpublic computer of a department or agency of the United States.Section 1030(a)(4) prohibits knowingly and with intent to defraud, accessing a protected computer without authorization (or in excess of authorization) and thereby obtaining anything of value greater than $5,000 within any 1-year period.Section 1030(a)(5)(A) is the main anti-hacking provision and contains three types of offenses. Subsection 1030(a)(5)(A)(i) proscribes knowingly causing the transmission of a program, information, code, or command, and as a result, intentionally causing damage without authorization to a protected computer. Prior to the amendment by the USA PATRIOT Act of 2001 ("PATRIOT Act"), the CFAA defined damage as "any impairment to the integrity or availability of data, a program, a system, or information that--(A) causes loss. aggregating at least $5,000 in value during any 1-year period to one or more individuals." Following the amendments by the PATRIOT Act, the CFAA eliminated the $5,000 jurisdictional requirement in criminal cases and damage is now broadly defined as "any impairment to the integrity or availability of data, a program, a system or information." While subsection 1030(a)(5)(A)(i) focuses more on intentionally causing damage (without regard to authorization), subsection 1030(a)(5)(A)(ii) focuses on intentionally accessing a protected computer without authorization. Subsection 1030(a)(5)(A)(ii) proscribes intentionally accessing a protected computer without authorization and thereby recklessly causing damage. Finally, subsection 1030(a)(5)(A)(iii) proscribes intentionally accessing a protected computer without authorization and thereby causing damage.Section 1030(a)(6) prohibits the trafficking of passwords through which a computer may be accessed without authorization.Finally, section 1030(a)(7) makes it a crime for someone to transmit a communication in interstate or foreign commerce that threatens damage to a protected computer for the intent of extorting money or other things of value. Of the seven prohibitions listed in the CFAA, two of these are particularly important to the prosecution of intrusive computer hackers— namely sections 1030(a)(2) and 1030(a)(5).As stated above, section 1030(a)(2) applies to a hacker who intentionally accesses a computer without authorization or exceeds authorization and obtains information from a protected computer involved in interstate communication. For example, a hacker may violate section 1030(a)(2) by obtaining unauthorized access to an Internet computer through war dialing or through a Trojan horse and then obtaining sensitive personal information such as social security numbers or credit card numbers from the hijacked computer.In addition, section 1030(a)(5) applies to a hacker that causes damage to a protected computer. If the damage was caused by the transmission of a program, information, code, or command, then subsection 1030(a)(5)(A)(i) is applicable. Therefore, a Trojan horse (and also other viruses and worms) would be such a "program, information, code, or command" invoking the prohibition of subsection 1030(a)(5)(A)(i). Alternatively, if the damage was caused from unauthorized access, then either subsection 1030(a)(5)(A)(ii) or subsection 1030(a)(5)(A)(iii) would apply. Once the hacker obtains access to the computer, either through a Trojan horse or other unauthorized means such as war dialing or buffer overflow attacks, damage can result from altering or deleting existing files or otherwise impairing "the integrity or availability of data, a program, a system or information."A violation of any of the seven prohibitions of the CFAA can result in criminal sanctions. However, for civil damages, a violation of the CFAA must include at least one of the five factors listed in section 1030(a)(5)(B). The most relevant of these five factors is the requirement of a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."This often presents a hurdle for victims who sometimes find it difficult to prove a loss of $5,000 in value. As described in the Appendix, intrusive computer hackers have a variety of tools available for them to breach the security of computer systems. Indeed, many hackers themselves freely share the tools and methods they have

developed or acquired. Hackers, in addition, also utilize several additional tools to help conceal their tracks. It is estimated that at most, only ten percent of successful intrusions are ever detected. Even if an intrusion is successfully detected, a rough estimate is that only between one and seventeen percent of these detected intrusions are ever reported to law enforcement. Finally, of the successful intrusions reported to law enforcement, only a small percentage of these cases are successfully prosecuted. A 1999 study by David Banisar ("Banisar"), who was involved with the Electronic Privacy Information Center, found that in 1998, of the 419 cases of computer fraud referred to federal prosecutors, only 83 cases were prosecuted. Moreover, of these 83 cases, only 57 cases reached disposition— with 47 ending in convictions and the remaining 10 ending unsuccessfully for prosecutors. Surprisingly, the average sentence was only five months and half of the defendants who were convicted received no jail time at all. Against this background, this paper will now discuss the technical, societal, and legal failures that contribute to the unsuccessful prosecution of computer hackers. The federal laws discussed in Part II— the ECPA and CFAA— are only effective against computer hackers if they are apprehended. In this section, the various tools and methods that computer hackers use to conceal their activities and evade law enforcement will be discussed. All computers communicating on the Internet are assigned an Internet Protocol ("IP") address. This IP address uniquely identifies a computer and is similar to how a street address identifies a particular home. Because malicious hackers want to make it more difficult for law enforcement to find them, they will oftentimes mask their activities. These hackers may utilize intermediate computers, delete log files, or utilize anonymous proxy servers as described below. If a hacker has compromised a computer, the hacker may utilize this compromised computer as a "launching pad" for attacks on other computers. By launching their attacks from intermediate computers, computer hackers can make it more difficult for law enforcement to trace their attacks. For example, the hacker can utilize compromised Computer A to connect to compromised Computer B, which is then used to attack the target computer. In this example, this means that law enforcement must penetrate two additional layers of anonymity (Computers A and B) before discovering the hacker's computer.As a first step, law enforcement will investigate the log file of the target computer (and its Internet Service Provide ("ISP")). The log file of the target computer (or its ISP) will indicate the IP address of Computer B. Investigators must then travel to Computer B and obtain its log file. The log file of Computer B (or its ISP) may point to the IP address of Computer A. Investigators must then go to Computer A (or its ISP) to obtain its log file, and, if lucky enough, will obtain the IP address of the hacker's own personal computer. Further, law enforcement will likely have to obtain subpoenas and court orders to obtain access to Computers A and B (or the ISP's of Computers A and B). In the above example, tracking a computer hacker from the target computer to the hacker's personal computer requires that the log files at intermediate Computers A and B (or their respective ISP's) be intact. Several problems may occur with respect to these log files: (1) some victim computers do not keep log files; (2) the hackers sometimes alter or delete log files upon gaining entry into the compromised computer; (3) or the ISP's log files have been routinely cleared before law enforcement sends the retention letter to the ISP. If any of these three events occur, then the chain from the target computer to the hacker has been broken and law enforcement will have to turn to traditional investigative techniques. Unfortunately, these traditional investigative techniques are oftentimes inadequate to identify the hacker. Most users access the Internet through legitimate proxy servers provided by reputable companies such as AOL or Earthlink. These legitimate proxy servers keep logs of the activities of their users. Successful ethical hackers possess a variety of skills. First and foremost, they must be completely trustworthy. While testing the security of a client's systems, the ethical hacker may discover information about the client that should remain secret. In many cases, this information, if publicized, could lead to real intruders breaking into the systems, possibly leading to financial losses. During an evaluation, the ethical hacker often holds the "keys to the company," and therefore must be trusted to exercise tight control over any information about a target that could be misused. The sensitivity of the information gathered during an evaluation requires that strong measures be taken to ensure the security of the systems being employed by the ethical hackers themselves: limited-access labs with physical security protection and full ceiling-to-floor walls, multiple secure Internet connections, a safe to hold paper documentation from clients, strong cryptography to protect electronic results, and isolated networks for testing. Ethical hackers typically have very strong programming and computer networking skills and have been in the computer and networking business for several years. They are also adept at installing and maintaining systems that use the more popular operating systems (e.g., UNIX or Windows NT) used on target systems. These base skills are augmented with detailed knowledge of the hardware and software provided by the more popular computer and networking hardware vendors. It should be noted that an additional specialization in security is not always necessary, as strong skills in the other areas imply a very good understanding of how the security on various systems is maintained. These systems management skills are necessary for the actual vulnerability testing, but are equally important when preparing the report for the client after the test. Finally, good candidates for ethical hacking have more

drive and patience than most people. Unlike the way someone breaks into a computer in the movies, the work that ethical hackers do demands a lot of time and persistence. This is a critical trait, since criminal hackers are known to be extremely patient and willing to monitor systems for days or weeks while waiting for an opportunity. A typical evaluation may require several days of tedious work that is difficult to automate. Some portions of the evaluations must be done outside of normal working hours to avoid interfering with production at "live" targets or to simulate the timing of a real attack. When they encounter a system with which they are unfamiliar, ethical hackers will spend the time to learn about the system and try to find its weaknesses. Finally, keeping up with the ever-changing world of computer and network security requires continuous education and review. One might observe that the skills we have described could just as easily belong to a criminal hacker as to an ethical hacker. Just as in sports or warfare, knowledge of the skills and techniques of your opponent is vital to your success. In the computer security realm, the ethical hacker's task is the harder one. With traditional crime anyone can become a shoplifter, graffiti artist, or a mugger. Their potential targets are usually easy to identify and tend to be localized. The local law enforcement agents must know how the criminals ply their trade and how to stop them. On the Internet anyone can download criminal hacker tools and use them to attempt to break into computers anywhere in the world. Ethical hackers have to know the techniques of the criminal hackers, how their activities might be detected, and how to stop them. Given these qualifications, how does one go about finding such individuals? The best ethical hacker candidates will have successfully published research papers or released popular open- source security software. The computer security community is strongly self-policing, given the importance of its work. Most ethical hackers, and many of the better computer and network security experts, did not set out to focus on these issues. Most of them were computer users from various disciplines, such as astronomy and physics, mathematics, computer science, philosophy, or liberal arts, who took it personally when someone disrupted their work with a hack. One rule that IBM's ethical hacking effort had from the very beginning was that we would not hire ex-hackers. While some will argue that only a "real hacker" would have the skill to actually do the work, we feel that the requirement for absolute trust eliminated such candidates. We likened the decision to that of hiring a fire marshal for a school district: while a gifted ex-arsonist might indeed know everything about setting and putting out fires, would the parents of the students really feel comfortable with such a choice? This decision was further justified when the service was initially offered: the customers themselves asked that such a restriction be observed. Since IBM's ethical hacking group was formed, there have been numerous ex-hackers who have become security consultants and spokespersons for the news media. While they may very well have turned away from the "dark side," there will always be a doubt. However, the existence of anonymous proxy servers make it much more difficult for law enforcement to find hackers because anonymous proxy servers intentionally do not keep any log files at all. Utilizing the same example above, this means that at best, the log file of Computer A (or its ISP) will give the IP address of the anonymous proxy server, which is insufficient to uniquely identify a hacker out of the perhaps thousands of people who connect to the Internet through the anonymous proxy server. Sometimes hackers are never caught because companies never alert law enforcement to the hacker's intrusive activity. At other times, even cases that are referred to law enforcement and prosecutors (assuming the hacker-defendant can be identified) result in relatively low prosecution rates. This subsection explains why companies fail to report and why prosecutors fail to prosecute. The 2003 CSI/FBI Computer Crime and Security Survey ("2003 CSI/FBI Survey") found that in 2002, only thirty percent of the companies and organizations surveyed reported computer intrusions to law enforcement. Some of their reasons for not reporting include competitive advantage concerns, negative publicity concerns, and lack of knowledge that anything could be done. When asked why their organization did not report intrusions to law enforcement, sixty-one percent of the respondents to the 2003 CSI/FBI Survey indicated that they feared that their competitors would use this information advantageously. For example, competitors may advertise that they are not subject to the same security loopholes as the hacked company. These competitors may then be able to divert customers from the hacked company.

As nowadays all the information is available online, a large number of users are accessing it, some of them use this information for gaining knowledge and some use it to know how to use this information to destroy or steal the data of websites or databases without the knowledge of the owner. The purpose of this paper is to tell what is hacking, who are hackers, what is ethical hacking, what is the code of conduct of ethical hackers and the need of them. A small introduction of Linux Operating System is given in this paper. All the techniques are performed on the Linux operating system named Kali Linux. After this some basic hacking attacks covered in the paper are MiTM Attack (Man in The Middle Attack), Phishing Attack, DoS Attack (Denial of Services Attack). Further what is Wi-Fi, what are the techniques used in the Wi-Fi protection and the methods used by the hackers to hacks Wi-Fi passwords is covered in the paper. As the computer technology advances, it has its darker side also; HACKERS. In today world the size of the internet is growing

at a very fast rate, a large amount of data is moving online, therefore, data security is the major issue. The internet has led to the increase in the digitization of various processes like banking, online transaction, online money transfer, online sending and receiving of various forms of data, thus increasing the risk of the data security. Nowadays a large number of companies, organizations, banks, and websites are targeted by the various types of hacking attacks by the hackers. Generally, after hearing the term hacker we all think of the bad guys who are computers experts with bad intensions, who tries to steal, leak or destroy someone's confidential or valuable data without their knowledge. They are the persons with very high computer skills who tries to break into someone else security for gaining access to their personal information, but all the times it is not like that. To overcome the risk of being hacked by the hackers we have Ethical Hackers in the industry, who are also computer experts just like the hackers but with good intensions or bounded by some set of rule and regulations by the various organizations. These are the persons who try to protect the online moving data by the various attacks of the hackers and keeping it safe with the owner. Further, this paper tells you more about hackers, ethical hackers and Linux operating system (kali Linux) and aware you about some attacks performed by the hackers on the internet.

In addition, once federal law enforcement gets involved, they oftentimes move at a painfully slow rate. Further, federal agents may freeze, and thus make unavailable for an extended period of time, the resources that were compromised by the hacker. The company may also have to expend additional resources in providing Federal agents with information about its business, in attending interviews, and in making employees available as witnesses for trial. Thus, many companies are concerned that if a substantial amount of their resources are diverted towards the investigation, their competitors may gain the competitive advantage and manage to outmaneuver them in the marketplace.Perhaps a good example of this occurred after hackers penetrated the systems of Egghead.com ("Egghead") in December 2000. Immediately after the intrusion, Egghead spent substantial resources hiring the "world's leading computer security experts" to investigate the extent of the security breach and to analyze the current security measures. While Egghead had expected to learn the extent of the security breach within 5 days, the investigation required 20 days, perhaps because a full forensics investigation had to be done.Further, law enforcement was simultaneously pursuing a criminal investigation. Shortly after the hacking incident, Egghead's business took a turn for the worse. Egghead blamed the shortfall in expected sales in the following fourth quarter (February 2001) on "softening of consumer demand for personal computers and related technology products." Perhaps Egghead, consumed with dealing with the hacking incident, was not able to recognize and respond quickly enough to the intense competition within the computer and software marketplace. Egghead's inability to respond quickly enough to the marketplace was permanently marked on October 15, 2001. On that day, Egghead filed for bankruptcy, citing an unexpected sharp drop in sales during the preceding several weeks. Egghead's fate was sealed when Amazon.com successfully purchased the assets of Egghead through a bankruptcy auction. The potential negative publicity that may come from reporting computer intrusions can be quite damaging and therefore can also be a contributing factor to the non- reporting of intrusive computer attacks. For example, the CDUniverse.com ("CDUniverse") hacking incident in 2000, where 300,000 credit card numbers were stolen by a hacker, was widely publicized by the media. Undoubtedly, CDUniverse lost many sales during the time that its web site was unavailable to potential customers. More importantly, however, many potential customers declined making purchases from CDUniverse for fear that their own credit card numbers would be stolen by hackers.

Indeed, "most companies believe that the public relations ('PR') costs of being identified with weak security are far greater than the damage most malicious hackers can inflict." Seventy percent of the respondents in the 2003 CSI/FBI indicated that negative publicity was a factor in not reporting intrusions to law enforcement. Accordingly, most large companies tend to handle the problem in-house rather than risk the potential costs of negative publicity. Fifty-three percent of respondents in the 2003 CSI/FBI Survey indicated that they did not know they could report these incidents. The survey narrates a highly probable explanation about the low rates of reporting: While [the lack of reporting] may seem strange, . . . it makes more sense in that it isn't always obvious who to turn to when someone has been hacking, say, your Web storefront's customer database. Should you turn to the local police? By and large, you won't get much help there. Should you turn to the FBI? In some cases they can help you and in others, theycan't (but it sure doesn't hurt to call).This lack of knowledge that anything can be done is not surprising given the low number of prosecutions of other hackers. Thus, the result is that many hackers that could be prosecuted if only reported are not being held accountable for their intrusive attacks. Notwithstanding the failure in reporting hackers, the failure in prosecuting hackers also creates a situation in which hackers are not being held accountable for their intrusive attacks. In this subsection, two factors for why hackers are not being prosecuted will be explored—a lack of understanding by law enforcement and the fact that computer crimes are difficult to prove. Law enforcement has struggled with prosecuting hackers because the technology is complex and difficult to understand. The result is that the vast amount of

evidence presented along with the lack of understanding by police and prosecutors oftentimes leads to unnecessary searches, arrests, and court delays. Thus, it is not surprising that in 1998, just under twenty percent of referred cases were prosecuted. Moreover, this twenty percent is slim compared to the overall federal prosecution rate in 1998, which was approximately sixty- one percent. In the 1999 Banisar study discussed above, of the 419 cybercrime cases referred to prosecutors, 336 were dismissed. The majority of these cases were dismissed for lack of supporting evidence.The lack of supporting evidence can result from either concealment by the hackers themselves (as discussed in Part III.A) or by delayed or improper actions by others. For example, as discussed above, Internet Service Providers may have routinely cleared their log files before receiving the retention order by law enforcement. All too often, companies that have been hacked into have not taken the proper steps to preserve evidence. Sometimes the hijacked computers remain in use, thereby overwriting all traces of the hacker's footprints. Or at other times, companies may inadvertently destroy the traces of the hacker as they try to ascertain the damage to the hijacked computer system. Indeed, proper preservation of evidence requires that deliberate and laborious steps be taken, including making a byte-stream copy of the hijacked computer's hard-drive and employing forensic software to uncover changes on the hijacked computer. Finally, there are some failures in the current federal laws that allow the problem of intrusive computer hacking to continue. This includes loopholes in the ECPA and the lack of deterrence by the CFAA. Moreover, the CFAA fails to hold software manufacturers liable for the negligent design of software. The courts themselves have conceded the shortcomings of the ECPA, which includes the Wiretap Act and the Stored Communications Act ("SCA") as described above in Part II.A. For example, in United States v. Steiger, the 11th Circuit stated that "our reading of the Wiretap Act to cover only real-time interception of electronic communications, together with the apparent non-applicability of the SCA to hacking into personal computers to retrieve information stored therein, reveals a legislative hiatus in the current laws purporting to protect privacy in electronic communications." As previously explained, the Wiretap Act applies only to acquisitions contemporaneous with transmission and, thus, typically would only apply to the hacker's use of network packet sniffers. However, other hacking tools described in the Appendix such as buffer overflow attacks and Trojan horses are not prohibited by the Wiretap Act (although may be prohibited by other federal and state laws). In addition, the SCA mainly applies against intrusive hackers whose attacks are against Internet Service Providers, email servers, and other electronic communication services.But, many computers that contain highly sensitive information would be more akin to a personal computer and not be considered an electronic service within the purview of the SCA. The rising growth of the internet and machinery whether its mobile or computer technology has brought many good and proficient things for people such as E- commerce, E-mail, Cloud Computing, Data Sharing, Application and many more but there are also a dark and hidden sides of it such as Network Hacks, Computer hacks, Mobile Breach, Backdoors etc. As we all know that Cybercrime been one of the common practices made by the computer experts and is increasing rapidly in numbers. Cybercrime is responsible for disrupting the Organization networks, stealing valuable data, documents, hacking bank account. Preventive measures have been taken by the government a lot many times. In this paper we will be discussing the types of hackers. The Wireless Local Area Networks frequently referred to as WLANs or Wi-Fi networks is being the widely used network in today's scenario. These are being installing in houses, institutions, offices and hotels etc., without any vain. But it also leads to increase in the probability of threats, vulnerabilities which may include as stealing passwords, hacking of Wi-Fi Networks and loss/hack of personal information of the users. This paper also discusses about the categories of different IT networks with their weaknesses. Lastly this paper will be discussing about the ways to breach or hack the Wi-Fi networks. Cyber security is the wide range of security on various types of networks. In glance with the topic there are many different types of security. Security is an interesting subject taught in college and schools to make people aware of the surroundings and make them more secure and ready with weapons to bear the attacks and viruses in a wealthy way. Cyber security is the field of technologies, processes and activities designed to protect you from hackers, viruses and malwares. It deals with both security and computer security. Hardware and security devices deal with physical devices that take care of security of a networking system. Widely driven software security is the idea of engineering that it continues to function correctly against a malicious attack. Elements of cyber security include Network security, Application security, Endpoint security, Data security, Identity management, Database and infrastructure security, Cloud security, Mobile security, Disaster recovery/business continuity planning, either and end-user education. But major areas covered under cyber security are application security, Information security Network security and data security. To make network less vulnerable some steps are taken as access control, authentication, integrity, nonrepudiation. Secondly cyber security deals in computer security which ensures the protection of computer systems from theft, viruses and damage to their Personal Computer. Cybercrime are of various types such as credit attack, computer fraud, identity theft, sharing files and information, spam, money laundering etc. ATM attacks which include spams like intercepting the details such as account

number, Passwords etc. is a cybercrime growing at a very high rate these include sending of fraud mails having malwares in it which attract the users saying that they have won ransom amount of certain greedy amount and ask for their account details to avail the offer, to which people easily get trapped in and they get hacked. A backdoor in computer systems or crypto-system is bye-passing normal authentication or security controls which may be added by hackers for their welfare. Ethical hacking is the way in which hackers only try to find weakness also known as "Penetration Testing". There are different phases in hacking. Ethical hacking is the type of hacking which hackers perform not to harm user's computers as it does not contain malicious content. Ethical hacking is the important thing in life in now a day, as information is the most important asset of an organisation keeping this information secured can only save the image of company. Ethical hacking is legal hacking tied within the rules, if the rules are denied then the hacker has to pay a high rated price in form of punishment which can be either monetary or any other way) which are are scanning, owning the system, zombie system as well as evidence removal. These are some phases that hackers do to bypass user's device. They initially try to gain access over user's PC, and after getting the access they run full system scan to fish out all private information with the help of their developed malicious viruses and malwares. After which the hacker jumps to the next step of zombie system in which he has access to user's system irrespective of the time. In zombie system, another hacker is debarred to access the already hacked system in future. The last step is aimed at removing all the user's data from the Personal computer thereby accessing all the private data. This is done by hacker in order to own all the data of the user and the alert for the hacking is not displayed to the user by any means of alert/message Hackers could obtain access to these non-electronic communication service computers by either using a launch-pad style attack (by utilizing a company's computer that is visible on the Internet to access a company's internal computer that is not accessible on the Internet) or through war dialing as described in Part C of the Appendix. While the ECPA provides only limited assistance to the problem of intrusive computer hacking, the current version of the Computer Fraud and Abuse Act (including changes made by the PATRIOT Act) has covered many of the deficiencies of the ECPA. Despite overcoming the deficiencies of the ECPA, the main problem with the CFAA is that it does not appear to be deterring intrusive computer hackers. In addition, the CFAA does not hold software manufacturers liable for the negligent design of their software. Twenty years have passed since the enactment of the first version of the CFAA in 1984, and the incidences of intrusive computer hacking have not declined but rather increased. The 2003 CSI/FBI survey indicated that system penetrations for respondents increased from fifty-two in 1999 to one hundred thirteen in 2002 and eighty-eight in 2003.A possibility is that computer hackers may not know of the seriousness of penalties for certain violations of the CFAA. There is some support for this proposition. Some of the broadening amendments, including the definitions of damage and protected computers have only occurred recently. Other provisions such as the strong protection of government computers have stood the test of time. Indeed, the CFAA was initially enacted in 1984 to protect government computers (and financial computers) from hackers. In 2002, a modern day hacker named HeX compiled a revised code of ethics for the hacking underground. Included among his revised code of ethics was to never take "stupid" risks such as trying to connect to a government computer. Undoubtedly, this was a recognition of the strong protection for government computers that has endured every revision of the CFAA. Not surprisingly, this revised code of ethics did not include a prohibition against hacking into personal or corporate computers.Another possibility is that these hackers are overly optimistic about their chances of not being caught or prosecuted. Some experts have indicated that a significant number of hackings are committed by young people who believe that "they are untouchable." Given the statistics compiled by Banisar regarding the actual number of prosecutions in 1998, these computer hackers may be justified in being overly optimistic. Prior to the 2001 PATRIOT Act amendment of 18 U.S.C. § 1030(g), several courts had expanded the reach of CFAA to include not only damages resulting from unauthorized computer use, but also damages resulting from software manufacturers who distributed faulty software. However, the last part of 18 U.S.C. § 1030(g) now explicitly states that "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware." This means that software manufacturers will not be held accountable for creating the security holes that allow computer hackers to hijack computer systems. Having established the technical, societal, and legal problems that contribute to the escalating problem of intrusive computer hacking, this paper now proposes a solution in the form of a national reporting requirement. First, as background, California's reporting requirement will be introduced. California is the first and only state with a reporting requirement. Next, a description of the proposed national reporting requirement and the interests to be protected will be presented. An argument will be made that such a proposed national reporting requirement is not only beneficial, but also necessary to tackle the problem of intrusive computer hacking. More specifically, this paper will argue that inaction by the national government could lead to an unworkable situation with piecemeal state-by-state legislation. Further, this paper will explain how such a proposed national reporting requirement can overcome the

technical, social, and legal failures described in Part III. California's reporting requirement (2002 Cal SB 1386, which amended the California Civil Code and took effect on July 1, 2003) was the first of its kind in the nation. In short, the reporting requirement means that businesses that store their customers' personal information in the form of computerized data must warn their customers when their personal information is stolen (or suspected of being stolen) by computer hackers or other criminals. Such a law is an attempt to extend and protect the privacy of individuals that transact with such businessesThe birth of the California reporting requirement was the result of a hacking intrusion that affected thousands of California's employees. On April 5, 2002, a hacker broke into a computer database housed at California's Stephen P. Teale Data Center in Rancho Cordova. The computer database, a personnel database, housed the personal information of the state's 265,000 employees.The personnel database included the names, Social Security numbers, and payroll information of the employees. Among the information included in the personnel database was the personal information of then-Governor Gray Davis.While the intrusion was discovered a month later on May 7, 2002, public disclosure of the intrusion did not occur until May 24, 2002. This delay in the public reporting provoked criticism from the California Union of Safety Employees ("CAUSE"). The public outcry from this incident was the main impetus behind the enactment of California's reporting requirement.On a broader level, the enactment of California's reporting requirement recognizes the growing problem of identity theft in California. For instance, in 2000, the Los Angeles County Sheriff's department reported 1,932 identity theft cases, representing a 108 percent increase over the prior year. The California law attempts to thwart the growth of such identity theft arising from personal information that is obtained from breaches into computer systems. California's reporting requirement became effective on July 1, 2003. Section 1798.29 of the California Civil Code, applicable to agencies, requires that:(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Similarly, Section 1798.82 has a reporting requirement for businesses: (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.Both provisions require that "the disclosure shall be made in the most expedient time possible and without an unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore reasonable integrity of the data system."In addition, for purposes of both Section 1798.29 and 1798.82, the Civil Code defines "personal information" as:an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.The required notice under both of these provisions can be satisfied with written or electronic notification. In the event that providing written or electronic notification would be too burdensome (because such notice would cost more than $250,000 or more than 500,000 persons would have to be notified), then substitute notice may be utilized instead. Substitute notice includes email notice, conspicuous notice on the web site page of the person or business, if the person or business maintains one, or notification to major statewide media. Through the allowance of substitute notice, California's law recognizes the potential heavy burden that individual notification places on agencies and businesses. Section 1798.84 of the California Civil Code expressly provides for damages for customers injured by violations of California's reporting requirement. More specifically, Section 1798.84 states that "any customer injured by a violation of this title may institute a civil action to recover damages." After California's reporting requirement went into effect on July 1, 2003, other states may be considering similar measures as well. If other states were to pass similar laws, an untenable piecemeal state-by-state regulatory scheme would result. For example, consider a hypothetical Internet company, Ames Corp. ("Ames"), that sells products throughout all fifty states and assume that each state has passed a modified version of California's reporting requirement. If hackers obtained access to one of Ames's customer databases, Ames would have fifty different reporting requirements to comply with. Not only would this result be burdensome and costly to Ames, but Ames could never be sure that it has fully complied with all of the requirements of each state. For example, while many states may have similarly-worded statutes, each state may have a slightly different interpretation of its own statutes.

As an initial matter, because Congress has not yet enacted a reporting requirement, California's reporting requirement does not conflict with any federal statute and thus is not preempted under the Supremacy Clause of the U.S.

Constitution. Further, while the positive aspects of the commerce clause permits Congress to regulate in this area (as will be discussed immediately below), the negative aspect of it, the dormant commerce clause, does not nullify California's reporting requirement (and perhaps the reporting requirements of other states, if enacted) even though it imposes limitations on interstate commerce. The dormant commerce clause, operating under the balancing test under Pike v. Bruce Church, Inc., requires that California's interest in a reporting requirement outweigh the burden the law imposes on interstate commerce. Based on the discussion above regarding California's interest in stopping identity theft, the Pike test is likely to be met and California's reporting requirement most likely survives dormant commerce clause considerations.On the other hand, Congress has the power to solve this piecemeal state-by-state regulatory scheme by adopting a unifying approach under the commerce clause. In United States v. Lopez, Chief Justice Rehnquist, in delivering the opinion of the Court, indicated three categories of activity that Congress may regulate under the commerce power: (1) the use of the channels of interstate commerce, (2) the instrumentalities of interstate commerce or persons or things in interstate commerce, even though the threat may come only from certain intrastate activities, or (3) those activities having a substantial relation to interstate commerce.A computer connected to the Internet would be using a channel of interstate commerce or an instrumentality of interstate commerce. The result is that Congress would indeed have the power to regulate this area.Thus, if Congress does not enact a reporting requirement similar to California's, then an unworkable state-by- state solution may evolve. As will be described below, the benefits of a single unified approach greatly outweigh such a state-by-state solution. In 2003, U.S. Senator Dianne Feinstein (D-California) proposed a national reporting requirement modeled after California's reporting requirement known as the Notification of Risk to Personal Data Act ("Feinstein proposal"). The Feinstein proposal would have required a business or government entity to notify an individual whenever there is a reasonable basis to conclude that a hacker has obtained unencrypted personal information. Personal information would have included an individual's Social Security number, driver's license number, state identification number, bank account number, or credit card number. Fines by the Federal Trade Commission for non-compliance with the Feinstein proposal would have been $5,000 per violation or up to $25,000 per day for continuing violations. Unfortunately, the Feinstein proposal has been stalled in committee. This paper now proposes a national reporting requirement ("proposed reporting requirement") for the problem of intrusive computer hacking. Two interests will be recognized here—first, the interest of each individual in his or her privacy and secondly, the interest in protecting property against damage by computer hackers. Wireless local-area networks — often referred to as WLANs or Wi-Finetworks — are all the rage these days. People are installing them intheir offices, hotels, coffee shops, and homes. Seeking to fulfill the wirelessdemands, Wi-Fi product vendors and service providers are popping up just about as fast as the dot-coms of the late 1990s. Wireless networks offer convenience,mobility, and can even be less expensive to implement than wired networks in many cases. Given the consumer demand, vendor solutions, and industry standards, wireless-network technology is real and is here to stay. But how safe is this technology? Wireless networks are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 set of standards for WLANs. In case you've ever wondered, the IEEE 802 standards got their name from the year and month this group was formed — February 1980. The ".11" that refers to the wireless LAN working group is simply a subset of the 802 group. There's a whole slew of industry groups involved with wireless networking, but the two main players are the IEEE 802.11 working group and the Wi-Fi Alliance. Years ago, wireless networks were only a niche technology used for very specialized applications. These days, Wi-Fi systems have created a multibilliondollar market and are being used in practically every industry — and in every size organization from small architectural firms to the local zoo. But with this increased exposure comes increased risk: The widespread use of wireless systems has helped make them a bigger target than the IEEE ever bargained for. (Some widely publicized flaws such as the Wired Equivalent Privacy (WEP) weaknesses in the 802.11 wireless- network protocol haven't helped things, either.) And, as Microsoft has demonstrated, the bigger and more popular you are, the more attacks you're going to receive. With the convenience, cost savings, and productivity gains of wireless networks come a whole slew of security risks. These aren't the common security issues, such as spyware, weak passwords, and missing patches. Those weaknesses still exist; however, networking without wires introduces a whole new set of vulnerabilities from an entirely different perspective.

This brings us to the concept of ethical hacking. Ethical hacking — sometimes referred to as white-hat hacking — means the use of hacking to test and improve defenses against unethical hackers. It's often compared to penetration testing and vulnerability testing, but it goes even deeper. Ethical hacking involves using the same tools and techniques the bad guys use, but it also involves extensive up-front planning, a group of specific tools, complex testing methodologies, and sufficient follow-up to fix any problems before the bad guys — the black- and gray-hat hackers — find and exploit them. Understanding the various threats and vulnerabilities associated with 802.11- based wireless

networks — and ethically hacking them to make them more secure — is what this review is all about. Please join in on the fun. In this chapter, we'll take a look at common threats and vulnerabilities associated with wireless networks. We'll also introduce you to some essential wireless security tools and tests you should run in order to strengthen your airwaves. Wireless networks have been notoriously insecure since the early days of the 802.11b standard of the late 1990s. Since the standard's inception, major 802.11 weaknesses, such as physical security weaknesses, encryption flaws, and authentication problems, have been discovered. Wireless attacks have been on the rise ever since. These standards have resolved many known security vulnerabilities of the 802.11a/b/g protocols. As with most security standards, the problem with these wireless security solutions is not that the solutions don't work — it's that many network administrators are resistant to change and don't fully implement them. Many administrators don't want to reconfigure their existing wireless systemsand don't want to have to implement new security mechanisms for fear of making their networks more difficult to manage. These are legitimate concerns, but they leave many wireless networks vulnerable and waiting to be compromised. Even after you have implemented WPA, WPA2, and the various other wireless protection techniques described in this book, your network may still be at risk. This can happen when (for example) employees install unsecured wireless access points or gateways on your network without you knowing about it. In our experience — even with all the wireless security standards and vendor solutions available — the majority of systems are still wide open to attack. Bottom line: Ethical hacking isn't a do-it-once-and-forget-it measure. It's like an antivirus upgrade — you have to do it again from time to time. Beyond these basics, quite a few things can happen when a threat actually exploits the vulnerabilities of a various wireless network. This situation iscalled risk. Even when you think there's nothing going across your wireless network that a hacker would want — or you figure the likelihood of something bad happening is very low — there's still ample opportunity for trouble. We could go on and on, but you get the idea. The risks on wireless networksare not much different from those on wired ones. Wireless risks just have a greater likelihood of occurring — that's because wireless networks normally have a larger number of vulnerabilities.

The really bad thing about all this is that without the right equipment and vigilant network monitoring, it can be impossible to detect someone hacking your airwaves — even from a couple of miles away! Wireless-network compromises can include a nosy neighbor using a frequency scanner to listen in on your cordless phone conversations — or nosy co-workers overhearing private boardroom conversations. Without the physical layer of protection we've grown so accustomed to with our wired networks, anything is possible.

III. CONCLUSION

Every job requires the right tools. Selecting and preparing the proper security testing tools is a critical component of the ethical- hacking process. If you're not prepared, you'll most likely spin your wheels and not get the desired results. Just because a wireless hacking tool is designed to perform a certain test, that doesn't mean it will. You may have to tweak your settings or find another tool altogether. Also keep in mind that you sometimes have to take the output of your tools with a grain of salt. There's always the potential for *false positives* (showing there's a vulnerability when there's not) and even *false negatives* (showing there's no vulnerability when there *is*). After you get everything prepared, it's time to roll up your sleeves and get your hands dirty by performing various ethical hacks against your wireless network.

IV.REFERENCES

[1] http://www.corecom.com/external/livesecurity/pentest.html
[2] http://www .network defense .com/ papers /pentest .html
[3] Internet Security Systems, Network and Host based Vulnerability Assessment
[4] http://www.infosecinstitute.com/blog/ethicalhacking computer_forensics.html