2011

Ethical Hacking & Penetration Testing

ACC 626: IT Research Paper

Emily Chow
July 1, 2011

I. Introduction

Due to the increasing vulnerability to hacking in today's changing security environment, the protection of an organization's information security system has become a business imperative[1]. With the access to the Internet by anyone, anywhere and anytime, the Internet's "ubiquitous presence and global accessibility"[2] can become an organization's weakness because its security controls can become more easily compromised by internal and external threats. Hence, the purpose of the research paper is to strengthen the awareness of *ethical hacking* in the Chartered Accountants (CA) profession, also known as *penetration testing*, by evaluating the effectiveness and efficiency of the information security system.

II. What is Ethical Hacking/Penetration Testing?

Ethical hacking and penetration testing is a preventative measure which consists of a chain of legitimate tools that identify and exploit a company's security weaknesses[3]. It uses the same or similar techniques of malicious hackers to attack key vulnerabilities in the company's security system, which then can be mitigated and closed. In other words, penetration testing can be described as not "tapping the door"[4], but "breaking through the door"[5]. These tests reveal how easy an organization's security controls can be penetrated, and to obtain access to its confidential and sensitive information asset by hackers. As a result, ethical hacking is an effective tool that can help assist CA professionals to better understand the organization's information systems and its strategy, as well as to enhance the level of assurance and IS audits if used properly.

III. Basic Characteristics of Penetration Testing

Different Types of "Hat Hackers"

There are different types of "hat hackers" that should be distinguished: black, grey, and white[6]. "Black hat hackers" perform unauthorized penetration attacks against information systems, which may or may not be illegal in the country they are conducting. On the other hand, ethical hackers are known as "white hat hackers" because they legitimately perform security tests bounded by a contractual agreement. Their main purpose is to improve the system which can then be closed before a real criminal hacker penetrates within the organization. "Grey hat hackers" are those in-between the black and white that perform their activities within legal legislations and regulations but may slightly go over the boundaries. Since penetration testing is an authorized attempt to intrude into an organization's network, the focus of the paper will be on the "white hat hackers".

---

[1] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."
[2] Nemati, Hamid. "The Expert Opinion."
[3] ibid
[4] Pulley, John. "Are there perils in penetration testing?"
[5] ibid
[6] Wilhelm, Thomas. "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab."

Penetration Testing: "Red Team"

Penetration testing generally consists of small group of teams from external auditors or consulting firms that provide penetration testing services[7]. These teams are also known as "red teams"[8]. Internal staff should not be part of the red team because it violates the basic principle of self-reviewing one's own system. Thus, it is expected that external personnel have minimal or no previous knowledge of the system and can conduct a closer and more realistic simulation as malicious hackers. Nevertheless, background checks, such as qualifications, good reputation, and experience, should be performed because the team will be dealing with confidential and sensitive information. They should also be supervised by someone who will be held responsible for any failures[9]. Thus, the main objective of the red team is to simulate the same or similar hacker activities by exploiting security vulnerabilities under a controlled testing environment. By doing so, these security gaps can be eliminated by the organization before unauthorized users can truly exploit them.

IV. Threats/Risks Relevant to Organizations

In order to conduct a penetration testing, threats and risks should first be identified and analyzed because this forms the basis of the test in which ethical hackers would attempt to attack an organization's system to expose those vulnerabilities. In the same manner, CA practitioners should be fully aware of the information security risks that are relevant to any organization because it can adversely affect their business operations and cause their security systems vulnerable to unauthorized access, increasing both business and information risks respectively. In the following, two major risks will be discussed – internal and external.

Internal Threat/Risks

Regardless of how strong a computer security system is designed, employees' lack of knowledge about security issues and other malicious employees can inflict enormous damages to any organization[10]. With limited employee security awareness, simple actions of opening a "joke email"[11], which may be infected with a virus, can place the organization at risk with thousands of lost revenue. Key statistics from a medium-size company case study have indicated that 100% of all employees use instant messaging[12], which should have been prevented by the corporate firewalls, and 44 out of 102 users use common dictionary words as legitimate and valid passwords[13] which can be easily guessed by other employees for unauthorized access. In addition, less than 25% of the employees have used an external device to copy files off-site[14] and 33% have transmitted confidential documents to a laptop[15]. Employees also run the

[7] Wilhelm, Thomas. "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab."
[8] Gallegos, Federick. "Red Teams: An Audit Tool, Technique and Methodology for Information Assurance."
[9] Raether, Ronald. "DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure."
[10] Styles, Martyn, and Theo Tryfonas. "Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users."
[11] ibid
[12] ibid
[13] ibid
[14] ibid

chance of using cloud services, such as Google Docs or Dropbox, for the convenience of transferring corporate data, and this bypasses the IT department for proper procedures and policies. As a result, companies are now exposed in ways that the cloud can compromise its sensitive and confidential information, increasing the risk of rogue IT[16]. This ultimately demonstrates that employees who are key personnel to running an organization successfully may also be the greatest weakness at the same time due to the unprotected exposure of unauthorized access.

External Threat/Risks

External threats include a wide range of activities that are performed by real criminal hackers. By identifying the security gaps in an organization's system, external hackers can exploit the system and gain authorized access to copy or delete sensitive information, such as customer's credit card information.

In any security system, "information is king"[17]. This essentially means that whenever an organization's information asset is compromised, this is a security issue which may be caused by technical issues, human errors or processing weaknesses[18]. As a result, both internal and external threats must be identified and proactively addressed by organizations because it can bring financial and non-financial losses, including lawsuits related to release of confidential, private, commercial or other highly-sensitive information, lost in revenue, damaged reputation, loss of credibility in the eyes of customers and loss of control in computer system[19].

V. Types of Penetration Testing

Automated vs. Manual

Automated and manual penetration testing can be both used as a means to evaluate an organization's security controls system. Automated testing has been the mainstream approach adopted by organizations because of the rapid technological changes to provide economies of scale compared to manual one. A thorough manual testing may consist of several weeks with an investment of thousands of dollars, whereas an automated can perform the tests within several hours with reduced costs[20]. This shows that automated tools can be more cost-effective and efficient if conducted properly. Another benefit of automation is that organizations can perform these tests as frequent as they want compared to ethical hacking practitioners who conduct testing only during working hours.

On the other hand, there can be an overreliance and false sense of security on automated tools because they do not guarantee that it will catch 100% of the security gaps in the system and are only as effective as the individuals who programmed and run these tests. In other words, there is a risk that an untrained employee who handles and manages the automated testing can cause more damages to the

---

[15] Styles, Martyn, and Theo Tryfonas. "Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users."
[16] Gohring, Nancy. "Policy, Education Key to Reining in Rogue Cloud."
[17] Raether, Ronald. "DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure."
[18] ibid
[19] "IS Auditing Procedure: Security Assessment – Penetration Testing and Vulnerability Analysis."
[20] Pulley, John. "Are there perils in penetration testing?"

organization than the expected benefit. Furthermore, an automated testing lacks the flexibility of substituting different scenarios as compared to an extensive manual testing performed by a knowledgeable and experienced ethical hacking practitioner[21].

An example of a company who performs automated penetration testing is iViz, the first cloud-based penetration testing that provides high quality of services for applications with "on-demand SaaS experience"[22].The benefits include the use of artificial intelligence to simulate all types of intrusion attacks, a zero false positive with the aid of "business logic testing and expert validation"[23], the flexibility to conduct a penetration test at any time, no required software or hardware, the scalability and the cost-subscription model. In comparison of Salesforce to customer relationship management, iViz has performed the same transformation to penetration testing[24].

External vs. Internal

As identified above, testing should be conducted to address the internal and external threats. Internal testing is performed within the organization's system and simulates what an authorized user or employee could potentially act. On the other hand, external testing attempts to simulate what an external hacker could potentially harm from outside the system. The red team would conduct intrusion attacks on the organization's network system through the use of the Internet or Extranet[25]. The red team generally targets the organization's servers or devices, such as "Domain Name Server, email server, web server or firewalls"[26]. It appears that an internal testing may be more comprehensive because an authorized user can either use the internal or external system to hack into an organization's information system.

Blind vs. Double-Blind vs. Targeted Testing

In a blind testing environment[27], the red team is only provided with publicly available information, such as the organization's website, domain name registry and any other related discussion boards on the Internet. With this limited information, penetration testing attempts to accumulate information to exploit an organization's security weaknesses. It can reveal information about an organization that it would not have known, but can be more time-consuming and expensive due to the extensive effort to conduct research prior to the testing phase.

In a double-blind testing environment[28], the blind testing process is expanded in which the organization's IT and other staffs are not informed beforehand about the intended testing activities. Hence, they are also considered "blind" to the test. In this type of scenario, very limited people within the organization are aware of the testing, and it requires continuous monitoring by the project sponsor to

[21]Pulley, John. "Are there perils in penetration testing?"
[22] Mohan, Sriram. "YourStory in conversation with Bikash Barai, CEO of iViZ on cloud-based penetration testing and raising Series A funding from IDG Ventures."
[23] ibid
[24] ibid
[25] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."
[26] ibid
[27] ibid
[28] ibid

ensure that the testing procedures can be eliminated once the objective has been attained. Furthermore, this test can reveal the effectiveness of an organization's monitoring, identification and response procedures to incidents.

In a targeted testing environment[29], the organization's IT and other staffs are notified about the testing activities beforehand and the penetration testers are provided with network design layout and other related information. This type of scenario may be more efficient and cost-effective because it tends to be less time-consuming than both the blind and double-blind testing. However, it may not offer a "complete picture of an organization's security vulnerabilities and response capabilities"[30].

VI. Penetration Testing Techniques

There are various technical and non-technical techniques that can be utilized as part of the penetration testing process to address the internal and external threats. The following is a list of the most common tools used in a penetration test:

1. ***Web Applications Software:*** Since many organizations sell many business applications over the Internet, testing can consist of evaluating the level of encryption used for processing confidential and sensitive information (128 or 256-bits), firewalls, the use of cookies stored on their customers' computers[31], the length and strength of passwords (upper and lower cases with numbers/letters) and the security of software configurations[32]. For instance, a message should not plainly indicate that there was an incorrect password only, and no problem with the login username.
2. ***Denial of Service:*** This testing depends on the organization's commitment of having continuous availability of the information system[33]. The red team evaluates the system's vulnerability to attacks that will either cause the system to deny service from legitimate access, or to become totally unavailable due the inability to handle high volume of traffic, such as instantly sending millions of spam messages to the organization's mail server[34].
3. ***War dialing:*** This testing consists of systematically calling numerous telephone numbers in order to identify "modems, remote access devices and maintenance connections"[35] that are present in an organization's network. Once identified, exploitation techniques, such as strategic attempts to guess the username and password, are performed to assess whether the connection can be used as a way to penetrate into its information security system[36].

---

[29] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."
[30] ibid
[31] ibid
[32] Basta, Alfred, and Wolf Halton. *Computer Security and Penetration Testing*. US: Thomson Course Technology, 2008. 1-403. Print.
[33] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."
[34] Basta, Alfred, and Wolf Halton. *Computer Security and Penetration Testing*.
[35] ibid
[36] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."

4. ***Wireless Network:*** Penetration testers will drive or walk around the office buildings to identify opened wireless networks[37] of the organization that should have not been present in the first place. The purpose is to identify security gaps or errors in the "design, implementation and operation"[38] of a company's wireless network system.
5. ***Social Engineering:*** Penetration testers would attempt to deceive the organization's employees and suppliers in order to gather sensitive information and penetrate into an organization's systems, such as claiming to be an IT representative and asking for the users' login and passwords. Even though this is a non-technical testing which involves human-related features, it is viewed as equally important to determine whether unauthorized users can gain access to the information system[39].
6. ***Google Hacking***: Since Google is the one of the most common search engines widely used by organizations, penetration testers should consider Google hacking as an effective web security practice. It uses the search engine to locate personal or sensitive information by taking advantage of Google's function of optimizing the search results anywhere in the websites. For instance, tests have found a directory with the social insurance number of more than 70 million deceased persons, and passport documents. In *Appendix A*, if a user types in "intitle: 'index of' site: edu 'server at'"[40], the screenshot illustrates a hyperlink to an 'old' folder which may potentially consist of sensitive information for a malicious hacker to exploit[41].

VII. Benefits of Penetration Testing

Penetration testing can help close the gap between safeguarding of an organization's security system and the exposure of its security risks by assessing whether the security controls are adequate and working effectively.

Core Security Technologies, the top leader of IT security and measurement solutions, states that "if [a company] is not doing penetration testing…then [it] is behind the curve"[42] on March 9, 2011. As IT attacks are always changing in "nature, complexity and method"[43], penetration testing can be viewed as a solution to the evolving security threat environment and assist the organization's IT system to stay constantly attentive and updated as part of the its overall security strategy. According to PCI and ISO 27001, managing security risks and threats is an essential management and IT process[44]. The rationale behind this is that organizations should fully understand their weaknesses before they can effectively defend and protect themselves from unauthorized access. Key statistics from *Core Security Technologies* have indicated that in 2004, 80% of the major security vulnerabilities experienced an attack within 60

[37] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."
[38] ibid
[39] ibid
[40] Lancor, Lisa. "Using Google Hacking to Enhance Defense Strategies."
[41] ibid
[42] Bowker, Dave, Lesley Sulliva, and Chenxi Wang. "Leading Industry Analyst Recommends Penetration Testing."
[43] ibid
[44] ibid

days, while in 2008, 85% had an attack within 10 days[45]. This clearly demonstrates that the "window of opportunity"[46] for malicious hackers and employees is becoming larger as the opportunities and time to exploit are widening at the same time. Hence, penetration testing can become a "hacker's-eye"[47] of any organization's security system. Instead of possessing the wrong attitude towards security in hopes of not being hacked, organizations should take the appropriate actions to mitigate and control risk. Penetration testing can strengthen an organization's security procedures and processes, as well as further improve the efficiency and effectiveness of its risk management. It can also consist of increasing the degree of transparency by assessing the type of sensitive data that can be potentially exposed, and how the network can be compromised by human elements. Ultimately, the main benefit is that organizations can learn from the penetration testing experience and further improve its security systems by thoroughly analyzing its weaknesses, properly implementing the changes, and informing all parties in a timely manner[48].

VIII. Limitations of Penetration Testing

According to the *Information Technology Association of Canada (ITAC),* penetration testing cannot be expected to identify all possible security weaknesses, nor does it guarantee that it is 100% secure. New technology and hacking methods can create new exposures not anticipated during the penetration testing. Thus, it is certainly possible that after a penetration testing, there could be hacking incidents thereafter because it is impossible to have full but rather only good protection for an organization's security system.

Penetration testing involves taking computer screen shots or copying sensitive information as evidence to prove that the system has key security weaknesses. However, there are many restrictions on the extent of information that will be available and legitimately accessible to the ethical hacker. This prevents a penetration testing from simulating as closely as possible of the malicious hackers' activities because they are not constrained by any limitations. Firstly, penetration testing may be governed by the laws and contractual obligations of the organization's system because if the test unintentionally retrieves highly confidential information, this may result in violating the laws and breaching of contractual agreements. If an ethical hacker accesses an individual's SIN, this information will then be regulated by *Personal Information Protection Electronic Documents Act (PIPEDA)*. In particular, the Gramm-Leach-Bliley Act specifically states that "[n]o provision of this section shall be construed so as to prevent any financial institution…from obtaining customer information of such financial institution in the course of (1) testing the security procedures or systems of such institution for maintaining the confidentiality of customer information"[49]. Thus, ethical hackers are permitted to acquire customer's information for the purpose of testing a company's security system under US legislations. Secondly, if data is located and

[45] Bowker, Dave, Lesley Sulliva, and Chenxi Wang. "Leading Industry Analyst Recommends Penetration Testing."
[46] ibid
[47] ibid
[48] Raether, Ronald. "DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure."
[49] ibid

secured in another country, the laws of that country may prohibit what an ethical hacker can perform. In the *European Union Article 25(1)*, it evidently indicates that personal data cannot be extracted from the *European Economic Area (EEA)* unless the country offers "adequate" protection, and US is not considered to have "adequate" protection laws[50]. Finally, companies that outsource their IT infrastructure may restrict similar techniques due to the licensing agreements. All of these restrictions imply that organizations and ethical hackers should take additional measures to reduce the risks of unwanted liability by having detailed written agreements between the company and ethical hacker to define the scope, objective, terms and any limitations in the engagement[51]. In addition, a penetration testing is usually performed within limited resources over a specific period of time. Therefore, once an ethical hacker has identified the current risk and threats exposed to the system, the organization should immediately take corrective action to mitigate these security loopholes and decrease the potential exposure to malicious hackers.

IX. Impact of the CA Profession

There is an increasing demand of assurance over the protection of an organization's information system from "management, audit committees, board of directors, customers, consumers and other stakeholders"[52]. Similar to audit opinions on the adequacy of controls of information systems such as SysTrust, WebTrust and Section 5900[53], penetration testing can also help provide this type of assurance to management and its auditors on how organization has managed the information system to protect its assets. In the same manner, legislations, such as PIPEDA, Gramm-Leach-Act and Sarbanes-Oxley Act, are placing a greater emphasis on the responsibility of organizations to protect the privacy, confidentiality and integrity of the information system[54]. As a result, penetration testing strengthens the assurance of audit opinions and conformity with various legislations.

The relationship between auditing and penetration testing is that auditors are simply trying to identify all of the security vulnerabilities that exist in the system while penetration testers use these flaws in an attempt to access in the same way that a malicious hacker does. As a result, these two services are often performed together in which an audit is first performed and then a penetration testing. This will provide a better understanding of the extent and magnitude of how each type of vulnerability can have a negative impact on the organization[55].

According to the Information Systems (IS) auditing standards, penetration testing is a form of IS auditing procedure. This is particularly relevant for IS auditors and those with *Certified Information Systems Auditor* (CISA) designations. *Controls Objective for Information and Related Technology* (COBIT)

---

[50] Raether, Ronald. "DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure."
[51] ibid
[52] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."
[53] ibid
[54] ibid
[55] Allsopp, Wil. *Unauthorized Access: Physical Penetration Testing for IT Security Team*.

is a widely accepted IT governance framework used by IS auditors to gain an understanding of the company's objectives, processes and control procedures. The framework explicitly states that "it is management's responsibility to safeguard all assets of the enterprise"[56]. Thus, management is required to take actions to mitigate and control security risk, and IS auditors are only responsible to identify the key weaknesses that management failed to place a control upon the system.

The main difference between an IS auditor's objective and a malicious hacker is that an IS auditor must identify all possible vulnerabilities in a system while it only takes one vulnerability for the hacker to exploit the system. *Appendix B* illustrates a suggested and comprehensive approach for penetration testing procedures which can be undertaken by an IS auditor. In addition, IS auditors can use the red team's method and extensive testing as an advantage to better understand the changing security risks and threats. Penetration testing goes beyond the traditional methods performed by auditors, and can be a seen as a valuable tool for them to assess an organization's security risks.

X. Examples of Penetration Testing Companies/Education

An example of a company that provides ethical hacking is *eTechSecurityPro*. The company identifies that when business have developed an "it-won't-happen-to-me"[57] attitude, this undoubtedly increases the chance of intrusion attacks into their systems. *eTechSecurityPro* also recognizes that regardless of a small, medium or large business, they are all equally vulnerable to IT attacks. As a result, the value-added services to an organization can be significant because it helps prevent and detect the occurrence of real online hacking before it is too late to mitigate the security gaps in the system.

Companies that specialize in the enhancement of employee security awareness are *Cyveillance* and *Wombat*, a leading cyber intelligence and cyber security training company respectively[58]. All of the employees promptly receive a threat assessment education session, and the two companies test users with simulated phishing attacks, such as deceiving them to assess whether they would click on a malicious hyperlink. This specialized phishing software allows the customization of "phishing and spare phishing email templates"[59] to simulate real phishing methods. After these tests, there would be follow-up training sessions on the employees who were identified as most susceptible and vulnerable to the attacks. It is critical that every employee is properly trained to strengthen their own level of security awareness. This will in turn lead to fewer successful social engineering attacks and network/system disruptions, as well as reduce the potential loss of sensitive information into the hands of an unauthorized user.

The current security education is that attacking is better than defense because it gives students a better understanding of how security systems fail, and teaches them to acquire faster abilities to tackle and solve security issues[60]. This may be in contrary to the norm in which defense should be taken rather than offence. Nevertheless, it is believed that any type of security technique can be used properly or

[56] "IS Auditing Procedure: Security Assessment – Penetration Testing and Vulnerability Analysis."
[57] Nemati, Hamid. "The Expert Opinion."
[58] "Cyveillance; Cyveillance and Wombat Security Technologies Team Up to Educate Organizations on Social Engineering Threats."
[59] ibid
[60] Mink, Martin. "Is Attack Better than Defense? Teaching Information Security the Right Way."

abused, such as penetration testing can either become “black hats” or “white hats”. The U.S. Air Force Academy is an example that supports offensive security methods to be undertaken by its students[61]. This shows that penetration testing, an offensive technique, is a more widely accepted method nowadays.

XI. Current Issues

With the increasing usage of Internet by organizations, it is changing the way how organizations conduct businesses with its customers. As a result, the security environment risks and threats are also evolving at the same time. In May 2011, Sony’s PlayStation video games were hacked and resulted in a loss of personal data from approximately 77 million users[62]. Even though Sony has taken the appropriate actions by strengthening its network against potential attacks in the future, these security measures were performed after-the-fact. Had a penetration test been performed as a preventative measure, Sony could have not been in breach of contract, the availability of PlayStation Network would have continued, no lawsuits would have resulted against the company for compensation and damages, no complimentary downloads for 30 days and no apology made by Sony. In addition to the PlayStation’s incident, Sony Ericsson’s Canada eShop[63] encountered a security breach in which 2,000 customer accounts (first and last names, email addresses and the hash of the encrypted passwords) were hacked. There have been at least 10 known Sony hacking activities since April 2011, emphasizing that Sony is a big target for hackers. This reinforces the fact that penetration testing is a worthwhile investment because it can help potentially mitigate all of the financial and non-financial losses of multi-billionaire companies such as Sony.

In 2011, there has also been a series of recent hacking at multiple corporations and financial institutions. Google’s Gmail accounts of hundreds of users, including “senior U.S. government officials, military personnel and political activities”[64] have been hacked on June 1. Furthermore, 200,000 of Citibank’s credit card customers have been stolen by malicious hackers who intruded into its online account website on June 9[65]. Hackers also successfully penetrated into a marketing company, Epsilon, with big customers such as Best Buy and Target Corporation[66].

Through these various attacks, organizations have realized that their security systems are inadequate and cannot properly protect their sensitive information database. This shows a greater need for penetration testing nowadays, especially for the high-profile corporations, due to the frequency and magnitude that hackers can negatively inflict on a corporation’s financial and non-financial status.

XII. Challenges to Overcome

One obvious aspect to consider is the challenge of quantifying the benefit from a penetration testing. The difficulty lies in the nature of being a preventative testing and can only be given a quantified number if hacking were to happen in absence of the test. As mentioned in the current security education,

[61] Mink, Martin. "Is Attack Better than Defense? Teaching Information Security the Right Way."
[62] "In latest attack, hackers steal Citibank card data."
[63] Yin, Sara. "Sony Hackers Take Canada."
[64] Pallavi, Gogoi, and Kelvin Chan. "In latest attack, hackers steal Citibank card data."
[65] ibid
[66] ibid

penetration testing is still a "hard sell"[67] for companies because they have developed a mentality that defense is better than offence, and do not fully understand that all of the benefits derived from the test. Preventing errors is more effective and less costly than detecting and correcting errors in the later stages. A rule of thumb is that one hour spent on preventing will reduce the time to correct errors from three to ten hours, and the cost of correcting the error amounts to approximately 50 to 200 times more than the preventative phase[68]. Furthermore, penetration testing should not be viewed as a disrespect or offence to the competence of any organization, and it should be explained that the red team engagement is an excellent technique to assess the company's overall effectiveness and efficiency. Auditors are also encouraged to increase their awareness of hacking tools by attending training sessions on a timely basis.

XIII. Recommendations

An organization should consider penetration testing as part of its overall security strategy based on two factors: *significance* and *likelihood* of security exploitation by malicious hackers[69]. "Security controls are the foundation of trust"[70] placed by stakeholders in the organization. Thus, the significance relates to the degree of the breach in trust by the customers, employees and other stakeholders. The likelihood of occurrence relates to the "target of choice"[71] and "target of opportunity"[72]. If an organization is large in size and has a high profile, such as the government or banks, they are the preferred target. If an organization has a lack of security controls, they are more susceptible to the higher incidence for attacks due to the relative ease of access. Therefore, if an organization estimates its security breaches would result in high significance and likelihood, then it may be cost-beneficial to run a combined automated and manual penetration testing with various internal and external techniques as part of its security strategy.

XIV: Conclusion

Penetration testing is an important component of an organization's overall security strategy and can definitely add value if there are major security weaknesses in its system controls, and a high risk of unauthorized access due to the nature and operations of the business. Through controlled attempts to intrude into computer's network system, a combination of penetration testing techniques and strategies can be developed to fit an organization's needs in terms of nature of business, size and complexity of its operations. This will in turn enhance the assurance provided from auditors in assessing a company's internal controls and security system at the same time. On the whole, ethical hacking and penetration testing should be considered as an efficient and effective means to mitigate and close security gaps and deficiencies before malicious hackers can otherwise exploit them.

---

[67] Gallegos, Federick. "Red Teams: An Audit Tool, Technique and Methodology for Information Assurance."
[68] Oezlem Aras, Barbara. "Secure Software Development—The Role of IT Audit ."
[69] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."
[70] ibid
[71] ibid
[72] Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk."

Appendix A: Screenshot of Google Hacking Technique[73]

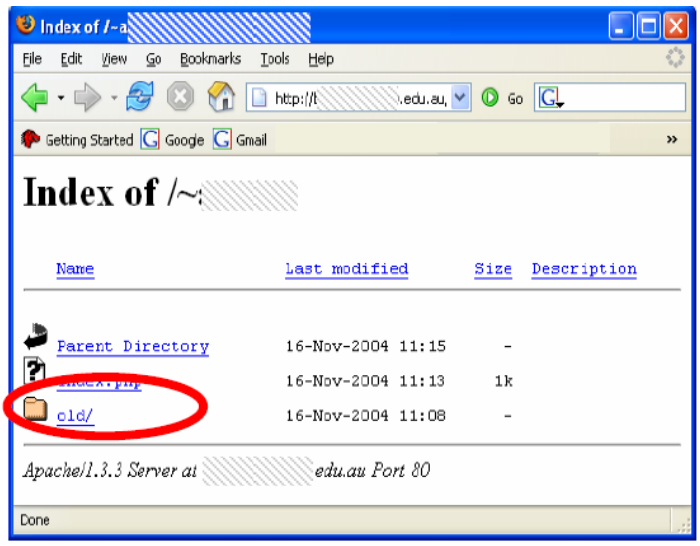


Figure 4. Results of an advanced operator query string

[73] Lancor, Lisa. "Using Google Hacking to Enhance Defense Strategies."

Appendix B: Example of Penetration Testing Procedures for IS Auditors[74]

SUGGESTED PROCEDURES

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Planning	Define the scope based on the nature, timing and extent of the evaluation.	
	Verify that no test will violate any specific law of local or national statute. Also, the auditor should consider obtaining a signed "authorisation form" from the organisation agreeing to the deployment of penetration testing tools and methods.	
	Investigate and use available automated tools to perform penetration testing and vulnerability assessments. These tools improve the efficiency and effectiveness of penetration testing.	
	Define the scope of the review by asking the following questions: ■ Will the chief information officer, computer security and IT personnel be told of the penetration test? ■ Will the audit testing focus on detecting control weaknesses from those accessing the information infrastructure from the Internet and dial-in access (external) or from inside the organisation (internal)? ■ How far into the network and information asset will the penetration testing be performed? For example, will the testing be performed to the extent of actually accessing the information assets or will it occur to an access check point (where access to the information assets is not accomplished but there is sufficient information that it could occur based on testing)? Will the test be intrusive or nonintrusive? ■ What level of overall system degradation, and for what duration, will be acceptable in performing the tests? ■ Can the test be performed off hours to avoid potential conflicts with causing critical system outage (e.g., executing nmaps against firewall off hours, such as Sunday morning, while web application services are not used)?	
	Obtain access to a (public) vulnerability database, such as bugtraQ, packetstorm, etc. The tester should determine that any tools used are up to date with the latest vulnerability database.	
Skills Required	Possess sufficient technical knowledge of, and ability to recognise and/or detect different types and variations of, security flaws/bugs/weaknesses/vulnerabilities. For example, the individual should have an understanding of the controls required over dial-in penetration, denial-of-service, password cracking, buffer overflows and wireless, as well as have access to up-to-date vulnerabilities database services.	
	Possess strong knowledge of how various technologies work, such as firewalls and routers, intrusion detection systems, and various types of authentication mechanisms.	
	Possess working knowledge of application programming, such as JAVA, Visual Basic and C++.	
	Possess knowledge of various operating systems, such as UNIX, Linux, NT/2000, Windows and OS/390 (or its current mainframe version).	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Skills Required continued	Possess working knowledge of TCP/IP and networking protocols.	
	Possess working knowledge of web server software, including Microsoft IIS and Apache.	
	Possess knowledge in utilising the penetration tools selected to detect bugs and vulnerabilities.	
	Possess knowledge of the effect on the internal system of executing penetration and vulnerability tools, including the NMAP, ISS, Whisker, Nikto, WebInspect, AppScan, ESM and Root, Nessus.	
Agreements	Keep all records, including specific and detailed logging of all keystrokes and verbal discussions, of all activities during the penetration and vulnerability testing. These records should be in sufficient detail to recreate the test, if necessary.	
	Keep all records of the penetration testing, including the results, confidential as they are the property of the organisation. All records of the penetration and vulnerability testing should be maintained within the organisation's control. The individual performing the test should sign nondisclosure and code of ethical conduct statements with the organisation regarding the confidentiality of the scope of the test and results.	
	If the test is to be performed by external consultants, include a contract to protect the organisation. The contract should state the boundaries and scope of the work to be performed, the ownership of the results and test procedures, as well as require confidentiality and ethical conduct of the consultants. In addition, the external consultant should provide insurance and a "hold harmless" clause to mitigate risks as a result of an inadvertent release of information.	
Scope Questions	Does the testing consist of evaluating the control environment based on penetrating the information infrastructure from inside vs. outside the network perimeter? For example, if the test consists of evaluating the firewall rule set based on attempted access to penetrate the network from the Internet, the evaluation is focused on determining the access control from outside the network perimeter. Testing of perimeter controls is limited in scope to the physical and logical controls that safeguard the information assets from those threats external to the organisation. However, once the perimeter security controls are compromised, a decision should be made, whether to continue testing to determine the adequacy of the controls over the target information systems. Conversely, the vulnerability testing may be focused on evaluating the internal control environment to prohibit access to information assets from inside the organisation.	
	Is the appropriate level of management, including IT security, notified of the penetration or vulnerability testing? If a formal announcement is made of the testing, strong cooperation and more thorough evaluation may be achieved. Conversely, unannounced testing may better represent the actual risks and management's response based on real-world threats from unauthorised access attempts. It is essential to assess the best-case scenario and level of assurance needed.	
	Are the individuals performing the test provided information about the organisation in advance? This question goes with whether management is notified of the nature and scope of the test. However, there are times when just the executive or high-ranking IT management is notified of the test and it is not announced to the staff. Nevertheless, if information is provided (i.e., network topology) and used by the tester, a more exact review of the target systems and processes can be examined, possibly resulting in better identification of risks and vulnerabilities. However, providing insider	

[74] "IS Auditing Procedure: Security Assessment – Penetration Testing and Vulnerability Analysis."

	possibly resulting in better identification of risks and vulnerabilities. However, providing insider information may result in difficulty in understanding the depth of the vulnerabilities and their likelihood of exploitation. In addition, the IP ranges, if provided by management ,should also be tested.	
Internet Penetration Testing	Network enumeration is the information obtained: network resources and shares, user logins including generic installation (out of the box) hardware and software vendor user IDs, IDs and their groups, and applications and banners. The steps to consider are: ■ Identify the domain name, IP address range and other critical information. Ordinarily, the "who is" query is used, which typically provides the address of the target network (i.e., domain name servers and IP address mapping), administrative contact and billing contact. The individual executing the "who is" query should provide reasonable assurance that all listings are obtained, and not just the first 50 items, which may require grouping the names into plurals or modified organisation names. ■ Identify IP address ranges that may be owned by the organisation. This is typically done by querying Internet number registries such as ARIN, RIP, APNIC and LACNIC. ■ Identify external e-mail servers by gathering MX record information from DNS servers. ■ Attempt a zone transfer between all systems identified as a DNS server (including back-up servers) to obtain the network IP listing and the machine host names. A zone transfer requests the complete list of matched IP addresses and host names stored within a DNS for a specified domain. In addition, the "nslookup," which is supported by both the UNIX and Windows platforms, may also be used to perform a zone transfer using a DNS server that is authoritative for the domain of interest. In addition, the machine's host names may indicate its purpose (i.e., mail server and firewall), which is one more critical piece of information. Recent technologies prevent the ability to perform a zone transfer without the initiating device. ■ Determine whether the organisation has outsourced its domain name function to an Internet service provider (ISP). In cases where this function is outsourced, it is recommended that the terms of the penetration test clearly state whether the hosted system is within the scope of the engagement. ■ Notify network staff that a penetration test may be underway because zone transfer can be detected. ■ Use ICMP (ping) or TCP ping (with a full or half TCP handshake) sweeps to determine which machines for IP addresses are "up" or "live." Though this step may provide critical information	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Internet Penetration Testing continued	regarding which devices are active, there is a likelihood that perimeter security devices or firewalls may drop the ICMP traffic to the host. It may be filtered and dropped with a response indicating the device is down, when it is not. It is recommended that randomising the order of the IP addresses being pinged helps avoid detection, as does varying the NMAP. NMAP is a popular tool used for UNIX-based systems and Pinger, and Ws PingPro Pack are used in Windows-based environments for performing Ping sweeps. ■ Use the traceroute method to identify the paths from the Ping packets to the destination target. The routes can then be traced to the destination live hosts, detected using the Ping sweeps to derive an estimated map of the organisation's architecture topology. The two commonly used tools are tracer route and tracert, available for both UNIX- and Windows-based operating systems. The purpose of this method is to identify the common and uncommon "hops" prior to reaching the destination targets, which could represent such things as firewalls, filtering routers or other gateways, load-balancing devices ,or web redirectors. It is not uncommon for network segments to have multiple connections to the Internet—unknown to the network group. However, these uncommon paths can lead to network compromises, if uncontrolled. ■ Send "bogus" e-mail messages to domains owned by the organisation in an attempt to receive a returned e-mail. Review the header of returned e-mails to determine possible network paths.	
	To perform a vulnerability analysis: ■ Assess possible methods of attacks based on identification of vulnerabilities. To do this, identified machines within the target network are examined to identify all open ports, the operating systems (OS), the applications and their hosts (including version number, patch level and/or service pack). In addition, this information is compared with Internet vulnerability databases to ascertain what current vulnerabilities and exploits may be applicable to the target network. ■ Identify the type of OS employed by target hosts. For those target hosts identified in the network enumeration phase, the NMAP tool can be used to identify the type of OS employed. The type of OS employed is critical in predicting the types of service available and then to tailor the targeted analysis of service rendered through that port, which, when executed, will determine if specific vulnerabilities exist. In conjunction with this step is the need to obtain a current list of vulnerabilities for the OS employed by searching the OS vendor's web site and vulnerability databases to obtain details of these vulnerabilities. ■ Obtain permission to execute a port scan for those destination target hosts that are "live." A port scan may be needed on all possible ports (1-65535), if the security group is aware of the penetration testing. The list of ports should include applications that have known vulnerabilities. Ports examined should relate to weaknesses, vulnerabilities or information gathering. For example, the ports for file transfer protocol (FTP), Telnet, and RealSecure (ports 21, 23 and 2998) are often selected to attempt to exploit vulnerabilities. NMAP is the standard tool and can be programmed to execute a port scan for those destination target hosts that are "live" (from a port scan). Port scanning is clearly unethical without the express permission of the port owner. Port scanning, as with many other vulnerability tests, is a	

Bibliography

Allsopp, Wil. *Unauthorized Access: Physical Penetration Testing for IT Security Team*. John Wiley & Sons Ltd, 2009. 242-244. Print.

Baker, Gary, and Simon Tang. "CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk." *The Canadian Institute of Chartered Accountants* . N.p., 2003. Web. 29 May 2011. <http://www.cica.ca/research-and-guidance/documents/it-advisory-committee/item12038.pdf>.

Basta, Alfred, and Wolf Halton. *Computer Security and Penetration Testing*. US: Thomson Course Technology, 2008. 1-403. Print.

Bowker, Dave, Lesley Sulliva, and Chenxi Wang. "Leading Industry Analyst Recommends Penetration Testing." *Core Security Technology* (2011): n. pag. *Factiva*. Web. 1 Jul 2011. <http://global.factiva.com.proxy.lib.uwaterloo.ca/ha/default.aspx>.

"Cyveillance; Cyveillance and Wombat Security Technologies Team Up to Educate Organizations on Social Engineering Threats." *Investment Weekly News* (2011): n. pag. *Factiva*. Web. 28 May 2011. <http://global.factiva.com.proxy.lib.uwaterloo.ca/aa/?ref=INVWK00020110506e75e0007v&pp=1&fcpil=en&napc=S&sa_from>.

Dimkov, Trajce, Andre Cleeff, Wolter Pieters, and Pieter Hartle. "Two methodologies for physical penetration testing using social engineering." (2010): 1-10. *ACM Digital Library*. Web. 1 Jun 2011. <http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/370000/366183/p15-mcdermott.pdf?ip=129.97.58.73&CFID=25246028&CFTOKEN=63747607&__acm__=1307142495_3348a0494410806a333778971294c570>.

Fath, Kim, and John Ott. "Risk Associated with Web Application Vulnerabilities." *ISACA Journal* 1. (2009): n. pag. Web. 31 May 2011. <http://www.isaca.org/Journal/Past-Issues/2009/Volume-1/Documents/jpdf0901-risk-associated.pdf>.

Gallegos, Federick, and Matthew Smith. "Red Teams: An Audit Tool, Technique and Methodology for Information Assurance." *ISACA Journal* 2. (2006): n. pag. Web. 1 Jun 2011. <http://www.isaca.org/Journal/Past-Issues/2006/Volume-2/Pages/Red-Teams-An-Audit-Tool-Technique-and-Methodology-for-Information-Assurance1.aspx>.

Gohring, Nancy. "Policy, Education Key to Reining in Rogue Cloud." IDG News. PC World, 15 12 2010. Web. 1 Jul 2011. <http://www.pcworld.com/businesscenter/article/213769/policy_education_key_to_reining_in_rogue_cloud.html>.

"In latest attack, hackers steal Citibank card data." *Security*. CBR, 02 05 2011. Web. 30 Jun 2011. <http://security.cbronline.com/news/sony-apologises-for-playstation-network-security-breach-020511>.

"IS Auditing Procedure: Security Assessment – Penetration Testing and Vulnerability Analysis." *ISACA Journal* (2004): 1-11. Web. 30 May 2011. <http://www.isaca.org/Knowledge-Center/Standards/Documents/P8SecAssess-PenTestandVulnerabilityAnalysis.pdf>.

Lancor, Lisa, and Robert Workman. "Using Google Hacking to Enhance Defense Strategies." (2007): 491-495. *ACM Digital Library*. Web. 2 Jun 2011. <http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/1230000/1227475/p491-lancor.pdf?ip=129.97.58.73&CFID=25246028&CFTOKEN=63747607&__acm__=1307145364_62994943eb553ec1ffffc9d24d24f769>.

Langley, Nick. "Find rich rewards but little glamour in ethical hacking." *Computer Weekly* (2006): 68. *ABI Inform*. Web. 22 May 2011. <http://proquest.umi.com/pqdweb?index=2&did=1165854241&SrchMode=2&sid=8&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306450335&clientId=16746>.

Mink, Martin, and Felix Freiling. "Is Attack Better than Defense? Teaching Information Security the Right Way." (2006): 44-48. *ACM Digital Library*. Web. 2 Jun 2011. <http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/1240000/1231056/p44-mink.pdf?ip=129.97.58.73&CFID=25246028&CFTOKEN=63747607&__acm__=1307144033_ea048a7de7c102a4e8d59de269baac83>.

Mohan, Sriram. "YourStory in conversation with Bikash Barai, CEO of iViZ on cloud-based penetration testing and raising Series A funding from IDG Ventures." *YourStory* (2011): n. pag. *Factiva*. Web. 28 May 2011. <http://global.factiva.com.proxy.lib.uwaterloo.ca/ha/default.aspx>.

Nemati, Hamid. "The Expert Opinion." *Journal of Information Technology Case and Application Research* 9.1 (2007): 59-64. *ABI Inform*. Web. 20 May 2011. <http://proquest.umi.com/pqdweb?index=1&did=1271340741&SrchMode=2&sid=4&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306449265&clientId=16746>.

Oezlem, Aras. "Secure Software Development—The Role of IT Audit ." *ISACA Journal* 4. (2008): 1-11. Web. 1 Jul 2011. <http://www.isaca.org/Journal/Past-Issues/2008/Volume-4/Pages/Secure-Software-Development-The-Role-of-IT-Audit1.aspx>.

Pallavi, Gogoi, and Kelvin Chan. "In latest attack, hackers steal Citibank card data." Yahoo News, 09 06 2011. Web. 25 Jun 2011. <http://old.news.yahoo.com/s/ap/20110609/ap_on_hi_te/as_citigroup_data_breach>.

Pashel, Brian. "Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level." (2006): 197-200. *ACM Digital Library*. Web. 2 Jun 2011. <http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/1240000/1231088/p197-pashel.pdf?ip=129.97.58.73&CFID=25246028&CFTOKEN=63747607&__acm__=1307146063_a6c7ccebb4b0c6d7c06a3395a3823375>.

Pulley, John. "Are there perils in penetration testing?." *Federal Computer Week* 21.4 (2007): 62-63. *ABI Inform*. Web. 20 May 2011. <http://proquest.umi.com/pqdweb?index=11&did=1230216401&SrchMode=2&sid=5&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306447619&clientId=16746>.

Raether, Ronald. "DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure." *Business Law Today* 18.1 (2008): 55-58. *ABI Inform*. Web. 22 May 2011. <http://proquest.umi.com/pqdweb?index=12&did=1574334521&SrchMode=2&sid=10&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306451474&clientId=16746>.

Styles, Martyn, and Theo Tryfonas. "Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users." *Information Management & Computer Security* 17.1 (2009): 44-52. *ABI Inform*. Web. 20 May 2011. <http://proquest.umi.com/pqdweb?index=2&did=1880591681&SrchMode=2&sid=4&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306442582&clientId=16746>.

Wilhelm, Thomas. "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab." *Google Books*. Elsevier Inc, 2010. Web. 23 May 2011. <http://books.google.com/books?id=AcscdZ6Bs40C&printsec=frontcover&dq=penetration+testing&hl=en&ei=GLriTY2jDNTTgQemudy9Bg&sa=X&oi=book_result&ct=result&resnum=3&ved=0CDgQ6AEwAg#v=onepage&q&f=false>.

Yin, Sara. "Sony Hackers Take Canada." *Security*. PCMag, 25 05 2011. Web. 30 Jun 2011. <http://security.cbronline.com/news/sony-apologises-for-playstation-network-security-breach-020511>.

Annotated Bibliography - Penetration Testing:

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Styles, Martyn (Allen & Overy LLP, London, UK) Tryfonas, Theo (University of Bristol, Bristol, UK)	Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users	Information Management & Computer Security	Vol.17, No.1, Iss.1	2009	44-52	May 20, 2011	ABI Inform. http://proquest.umi.com/pqdweb?index=2&did=1880591681&SrchMode=2&sid=4&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306442582&clientId=16746

Annotation #1: Increase Security Awareness of Employees:

- Strong computer security system arises from the employee's enhanced security awareness because their lack of knowledge about security issues may inflict more damages to a company's computer system than malicious employees.
- Companies are encouraged to focus on user involvement in security awareness initiatives rather than investing in the most updated security technology
- Case study:
  - *Password Cracks Software:* 61.49% of all employee passwords classified as high risk, cracked in less than 1 minute
  - *Security Awareness Questionnaire*: 44/102 employees believed that common dictionary words were appropriate and legitimate passwords, and many have followed cars into the office parking lot because they forgot to bring their access card, and only 28% have questioned an unknown visitor walking around in the office workplace
  - *Email Scam Test (Phishing*): 19% could not recognize a fake PayPal request for verifying account information, 23% could not recognize a fake Lloyds bank account request, and 16% could not recognize a false MSN verification account
- Key success factors to enhance stronger internal security environment:
  - Externalizing exposure
  - Engagement of senior management
  - Assessment based on online survey
  - Tests based on real-incident data
  - Involving IT security component at all staff levels (including technical and non-technical)

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Pulley, John	Are there perils in penetration testing?	Federal Computer Week	Vol. 21, Iss. 4	2007	62-63	May 20, 2011	ABI Inform. http://proquest.umi.com/pqdweb?index=11&did=1230216401&SrchMode=2&sid=5&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306447619&clientId=16746

Annotation #2: Pros and Cons of Automated Penetration Testing:

- Penetration testing goes beyond “tapping at the door”, but it “breaks through the door”
- A detailed, manual penetration testing could take up to a several weeks to complete and cost thousands of dollars, but automated-assisted tools can perform test within several hours only.
- Increasing vulnerability of identity theft such as cybercrimes of online hacking → improvement of computer systems and networks against both internal and external threats.
- Pros of automated penetration testing:
  - It helps to perform maintenance between “full-blown” security assessments
  - It can add value to a computer system if it is managed and executed properly
  - It can be cost-effective and efficient
  - It has the ability to perform penetration testing as frequent as they want in the organization
- Cons of automated penetration testing:
  - Using automated tool may not be always effective because it is a step behind the “elite attacker’s exploits”
  - Overreliance of automated penetration testing can lead to a false sense of security because those tests are only as effective as the people who are running those automated tests. It is not a “silver bullet” that can guarantee to catch 100% all the holes in the system.
  - “A fool with a tool is still a fool”: This quote means that if an untrained employee handles the automated penetration testing, this could do more harm to the company than the good intentions
  - This is a lack of substitution and incomparability to an extensive manual testing performed by a knowledgeable and skilful practitioner

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Nemati, Hamid R	The Expert Opinion	Journal of Information Technology Case and Application Research	Vol. 9, Iss. 1	2007	59-64	May 20, 2011	ABI Inform. http://proquest.umi.com/pqdweb?index=1&did=1271340741&SrchMode=2&sid=4&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306449265&clientId=16746
Annotation #3: Example of Ethical Hacking Company (eTechSecurityPro): • How IT security and consulting company can help businesses with ethical hacking/penetration testing procedures: • Internet's greatest strength of its "ubiquitous presence and global accessibility" is also its greatest weakness at the same time. • Many types of hacking such as viruses, Trojan horses, and denial of service attacks, such as 60 to 80% of U.S. companies were affected by the Melissa and "I Love You" viruses in 2000 • Business have developed an "it-won't-happen-to-me" attitude → increase chance of hackers to attack anyone and anywhere • Regardless of a small, medium or large business, all are equally vulnerable to a cyber attack • Ethical hacking services to help prevent and detect the occurrence of real online hacking before it is too late to correct the loopholes in the system							
Langley, Nick	Find rich rewards but little glamour in ethical hacking	Computer Weekly.	n/a	2006	68	May 22, 2011	ABI Inform. http://proquest.umi.com/pqdweb?index=2&did=1165854241&SrchMode=2&sid=8&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306450335&clientId=1674
Annotation #4: Career Designation as an Ethical Hacker: • Ethical hackers attempt to use the same or similar techniques as criminal hackers would use to attack/break into an organization's systems to expose security gaps, which would later be closed. • It should be noted that those who have great hacking abilities and break into unauthorized systems may be forever blacklisted and reputable companies, such as IBM, have explicitly stated that they will not hire "criminal hackers no matter how talented they are". • The Institute for Security and Open Methodologies offer to train ethical hackers and certifications are provided with the University of Glamorgan							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Raether Jr, Ronald	DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure	Business Law Today.	Vol. 18, Iss. 1	Sep/ Oct 2008	55-58	May 22, 2011	ABI Inform. http://proquest.umi.com/pqdweb?index=12&did=1574334521&SrchMode=2&sid=10&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1306451474&clientId=16746

Annotation #5: Elements of Ethical Hacking:

- Testing: most important process of ethical hacking because it is the fundamental concept of any effective data security network and requires constant monitoring and having "controlled attempts" that attack the computer's security barriers
- "Ethical or white hat hackers": Using similar or the same techniques/tools of a malicious hacker
- Benefits of Penetration Testing
    - Learn from the experience and further improve security if lessons learned are properly analyzed, changes implemented and information is distributed to all parties
- Penetration Testing Risks: Specific restrictions will define how far an ethical hacker can exploit the system or network
    1. May violate laws and contractual obligations that govern the system, such as Gramm-Leach-Bliley Act states that "[n]o provision of this section shall be construed so as to prevent any financial institution . . . from obtaining customer information of such financial institution in the course of (1) testing the security procedures or systems of such institution for maintaining the confidentiality of customer information."
    2. If the data is secured in another country, the laws of that country may restrict what can be performed by an ethical hacker
    3. Companies that outsource their entire IT infrastructure may prohibit similar techniques due to license agreements.
- Security concerns: technical problems, human error/mistakes and processing deficiencies such as deceiving employees into revealing sensitive information (social engineering or pre-texting) → attackers can compile and integrate the accumulated information to identify and exploit these opened weaknesses
- "For security, information is king"
- Identification of an ethical hacker:
    - Can be an internal employee or a third-party contractor
    - Perform background checks and ensure they are closely monitored by a person who is accountable by any failures
- Remedies and corrective action must be taken immediately because an ethical hacker can decrease the potential exposure to malicious hackers without negatively affecting the efficiency and purpose of penetration testing.

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Wilhelm, Thomas	Professional Penetration Testing: Creating and Operating a Formal Hacking Lab	Elsevier Inc	n/a	2010	13-18	May 23, 2011	Google Books. http://books.google.com/books?id=AcscdZ6Bs40C&printsec=frontcover&dq=penetration+testing&hl=en&ei=GLriTY2jDNTTgQemudy9Bg&sa=X&oi=book_result&ct=result&resnum=3&ved=0CDgQ6AEwAg#v=onepage&q&f=false

Annotation #6: Ethics and Hacking

- Black Hat Hackers: "bad guys"
  - Those who perform unauthorized penetration attacks against information systems, which may or may not be illegal in the country they are conducting
  - Intention of black hat hackers varies from simple curiosity to attaining a financial gain. They also do not follow any rules of engagement or legal regulations
- White Hat hackers (Ethical Hackers): "good guys"
  - Those who conduct security assessments within a contractual agreement, and they help improve the client's security system by discovering and exploiting the vulnerabilities, which are then mitigated by the company → concept of ethical hacking – breaking into the computer security for legitimate and appropriate reasons
- Grey Hat Hackers: "catch-all" group
  - Those who usually conduct their activities within the legal legislations and regulations, but may slightly go over the boundaries

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Cyveillance	Cyveillance; Cyveillance and Wombat Security Technologies Team Up to Educate Organizations on Social Engineering Threats	Investment Weekly News	n/a	2011	n/a	May 28, 2011	Factiva. http://global.factiva.com.proxy.lib.uwaterloo.ca/aa/?ref=INVWK00020110506e75e0007v&pp=1&fcpil=en&napc=S&sa_from

Annotation #7: Increase Security Awareness of Employees (Cyveillance & Wombat Companies):

- Cyveillance (a leading cyber intelligence company) and Wombat Security technology (a leading cyber security training and filtering technologies company) provide specialized training and testing for companies in response to the emerging social engineering threats
- All employees will receive threat assessment education on a timely basis
- It involves testing users with simulated phishing attacks, such as clicking on a malicious hyperlink
- With the increasing trend for social networks, blogs, it is critical that every single employee is properly train to increase their own level of security awareness. This will in turn lead to fewer successful social engineering attacks and consequently fewer network disruptions and loss of proprietary and sensitive information into the hands of an unauthorized user
- The specialized phishing software allows cyber security professionals to customize the "phishing and spare phishing email templates" to mock phishing methods in a timely manner, access the employees' cyber security awareness level and then offer appropriate training to those who are most susceptible and vulnerable to those cyber attacks

Author	**Title of Article**	**Periodical/ website**	**Vol. / No. / Edition**	**Year Pub**	**Pages**	**Date accessed**	**Location, data base, website, link**
Mohan, Sriram	YourStory in conversation with Bikash Barai, CEO of iViZ on cloud-based penetration testing and raising Series A funding from IDG Ventures	YourStory	n/a	2011	n/a	May 28, 2011	Factiva. http://global.factiva.com.proxy.lib.uwaterloo.ca/ha/default.aspx

Annotation #8: Automated Penetration Testing (iViz Company):

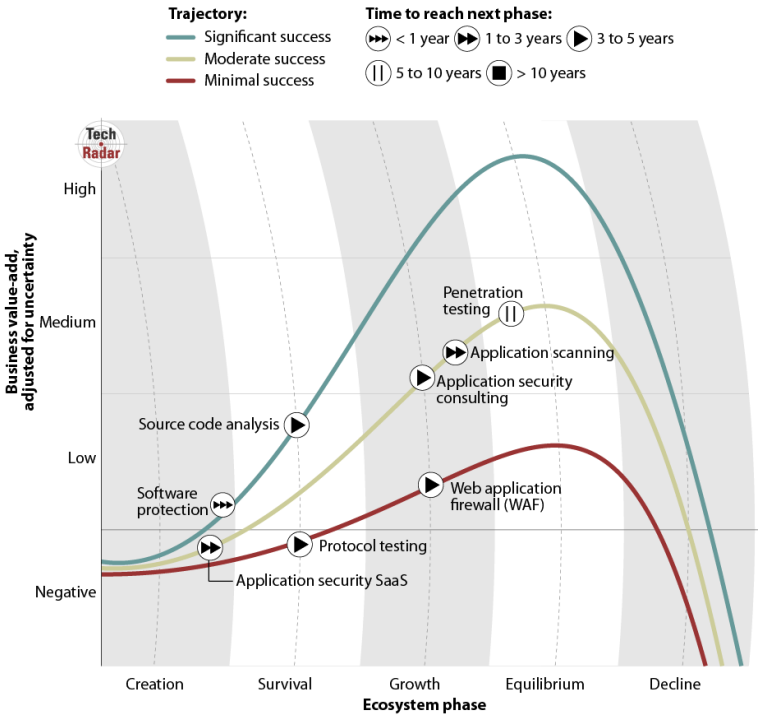
- iViz is the industry's first cloud-based penetration testing company and was nominated as the Top 6 Security companies by US Navy
- It is identified that there is a growing information security market
- Benefits of iViz/automated penetration testing:
  - Provides a high level of penetrating testing quality for applications with "on-demand SaaS experience"
  - Guarantees a zero false positive with the usage of "business logic testing and expert validation"
  - The use of artificial intelligence to simulate all different types of attacks
  - The ability and flexibility to test at anytime, anywhere and anyhow vs. consultants can only work during regular working hours
  - Eliminates the high consultant costs for manual testing
  - No software or hardware is necessary
  - Scalable
  - Subscription-based penetration testing for applications (SaaS)
- Salesforce comparison:
  - "What Salesforce did to CRM, iViz did to penetration testing"

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Bowker, Dave Sulliva, Lesley Wang, Chenxi	Leading Industry Analyst Recommends Penetration Testing	Core Security Technology	n/a	2011	n/a	May 28, 2011	Factiva. http://global.factiva.com.proxy.lib.uwaterloo.ca/aa/?ref=BWR0000020110329e73t000io&pp=1&fcpil=en&napc=S&sa_from

Annotation #9: Benefits of Penetration Testing

- Penetration testers help close the gaps between safeguarding the security information and mitigating/managing the key business risks
- Penetration testing can provide continuous automated testing to assess whether the security controls are adequate and are working effectively or not
- Security threat environment is ever-changing and companies are even at more risk because the stakes (financial loss, reputation) are high
- "If a company is not performing penetration testing, it is already behind the curve"
- Keeping up to date with the vulnerabilities in the security environment is a critical component of strategy because a company needs to understand its own weaknesses before it can protect and defend itself
- Cyber attacks are always changing in "nature, complexity and method "
- According to PCI and ISO 27001, managing vulnerabilities and threats is a key management process and a core IT function
- Exploit Statistics:
    - In 2004, 80% of key security vulnerabilities had an exploit within 60 days vs. in 2009, 85% had an exploit within 10 days
- "Window of Opportunity" is becoming larger as the time of the exploitation and eradication of the vulnerability is also widening
- A "hackers-eye" view of a company's network
- Wrong attitude: companies should not hope that they will not get hacked, but should take the measures to mitigate and control risk
- Strengthens the real-life security procedures and processes, improves efficiency and effectiveness of vulnerability management
- Increases transparency by determining the type of data that can be potentially exposed and how it can be attacked and by incorporating human-related elements such as social engineering and phishing techniques

Comparative Diagram: Penetration Testing: High Business Value-Add, Adjusted for Uncertainty



Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Baker, Gary (ITAC member) Tang, Simon (CPA) CISSP of Deloitte & Touche	CICA ITAC: Using an Ethical Hacking Technique to Assess Information Security Risk	The Canadian Institute of Chartered Accountants	n/a (Classic Paper for ITAC, whitepaper)	2003	1-17	May 29, 2011	http://www.cica.ca/research-and-guidance/documents/it-advisory-committee/item12038.pdf

Annotation #10: Ethical Hacking Implications – Teams, Limitations, Impact on Audit, Risk Level, Testing Methods:

- Consists of a chain of activities undertaken to identify and exploit security vulnerabilities – to discover how easy or difficult it is to "penetrate" an organization's security controls or to gain unauthorized access to the company's confidential information and its information systems
- Penetration testing teams:
    - Internal Audit department
    - IT department or
    - Specialized consulting firms for penetration testing services
- Limitations:
    - Cannot guarantee that an organization's information is secure because it is only conducted at one point in time
    - Changing technology, introduction of new hacker tools, and changes to organization's IT system can give rise to new unanticipated security risk exposures
    - Conducted with "finite resources over a finite period of time". Unlike real-life situations, hackers can break into any system at anytime, anywhere and are not restricted by these restrictions at all
- Impact on audit:
    - Audit opinions on adequacy of controls over IS, such as SysTrust, WebTrust and Section 5900 opinions, are increasingly used to provide this type of assurance on security
    - Legislations such as PIPEDA, Gramm-Leach-Bliley Act and Sarbanes-Oxley Act are placing a greater emphasis on the responsibility of companies to protect the privacy, confidentiality and integrity of information and information systems.
    - Penetration testing can provide that assurance in which management and auditors need on information security components to assess the adequacy of how a company uses and leverages its resources to safeguard its assets
- Risk of Unauthorized Intrusion:
    - High significance: security controls are foundation of trust, impact on audit (above)
    - High likelihood: "Target of choice" and "target of opportunity"
- Testing strategies: 1) external vs. internal testing, and blind and 2) double blind vs. targeted testing strategy
- Types of testing: application security testing, denial of service testing, war dialing, wireless network penetration testing, social engineering

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
ISACA	IS Auditing Procedure: Security Assessment – Penetration Testing and Vulnerability Analysis	Information Systems Audit and Control Association	Document P8	2004	1-11	May 30, 2011	ISACA Journal. http://www.isaca.org/Knowledge-Center/Standards/Documents/P8SecAssess-PenTestandVulnerabilityAnalysis.pdf

Annotation #11: IS audit (internal and external auditors):

- Planning Stage:
  - Formal risk assessment should be performed by identifying threats, hardware/software failures, as well as internal/external attacks
  - Unauthorized access risks: financial loss, inappropriate leakage of personal, commercial or politically-sensitive/confidential information, damaged reputation, loss of control in system
- Types of Penetration Testing:
  - External: Uses the Internet to attack targeted network, dial-in
  - Internal: vulnerabilities inside the network perimeter
  - Physical/Access Controls: rogue access
  - Social Engineering: telephone access, garbage viewing, desktop review
  - Wireless Technology: WEP for encryption, using the same server for wireless networks and other types of networks, default passwords, denial of service
  - Web Application: manual vs. automated
- Report: in accordance with ISACA IS Auditing Standards (scope, objectives, work performed, nature/timing/extent, conclusion)
- “human factor is typically the weakest link”

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Oezlem Aras, Barbara L. Ciaramitaro, Ph.D., CISSP, and Jeffrey Livermore, Ph.D	Secure Software Development—The Role of IT Audit	Information Systems Audit and Control Association	Volume 4	2008	n/a	May 31, 2011	ISACA Journal. http://www.isaca.org/Journal/Past-Issues/2008/Volume-4/Pages/Secure-Software-Development-The-Role-of-IT-Audit1.aspx

Annotation #12: Penetration Testing in SDLC Testing Stage:

- Testing phase in SDLC is essential
- In the process of testing security, the penetration tester has to think and act like an attacker by developing similar test scenarios to uncover potential vulnerabilities exposed in the organization's security system
- Weakness:
  - "Perhaps the most egregious mistake made in penetration testing processes, from the standpoint of their applicability to software development, is that they're almost always applied far too late in the life cycle."24 Penetration testing should be used early in the SDLC, as a form of stress testing a software system, to determine signs of vulnerability or breakability.
- Significant but worthwhile investment:
  - Preventing errors in early stages of SDLC is more cost-effective than correcting errors in the later stage
  - Rule of thumb: 1 hour spent for preventing will reduce the repairing/fixing error time from 3 to 10 hours, and repairs typically cost around 50 to 200 times more than in the requirements/beginning stage
  - Non-financial costs: damaged/negative reputation, loss of credibility, loss of trust in the eyes of customers/public

Fath, Kim Ott, John	Risk Associated with Web Application Vulnerabilities	Information Systems Audit and Control Association	Volume 1	2009	n/a	May 31, 2011	ISACA Journal. http://www.isaca.org/Journal/Past-Issues/2009/Volume-1/Documents/jpdf0901-risk-associated.pdf

Annotation #13: Web Application Software Vulnerabilities

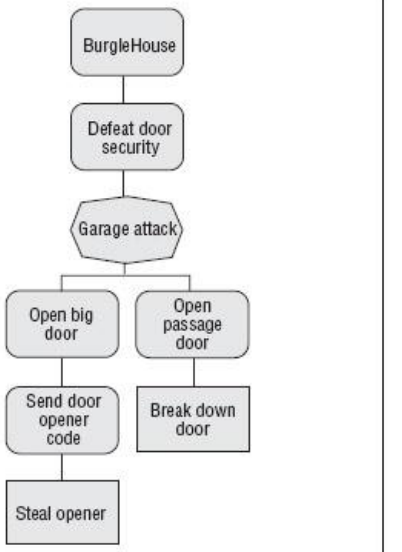
- Emgering Information technology environment:
  - Web application software is one of the top security weaknesses that can be exploited from the Internet (part of penetration testing)
  - Hackers are developing more advantaged and sophisticated tools in identifying weaknesses
- 3 rules to minimize risks associated with the web:
  - *Control access to sensitive information*: Example: A message should read, "An error has occurred by entering either an incorrect logon account or password," and should not plainly indicate that it was the incorrect password, and not the logon account
  - *Strong edit controls over data input*: never trust data transmissions when transferring on the browser, web server
  - *Embed vulnerability testing into SDLC:* Many large-size IT consulting and audit firms provide web application penetration testing - manual and automated

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Gallegos, Frederick Smith, Matthew L.	Red Teams: An Audit Tool, Technique and Methodology for Information Assurance	Information Systems Audit and Control Association	Volume 2	2006	n/a	June 1, 2011	ISACA Journal. http://www.isaca.org/Journal/Past-Issues/2006/Volume-2/Pages/Red-Teams-An-Audit-Tool-Technique-and-Methodology-for-Information-Assurance1.aspx

Annotation #14: Red Team – A Group of Penetration Testers – IS Auditors:

- What is a red team?
  - It consists of skilful and knowledgeable individuals who perform ethical hacking - rather than inflicting damages on the systems or stealing sensitive information, and the findings about the system flaws are reported back to the company
  - Red teams should not include internal staff because it violates the basic principle of testing your own system. Therefore, external auditors who perform a red team audit are not given information about network in order to exercise a real simulation of an unauthorized external attack
- How the red team audit engagement can assist IS auditors:
  - IS auditors can use the red team method to develop a better understanding of the changing security risks and threats
  - Red teaming process is part of both the assessment and maintenance phase of information security life cycle
  - Can help develop policy-making and improve all elements/functions in the information security life cycle
  - Based on the size of information system, auditors does not need to be directly participating with the red team engagement
  - Red team can be a valuable tool for auditors to assess risks to IS, going beyond the traditional techniques used by auditors
- Cultivating Security in the Organizations:
  - Auditors should understand the red team is not an offence or mockery to the competence of organization, but should explain that the red team engagement is a great and encouraging technique to assess the company's overall effectiveness and efficiency
- Attack Tree Figure:
  - Example: in order to break into payroll database, the attacker is required to guess the password. The estimated cost, ability and tolerance of the attack are then evaluated because it will help define the scope and timing of the red team engagement. This is an efficient process because it immediately eliminates those tests that are related to low chance and low value risks.
  - The Attack tree focuses on 3 points of vulnerability: 1) people, 2) policies and 3) technology
- 2 Difficulties to Overcome for IS Auditors:
  1. Auditors should heighten their awareness of tactics used by hackers by attending training sessions
  2. "Ethical Hacking" is still a "hard sell" for companies, and there is no easy approach for organizations to fully understand, accept and embrace the benefits of the red team (which outweighs the limitations)

Figure 3—Attack Tree



Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Dimkov,Trajce Cleeff,André van Pieters,Wolter Hartel,Pieter	Two methodologies for physical penetration testing using social engineering	University of Twente, The Netherlands	n/a	2010	1-10	June 1, 2011	ACM Digital Library. http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/370000/366183/p15-mcdermott.pdf?ip=129.97.58.73&CFID=25246028&CFTOKEN=63747607&__acm__=1307142495_3348a0494410806a333778971294c570

Annotation #15: Physical Penetration Testing using Social Engineering:

- Penetration tester directly communicates with the employee and uses deceptive tactics that can greatly damage or violate the employee's privacy and trust in the organization
- 5 requirements to an effective, meaningful and valuable penetration testing: realistic, respectful of employees, reliable to not damage the productivity loss of employees, repeatable, and reportable
- 2 Methodologies: Goal: to gain the asset by using social engineering techniques
    - *Environment-focused methodology (EF)*: measures security of environment where asset is located, i.e.) security of assets is in the CEO's office, but he is not aware of the asset; but the custodian is aware of the penetration testing
    - *Custodian-focused methodology (CF)*: more general, and the custodian is not aware of the test, but presents a more realistic approach that is less reliable and respectful to the employees ; it also tests the security awareness of the custodian

	EF methodology	CF methodology
Reliable	+++	++
Repeatable	-	-
Reportable	+++	+++
Respectful: actors	++	+
Respectful: trust relations	-	++
Realistic	+	+++

Figure 9: Evaluation of both methodologies

- CF methodology improves upon the EF one in many different ways, however the EF is considered more reliable as it does not deceive the custodian and fully informs all of the actors in the testing environment
- The paper has proven that physical penetration tests using social engineering can decrease the negative impact of the employee's actions, and provide useful and valuable information about the company's current security level

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Mink, Martin Freiling, Felix C.	Is Attack Better than Defense? Teaching Information Security the Right Way	InfoSecCD '06 Proceedings of the 3rd annual conference on Information security curriculum development	n/a	2006	44 - 48	June 2, 2011	ACM Digital Library. http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/1240000/1231056/p44-mink.pdf?ip=129.97.58.73&CFID=25246028&CFTOKEN=63747607&__acm__=1307144033_ea048a7de7c102a4e8d59de269baac83

Annotation #16: Attack is better than Defense

- Current trends in security education: it is recommended to teach offensive techniques performed by hackers over defensive ones, reflecting that penetration testing is a becoming a widely accepted practice
- Claim: teaching offensive methods is a "better" choice for security professionals than teaching defensive methods by itself
  - "Better understanding of how security systems fail
  - Faster to solve system issues, or
  - Can write better security programs"
- There is a flaw in the minds of people: If is actually criticized that offensive methods may increase the population of malicious employees or hackers.
- However, the paper argues that any security technique can be used properly or abused → penetration testing (offensive techniques) are used to increase level of company's security→ can become either black hats or white hats
- Examples supporting offensive techniques:
  - In 1999, University of Technology in Germany held a "Hacker Contests" in which students would try to utilize exploitation methods to attack the system in order to subsequently strengthen the defense measures
  - Wargames: capture-the-flag or deathmatch contests were held in which competing teams would battle over the network controls, Root-Fu contest in USA
  - offensive information security methods are positively supported by U.S. authorities, U.S. Air Force Academy

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Lancor, Lisa Workman, Robert	Using Google Hacking to Enhance Defense Strategies	SIGCSE '07 Proceedings of the 38th SIGCSE technical symposium on Computer science education	n/a	2007	491 - 495	June 2, 2011	ACM Digital Library. http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/1230000/1227475/p491-lancor.pdf?ip=129.97.58.73&CFID=25246028&CFTOKEN=63747607&__acm__=1307145364_62994943eb553ec1ffffc9d24d24f769

Annotation #17: Google Hacking

- Taking into consideration of Google hacking is effective web security measure because many businesses use Google as their primary search engines
- Google hacking: using the Google search engine to locate personal or sensitive online information where there is lack of data protection
- Example: found a directory with SIN of more than 70 million deceased persons, scanned passport documents, and a Justice Department site that lists all of the employee's business credit card numbers
- Penetration testers use Google hacking techniques during their investigation stage
- Screenshot:
    - Using the search query "intitle: "index of" site:edu "server at" → Google systematically locates and optimizes the search results anywhere in the webpages. Below shows a hyperlink to a folder "old" which may potentially consist of sensitive information for a malicious hacker to exploit

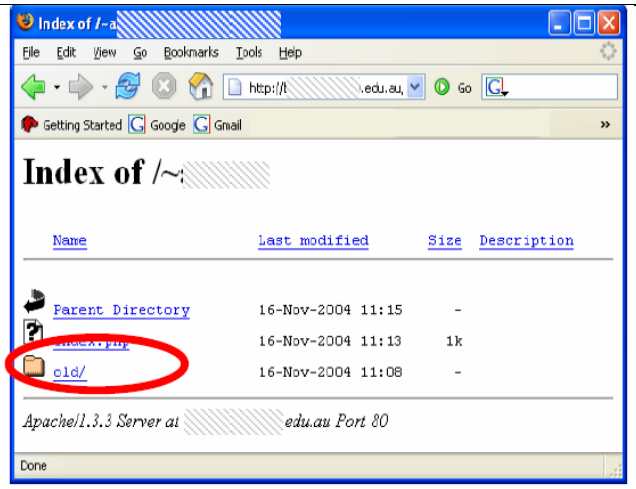


Figure 4. Results of an advanced operator query string

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Pashel, Brian A	Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level	InfoSecCD '06 Proceedings of the 3rd annual conference on Information security curriculum development	n/a	2006	197 - 200	June 2, 2011	ACM Digital Library. http://delivery.acm.org.proxy.lib.uwaterloo.ca/10.1145/1240000/1231088/p197-pashel.pdf?ip=129.97.58.73&CFID=25246028&CFTOKEN=63747607&__acm__=1307146063_a6c7ccebb4b0c6d7c06a3395a3823375

Annotation #18: Ethical Hacking

- Hacking is a widespread issue, especially with full access to the internet and other digital sources by anyone
- Ethical Hacking: “practice of hacking without the malicious intent”
- White Hats: hackers who use their hacking ability ethically, such as employees who attack a company’s network with permission to identify weaknesses
- Black Hats: highly skilled but used for criminal purposes
- Gray Hats: those who use computers to investigate or punish criminals, but are outside the scope of legal authorities and do not have the

consent and permission of the users

- Teaching university students on how to hack an organization's security system is a legitimate and effective method of identifying its critical weaknesses and act as a preventative measure of malicious attacks in the future

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Allsopp, Wil	Unauthorized Access: Physical Penetration Testing for IT Security Team	John Wiley & Sons Ltd	n/a	2009	242-244	June 2, 2011	University of Waterloo Davis Centre Library.

Annotation #19: Physical and Electronic Penetration Testing, Auditors and Penetration Testers

- "Security is only as strong as the weakest link in the chain" → security comes down to the people and trust
- 2 types of penetration tests:
  - *Physical testing*: it is challenging to decide who should be the testers, but a company is recommended to look for 1) proven experience firms, 2) documented methodology, and 3) respect in the industry
  - *Electronic Testing*: More popular and mature industry, most of the conducted testing is known as "security auditing"
- Relationship between Auditing and Penetration Testing:
  - It is about finding flaws and gaining access the same way as a hacker does while "auditing is simply trying to find and report on all the vulnerabilities present in the systems under test"
  - 2 services are often combined by performing an audit first, and then a penetration testing to have a clear distinction and demonstration of the types of vulnerabilities exposed
- Limitations:
  - Penetration test is only performed at a point in time and it does not guarantee that it will be secured next week or month
  - Testing will only give companies a general idea of where they are situated, and the nature of these attacks change constantly
  - Security is an on-going process and testing is only as good as those who are performing/developing the test

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year Pub	Pages	Date accessed	Location, data base, website, link
Basta, Alfred Halton, Wolf	Computer Security and Penetration Testing	Thomson Course Technology	n/a	2008	1-403	June 2, 2011	University of Waterloo Davis Centre Library.

Annotation #20: Types of Hacking:

- *Sniffers*– applications that "monitor, filters, and captures data packets" that are transferred over the network. It is unethically used to exploit basic operation network interfaces and TCP/IP
- *Encryption and Password Cracking*: the use of cryptography to hide the actual text passwords or encryption of asymmetric/symmetric keys; Password cracking program: Cain and Abel
- *Spoofing*- misrepresenting the sender's message (i.e. email, letter, resume) that causes the recipient to behave in a particular manner; it relates to the amount of information that was copied and the degree of data sensitivity → tangible (economic/strategic loss) and intangible losses (negative reputation, litigation)
- *Session Hijacking* – man in the middle attack, attempt to place themselves into an authenticated conversation dialogues/sessions between parties
- *Denial of Service Attacks* – denies access to legitimate network traffic, disables or damages network connections, and the organization would suffer loss of sensitive/confidential information and financial loss (i.e. sending 5 million spam messages to mail server)
- *Web Applications Vulnerabilities* – intranets can be hacked in order to gain access to customer information, hackers seek for openings/flaws in the application software, i.e.) weak passwords, insecure software configurations