004.7.056.5 Review

CYBER SECURITY AND PROTECTION OF COMPUTER SYSTEMS

Emilija SPASOVA KAMCEVA, PhD
FON University – Faculty of Informatics
E-mail: emilija.kamceva@fon.edu.mk

Nikolco SPASOV, PhD
The Intelligence Agency of the Republic of Macedonia
E-mail: spasov.nikolco@yahoo.com

Abstract

The work presents the methods for raising the awareness regarding the safety of the Internet, i.e. the safety related to the production and maintenance of the web applications in order to preserve the reputation and to prevent loss of money as well as leak of information through those web applications, to point out the dangers that the unprotected web application contain and to join the theory with the practice in order to make the web application safer. The main purpose of OWASP TOP 10 is to educate researchers, designers, architects, managers and organizations regarding the possible consequences of the most significant security weaknesses within the web applications. Top 10 offers the basic techniques for protection against these very dangerous problems, and provides directions for further development and protection.

The basic aim is to provide high degree of protection and to make a holistic approach towards the safety problem resolution by continuous development and improvement of new protection mechanisms.

Key words: cyber security, information, web application,
safety flaws and ethical hacking.

Introduction

The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this paper describes ethical hackers, their skills and how they go about helping their customers and plug up security holes. Ethical hackers perform the hacks as security tests for their systems. This type of hacking is always legal and trustworthy. In other terms ethical hacking is the testing of resources for the betterment of technology and is focused on securing and protecting IP systems. So, in case of computer security, these tiger teams or ethical hackers would employ the same tricks and techniques that hacker use but in a legal manner and they would neither damage the target systems nor steal information. Instead, they would evaluate the target system's security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them. Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results is a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them. We can easily say that Ethical hacking does perfectly fit into the security life cycle shown in the below figure. (Gurpreet K. Juneja, 2013).

What is Hacking?

Hacking is the technique in which the persons, what's in a name? Call them hackers, crackers, intruders, or attackers, they are all interlopers who are trying to break into your networks and systems. Some do it for fun, some do it for profit, or some simply do it to disrupt your operations and perhaps gain some recognition. Though they all have one thing in common; they are trying to uncover a weakness in your system in order to exploit it. (Bhawana S. , Ankit N. and Shashikala K.:,2014).

Local network test simulates an employee or other authorized person who has a legal connection to the organization's network. The primary defenses that must be defeated here are intranet firewalls, internal Webservers, server security measures, and e-mail systems. In Stolen laptop computer test, the laptop computer of a key employee, such as an upper-level manager or strategist, is taken by the client without warning and given to the ethical hackers. They examine the computer for passwords stored in dial- up software, corporate information assets, personnel information, and the like. Since many busy users will store their passwords on their machine, it is common for the ethical hackers to be able to use this laptop computer to dial into the corporate intranet with the owner's full privileges. (Bhawana S. , Ankit N. and Shashikala K.:,2014). Social engineering test evaluates the target organization's staff as to whether it would leak information to someone. A typical example of this would be an intruder calling the organization's computer help line and asking for the external telephone numbers of the modem pool. Defending against this kind of attack is the hardest, because people and personalities are involved. Most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his or her badge. The only defence against this is to raise security awareness. (Bhawana S. , Ankit N. and Shashikala K.:,2014). Physical entry is test acts out a physical penetration of the organization's building. Special arrangements must be made for this, since security guards or police could become involved if the ethical hackers fail to avoid detection. Once inside the building, it is important that the tester not be detected. One technique is for the tester to carry a document with the target company's logo on it. Such a document could be found by digging through trash cans before the ethical hack or by casually picking up a document from a trash can or desk once the tester is inside. The primary defenses here are a strong security policy, security guards, access controls and monitoring, and security awareness. Each of these kinds of testing can be performed from three perspectives: as a total outsider, a semi-outsider, or a valid user. A total outsider has very limited knowledge about the target systems. The only information used is available] through public sources on the Internet. This test represents the most commonly perceived threat. A well-defended system should not allow this kind of intruder to do anything. (K.Bala Chowdappa et al, :2014). A semi-outsider has limited access to one or more of the organization's computers or networks. This tests scenarios such as a bank allowing its depositors to use special software and a modem to access information about their accounts. A well-defended system should only allow this kind of intruder to access his or her own account information. A valid user has valid access to at least some of the organization's computers and networks. This tests whether or not insiders with some access can extend that access beyond what has been prescribed. A well-defined system should allow an insider to access only the areas and resources that the system administrator has assigned to the insider (Bhawana S., Ankit N. and Shashikala K.: 2014). Ethical hacking is also known as "Penetration Hacking" or "Intrusion Testing" or "Red Teaming". (K.Bala Chowdappa et al,:2014)

Ethical hacking is defined as the practice of hacking without malicious intent. The Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security. According to Palmer (2004, as quoted by Pashel, 2006): "Ethical hackers employ the same tools and techniques as the intruders, but they neither damage the target systems nor steal information. Instead, they evaluate the target systems' security and report back to owners with the vulnerabilities they found and instructions for how to remedy them". The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results is a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them. (Bhawana S., Ankit N. and Shashikala K.:,2014)

Types of hacking and hackers

"Hacker" is a loose term and has different meanings. Generally the term "Hacker" is someone who breaks into computer networks for the happiness he gets from the challenge of doint it or with some other intentions like stealing data for money or with political motivations. Hackers are classified to different types. Some of them are listed below.

A White Hat hacker is a computer network security professional and has non-malicious intent whenever he breaks into security systems. A White Hat hacker has deep knowledge in Computer Networking, Network Protocols and System Administration (at least three or four Operating Systems and very good skills in Scripting and Programming).

White Hat hacker has also good knowledge in hacking tools and know how to program hacking tools. A White Hat hacker has the skills to break into networks but he uses his skills to protect organizations. A White Hat hacker can conduct vulnerability assessments and penetration tests are also known as an Ethical Hacker. Often White Hat hackers are employed by companies and organizations to check the vulnerabilities of their network and make sure that no hole is available in their network for an intruder. (K.Bala Chowdappa et al,:2014). A Black Hat hacker, also known as a cracker, is a computer professional with deep knowledge in Computer Networking, Network Protocols and System Administration (at least three or four Operating Systems and very good skills in Scripting and Programming). Black Hat hacker has also good knowledge in many hacking tools and know how to program hacking tools. A Black Hat hacker uses his skills for unethical reasons. A Black Hat hacker always has malicious intention for intruding a network. Example: To steal research data from a company. To steal money from credit cards, Hack Email Accounts etc. (K.Bala Chowdappa et al, :2016). A Grey Hat hacker is someone who is between White Hat hacker and Black Hat hacker. Grey Hat normally do the hacking without the permissions from the administrators of the network he is hacking. But he will expose the network vulnerabilities to the network admins and offer a fix for the vulnerability for money. A Script Kiddie is basically a hacker amateur who doesn't has much knowledge to program tools to breaks into computer networks. He often use downloaded hacking tools from internet written by other hackers/security experts. (H.M David,:2004). A Hacktivist is a hacker with political intentions. The hacktivist has the same skills as that of a hacker and uses the same tools as the hacker. The primary intention of a hacktivist is to bring public attention to a political matter. Phreaker is a telecom network hacker who hacks a telephone system illegally to make calls without paying for them.

Hacking Phases

The overall hacking methodology consists of certain steps which are as follows:

Reconnaissance can be active or passive: in passive reconnaissance the information is gathered regarding the target without knowledge of targeted company (or individual). It could be done simply by searching information of the target on internet or bribing an employee of targeted company who would reveal and provide useful information to the hacker. This process is also called as "information gathering". In this approach, hacker does not attack the system or network of the company to gather information. Whereas in active reconnaissance, the hacker enters into the network to discover individual hosts, ip addresses and network services. This process is also called as "rattling the doorknobs". In this method, there is a high risk of being caught as compared to passive reconnaissance. (H.M David,:2004). In Scanning Phase, The Information Gathered In Phase 1 Is Used To Examine The Network. Tools like Dialers', Port Scanners Etc. are being Used by the Hacker to Examine the Network So As To Gain Entry in the Company's System And Network. Owning the System Is The Real And Actual Hacking Phase. The Hacker Uses The Information Discovered In Earlier Two Phases To Attack And Enter Into The Local Area Network (LAN, Either Wired Or Wireless), Local Pc Access, Internet Or Offline. This Phase Is Also Called As "Owning The System".

Once the hacker has gained the access in the system or network, he maintains that access for future attacks (or additional attacks), by making changes in the system in such a way that other hackers or security personals cannot then enter and access the attacked system. In such a situation, the owned system (mentioned in Phase 3) is then referred to as "Zombie System". Evidence Removal is phase where the hacker removes and destroys all the evidences and traces of hacking, such as log files or Intrusion Detection System Alarms, so that he could not be caught and traced. This also saves him from entering into any trial or legality. Now, once the system is hacked by hacker, there are several testing methods available called penetration testing to discover the hackers and crackers. (Chowdappa et al, :2014)

What is Web Application Security?

Web application security is a branch of Information Security that deals specifically with security of websites and web applications. It differs from the other branches of Information Security in that web application security is focused on vulnerabilities within the application code that is exposed during a user session on the web. The other areas of information security—that are not directly discussed in this document—are Network Security, Infrastructure Security, Database Security, and Operational Security. A majority of the attacks against web servers are through network firewalls and through the http (80) or https (443) ports. Some of the most commonly used hacking techniques include denial of service, leakage, cross-site scripting, SQL injection and disclosure. (Jon Panella, 2011). Due to the complexity of web applications and their supporting architectures (i.e. operating systems, databases, middleware, etc.), web attacks can be very sophisticated with serious, far-reaching implications. The complexity of web applications can also make web application security a more challenging endeavor than other branches of Information Security. Hackers target web applications because it can be very lucrative for them to do so. For example, a successful attack on a bank's web server could yield thousands of bank account numbers and user passwords information. The hacker could then use that information to gain a fortune by doing unauthorized money transfers and with drawls. (Jon Panella, 2011)

The Open Web Application Security Project

The Open Web Application Security Project (OWASP) is an open-source application security project. Its membership includes corporations, educational organizations, and individuals from around the world. The OWASP works to create freely-available articles, methodologies, documentation, tools, and technologies for web security. The OWASP Top 10 is a set of classes of vulnerabilities that are very high risk. Application developers can judge whether their applications meet best practices based on whether or not they has facilities to protect against these vulnerabilities. The OWASP Top 10 represents a broad consensus regarding the most critical vulnerabilities for web application security. A variety of security experts from around the world contribute their expertise to produce the OWASP Top 10. (Jon Panella, 2011)

The OWASP Top 10 and PCI DSS requirement 6.6 have been linked together as a best practice implementation of web application security. Many organizations "cross reference" the two standards. (Jon Panella, 2011). The following vulnerabilities, in descending order of severity, comprise the OWASP Top 10:

- A1 – Injection Vulnerability
- A2 – Cross Site Scripting (XSS) Vulnerability
- A3-Broken Authentication and Session Management
- A4 – Insecure Direct Object References
- A5 – Cross Site Request Forgery (CSRF) Vulnerability
- A6 – Security Misconfiguration
- A7 – Failure to Restrict URL Access
- A8 – Unvalidated Redirects and Forwards
- A9 – Insecure Cryptographic Storage
- A10 - Insufficient Transport Layer Protection

Limitations of Ethical Hacking

Ethical hacking is based on the simple principle of finding the security vulnerabilities in systems and networks before the hackers do, by using so-called "hacker" techniques to gain this knowledge. Unfortunately, the common definitions of such testing usually stops at the operating systems, security settings, and "bugs" level. Limiting the exercise to the technical level by performing a series of purely technical tests, an ethical hacking exercise is no better than a limited "diagnostic" of a system's security (Gupta, B. B., et al.2015). Time is also a critical factor in this type of testing. Hackers have vast amounts of time and patience when finding system vulnerabilities. Most likely you will be engaging a “trusted third party” to perform these test for you, so to you time is money. Another consideration in this is that in using a “third party” to conduct you tests, you will be providing “inside information” in order to speed the process and save time. The opportunity for discovery may be limited since the testers may only work by applying the information they have been given. 21. (Gupta, B. B., et al.2015)

A further limitation of this type of test is that it usually focuses on external rather than internal areas, therefore, you may only get to see half of the equation. If it is not possible to examine a system internally, how can it be established that a system is “safe from attack”, based purely upon external tests? Fundamentally this type of testing alone can never provide absolute assurances of security. Consequently, such assessment techniques may seem, at first, to be fundamentally flawed and have limited value, because all vulnerabilities may not be uncovered. (Bhawana S., Ankit N. and Shashikala K.: 2014)

Conclusion

The rapid development of technology brings positive and negative changes in society. Positive changes are obvious, while for negative we are sometimes unaware of ourselves. In order to be information security protected it is necessary to have primarily a security culture, especially on social networks such as: Facebook, Twitter, Linkin, etc.

Information security protection is of great importance to institutions, banks, companies, etc. Therefore penetration testing is recommended. Penetration testing determines all weaknesses of information systems and database servers in a given institution. Another convenient way to protect is to use the above-described Open Web Application Security Project (OWASP) that meets all the standards.

Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hackers help to understand the companies’ their security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits which may allow a malicious hacker to breach their security system. This also concludes that hacking is an important aspect of computer world. It deals with both sides of being good and bad.

Bibliography:

1. Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala (2010) , "Ethical Hacking ", International journal of Computer Applications, Vol. 1 No. 10.
2. Ajay S. (2016). "Web Application Hacking." Certified Ethical Hacker (CEH) Foundation Guide. 131-141.
3. Aury M. Curbelo, Alfredo Cruz (2013), "Innovation in Engineering, Technology and Education for Competitiveness and Prosperit", Faculty Attitudes Toward Teaching Ethical Hacking to Computer and Information Systems.
4. Beaver Kevin (2006) "Hacking for dummies", 2nd edition, New Jersey: John Wiley and Sons.
5. Bhawana S. , Ankit N. and Shashikala K. (2014) "Study Of Ethical Hacking", International Journal of Computer Science Trends and Technology (IJCST) ,–Vol. 2, Issue 4.
6. Chowdappa K.Bala et al. (2014), "Ethical Hacking Techniques with Penetration Testing", International Journal of Computer Science and Information Technologies, Vol. 5, Issue 3.
7. Desai Manthan (2010) "Hacking for beginners", my.safaribooksonline.com/.../ introduction-to-ethical-hacking-ethics-legality.
8. Dodson, J., et al. (2016) "Database and Security: Creating a Secure Database for a Capstone Application Development Project." Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
9. Ethical Hacking Techniques to Audit and Secure Web Enabled Applications, (2002). Sanctum Inc.
10. Gupta, B. B., et al. (2015) "Cross-site scripting (XSS) abuse and defense: exploitation on several testing bed environments and its defense." Journal of Information Privacy and Security 11.2 : 118-136.
11. Gurpreet K. Juneja (2013), "Etihical Hacking: A Technique to enhance information security", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 12.
12. Hafele David, (2004), Three Different Shades of Ethical Hacking: Black, White and Gray, SEC Practical Assignment, Version 1.4b, SANS Institute, accessed: https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390.

13. Hwang, Yong Ho. (2015) "Iot security & privacy: threats and challenges." Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. ACM.
14. Ishu J., R. Johari, and R. L. Ujjwal.(2014) "CAVEAT: credit card vulnerability exhibition and authentication tool." International Symposium on Security in Computing and Communication. Springer Berlin Heidelberg.
15. Jamil Danish and Ali Khan Muhammad (2011) "Is Ethical Hacking Ethical?", International journal of Engineering Science and Technology, Vol 3 No. 5.
16. Jason C., C. Morisset, and N. Zannone (2015) "On missing attributes in access control: non-deterministic and probabilistic attribute retrieval." Proceedings of the 20th ACM Symposium on Access Control Models and Technologies. ACM.
17. Leiner, Barry M., et al. (2009) "A brief history of the Internet." ACM SIGCOMM Computer Communication Review 39(5).
18. Manuel V.and A.Petrini (2016). "Virtualization Laboratory for Computer Networks at Undergraduate Level." International Conference on EUropean Transnational Education. Springer International Publishing
19. Mahrouqi, A., et al. (2016) "Simulating SQL-Injection Cyber-attacks using GNS3." International Journal of Computer Theory and Engineering 8.3: p p 213.
20. Nitin N. (2016) "Building a virtual system of systems using docker swarm in multiple clouds." Systems Engineering (ISSE), IEEE International Symposium.
21. Panella Jon, (2011) "Web Application Security and the OWASP Top 10", Sapient's Global Commerce Practice, Sapient Corporation.
22. Reto B. (2002), "Ethical Hacking", in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24.
23. Salas, M. I. P., and E. Martins (2014) "Security testing methodology for vulnerabilities detection of xss in web services and ws-security." Electronic Notes in Theoretical Computer Science 302.
24. Smith B., Yurcik W., Doss D. (2002), "Ethical hacking: the security justification redux", conference paper presented at Technology and Society International Symposium.
25. Steinmetz, Kevin F. (2015) "Craft (y) ness An Ethnographic Study of Hacking." British Journal of Criminology 55 (1).
26. Tatwani, L. Narayan, and R. Tyagi. (2015) "Security and Privacy issues in Cloud Computing." International Research Journal of Computer and Electronics Engineering.