Hacking and Penetration Testing

Tobias Glocker
University of Vaasa
Tobias.Glocker@uwasa.fi

June 24, 2013

1 INTRODUCTION

Nowadays most of the data is exchanged over the Internet and many data are stored on servers to be accessible to trusted organizations and persons. These data are very sensible and normally they are secured by the use of the newest security software (firewall, Anti-Virus Software etc.). But no system has a security of 100% and thus can be hacked by hackers. The aim of the hackers is to get access to the sensible data stored on the servers. In some countries it is common that companies hire hackers to get data of their competitors in order to know what trend they will follow in the future or to get information about their current products. This report contains a learning diary of the guest lecture about "Hacking and Penetration testing" given by Professor Rui Miguel Soares Silva.

2 LECTURE I (Morning)

The first part of the lecture covered information about hacking such as the hacker path, the ethics and hacking, useful professional certifications for hacking, hacker communities, and useful mailing lists and conferences for hackers. There are three kind of hackers, white hat hackers, black hat hackers and gray hat hackers. White hat hackers are security professionals that act according to the law while a black hat hacker acts aside the law. A gray hat hacker is in-between those hackers and acts generally according to the law but not always. To work for companies as a professional hacker an academic degree might not be enough. Several useful professional

certificates for hackers like Information Assurance Technical (IAT), Information Assurance Management (IAM), Computer Network Defense (CND) etc. have been introduced. The previous mentioned certificates are more for government employees but there are also trade independent certificates such as Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Global Information Assurance Certification (GIAC) and so on. Furthermore hacker communities, mailing lists and conferences for hackers have been mentioned in this part of the lecture.

In the second part information about Penetration Tests Methodologies were given. A Penetration Test is based on the use of attack techniques that allow the identification of methods to overcome the security measures of an application, a system or a network. It "is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats" (Wikipedia 2013). The Penetration Testing Execution Standard defines seven phases, the Pre-Engagement, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation and Reporting. In the Pre-Engagement the scope and terms such as estimated time, compromised rules, payment terms etc. should be specified. The second phase is the Intelligence Gathering where information is gathered from public (Trustiness, Religion of the employee) and non public sources (Intelligence about people). The objective of the third phase, the Threat Modeling phase, is to find the Assets of the organization (specific documents) in order to attack them. In the Vulnerability Analysis the aim is to encounter the vulnerability of the system or an application to attack it. To discover the weakness of a system or application, vulnerability scanners such as Nessus can be used. In the Exploitation phase, the target is to overcome the defense security measures. To these security measures belong Anti-Virus, Firewall etc. It is also essential to use techniques that avoid a detection during the attack. The Post Exploitation objective is to "determine the value of the compromised machine and keep control to access it". When doing a Penetration Test it is important to respect the contract rules that are made between the client and the Penetration Test executor. At last, a report containing the results of the Penetration Test must be written. This report should contain information an Executive Summary destined to managers and a Technical Report destined for Technicians. Besides the Penetration Test also possible attack targets, Vulnerability Repositories and Exploit Repositories have been introduced. In addition, methods used in the Information Gathering Phase and in the Vulnerabilities Identification Phase of Chosen Target Attacks have been presented. (Silva 2013.)

3 LECTURE II (Afternoon)

In this lecture a Buffer Overflow Attack was shown. A buffer overflow happens when someone writes more data into the buffer than allowed. Every buffer has a maximum amount of memory and if this amount is exceeded then the program crashes. Assume a cracker (hacker that does something vulnerable) tries to connect with an File Transfer Protocol (FTP) Server and the cracker wrote a program that sends a huge string of bytes for the password which leads to a buffer overflow. After the program crashes it is still possible to upload and to execute a malicious code. The cracker needs to know the address where the Extended Stack Pointer (ESP) points to in order to upload the malicious code to the top of the stack. Finally the cracker only needs to initialize the Extended Instruction Pointer (EIP) with the starting address of the malicious code. It is to mention, that the EIP always points to the memory address from which the Central Processing Unit (CPU) tries to run its next execution. Then the malicious code will be executed and it does for what it was programmed for.

4 CONCLUSION

In this one-day lecture given by Professor Rui Miguel Soares Silva, the audience got a lot of knowledge about hackers and Penetration Tests as well as attack phases and Ethical Hacker Tools. The most interesting part was given in Lecture II where a Buffer Overflow Attack was demonstrated. It is to mention that this one-day lecture was very interesting and that the audience got a lot of valuable information.

5 BIBLIOGRAPHY

Silva, Rui M. (2013). Hacking and Penetration Testing. Guest Lecture at the University of Vaasa. Presentation Slides.

Wikipedia (2013). Penetration test. Available from the Internet: <URL: http://en.wikipedia.org/wiki/Penetration_test>