Ethical hacking a general overview

Francisco Bolaños Burgos, Ing
IT Department
InterAmerican Academy (IAA)
Puerto Azul. Km 10.5 Vía a la Costa
Postal Code 0906-209U. Guayaquil, Ecuador
fbolanos@interamerican.edu.ec

Abstract

Nowadays security plays an important role in enterprises due to the value of information and how this is processed. As technology advances, threats progress too, which challenge the IT staff in order to be updated and able to detect and prevent them. For this reason, Ethical hacking has been created with the main objective of testing and improving the security of the enterprise. The objective of this paper is to show a general overview of what ethical hacking implies such as: main concepts, common vulnerabilities, stages and tools. With the knowledge gained from this paper, the IT staff will have a baseline to apply a professional methodology for security audit like: Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAT) or ISO27001:2005.

Keywords: *information, Ethical hacking, common vulnerabilities, OSSTMM, ISSAT, ISO2007:2005.*

1. Security Fundamentals

In the technology field, security has two main concepts: security information and computer security. The first protects the information from a wide spectrum of threats, in order to ensure business continuity, minimize damage to the organization and maximize the return on investment and business opportunities. Meanwhile, the second concept ensures the resources of the information systems (hardware or software) of an organization are used in the proper way. The main difference is that security information is focused on the whole company and computer security on the IT department.

There are four features of computer security: confidentiality, integrity, availability and accountability. Confidentiality is the property of keeping the information private; only the owner can access it. Integrity refers to the fact that the information will remain the same and will not suffer any change from any party (user). Availability makes the information always available without any kind of disruption. Accountability is the capacity of keeping track based on the generation of files. If one of these four features is not protected properly, hackers can take advantage of it and gain access to the information assets.

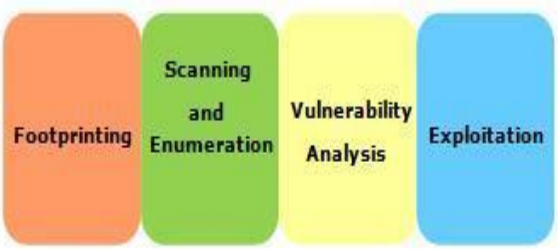
Based on the OSSTMM [1] the definition for ethical hacking is a penetration test of which the goal is to discover trophies throughout the network within the predetermined project time limit. Basically the main purpose of ethical hacking is to test and improve the network security and everything relies in the person's ethics.

The common vulnerabilities found in an ethical hacking test are:

- Wrong router configurations.
- Remote Access Service (RAS) not secured and either monitored.
- Leakage of information.
- Unnecessary services.
- Weak passwords.
- Accounts with too many privileges.
- Internet services not well configured.
- Firewalls not well configured.
- Lack of patches or configurations by default.
- No authenticated services.

2. Traditional Ethical hacking

Usually, ethical hacking is not based on a particular methodology. It follows standard steps that allow the ethical hacker to succeed in his task. The following figure shows the traditional hacking stages.



Figures 1: Traditional ethical hacking stages

There are different types of tools people can use in an ethical hacking test such as: proprietary and open source tools. In this paper open source tools will be used due their advanced features as well as their cost (no payment for them). A list of tools for the difference stages is shown in the annex.

2.1 Footprinting

It is the technique of gathering information about the target or victim. The more information you can get from this stage the more accurate your attack will be. The purpose is to create a profile of the target and get familiar with it. Any type of tool could be used such as automated and/or manual tools or social engineering techniques (It is a technique that gets information without using technology. It is known as an act of physiological manipulation). This is a passive search because the target wouldn't know about it. The command ping, whois and TouchGraph [2] were used in this stage.

2.2 Scanning and enumeration

Scanning is based on Footprinting because with the information gathered from the Footprinting stage is possible to identify the resources of the target like: access points, open ports, active machines, uncovering services on ports and operating systems. Meanwhile enumeration list all the resources found in the scanning with the purpose of having a general network schema and possible vulnerabilities of it.

Nmap [3] was used as a scanning and enumeration tool.

2.3 Vulnerabilities Analysis

It is an active process in which the possible security holes are confirmed or discarded based on the enumeration stage. In order to succeed in the analysis, different automated tools should be used.

Nessus [4] was used as a vulnerability analysis tool.

2.4 Exploitation

In this stage the attacker is going to get access, escalate privileges and get or manipulate the data of his/her victim. In other words, the intruder will hack the company. No tool was used because the objective of this article is to show how to hack in order to protect the assets of the enterprise.

3. Conclusions

Security information has an important impact in the current days. The IT staff should be trained on this topic in order to prevent any kind of security issues. Once the IT staff gets the basic knowledge about ethical hacking, it would be able to apply professional methodologies for security audits such as: OSSTMM, ISSAT, ISO2007:2005. The IT people have to keep in mind that hacking is art and the security evaluation is science. Therefore, in order to protect the information assets you have to think like a hacker.

4. References

[1] "ISECOM - Open Source Security Testing Methodology Manual (OSSTMM)."*ISECOM*. ISECOM. Web. 14 Mar. 2012. <http://www.isecom.org/research/osstmm.html>.

[2] "TouchGraph." *Graph Visualization and Social Network Analysis Software*. TouchGraph. Web. 14 Mar. 2012. <http://www.touchgraph.com/navigator>.
[3] "Nmap - Free Security Scanner For Network Exploration & Security Audits." *Nmap*. Nmap. Web. 14 Mar. 2012. <http://nmap.org/>.
[4] "New in Nessus 5: Customized Reporting." *Tenable Network Security*. Tenable Network Security. Web. 14 Mar. 2012. <http://www.tenable.com/>.

ANNEX

MANUAL AND AUTOMATED TOOLS

- **FOOTPRINTING**

Google Hacking.
Bing browser
Dnsmap
Metagoofil
TouchGraph
Kartoo
Fierce DNS
Programmed scripts
www.netcraf.com
www.zone-h.oorg
www.clez.net
www.shoclanhq.com
www.johnny.ihackstuff.com/ghdb/
www.exalead.com (one web search)
www.domaintools.com
www.netcraft.com
www.archive.org (wayback)
www.edgesecurity.com/theHarvester.php

- **SCANNING AND ENUMERATION**

Nmap
Wireshark
SuperScan
HAKTEK
Megaping
LANGuard
Unicorn Scan
Port Bunny
Scapy

- **VULNERABILITY ANALYSIS**

N-Stalker
WebInspect
Nikto
AppDetective
Paros
Acunetix
Burp
Nessus
SAINT
NeXpose
ISS Internet Scanner
Shadow Security Scanner
Retina
LanGuard Network Security Scanner
VLAD

- **EXPOLOITATION**

Metaexploit
URL Obfuscation
XSS
SQL injection
w3af
NetCat (covered channels)