HT METHODOLOGY

ETHICAL HACKING

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

© 2008 HT | | Pag 1 of 4

Diritti riservati. E ' espressamente vietato riprodurre, distribuire, pubblicare, riutilizzare anche parzialmente articoli, testi, immagini, applicazioni, metodi di lavoro del presente documento senza il previo permesso scritto rilasciato dalla società proprietaria Hacking Team S.r.l., ferma restando la possibilità di usufruire di tale materiale per uso interno della Società nel rispetto di quanto stabilito dal contratto di fornitura sottoscritto.

HT'S ETHICAL HACKING ACTIVITY

In order to approach this complex and sometimes chaotic scenario, one of the most popular services of Hacking Team is *Ethical Hacking*. This service is focused on detailed security testing by means of simulated attacks upon client's request. Ethical hacking has the goal of defying client's security infrastructure and possibly correcting the mistakes made through security bugs, human errors and time, following the trend of a confused security market.

Our clients are large and world-known institutions. The point of ethical hacking could be posed as follows: "What would the consequences of an attack to my network by malicious hackers really be?" Or: "Is my security infrastructure really working?" The results of a ethical hacking activity are usually very surprising. For instance, the simulated attack goes totally unnoticed most of the times. It is not uncommon that we are able to access company confidential information (such as the payroll database) or mission-critical information (such as intellectual-property data). It is also not uncommon that we completely defeat firewalls, public key systems, hardware token systems, company proprietary security systems, etc.

HT follows methodology created in direct depending on requests of our customers.

NON-INVASIVE ANALYSIS

FOOTPRINTING

In this step HT is determining domains, network blocks and IP addresses of computers connected directly to Internet. Goal is deep examination and information gathering. Resources used are: Search Engines, whois servers Arin/Ripe data base, interrogation to dns etc.

SCANNING

Scope of this step is to obtain a clear picture of network's complexity and its subjects which are going to be attacked. Aim is to define activated services and operating systems. In fact, to obtain all the information regarding servers that may be useful for further invasive activities. Resources: ICMP interrogations, scanning tcp and udp ports, fingerprint of stack etc.

INVASIVE ANALYSIS

ENUMERATION

In this step is starting invasive activity. More exactly, "enumeration" activity is starting with direct connections to servers. We are looking for a possibility to identify computers which responded as "reached" in non-invasive fazes. Through enumeration we are defining the presence of valid accounts, shared resources, active applications that are listening to different ports. Used resource depends on operating system within the computer.

ATTACK

During this phase, resources are: published, non published and custom created or generated attacks (exploits).

GAINING ACCESS

Once obtained information from the steps above, it starts a real attack that has the goal to enter into the remote system.

ESCALATING PRIVILEDGES

The goal of this phase is to exploit results obtained during the previous phases intending to obtain full control of remote system that we are attacking.

CONSOLIDATION

PILFERING

Once obtaining full control of targeted system, HT is free to analyze system's configuration and to use it in further attacks. It means that in this moment computers became "trampolines" that allow us to attack other computers within the network.

COVERING TRACKS

When attack is finished HT is looking for a possibility to cover all the tracks which have been created during the attack. Details are included in the report.

HT Ethical Hacking service is divided in four levels and it can be customized in depending of customer's needs.

I LEVEL: attack simulation made from Internet

This type of probe is based on verifying the "strength" of the system's defensive perimeters (router's acl, firewall, configuration of the servers that can be accessed from the outside, etc). There is a simulation of the situation that the hacker would encounter if, from any part of the world, he was about to try to attack the network trough the Internet network.

II LEVEL: attack made **inside** the LAN

In the second level probe we are probing security of internal network;

Two possible sceneries are simulated:

- Situation in which a hacker would be if he had managed to go beyond the perimeter defenses by insinuating himself telemetrically into an internal machine and reaching a discreet degree of knowledge of the internal network;

- Possibility that a hacker may have physical access, even temporarily, to the LAN; we are led to this scenery also by the possibility of a hacker being an employee or a collaborator of the structure that is about to be attacked.

III LEVEL: Application security

In this phase HT is attacking directly applications available within the company's servers. If any problem is found, we are doing analysis and review of a complete source code with an aim to avoid any possibility of exploiting it. (See attached file: HT Application Methodology).

IV LEVEL: Advanced technologies probing

The forth level is designed to support probing of advanced technologies using specific techniques that may be specifically requested by client. Such as: WarDialing, WarDriving, Social Engineering …