]HackingTeam[| Chemtex

Chemtex International Inc.

Network Vulnerability Assessment

Scope and Methodology

Milan

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*

Document Versions		
Version	Date	Modifications
1.0	August 9th, 2005	First Issue
//	//	//
//	//	//

Document Details	
Released	August 9th, 2005
Version	1.0
Document Type	Activity Description
Pages	8
Attachments	0
Written by	Federico Guerrini
Verified by	Gianluca Vadruccio

Table of Contents

1 Customer's Request 4
2 Scope 4
3 Hacking Team' Ethical Hacking Services 5
4 Hacking Team's Methodology 5
4.1 Non-invasive Analysis 6
4.1.1 Footprinting 6
4.1.2 Scanning 7
4.2 Invasive Analysis 7
4.2.1 Enumeration 7
4.2.2 Attack 7
4.2.3 Gaining Access 7
4.2.4 Escalating Privileges 7
4.3 Consolidation 7
4.3.1 Pilfering 7
4.3.2 Covering Tracks 8
4.4 Reporting 8

1 Customer's Request

M&G Finanziaria Holding requested a network security assessment for Chemtex's Indian offices in Mumbai and Banglore. The assessment is to involve only the external networks of the two offices, i.e. only the systems, applications and network devices that can be reached, either directly or indirectly, from the Internet.

M&G's aim is to discover and fix any unpatched vulnerabilities, misconfigurations and overlooked best practices that could lead to unauthorized access to Chemtex's applications and data.

This document describes HT's assessment methodology and how it will be applied to Chemtex's network.

2 Scope

The scope of the vulnerability assessment is defined by the range of IP addresses that will be taken into account and the set of probes performed into each network service detected on them. According to the customer's request, the vulnerability assessment will include:

- for the office in Mumbai:
  - the IP range 202.54.16.17 - 202.54.16.30;
  - probes into the following network services:
    - SMTP;
    - DNS;
    - FTP;
    - Intranet-ERP;
    - Terminal Servers;
    - VPN connection (Win2003, host-to-host);
  - probes into the following applications:
    - REBOL;
    - Tarantella;
    - Inforouter (Document Sharing);
- for the office in Banglore:
  - the IP range 202.144.86.193 – 202.144.86.198;
  - probes into the following services:
    - SMTP;

- DNS.

3 Hacking Team' Ethical Hacking Services

Ethical hacking is used to determine the reliability and strength of a firm's Internet security measures. Ethical hackers employ attacks, exploits and other techniques to audit and assess networks, servers and applications. The process usually involves a review of the overall network design, in order to determine how it effectively isolates untrustworthy, outside networks from internal, trusted networks and systems. Hacking Team's ethical hacking services goal is to violate the customer's security infrastructure and possibly to correct its weaknesses (security bugs, human errors and time).

A security probe is a means of pro-active security: the weaknesses of a network are pointed out through a pragmatic approach; that is, trying to effectively attack the network using the same attacks that real hackers would apply.

The only difference between a real attack and a security probe is represented by the consequences of attack. Instead of really penetrating into the systems and stealing/modifying the data, a security probe generates a detailed report of all the security elements that were probed and a description of the weaknesses that would allow non-privileged and dishonest users (the hacker) to get unauthorized access to systems and data.

Attacking a network before hackers do allows, therefore, correcting possible configuration errors and/or applicative weaknesses before others can use them.

4 Hacking Team's Methodology

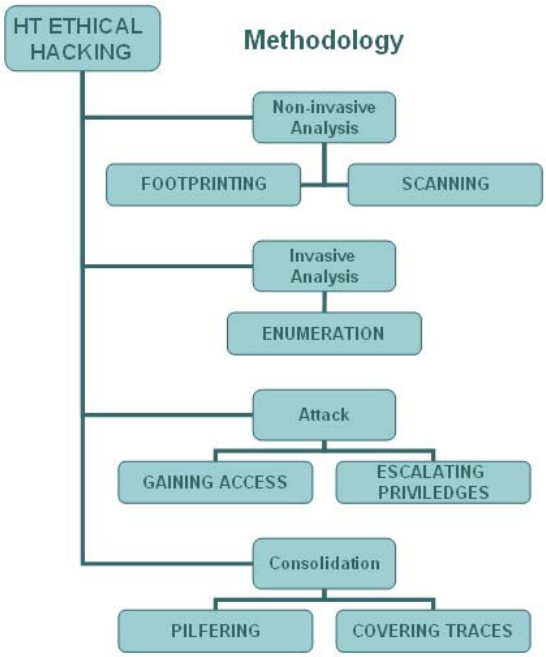
Hacking Team's methodology is comprised the following four phases.

- ***Non-invasive analysis***: this phase includes a broad spectrum of activities aimed at gathering information about the systems to be attacked. Such activities are referred to as "non-invasive" because no interaction with the active services is performed but a single connection in order to discover their presence.
- ***Invasive analysis***: this phase includes the initial attacks aimed at getting access to the target network. Such activities are referred to as "invasive" because they can include deep interaction with the active services.
- ***Consolidation***: this phase only takes place if successful attacks are found during the previous one. If this is the case, the systems that were accessed are analyzed in order to

assess the possibility of a deeper intrusion. The aim is to give the customer an estimate of the impact of the successful attacks on internal data and systems.

- ***Reporting***: in this phase documentation is produced that describes that probes that were performed, their results, the vulnerabilities that were discovered and their impact. Reports also include, for each vulnerabilities, detailed description of the countermeasures suggested by Hacking Team.

Every phase includes activities that are shown in the following figure and described in greater detail in the following paragraphs.



4.1 Non-invasive Analysis

4.1.1 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.

4.1.2 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.

4.2 Invasive Analysis

4.2.1 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.

4.2.2 Attack

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

4.2.3 Gaining Access

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

4.2.4 Escalating Privileges

The goal of this phase is to exploit results obtained during the previous phases in order to obtain full control of remote systems.

4.3 Consolidation

4.3.1 Pilfering

Once obtaining full control of a targeted system, Hacking Team analyzes its configuration and tries to mount further attacks. That is, exploited systems become "trampolines" that allow attacking other computers within the network.

4.3.2 Covering Tracks

When the attack is finished, Hacking Team seeks for the possibility of covering all the tracks that have been created during the attack. Details are included in the report.

4.4 Reporting

After completing the probes, Hacking Team produces and delivers a technical report that includes every detail of the attacks. The report is then presented to and discussed with the client's IT personnel. Also, Hacking Team produces a higher-level report for the management, that describes the major results in a non-technical form.