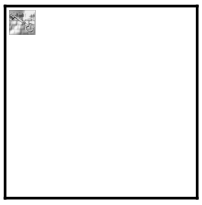


Bites-PenTesting

Penetration Test Report

Client:

Date of test:

Due to the removal of sensitive information the formatting of this report has become slightly off.

Contents

Chapter 1

Introduction to the penetration test

The aim of this penetration test is to help the administrator of the com- pany to secure the network. Although this report contains technical terms, it has been written so that a non-initiated reader with a basic knowledge of computing would understand it. However, references to more technical content, to be found in the appendices, is given along the test report for the administrator and security consultant of Bites-PenTesting to review them and possibly reproduce the test. Should the reader meet difficulties at un- derstanding the penetration test report, going directly to the "Conclusions and Recommendations" section will give him the executive information. For further help, we remain open to answer any of your questions.

In order to increase the understanding of the reader, some definitions and clarifications are given in the following sections.

1.1 Some definitions

- Hacker: word given by the masse media to define what we will more accurately call attacker or intruder in this report.
- Vulnerability: a bug in computer program that may be abused to gain privileges on a computer.
- Exploit: a program or strategy to exploit a vulnerability. Depending on the vulnerability, an exploit may be either local, in which a previous "local" access to the target computer is required prior gain higher privileges, or remote where the exploit can be run without this prerequisite.
- Rootkit: a set of programs replacing the tools, that an administrator would generally use to detect the presence of an intruder, by modified versions detecting everything but the presence and activities of the intruder, thus making the administrator confident that the system is free of any intrusions.

1.2 Motivation of an attacker

There are mainly three reasons why someone might want to penetrate your network.

- Information theft: to steal valuable information of your business such as contracts, documents or e-mail communication. In other words, information that, for example, competitors may like to know.

- Identity theft: by using your network as relay to attack other networks, an attacker can mask his identity.

- Challenge to overcome: to most attackers, your network represents a challenge that must be conquered or a way to prove their superior intelligence and technical skills.

Understanding the psychology of an attacker helps considering why your network is at risk whenever it is connected to the Internet and how to protect it. Indeed, whatever the final motivation really is, gaining access to a network always remains a challenge for an attacker. Though intruding a network is rewarding for his ego, failing to gain the access brings a high level of frustration. An attacker, usually, doesn't give up easily and will try, again and again, by any means, to get all kind of information that might be useful to detect weaknesses and mount attacks.

Therefore, while performing the penetration test, we have been through the same stages as an attacker would have, even though our strategy or tools might be slightly differ.

Chapter 2

The penetration test

The test was carried out from two machines, one running Mac OSX 10.8.9 and the other a Linux distribution. The Linux machines was rebuild prior to the test to ensure no information from previous tests could interfere. The OS X machine was used for information gathering and most of the time did not need to touch the target network.

2.1 .com Network

The first part of the test was targeted at a web server with the address stipulated in the penetration test agreement as www.emersoncranes.co.uk We quickly located the IP address for this domain to be 109.75.163.20 by running the 'nslookup' command on the Linux box

2.2 Footprinting

Prior to any penetration attempts, the very first thing that an attacker needs to do is gathering as much information as possible. The first process was mapping the target using the google filters:

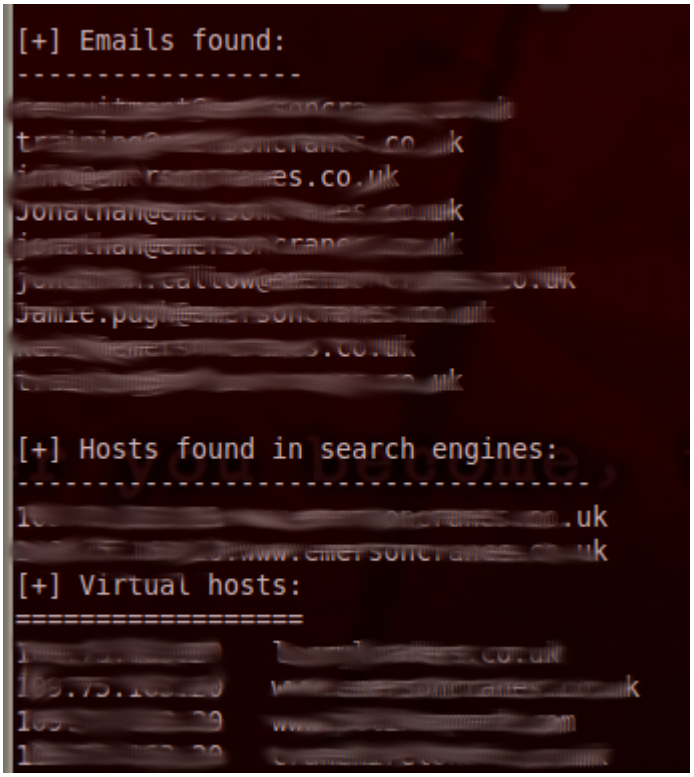
site:[target] - This shows all target pages.
site:[target] admin - To locate admin pages that could be brute forced.
insite:[target] login - To locate any login pages.

Using Google to map the target means we do not directly touch the target network and therefor do not leave traces of our presence.

No login or admin pages were located using this technique so I ran a python script to locate admin pages. This also came up empty as no 404 error is produced from the target when no page is found.

Using a program call ‘theHarvester’ I was able to automate the search and use multiple search engines to find information very quickly for anything relating to the target. The results were a number of email addresses and sub domains.

The email addresses can now be added to our list of potential user names. As for the sub domains they will be checked for top level vulnerabilities as they are on the same IP address to make sure they do not provide a back door into the root directory.



Port Scanning

Next was a scan of all ports on the IP *IP REMOVED* using ‘nmap’ command:

nmap -sS *IP REMOVED*

This returned the following results:

21/tcp open ftp
22/tcp open ssh
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
1723/tcp closed pptp
3306/tcp open mysql

There are a lot of ports open that I did not expect to see. After our telephone conversation prior to the penetrations test I was on the understanding that the web server

was a basic and simple website only. In which case I assume that port 21, 22 and possible 3306 can be closed.

I did not test any further with 21, 22 and 3306. Port 21 is the first port to attack to gain entry to a system as it is one of the most un-secure. It would be possible to test them further with custom packets and I would advise this IF these ports are meant to be open.

Using the switch -sV nmap probes the list of open ports to establish the service running and what version it is. I ran the list through a database of known vulnerabilities and none were found.

I then felt it was time to scan the target IP further using 'OpenVas'. This is an open source application with build in exploits and a vulnerability database. I configured OpenVas with the target specifications and scan configuration then launched the test.

Returned from the scan were two vulnerabilities:

DNS Amplification Attacks

Port - domain (53/tcp)
cvss base - 5.0
cvss base risk factor - Medium
cve - CVE-2006-0987
Summary:
A misconfigured Domain Name System (DNS) server can be exploited to participate in a Distributed Denial of Service (DDoS) attack.

A Domain Name Server (DNS) Amplification attack is a popular form of Distributed Denial of Service (DDoS) that relies on the use of publically accessible open recursive DNS servers to overwhelm a victim system with DNS response traffic.

The basic attack technique consists of an attacker sending a DNS name lookup request to an open recursive DNS server with the source address spoofed to be the victim's address. When the DNS server sends the DNS record response, it is sent instead to the victim. Attackers will typically submit a request for as much zone information as possible to maximize the amplification effect. Because the size of the response is typically considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. By leveraging a botnet to perform additional spoofed DNS queries, an attacker can produce an overwhelming amount of traffic with little effort. Additionally, because the responses are legitimate data coming from valid servers, it is especially difficult to block these types of attacks.

We send a DNS request of 17 bytes and received a response of 436 bytes.

References : URL:http://www.us-cert.gov/ncas/alerts/TA13-088A, URL:http://www.isotf.org/news/DNS-Amplification-Attacks.pdf, URL:http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-0987

jolt2

General/tcp
cvss_base - 5.0
cvss base risk factor - Medium
CVE-2000-0482
Summary:
The machine (or a gateway on the network path) crashed when
flooded with incorrectly fragmented packets.
This is known as the jolt2 denial of service attack.

An attacker may use this flaw to shut down this server or router,
thus preventing you from working properly.

Solution:
contact your operating system vendor for a patch.
CVE : CVE-2000-0482

IMAGE REMOVED

Office Network

Using supplied IP address *IP REMOVED* I found the bellow ports open.

PORT STATE SERVICE
80/tcp open http
443/tcp open https
1723/tcp open pptp
8085/tcp open unknown

Then using OpenVas I found one vulnerability.

TCP Sequence Number Approximation Reset Denial of Service Vulnerability.

cvss base - 5.0
cvss base risk factor - Medium
CVE-2004-0230
Summary:
The host is running TCP services and is prone to denial of service vulnerability.

Vulnerability Detection:
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Vulnerability Insight:
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.
Impact:
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.
Affected Software/OS:
TCP/IP v4
Solution:
Please see the referenced advisories for more information on obtaining and applying fixes.
CVE : CVE-2004-0230
BID : 10183
Other references : http://www.osvdb.org/4030, URL:http://xforce.iss.net/xforce/xfdb/15886, http://www.us-cert.gov/cas/techalerts/TA04-111A.html, URL:http://www-01.ibm.com/s↵
upport/docview.wss?uid=isg1IY55949, URL:http://www-01.ibm.com/support/docview.wss?uid=isg1↵
IY55950, URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006, URL:http://www.mic↵
rosoft.com/technet/security/Bulletin/MS05-019.mspx, URL:http://www.microsoft.com/technet/s↵
ecurity/bulletin/ms06-064.mspx, URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040↵
420-tcp-nonios.html, URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-non↵
ios.html

Chapter 3

Conclusions and recommendations

3.1 General overview

SECTION REMOVED

3.2 Recommended actions

By “relevant actions”, we ideally recommend to go through the following steps:

- Backing Up: do a backup of all the data that you consider to be needed for your business and double check that what you back up does not contain any viruses. Do not backup any programs, as they may contain backdoors (their reinstallation will need to be done from the original medium).

- Requirements learning: get to learn what services your business re- quires you to run on the network as well as which users require to get access to which systems or shared directories and with which permis- sions.

- Cleaning: after formating the hard disks, do a clean install, limit the services, accesses and permission to what has been defined as truly required during the previous stage. Make sure that all running services are up-to-date.

- Monitoring and being up-to-date: monitor your network activity (especially at the gateway) to detect unusual activities. Check the integrity of your servers file systems to detect unexpected modification or addition of files that could turn out to be backdoors or rootkits.

- Educating: tell the users (from their angle) why such measures are required and what are the consequences of poor security management for the business but also for them (privacy and confidentiality of their information, documents, e-mails, etc).

However going through these steps would be ideal to carry out this crit- ical mission, we appreciate that, from a business continuity point of view, this exact plan is not appropriate and we must define where the priorities are.

As far as the back up stage is concerned, it remains the highest prior- ity since your business data are truly at risk. Once these data have been saved and checked to be free from any viruses, check that you are in posses- sion of the original installation medium for all the software required by your users. Prior to any reinstallation of systems, create a list of the services that your business requires. If this list is not complete, be confident that your users will soon notice missing services after the reinstallation and inform you.

Although these tasks will not improve immediatly the security of your network, they are a solid basement to the further stage: a clean reinstalla- tion. We advise you to start by reinstalling the gateway, because this host is where an attacker would sniff all your communication to the outside world (ie, Internet)

such as e-mails. You should then reinstall the GNU/Linux servers as this task will only disrupt some services for a certain period of time but not completely avoid users to work. The more critical task comes next and consists in reinstalling the users workstations. You should start with the users who need less software and special settings. As their reinstallation will be shorter than others, you will get more potentially compromised machines out of the network quickly. Finally, generate relatively hard-to-crack pass- words (containing both alphanumerical and non-alphanumerical characters) for your users and introduce them to the need of more stronger passwords.

At this point, your network will hopefully be secure. However, if you want to avoid the same critical situation to happen again, you are to monitor your network, check the integrity of your servers file systems and keep yourself informed of security updates for the services you are running. We appreciate that all of this might seem quite difficult to achieve on a day-to-day basis and therefore our company has created a security service to which our clients can subscribe and in which we offer the following options:

- Net. Activity Monitoring™: we install the relevant network sen- sors software on your network, analyse the daily reports and contact you in case an unusual activity has been detected

- FileSys Integrity™: we install tripwire (the most renowned file sys- tem integrity checker) on your servers, analyse the reports and deal with you in case an integrity violation is detected. (Please note that, to guarantee the efficiency of this option, we require to install tripwire straight after the installation of the system and before the machine is ever plugged to the network)

- Up2Date Services: after you have provided us with the list of services you are running and the software you are using for that purpose (e.g., apache for the web), we will contact you when security patches are to be applied and give you advices.

All of this is done remotely from our office through a secure connection. All information about your network is kept confidential.

After all these is in place, we recommend to run another penetration test in order to find possible issues left over and to be addressed. Through a cycle of test, report and correction run on a regular basis, we shall not only bring but, moreover, keep your company network to a high level of security.

USERNAMES, PASSWORDS AND OTHER SENSITIVE INFORMATION HAS BEEN REMOVED FROM THE FOLLOWINF SECTIONS

4.1.2.10 Host

4.1.2.11 Host

4.2 Appendix B

4.2.1 Connection to telnet on

4.2.2 Banner of FTP service

4.2.3 Output of FTP exploit

4.2.4 Adding the ssh public key

4.2.5 Exploit of Apache with OpenSSL

4.2.6 Shell of the apache user

4.2.7 Version of the Linux kernel

4.2.8 Out put of finger (showing our presence)

4.2.9 Local exploit of ptrace vulnerabilities in Linux

4.3 Appendix C

4.3.1 Listing of the current working directory

4.3.2 Host

User Account

Password

4.3.3 Host

User Account Password

4.3.4 Host

User Account Password

4.3.5 Host

User Account Password

4.3.6 Host

User Account Password

4.3.7 Host

User Account	Password

4.3.8 Host

User Account Password

Bibliography

[FPING] fping, a program to ping hosts in parallel, D. Papp, T. Dzubin. http://www.fping.com

[NMAP] nmap, a free open source utility for network exploration or security auditing. http://www.insecure.org/nmap/

[CA-2001-33] Multiple vulnerabilities in WU-FTPD, http://www.cert.org/advisories/CA-2001-33.html

[CA-2002-23] Multiple vulnerabilities in OpenSSL, http://www.cert.org/advisories/CA-2002-23.html

[CAN-2003-0127] Linux Kernel Privileged Process Hijacking Vulnerability, http://www.securityfocus.com/bid/7112

[BID-3163] Sendmail Debugger Arbitrary Code Execution Vulnerability, http://www.securityfocus.com/bid/3163

[RHSA-2003-073] Remote Buffer Overflow in Sendmail, http://www.redhat.com/support/errata/RHSA-2003-073.html

[RHSA-2003-120] Remote Buffer Overflow in Sendmail, http://www.redhat.com/support/errata/RHSA-2003-120.html

[BID-5122] Sendmail DNS Map TXT Record Buffer Overflow Vulnerability, http://www.securityfocus.com/bid/5122

[BID-5093] OpenSSH Challenge-Response Buffer Overflow Vulnerabilities, http://www.securityfocus.com/bid/5093

[BID-4241] OpenSSH Channel Code Off-By-One Vulnerability, http://www.securityfocus.com/bid/4241

[BID-4560] OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow Vulnerability, http://www.securityfocus.com/bid/4560

[BID-8628] OpenSSH Buffer Mismanagement Vulnerabilities, http://www.securityfocus.com/bid/8628

[BID-3614] OpenSSH UseLogin Environment Variable Passing Vulnerability, http://www.securityfocus.com/bid/3614

[BID-2347] SSH CRC-32 Compensation Attack Detector Vulnerability, http://www.securityfocus.com/bid/2347

[JOHN] John The Ripper, Password Cracker, http://www.openwall.com/john/

[BID-1806] Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability, http://www.securityfocus.com/bid/1806

[GFI-LANGUARD] Network Security Scanner & Port Scanner, http://www.gfi.com/lannetscan/

[GNOMBA] Gnomba, GUI Samba Browser, http://www.gnu.org/directory/gui/other/gnomba.html

[NETCAT] The GNU Netcat, http://netcat.sf.net/

[BID-3581] Wu-Ftpd File Globbing Heap Corruption Vulnerability, http://www.securityfocus.com/bid/3581

[BID-2550] Solaris ftpd glob() Expansion LIST Heap Overflow Vulnerability, http://www.securityfocus.com/bid/2550

[BID-2308] Sendmail Invalid MAIL/RCPT Vulnerability, http://www.securityfocus.com/bid/2308

[NACS] SunOS 2.6 7 8 :Remote Buffer Overflow Vulnerability in Solaris Print Protocol Daemon], http://www.nacs.uci.edu/security/archive/msg00262.html

[SecuriTeam] Solaris TTYPROMPT Security Vulnerability (Telnet), http://www.securiteam.com/unixfocus/6R0050K5PC.html

[NESSUS] A free, powerful, up-to-date and easy to use remote security scanner., http://www.nessus.org/intro.html