SHOW/HIDE MENUS

THE ETHICAL HACKING GUIDE TO CORPORATE SECURITY

With the correct mix of technical explanations and subsequent business implications, this e-book draws a direct correlation between computer security and business profitability.

by ANKIT FADIA

CENTROATLANTICO.PT

The Ethical Hacking Guide to Corporate Security

by Ankit Fadia

Published by

CENTROATLANTICO.PT

The Ethical Hacking Guide to Corporate Security
by Ankit Fadia

Published by
Centro Atlântico, Lda.
Av. Dr. Carlos Bacelar, 968 – Escr. 1 – A – 4764-901 V. N. Famalicão
Rua da Misericórdia, 76 – 1200-273 Lisboa
Portugal
geral@centroatlantico.pt
www.centroatlantico.pt

Editorial Director: Libório Manuel Silva
Interior design by Centro Atlântico
Final Revisor by José Manuel Dias Cardoso
Cover design by António José Pedro

1st edition: January 2005
ISBN: 989-615-004-4

Centro Atlântico also publishes its books in paper format. Some content that appears in electronic books may not be available in print.

The information in this e-book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor Centro Atlântico, Lda. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

Trademarks: *centroatlantico.pt*, the Centro Atlântico logo and *centroatlantico.pt magazine* are registered trademarks of Centro Atlântico, Lda. and may not be used without written permission. All other trademarks are the property of their respective owners. Centro Atlântico, Lda., is not associated with any product or vendor mentioned in this e-book.
Trademarked names are used throughout this e-book. Rather than use a trademark symbol with every occurrence of a trademarked name, the publisher states that it is using the names only for editorial purposes and to the benefit of the trademark owner, with no intention of infringing upon that trademark.

About the Author

Ankit Fadia is an independent Computer Security and Digital Intelligence Consultant and has definitive experience in the field of computers. He has authored several best-selling books on Computer Security, which have been appreciated by professionals and industry leaders, all over the world. His books sold a record 80,000 copies across the globe. Fadia is also a widely recognized cyber terrorism expert.

Fadia is however, more well known for his significant work in the field of digital intelligence, security consultancy and training.

Moreover, Fadia has also conducted more than a 100 training sessions on various topics related to Computer Security to an audience comprising of international defense personnel, software professionals and college students.

For his work in the field of computer security, Fadia has been honoured with numerous awards namely: Person of The Year 2002, Limca Book of Records, Silicon India Person of the Week, Embassy State Award, Best Speaker Award (3 occasions), Hall of Fame Award, Outstanding Young Achiever's Award, Student of the Year 2002-03 and many more.

Quite recently, Fadia travelled to Australia, Singapore and Malaysia where he addressed hundreds of CEO's of various IT companies and provided them solutions to protect their network and keep their data safe. He has also been conducting a number of learning events for Young Entrepreneurs and Young Presidents of the most successful companies and businesses all across India.

Fadia is currently pursuing his studies in Computer Science with specialization in Information Security at Stanford University, USA.

INTRODUCTION

The Internet has considerably enhanced various business critical operations of companies in different industry sectors across the globe. However, as more and more Organizations become partially or completely dependent on the Internet, computer security and the serious threat of computer criminals comes to the foreground. A single network infiltration can cause severe losses totalling in millions of dollars. Unfortunately, most organizations across the globe continue to remain oblivious of to the threat posed by computer criminals, corporate espionage and cyber terrorism. '*The Ethical Hacking Guide to Corporate Security*' dismisses this incompetent approach adopted by many companies and clears up some of the most horrific cyber crime cases that hit the corporate world across 17 different countries in 5 continents. With the correct mix of technical explanations and subsequent business implications, this book draws a direct correlation between computer security and business profitability. The comprehensive yet easy to understand analysis of some of the most dangerous security threats and vulnerabilities on the Internet, lays down the path that companies need to follow to safeguard their networks. This book places a great deal of emphasis on investigating and solving real attacks faced by companies. Moreover, the thoroughly researched attack strategies, working and countermeasures described in this book are organized in an extremely unique easy to understand format. This book is not only aimed at serious hardcore system administrators, but it also contains information that will be relished by top-level management gurus working in various industry sectors.

Contents

II Denial of Services (DOS) attacks

IV Input Validation Attacks

VI Instant Messenger Threats

VII Social Engineering Attacks

III. E-MAIL SECURITY

Threat Level: HIGH (8/10)

Ease Level: HIGH (10/10)

Incident Level: LOW (4/10)

Business Threats: Intellectual Property Theft, Social Engineering, Corporate Espionage, Virus attack on critical Business Infrastructure, Defaming corporate honchos, Online Abuse.

Introduction

E-mail is one of the most popular utilities of the Internet. Staying in touch with friends and relatives, closing business deals within minutes and forwarding mass e-mails to all addresses in the address book— are just a few common uses of e-mail. E-mail has rapidly replaced snail mail in almost all domains and has become the preferred form of communication for most people. However, an e-mail message is definitely not as harmless as it might seem at first glance. There are a lot of dangers, abuse and problems associated with the rapidly increasing popularity of e-mail.

E-mail has become ubiquitous, especially in the corporate world. Most businesses cannot survive without the use of e-mail. However, in spite of the rapidly growing popularity of e-mail as the preferred communication medium, very few people are actually aware of the numerous security risks involved. In the recent years, there has been an alarming increase in the number of e-mail fraud cyber crime cases on the Internet. Hence, it has become extremely important for all businesses to take the necessary precautions against the menace of e-mail fraud.

Business Definition

"…E-mail on many occasions is misused by internal disgruntled employees or external malicious people to steal intellectual property, to make abusive attacks, to perform social engineering, spread business rumors, harassment, ransom threats, Spam, identity thefts, mail bombing and many other related attacks. Attackers sometimes also use e-mail to carry out impersonation or identity hijacks for social engineering purposes against employees, clients or media representatives…"

E-mail Threats

Almost all employees in corporations across the globe use e-mail on a daily basis for either business or personal purposes. Some of the most common threats associated with e-mail are as follows:

1. Very few corporations, if any, actually use encrypted e-mail. Most e-mails on the Internet are sent in the plaintext form and hence can easily be recorded and spied with the help of a simple sniffer. Hence, e-mail provides the bad guys with a lot of opportunities to carry out information theft attacks. E-mail not only puts personal

conversations at risk, but even sensitive business deals can be violated with the help of simple sniffer tools.

2. Almost all regular (ISP or web based) e-mail systems rely on external untrusted systems to send an e-mail from the source to the destination system. This means that while e-mail is being sent from one point to the other, there are plenty of methods with which the bad guys can get their hands on the sensitive contents of e-mail.
3. It is very easy for an attacker to send out abusive e-mails to the victim and remain completely anonymous at the same time. Most sexual harassment and mental torture cyber crimes cases on the Internet occur either on IM or through e-mail. Office related online sexual escapades have indeed become extremely common. Hence, both corporations and individuals need to be very careful as far as using e-mail is concerned.
4. Most employees use popular e-mail clients like Outlook Express, Microsoft Outlook, Eudora Pro, etc. to receive and send e-mail. Due to their ever-growing massive popularity, e-mail is the obvious target for an extremely large number of virus creators. Today, a high number of viruses and worms choose e-mail systems as the preferred method for propagation. This means that unfortunately, a majority of viruses and worms on the Internet spread by exploiting the numerous security vulnerabilities existing in such e-mail clients. Hence, corporations must take the necessary steps to stop the spread of viruses and worms through e-mail clients.
5. Another common problem with e-mail clients is that while a user is being authenticated, the username and password pair is sent in plaintext to the mail server. This makes it very easy for an attacker to use a sniffer to sniff the password of a victim and carry out malicious activities. Moreover, if the *save password* option has been enabled (i.e. if the password of an e-mail account has been stored on the local machine) then it is quite easy for an attacker to crack the password using a basic password cracking tool.

6. E-mail forging has become an extremely widespread problem. Through e-mail forging an attacker sends a forged e-mail to a third party (client, partner or customer) in such a way that the e-mail seems to have been originated from the victim corporation's CEO's e-mail account. Such e-mail forging attacks can easily be used to create a number of misunderstandings, cancel orders, spoil relationships, defame corporations and carry out numerous other business related losses.
7. Attackers commonly use e-mail to carry out social engineering attacks— both human and computer based. Read the section of Social Engineering for more information.
8. Most online e-mail service providers are very vulnerable as far as input validation attacks, DOS attacks, buffer overflows and other attacks are concerned.
9. Spam has become an extremely big problem for all e-mail users. A recent report revealed that Spam contributed more than 70% of all e-mail on the Internet. Spam e-mails not only clutters up your Inbox, but it also leads to a waste of time and resources in the storing and reading of useless information.

Business Cheats, Cons and Crimes

1. Are your employees leaking sensitive information about your corporation to the bad guys through e-mail?
2. Are you sure your sensitive official e-mails are not being watched or recorded by malicious attackers?
3. Are the bad guys sending forged e-mails (that seem to originate from your e-mail account) to your clients and hence defaming your name?

4. Is your daughter receiving abusive e-mails studded with tons of sexual content?

Case Studies

Karachi, Pakistan: Individual

The daughter of a Police Commissioner had just joined a college, when she suddenly started to receive a number of abusive e-mails that threatened sexual harassment unless a particular criminal (imprisoned by her father) was set free. It was certainly not possible for the police to agree with the attacker's demands. Computer forensic experts began to examine and study the abusive e-mails received by the victim in a bid to trace them to the culprit. However, investigations revealed that the abusive e-mails received by the victim were forged. The e-mail exam revealed that the attacker used to go to a local Internet café, connect to a remote mail server and send out forged abusive e-mails to the victim. The e-mail forging continued for almost a couple of months without the forensic experts being able to identify the culprit. The forensic experts even contacted the local ISP and local Internet café owners, however, without much success. The attacker was quite smart and never used the same Internet café twice. However, fortunately soon the frequency of the abusive e-mails started dropping and slowly completely died down. This cyber crime clearly reiterates the anonymity that an attacker can enjoy with the help of e-mail forging and Internet cafes. This cyber crime had numerous adverse consequences:

- Mental torture and fear for the victim and her family.
- The victim had to keep changing her e-mail address.
- Inconvenience.

Dubai, UAE: Individual

There was an engineer who was working for a big multinational company in Dubai, UAE. He enjoyed a good salary and quite hefty perks as well. However, he was not sure whether he wanted to continue doing (what his job profile demanded) for the rest of his life. One day he received an e-mail from another multinational company offering him a job with not only higher perks and a better salary, but also projects that were more challenging and interesting. After a few promising e-mail exchanges with his prospective project manager in the other company, he took the bold step to quit his secure job and take up this exciting new job opportunity. When he went to the company address (as mentioned in the contract that his prospective boss had e-mailed him), not only did he not find any job waiting for him, but also to his utter despair his so-called boss did not even work in that company. The consequences of this cyber crime were:

- Victim lost his secure job.
- Financial and Emotional Loss to the victim and his family.
- Had to desperately hunt for a new job.
- Victim Company lost a talented and experienced individual.

Different Types of E-mail Threats

As discussed above, there are a variety of e-mail related threats on the Internet. However, some of the most common attacks are as follows:

1. Abusive E-mails
2. E-mail Forging
3. Spam

Abusive E-mails

Introduction

Before one can actually become involved in the termination of abusive or obscene e-mail messages, we must understand the way how e-mail travels on the Internet. E-mail travels from the source computer to the destination computer on the Internet in a manner analogous to that of snail mail in real life.

Typically the sender of an e-mail connects to a mail server (post office) and sends the e-mail to a particular destination e-mail address. This source mail server then routes the e-mail through several other interim mail servers, until the e-mail reaches the actual destination address. In other words, every e-mail originated at a particular mail server, is routed through a number of different interim mail servers on a specific route and then finally arrives at the actual destination:

Sender Outbox-----→Source Mail Server-----→ Interim Mail Servers-----→ Destination Mail Server------→ Destination Inbox

In other words, if one is able to pinpoint the source mail server of an e-mail, then one could potentially even pinpoint the identity of the person who sent that particular e-mail. When an e-mail is sent across the Internet, t carries not only the actual message content, but also carries embedded information about the path it use from the sender to the receiver. This information about the path traveled by an e-mail is contained in the *e-mail headers* of the e-mail itself. This means that by reverse engineering the path traveled by an e-mail, one can easily figure out its source. This means that each time one receives an abusive e-mail, one should open the e-mail headers and try to trace its source.

Unfortunately, statistics show that the most common reaction to an abusive e-mail is to hit the DELETE key. However, ignoring the problem will not put an end to it. Ideally each time you receive an abusive e-mail, you should follow the easy steps described below and try to trace the identity of the person who sent the e-mail:

1. View the e-mail headers of the received abusive e-mail.
2. Identify the IP Address of the computer that was used to send the e-mail.
3. Trace the IP address to pinpoint the identity of the culprit.

E-mail Headers

E-mail headers certainly contain the key to tracing an e-mail to the real culprit who actually sent the e-mail. Typically e-mail headers contain specific information about the e-mail client, mail server platform, time stamps and most important accurate coordinates of the path traveled by the e-mail from the source to the destination computer. E-mail headers are generated and embedded into an e-mail message both during composition and transfer between systems. Hence, by analyzing the e-mail headers of an e-mail, you can actually reverse engineer the path traveled by the e-mail and arrive at the originating system. For example, a typical e-mail header would look like the following one:

```
Return-Path: <blah@blah.com>
Received: from smtp3.Blah.com (8.12.11/8.12.11)
        by pobox4.Blah.com (Cyrus v2.1.16) with LMTP; Mon, 22 Mar 2004 12:28:42 -0800
Received: from LIZ-Laptop.blah.com ([64.163.150.1])
        by smtp3.Blah.com (8.12.11/8.12.11) with ESMTP id i2MKSfQI025425
        for <abc@blah.com>; Mon, 22 Mar 2004 12:28:42 -0800
Message-Id: <5.2.1.1.2.20040322122800.025d9320@liz.pobox.blah.com>
X-Sender: liz@liz.pobox.blah.com (Unverified)
X-Mailer: QUALCOMM Windows Eudora Version 5.2.1
Date: Mon, 22 Mar 2004 12:28:19 -0800
To: abc@blah.com
```

```
From: Liz <blah@blah.com>
Subject: Hi
Mime-Version: 1.0
Content-Type: text/plain; charset="us-ascii"; format=flowed
```

Tracing E-mails

The best way to analyze e-mail headers is to divide the header information into separate chunks, examine each chunk as an independent entity and then finally put back all the individual puzzle pieces together. In this example, the e-mail headers can be divided into the following chunks:

```
Date: Mon, 22 Mar 2004 12:28:19 -0800
To: abc@blah.com
From: Liz <blah@blah.com>
Subject: Hi
Mime-Version: 1.0
Content-Type: text/plain; charset="us-ascii"; format=flowed
```

This e-mail header chunk tells us that this e-mail was sent by blah@blah.com to abc@blah.com on 22nd March 2004 at 12:18. It also contains the MIME version and data type carried by the e-mail.

```
Return-Path: <blah@blah.com>
X-Sender: liz@liz.pobox.blah.com (Unverified)
X-Mailer: QUALCOMM Windows Eudora Version 5.2.1
```

The above e-mail header reveals that the sender of this e-mail is running a version of Windows and is using Eudora 5.2.1 as the e-mail client. It also identifies the e-mail address blah@blah.com as the sender of this e-mail.