Attack methods to compromise availability of computers computer science

THE SUCCESS MISUSES of computer systems security breaches increased slightly in 2005, according to the FBI and the Computer Security Institute (CSI). Many security issues that apply to large enterprises definitely apply to SMBs, especially as SMBs become more technologically sophisticated, according to Andrew Kellett, senior research analyst with U. K.-based Butler Group. You dont have to be a particular large organization to have some pretty complex supporting systems in place, he says. (Fred Sandsmark, p11)

The above-mentioned stated that there was slightly increase in computers attack in 2005. As technology evolving, companies willingly to spend more money on computer systems to do business activities with their associate and partners.

This will increase more and more security breaches on the computer systems.

The purpose of this analysis report is to examine the various possible attack methods to compromise the availability of the computers, information and associated resources of a small firm.

Research for this report includes an attack tree diagram, showing how the hacker can compromise the availability of the systems services, associated resources and to access sensitive information through different attack techniques. Each technique is the subset of the different type of attack methods, with possible assumptions attach to each methods, the attack tree will be discussed in greater details.

INTRODUCTION

The manager of the Raylee Pte Ltd has recently heard through the media and newspaper publications that there are numerous threats which could compromise the availability of the computers, information and associated resources.

Management of Raylee Pte Ltd has decided to hire the security consultant firm Red Alert Security Pte Ltd to undertake a details analysis of its current computer and network state in order to prevent the hackers to compromise the availability of the computers services, information and resources. The under-mentions are the network and desktop environments of the Raylee Pte Ltd.

There are six computers and one internal server (for processing orders) within the firm.

Each computer encompasses Microsoft Windows 7 and Microsoft 2007

Each workstation has been patched with all updates as of March 25th, 2010.

The company shares an ADSL 2+ connection amongst all computers.

Server backups are done fortnightly and stored on a DVD spindle name backup1

Workstation backups are done bi-monthly and stored on a DVD spindle name backup2

Employees have email addresses provided by the Internet Service Provider.

Documents are shared amongst employees through a D-Link DNS-323 NAS

The router is utilising a default settings and consists of a D-Link DSL G604t.

Each workstation is utilising Microsoft Windows Malicious Software Removal Tool.

SCOPE

Security consultant of Red Alert Security Pte Ltd will analyse of the company current computer system, network state and desktop environment in order to prevent the hackers to compromise the availability of the computers services, information and resources. Then the consultant will submit a detail analysis report to the Management of Raylee Pte Ltd for recommendations

METHODOGLY

The security consultant uses a technique known as attack tree to identify the best possible options to compromise the availability of the system services, information and resource in the quickest time. Below is the attack tree he comes up with.

Compromise The Availability Of Computers, Information And Associated Resources

1. Remote Access Router:

D-Link DSL G604t

2. Access NAS:

D-Link DNS-323

3. 3. Gain Access Internal Server

(Processing Orders)

Orders)

4. Steal Password: Workstations

METHODOLOGY

From the attack tree in the previous page, each of the sub attack tree will be discussed in more detail.

Figure 1

1. Remote Access Router :

D-Link DSL G604t

1. 1 Determine the password

1. 1. 1 Learn password

1. 1. 2 Use widely know password

1. 1. 3 Dictionary attacks

1. 1. Determine password

Hacker and cyber criminal will try to determine the password of the router in order to access the network environment and do whatever they want. We will briefly explain the methods as follows

1. 1. 1 Learn password

If the user has not set new password and is using the default which is normally blank.

Hackers can easily search online for the manual of the particular wireless router and know the password. Hackers login the wireless router configuration page to change the setting and sabotage the network. For instance, hacker can surf this link http://www. routerpasswords. com/index. asp

to get the default password for all the routers.

1. 1. 2 Use widely know password

The common used passwords are admin, password, , 123456,

666666, qwerty, 00000000 and etc. These widely used passwords allow hackers to easily access the router.

1. 1. 3 Dictionary attacks

As the word dictionary it implies that it is one of the attack techniques use by the hackers to determine its decryption key, password or passphrase by searching the all the words which are usually seven characters or lesser chosen by the user in the dictionary.

METHODOLOGY

Figure 2

2. Access NAS : D-Link DNS-323

2. 1 FTP server

2. 2 Folder & File Permission

2. 3 P2P distribution

2. 1. 1 Bounce Attack

2. 1. 2 Misconfigure

2. 3. 1 File poisoning

2. 3. 2 Sybil attack

2. 1 FTP server

Most of the Network Attach Storage device comes with the feature of the FTP server

which allows user to download or upload file remotely anywhere. However, this service

creates a loophole for attacker to retrieve sensitive information and data. The various attack methods on FTP server are discussed as follows

2. 1. 1 Bounce Attack

FTP bounce attack is another attacking technique use by the hacker to exploit the ftp protocol so that he can use the PORT command to send

request access to the ftp port indirectly to another victim machine which acts as third party for such request to access the ftp.

2. 1. 2 Misconfigure

One of the common problems is to misconfigure the ftp server which allows users to download and upload the files in the same directory (global/tmp directory) for people to share data with each other. It will create an opportunity for attacker or theft to steal the data or upload virus program to the directory. Hence employee will accidentally install the virus program and infect to the computer systems and network.

2. 2 Folder & File Permission

Proper folder and file permission must be set according to the employee roles and responsibilities. If there is no permission setting on the files and folder and gives everyone permission to read, write and execute it. Then it will be easily for attacker to retrieve information upon hacking into the company network.

2. 3 P2P Distribution

It is a peer-to-peer file transfer protocol to allow users each download different pieces of the broken file from the original uploader (seed). Users exchange the pieces with their peers to obtain the broken ones which are missing. IT savvy employees can make use of the P2P to download their favourite movies, videos, music and software. Hacker will make use of the

P2P attacks to gain access into the network. There are two types of attacks which are file poisoning and Sybil attack.

2. 3. 1 File Poisoning

File poisoning attacks operate on the data plane and have become extremely commonplace in P2P networks. The purpose of this attack is to replace a file in the network by a fake one and this file will be corrupted and no longer in use.

2. 3. 2 Sybil Attack

The idea behind this attack is that a single malicious identity can present multiple identities, and thus gain control over part of the network. Once the attacker gains the control, he can abuse the protocol in any way he likes.

METHODOLOGY

Figure 3

3. Gain Access Internal Server

(Processing Orders)

3. 1 Steal sensitive information from the database

3. 1. 1 Gain access by internet

3. 1. 2 Physical access to the server

3. 1. 3 Access server from workstation

OR

OR

3. 1. 1. 1 Monitor network traffic

3. 1. 1. 2 Use remote exploit

3. 1 Steal sensitive information from the database

Sometimes hackers are hired by the competitor to create chaos in the company network and to steal confidential information such as customer data, vendor data, pricing information, new product launch information from the computer systems. There are various methods to steal information from the database and there are as follows:

3. 1. 1 Gain Access By Internet

Attack corporate network by using internet is becoming more sophisticated as technologies evolving. There is an increase of internet attacks orchestrate by the hackers to strike highly protected targets, to coordinate waves of scripted exploits and/or to conceal the true origin of

an attack.

3. 1. 1 . 1 Monitor Network Traffic

Cyber criminal use network monitor tools to monitor the local area networks or wide area networks. Some of the network monitoring tools such as Microsoft Network Monitor, Ettercap, TCP Dump and DSniff can be download

freely from the internet. This program can intercept and log the traffic passing over the network or part of the network. Once the information is captured by the program, hacker will decodes and analyse its content according to the appropriate RFC or other specifications.

3. 1. 1 . 2 Use Remote Exploit

The server is connected to the internet and the operating system is not updated the latest patches, then the cyber attacker will use remote exploit the vulnerability of the system to infiltrated the system to steal the information and sabotage the server by destroy the database and hard disk. Since the server backups are done fortnightly, management will be facing difficulties in recover the data.

3. 1. 2 Physical Access To The Server

Due to the space constraint, sometime the server share space with someones cubicle or office.

This creates an opportunity for an attacker who able to access files and other data by removes the hard disk, and then attaches it to another computer. He can also use third-party operating system CD to start the computer and steal corporate data or insert USB drive to inject virus into the system.

3. 1. 3 Access Server From Workstation

Cyber attacker is not limited to hack into the server. Workstation is the often the first target the hacker will try to access because from there, he can learn about the network environment and security loopholes to attack the server.

He will use the workstation as the stepping-stone to server-level break-in by stealing administrator passwords.

METHODOLOGY

Figure 4

4. Steal Password: Workstations

4. 1 Users Login password

4. 1. 2 Obtain password illegally

4. 1. 1 Social Engineering

4. 1. 1. 1 Share password

4. 1. 1. 2 Phishing

4. 1. 2. 2 Find written password

4. 1. 2. 1 Steal password

4. 1. 2. 1. 2 Install keyboard sniffer

4. 1. 2. 1. 1 Obtain sniffer output file

AND

4. 1 Users Login Password

Companies must know that hackers not only interested in the corporate data, they are also interested in the employees personal data such as bank account, credit card, email address

and others. To break into the workstation, hackers will need to know the users login password.

4. 1. 1 Social Engineering

Social engineering is the method of non technical hacking into the system by manipulating people through social interaction via email or phone to reveal their password.

4. 1. 1. 1 Shared Password

It is very common for employees to share computer password with their colleagues. Sometimes in their absence in the office, they will usually call one another to help them login to the computer to retrieve some information.

4. 1. 1. 2 Phishing

Hacker can create an email or instant messaging with attach fake website link which looks almost the same as the real one to lure the user enters their personal details such as username, password, credit card details and banking credential. All these information will be sending to

the hacker.

4. 1. 2 Obtain Password Illegally

Weak password makes hacker to obtain password illegally and faster. Cyber attackers will steal the password by infect the workstation with trojan. Basically there are three types of trojan attackers can use to steal the password namely: keyboard sniffer, login spoofing and password stealer. When attacker install the keyboard sniffer program which will monitor each keystroke the user has entered and this program generate the sniffer output file which send to the attacker. Sometimes hacker can pose as companys guest to access the premises. Upon entering the office, he will look

for password which the employee written on a piece of paper and paste it around the working cubicle.

CONCLUSION

Companies are constantly at risk of losing sensitive corporate data. In this report,

we have use the attack tree model to analyse various attacks method the attackers use to steal sensitive information on the server, network attach storage device, router and workstations. The most common and easier method is to obtain the users password by learn the password, use widely common password, dictionary attack, shared password, phishing, find written password and steal passwords. Cyber attackers and novice hackers are usual like to steal the passwords by downloading keyboard loggers, passwords cracking software, keyboard sniffers and others which are available on the website to test on their skill.

Management should implement counter measures to prevent hackers to attack their system and security breaches. We recommend antivirus program to be installed on

the workstation and server as they are utilising Microsoft Windows Malicious Software Removal Tool which is not enough for the prevention of the cyber attacks.

Local group policy of the password needs to enforce on the networking devices, workstation and server so that the password is not being easily crack by the hackers.

Lastly, passwords should be set minimum 8 characters and contain alphanumeric and symbols for complexity.

In conclusion, steal password is the easiest method for hackers to attack the computer system because local authorities might face difficulties in tracking them down if they are distant hackers.

GLOSSARY

Attack tree Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes. (Source : http://www. schneier. com/paper-attacktrees-ddj-ft. html)

Social Engineering In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human

interaction and often involves tricking other people to break normal security procedures.

(Source : http://searchsecurity. techtarget. com/sDefinition/0,, sid14_gci531120, 00. html)

3. Phishing Phishing is a technique of fraudulently obtaining private information.

(Source : http://en. wikipedia. org/wiki/Social_engineering_(security)#Pretexting)

4. Keyboard Sniffer – A program which reads the keystrokes made by a user and transmits them to

someone else. Such programs are usually used by intruders into computer systems in order to

capture important information such as passwords.

(Source : http://www. encyclopedia. com/doc/1O12-keyboardsniffer. html)

5. RFC – Short for Request for Comments, a series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard. Each RFC is designated by an RFC number. Once published, an RFC never changes. Modifications to an original RFC are

assigned a new RFC number. (Source : http://www. webopedia.

com/TERM/R/RFC. html)