NISER
National ICT Security and Emergency Response Centre

e-Security

National ICT Security and Emergency Response Centre

NISER'S Quarterly Bulletin Volume 2

Editor

Philip Victor
Training & Outreach Unit, NISER

Contributors :

From the Editor's Desk

This is our 1st Quarter Issue for 2005 and packed with more information from our previous issue. We would like our reader to note that some articles are made up of a series which started in the previous issue. It would be good if readers get a copy of every issue in order to have a follow up of these articles and also be updated on the latest happenings and events in the ICT Security world.

We would like to thank our readers on their feedback on our first newsletter, which was the previous issue. We have made some amendments to our current newsletter and welcome more feedback for continual improvement. Tell us what you would like to see in this bulletin and if you are interested to be a contributor.

Well, since our last newsletter, NISER has achieved another milestone by partnering with ISC2 to offer the prestigious CISSP program here in Malaysia. Having realised that our country is lacking cyber training spaces that produces competent and certified information security professionals, NISER has extended its service by providing a platform for information security professionals to move one step further through certification.

Finally, we hope that this bulletin can provide you with some useful information and knowledge to help you in your current environment. Feel free to contact us for contribution, feedback or information.

Philip Victor
vphilip@niser.org.my

Reader Enquiry

Training & Outreach Unit
National ICT Security & Emergency Response Centre
MIMOS Bhd
Technology Park Malaysia, 57000
Kuala Lumpur, Malaysia
Tel: 60 3 86577042

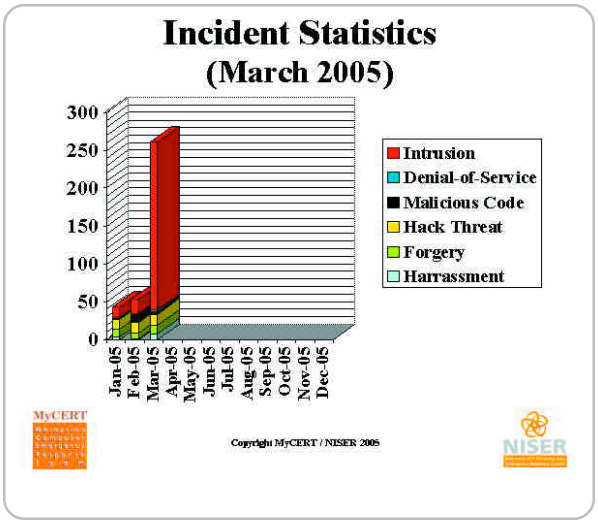
Email: training@niser.org.my

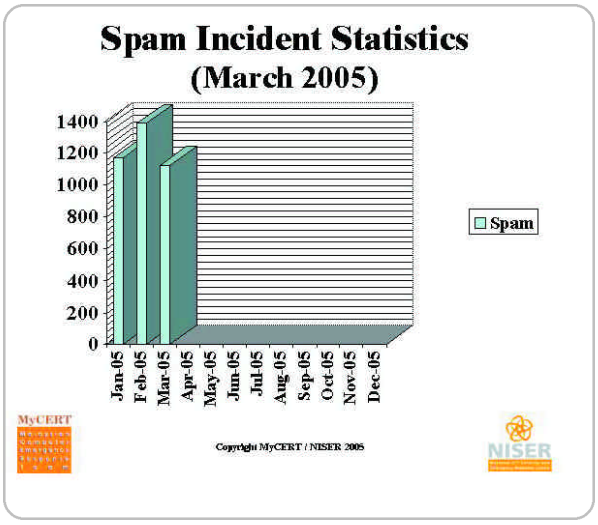
MyCERT Quarterly Summary MA-090.042005 (Q1) 2005
Original Issue Date: 12th April 2005

The MyCERT Quarterly Summary is a quarterly report to wrap up incidents reported to us with some brief descriptions and analysis of major incidents observed during that period. Included are highlights on the statistics of attacks/incidents reported, as well as other noteworthy incidents and new vulnerability information is inclusive.

Additionally this summary also directs to resources in dealing with problems related to security incidents, including patches, service packs, upgrades and hardenings

Complete figures and statistics graph on the Abuse Statistic released by MyCERT monthly is available as below:





Recent Activities

The 1st Quarter of 2005 was hectic as compared to previous quarters. Significantly, during this period, we received an overwhelming number of reports on web defacements of local websites, which had caused lots of annoyances and disturbances to our country that a crisis was declared during this period. However, no severe impact to the network infrastructure of the country was observed. Generally, the number of incidents had increased in this quarter to previous quarter with a 6.7% increase. Hack attempts, intrusion, denial of service and spam had increased this quarter compared to previous quarter. Malicious code, forgery and harassment had dropped this quarter compared to the previous quarter.

Tremendous Increase on Intrusion

This quarter also saw a significant increase in Intrusion, with a total of 256 incidents compared to 42 incidents in the previous quarter, which represents more than a 100% increase. The significant increase to Intrusion in this quarter is mainly due to mass defacement as a result of recent issues presented by the media.

Most of the defaced sites were left with hatred/dissatisfaction against the Government of Malaysia and its Ministers/Ministries. A total of 216 Malaysian websites were defaced during this period, which began on 6th of March until the 21st of March 2005.

MyCERT had produced 2 alerts on the recent mass defacements of Malaysian websites, available at:
http://www.mycert.org.my/advisory/MA-088.032005.html
(Released on 11th March 2005)
http://www.mycert.org.my/advisory/MA-087.032005.html
(Released on 9th March 2005)

Our findings, based on the log analysis extracted from the victims' machines indicate that the mass defacements were done using the following exploits:

a. SQL Injection
b. Vulnerable PHP Scripts
c. Vulnerable AWStat

The crisis was handled successfully by MyCERT team and we observed a significant decrease in the defacement beginning 15th March onwards until the situation was declared peace. The Indonesian CERT had responded to MyCERT's request by urging the Indonesian hackers to stop defacing our sites. This urge had helped in reducing the number of defaced sites and finally stopped the activities.

MyCERT would like to advise all System Administrators and owners of systems/networks to upgrade and patch software/services/applications they're currently running. In addition, it is also recommended to disable unnecessary/unneeded default services supplied by vendors. Our analysis showed that majority of previous Intrusions such as web defacements were due to vulnerable and unpatched services running on the server. Web defacements involving Linux machines are due to running of older versions of the Apache servers, PHP scripts and OpenSSL. As for IIS web servers, web defacements were commonly due to Microsoft IIS extended Unicode directory traversal vulnerability, Microsoft Frontpage Server Extension vulnerability and WEBDAV vulnerability.

Details of the vulnerabilities and solutions are available at:

1. **Apache Web Server Chunk Handling Vulnerability**
   http://www.cert.org/advisories/CA-2002-17.html

2. **Vulnerabilities in PHP File upload**
   http://www.cert.org/advisories/CA-2002-05.html
3. **Vulnerabilities in SSL/TLS Implementation**
   http://www.cert.org/advisories/CA-2003-26.html
4. **WEBDAV Vulnerability**
   http://www.cert.org/advisories/CA-2003-09.html
5. **Microsoft IIS extended Unicode directory traversal vulnerability**
   http://www.mycert.org.my/advisory/MA-024.042001.html

Web servers running Windows IIS servers, may use the IIS Lockdown tool to harden their server.

IIS Lockdown Wizard version 2.1 works by turning off unnecessary features, thus reducing attack surface available to attackers.

The IIS Lockdown tool can be downloaded at:
http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en

Web servers running on Linux, may use the TCP filtering mechanism such as TCP Wrappers at the server or gateway level. TCP Wrappers is a tool commonly used on UNIX systems to monitor and filter connections to network services.

TCP Wrapper can be downloaded free at:
http://www.cert.org/security-improvement/implementations/i041.07.html

Hack Attempts on the Rise

Incidents on hack attempts had increased for this quarter compared to previous quarter with a 95.2% increase. A total of 41 reports were received on hack attempts for this quarter compared to 21 reports in the previous quarter, targeting mainly on organizations' systems/networks. Home users PCs are also becoming a target among attackers on port scannings.
MyCERT's findings for this quarter shows that the top targeted ports for scanning are SSH (22/TCP), HTTP (80/TCP), MS SQL (1433/TCP) and Netbios (137/TCP), (138/TCP), (139/TCP). Port scanning is actively carried out once a new bug or exploit is released to the public. Besides scanning for open ports, scannings are also actively done to detect any machines running vulnerable programs and scripts, such as scanning for Unicode vulnerability on IIS web servers and scanning machines running vulnerable PHP scripts.

MyCERT recommends the following preventive measures:
* Close all ports or unneeded services except http service and other required ports/services should be filtered and patched accordingly.
* All machines/systems are properly patched and upgraded with the latest patch, service packs and upgrades to fix any vulnerability that may be present in the machines/systems.
* Organizations can install network based or host based IDS to alert scannings and other malicious attempts to their hosts.
* It is recommended that home users install personal firewalls in order to alert the owner of any unauthorized scanning to their machine, and to block any penetration into their system.

More information on home PC security is available at:
http://www.mycert.org.my/homepcsecurity.html

Harassment and Forgery Has Dropped

Incidents on harassment have decreased compared to the previous quarter by about 53.8%. Majority of harassment incidents received, involved harassments committed via emails, chat forums and web forums where majority of them were referred to the law enforcement agencies for further investigation. MyCERT were also involved in assisting Law Enforcement Agencies, such as the police, Attorney General, Malaysian Communications and Multimedia Commission (MCMC) in investigating some harassment incidents.

We advise users who are harassed via Internet or any individuals who observed any kind of harassments via web forums that has implications to religion, social, politic and economy of the country to report to MyCERT for further analysis.

This quarter also witnessed a decrease of 26.8% in Forgery incidents compared to the previous quarter. We received 30 reports on Forgery for this quarter which includes phishing scams and email forgery with a majority coming from the former. We continue to receive reports on phishing activities for this quarter, involving local and foreign banks. The phishing activities reported to us includes local and foreign banks becoming victim of these scams and users who receive phishing emails purportedly from trusted banks.

MyCERT strongly urge users who receive emails purportedly from a bank requesting to change their logon and password to ignore/delete such emails immediately. Users are also advised to refer and verify any such emails with their ISPs, CERTs or with the Particular Financial institutions mentioned.

Incident on Malicious Code Continue to Drop

The 1st quarter of 2005 saw a decrease in virus/worm incidents again with only a total of 17 incidents which is about 46.8% decrease compared to the previous quarter. No significant worm outbreak was reported in this quarter. Though we received information of some minor worm outbreaks from overseas, we were not affected by them.

MyCERT advise users to always take precautions against worm incidents, eventhough no major worm outbreaks were observed within our constituency. Some of the precautions that users can take are:

a)Email Gateway Filtering

Sites are encouraged to apply filters at email gateways to block any attachments associated to the worm.

b)System/Host

i) Users must make sure that their PCs are installed with anti-virus software and are updated continuously with the latest signature files. Users who do not have an anti-virus installed on their PCs may download an anti-virus from the following site: http://www.mycert.org.my/anti-virus.htm

ii) Users need to make sure that their PCs/machines are always updated with the latest service packs and patches as some worms propagate by exploiting unpatched programs present in PCs/machines.

iii) Users are also advised to install personal firewalls, such as Zone Alarm on their PCs/machines.

iv) Organizations are also advised to close unnecessary services and ports except for http port. If oth er services/ports need to be utilized, then they should be filtered to allow authorize users only.

c)Safe Email Practices

MyCERT strongly advice users not to open any unknown attachments that they receive via emails. They should delete any suspicious emails or they may forward to the respective ISPs or CERTs for verification. Users may refer to the following guidelines on safe email practices: http://www.mycert.org.my/faq-safe_email_practices.htm

Other Activities

Spam incidents still remain on top with a total of 3683 incidents for this quarter, representing 1.6% decrease compared to the previous quarter.

It is almost impossible to completely eradicate spamming activities; however it can be minimized to a certain extent by following best practices, spam filters for end users and guidelines to minimize the daily annoying spam emails they received which is available freely in the Internet. In addition, home users may also subscribe to their ISP's Spam Filtering service, which is available for a very reasonable fee. Users may contact their ISPs for further information on this service.

We received 3 reports on Denial of service compared to 1 report in the previous quarter, representing more than a 100% increase. Denial of service attacks have become less popular nowadays compared to years ago, which makes incidents related to these categories much lesser. However, System/Network Administrators should not take these attacks for granted.

MALAYSIA WILL SOON HAVE A NATIONAL STANDARD ON BUSINESS CONTINUITY MANAGEMENT (BCM)

A working group on Business Continuity Management (BCM) was established under the SIRIM Berhad umbrella earlier this year with the objective of developing a national BCM standard. NISER has been actively involved in promoting the establishment of the working group and NISER has prepared a proposal paper that was submitted to SIRIM Berhad. At present, the working group has 12 members from both the public and private sectors and NISER is represented by Zahri Yunos.

The proposed BCM standard can be used by organizations from both the public and private sectors. The framework provides a set of recommendations of processes to implement BCM effectively in organisations.

The need for a national standard in BCM is important as it will then enable organizations to adhere to a common interface or framework for when implementing BCM. When a disaster strikes, it takes the cooperation of all the parties involved including business partners, service providers, the emergency services and other relevant bodies to help restore and resume the business operations back to normal. In order for this to happen, a common platform must be established, so that each organisation's business continuity plan can easily interface or interact with the relevant bodies. As Malaysia embarks to achieve a fully developed nation status and transform our society into a knowledge-based society, it is imperative to ensure that our critical information infrastructures, operations and businesses are well protected and continue to operate in the event of disasters.

The working group has agreed for the BCM framework to be divided into 3 parts and to be developed in stages:

* Part 1: BCM Better Practices. Part 1 provides high-level information of BCM. This part addresses issues pertaining to the definition and scope of BCM. This part also addresses processes involved in the development of an organization within the BCM framework.

* Part 2: BCM Guidelines. Part 2 complements Part 1 by providing guidelines, templates and hints on how to implement BCM Better Practices as in Part 1.

* Part 3: BCM Self Assessment Checklist. Part 3 provides information on how to assess the implementation of BCM. Part 3 complements both Part 1 and Part 2 by providing the method of assessing the current BCM framework.

The working group is currently developing the contents of Part 1. This has started since March 2004 and the first draft of Malaysian Standards on BCM – Part 1: BCM Better Practices is expected to be ready by the year end.

WLAN THREATS

It is already known that Wireless Local Area Network (WLAN) or better known as Wireless Fidelity (Wi-Fi) has experienced a rapid growth over the past few months. Indeed, wireless connectivity will be the most sort after ICT technology in time to come in many applications and Wi-Fi product sales such as Access Point (AP) can be seen as a good example. Nowadays, Wi-Fi products can be seen in offices, restaurants, schools and has now reached home users. The evolution is tremendous and would be difficult to catch up.

Just to recap, in the previous issue of e-Security by NISER (National ICT Security and Emergency Response Centre) dated 17 January 2005, the article on WLAN Overview showed a brief understanding of the technology. In the said article, it was an opening to a series of WLAN write-ups in this year bulletins, it gave a brief but thorough description of WLAN background such as the frequency spectrum it utilizes, frequency modulation techniques, network set up preferences, its IEEE 802.11 standards and also the security options it offers for end users to decide for deployment.

It is hoped that this small introduction will be sufficient as an adhoc reference and of course more information can be gathered from the internet, bookstores or library for more in depth knowledge in this technology. Perhaps, some companies might want their WLAN administrator to enroll for well known certification based WLAN training to perform a site survey before building up the system. This is a valuable and smart approach. Nevertheless, if any readers wish to have more information regarding this subject matter, you are very much welcome to contact NISER.

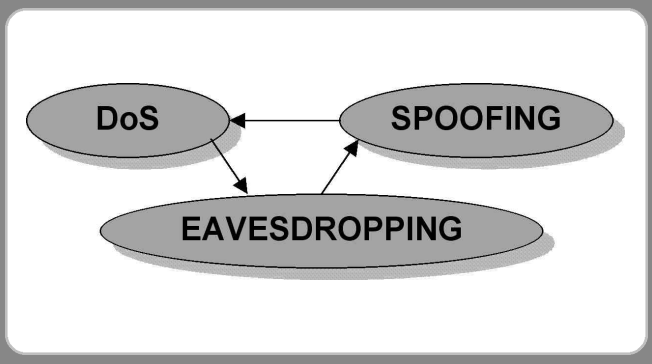
Next, in this issue of e-Security, is to bring the reader's attention to some of the existing threats in WLAN that has long been an issue in the ICT security community but not to the naive consumer. Sad to say that many WLAN end users are unaware of these WLAN threats until they encounter it. Some may not even notice that their WLAN is constantly been probed by others who are not supposed to have this privilege access. Valuable company data may be exposed such as the payroll, marketing plan, accounts or other sensitive information that can be made available for its competitor. This situation will eventually damage the organization's reputation.

Thus, the consumers are in full capacity to inquire on the WLAN security as it is the end users that would be performing e-commerce transactions and this is a major concern. Just imagine that someone might be able to collect all your personal information. This epidemic has got to be thwarted once and for all. Hence, every WLAN users must have the full commitment to secure their system according to the level of their data confidentiality and budget

Therefore, in order to counter the malicious doings, a proactive step is being able to identify all the possible WLAN threats. All identified WLAN threats must be broadcasted and acknowledged by the consumer so that all the necessary precautions could be established to mitigate or prevent these threats.

So, what are the well known WLAN threats?

The first common threat is eavesdropping. Eavesdropping is an attack against the confidentiality of the data that is being transmitted across the WLAN. It is very popular among the WLAN crackers after Wardriving (an activity to find unsecured WLAN for internet access connection) is performed. Occasionally, when an unsecured WLAN is found the attacker would try to sniff and capture sensitive data transmission over the air from a distance, as an example from a parking lot outside a corporate building without any physical connection. Then, the WLAN cracker or anybody for that matter might be able to gather all important data and if it is a banking transaction, just think and imagine the bad outcome of this threat.



Common WLAN Threats

Besides sniffing, spoofing is another type of threat. Spoofing is where the WLAN cracker gains access to the network by assuming a legitimate identity of a valid network user. Usually this is done after eavesdropping, when a valid username and password is captured. The attacker would then have the right to access the network services for confidential data resources.

Last but not least is Denial of Service (DoS) attack with the aim to degrade the WLAN connectivity. This attack is sometimes considered normal and vulnerable to DoS due to the fact of the 2.4GHz limited WLAN bandwidth. With this threat, the attacker will flood the WLAN network with useless packets or by using a powerful transceiver generating radio interference to jam the WLAN radio path.

It is sad that over the internet, many freely script kiddie tools are available to, crack the WLAN, spoof a rightful user and gain access to critical information. In the next issue of e-Security, readers will be given some possible WLAN security solutions concerning applying authentication and encryption to defend the system from each of these WLAN threats.

WHAT YOU NEED TO KNOW ABOUT SECURITY POLICY

What is a Security Policy?

Security policy is defined as a high-level statement of organizational beliefs, goals, and objectives and the general means for their attainment as related to the protection of organizational assets. It is brief, is set at a high level, and never states "how" to accomplish the objectives.

Why Implement a Security Policy?

We live in a world where computers are globally linked and accessible, making digitized information especially, vulnerable to theft, manipulation, and destruction. Security breaches are inevitable. Crucial decisions and defensive action must be prompt and precise. A security policy establishes what must be done to protect information stored on computers. A well written policy contains sufficient definition of "what" to do so that the "how" can be identified and measured or evaluated.

Without a security policy, any organization can be left exposed to the world. It is important to note that, in order to determine your policy needs, a risk assessment must first be conducted. This may require an organization to define levels of sensitivity with regards to information, processes, procedures, and systems.

What are the Components of a Security Policy?

When developing a security policy, there is as much danger in saying too much as there is in saying too little. The more intricate and detailed the policy, the more frequent the update requirements and the more complicated the training process for those who adhere to it.

The components of a security policy will change by organization based on size, services offered, technology, and available revenue. However, most organizations have a guide which dictates the makeup of all company policies. This guide likely contains some or all of the following:

* Purpose – this section states the reason for the policy.
* Scope – this section states the range of coverage for the policy (to whom or what does the policy apply).
* Background – this section provides amplifying information on the need for the policy.
* Policy statement – this section identifies the actual guiding principles or what is to be done. The statements are designed to influence and determine decisions and actions within the scope of coverage.
* Enforcement - this section should clearly identify how the policy will be enforced and how security breaches and/or misconduct will be handled.
* Responsibility – this section states who is responsible for what. Subsections might identify who will develop additional detailed guidance and when the policy will be reviewed and updated.
* Related documents – this section lists any documents (or other policies) that affect the contents of the policy.
* Cancellation – this section identifies any existing policy that is cancelled when this policy becomes effective.

What determines a good Security Policy?

An organization may have a written policy, but it may be confusing and hard to read. It may also contain 'gaps' where some key issues are addressed, but others are not. In general, a good security policy does the following:

* Communicates clear and concise information and is realistic;
* Includes defined scope and applicability;
* Consistent with higher-level policies and guidance;
* Open to change based on new risks and vulnerabilities;
* Identifies the areas of responsibility for users, administrators, and management;
* Provides sufficient guidance for the development of specific procedures;
* Balances protection with productivity;
* Identifies how incidents will be handled; and
* Is enacted by a senior official.

A key point to consider is to develop a security policy that is flexible and adaptable as technology changes. Security policy should also be a living document, routinely updated as new technology and procedures are established to support the mission of the organization. Additionally, organizations should be aware that the development of a security policy should be a collaborative effort with security officials, management, and those who have a thorough understanding of the business rules of the organization.

It is important to acknowledge that a security policy should not impede an organization from meeting its mission and goals. However, a good security policy will provide the organization with the assurance and the acceptable level of asset protection from external and internal threats.

PASSWORD - CHOOSING THE RIGHT FOUNDATION

Introduction

Believe it or not, most operating systems in this world use login and password as the only authentication method for security defence for the entire organization. UNIX and all UNIX-like operating systems are sure to use it to make the user integrate with the system. Most of the login is base on the user name and password, which is hidden while typing (huh)! Since we always believe that no one should know other people's password, we have forgotten one very basic thing, that, if the attackers can get the root password, the game is over. Since this is the easiest way to gain illegitimate access into a system, hackers and crackers will try password cracking as their first methods of attack after they have scanned for vulnerabilities in the system.

Hackers use various types of available tools and documents on the net to complete their tasks. I hate to write this, but the new hacking tools are so easy to use. Anyone, even a 15 year old boy hacker wannabe with minimum knowledge about the internet and even without in-depth knowledge on how certain password cracking tools such as l0pthcrack or John The Ripper work, can crack weak passwords within two hours. These tools are available online for free. Often, a good hacker will create these tools and later share it with others. Hacker groups are found globally and has become the biggest challenge for CERTs and all authorization bodies around the world to handle. Most hacking cases happen because of the lack of perimeter defence and due to human error. The vulnerabilities and weaknesses detected on the server usually due to a failure to patch up systems, usage of weak passwords and using the default installation settings.

Password Configuration

In UNIX, the password file is located in the /etc/passwd and /etc/shadow directories. In Windows NT and 2000, the password file uses the extension *.sam. Both files are encrypted and cannot be viewed as plain text. Bear in mind, there is no unbreakable password and with persistent effort, usually it is only a matter of time before they are broken. As for defence in depth strategies, we need to ensure that the best password combination is chosen. It means that if a more longer and complex password combination is used, the chances of it being cracked is much more minimal.

The hacker will try to own the victim's server via root compromise or by obtaining the root account. Since most (95%) system installations are done using the default installation, the file permission is not set to the level of security needed. This situation will assist the hackers to get to the root password faster. By obtaining just one weak user login name and password, they can download the password file and crack it from their machine without anyone noticing it, and a few moments later, they will literally "own" the system. This is one example why all users need to have ensure they practise secure password practices. Systems administrator should ensure that the file permission is set as securely as possible. Apply the principle of privileges on an as needed basis. This principle means that access to file are given to users based on their needs only.

Choosing Login and Password

"Trust No One"

Believing in this phrase will help you a lot when dealing with login and password issues. Firstly, do not share your password with others, even if it is with your best friend. If you lost your password, tell you system admininstrator to change it immediately. Treat your password as carefully as you would do with your bank account PIN (Personal Identification Number). You would not like other people to have your PIN, wouldn't you? As a human being, we can remember the word "thecatisblack" better than " **7YulO-@#dd". Based on that, we found most of the logins are using simple words such as the user's name or words found in a dictionary. For example, if John Smith is choosing his email login, he will probably choose Jsmith@company.com. Why? Because it is easy to be identified and remembered . Thus, he may choose jsmith123 as the password for the same reasons. The problem is, most of the password cracking tools contains a database of dictionary words and also can perform plain text guessing features. The latest password-cracking tool is much more powerful and is also equipped with a brute force password cracking method that can basically break any type of password, as complex as it may be.

Who should be in charge in password management? Should it be the system administrator's job or the manager's? The answer is it should be everybody. Imagine one large company consisting of more than 3000 users. Each and everyone has his or her own e-mail address. It may not be possible for the systems administrator to monitor each login and password. This is the reason that a password policy should be made available. A good password policy is only effective when everybody follows the contents effectively.

One of the most proven and often used methods to obtain passwords is using social engineering methodology. You can try doing this to your own company, but make sure thar you already have written permission from your authority. Remember the Randall Schwartz case? He got caught when accessing his company's system to test for vulnerabilities when in fact he only actually wanted to help his company.

Try this. Call the help desk. Just pretend to be one of your company's existing staff and inform them that your had forgotten your password. Tell them that you need to access the e-mail for some urgent matter that you need to complete for the CEO. Ask them to email the new password to your web base email, implying it to them that it is for security reasons. Once this is successfully done, the game is practically over. With the obtained user login name and password, a perpetrator can create various damages to the company. People can spread hoax, spam, and harassing e-mails to all employees and in the worst case scenario, send confidential emails to the competitors. Such cases often happen and had made many companies suffer..

Therefore, it should be made mandatory to all staff to comply to the password policy. The tips below can be used as part of good password policy practices:-

* No usage of dictionary passwords allowed. (i.e. golf1234, admin2001, myname444,)
* Use at least 8 characters and it must consist of numbers, letters and special characters (i.e. T3$_8alk*, 4c6_*!oo, c4r|n9L0v3,)
* Force users to change passwords after a certain period of time(i.e. Every 1 month)
* Do not rotate the password

For a system administrator, make sure that the minute an employee resigns from the company, their login privilidges are removed. Many cracking cases are caused by disgruntled ex-employees. Also ensure that the system implement strict password policies.. Users should also discouraged from writing down their passwords on a piece of paper and paste it on the PCs and tables. If users have problems remembering their passwords, they should adopt the substitution method when creating new passwords.You may want to choose a word that consists of at least 8 letters and substitute some of the letter them with numbers and special characters to make them more complex. Run a password auditing tool to test the strength of the passwords. Remember this though, there is no password that can't be broken, so for security purposes, try to make it as complex as possible.

Conclusion

Choosing a good password is very important and everybody should follow good and secure password practices. The hacker's ultimate goal is to own the system and they will try everything. Believe me, everything. As a defense in depth strategy, system administrators should study their perimeter defense, and make sure there is no weak point that can be used as hacker gateway to their systems. A weak password is a "welcoming back door" and it will always be so if the user continues to ignore it's importance. Preparing and implementing a good password policy also can help to harden the system from suffering the ill-effects of hacking activities.

PROTECTION OF MALAYSIAN CYBERSPACE : AN AGENDA FOR ACTION

Introduction

Cyberspace provides a great interactive communication medium in today's world where people could freely and virtually communicate with one another from all over the world through computer systems equipped with Internet connection. However, many of the essential services have been shifted to networked information systems without much consideration on information security. Such a shift creates new vulnerabilities and unprecedented opportunities to those who have malicious intent to the users, organisations and the country as whole.

Cyber Threats and the Related Incidents

Cyber world is borderless and is exposed to various threats and incidents such as intrusion, worms/virus and hack attempts. Today, cyber warfare becomes an attractive proposition to many parties as it is relatively cheaper than the conventional and space warfare. Cyber warfare is more about gaining control of information and information systems rather than destroying the enemies' life or gaining ground and some of the incidents include denial of service (DoS) attacks and websites being defaced. As an example, the South Korean Government's computers were hit by massive cyber attacks in July 2004, where the hackers had broken into 211 computers at 10 government agencies using an sophisticated information-stealing virus. Important data may have been stolen during the incidents.

In Malaysian scenario, security incidents continue to increase as reported by Malaysian Computer Emergency Response Team (MyCERT). In year 2004 (until October 2004), the number of incidents which includes Spam reported more than 12,000 cases compared to 4000 cases reported in 2003 (Source: www.mycert.org.my). The statistics shows that mail spamming, intrusion and virus attack are the most common security breaches. Malaysia also experienced bad moments during the attack by the Code Red Worm in 2001 and the Blaster and Nachi worms in 2003 .

Some Initiatives on the Protection of Malaysian Cyberspace

Malaysia has progressively worked on the initiatives for the protection of cyberspace in the country. NISER, for example, plays an important role in creating the awareness among the individual users and organisations, particularly Internet communities on ICT security matters. Together with other parties from various groups and industries including government and private sectors the following initiatives are created :-

i) The proposal of *National Infostructure Protection Agenda (NIPA)* is the outcome of a series of brainstorming sessions by the Panel of Experts (PoE), a group of experts in ICT Security established by NISER in 2001. The main objectives of NIPA are to address the nation information security issues, to develop capabilities in cyber security and to protect national e-sovereignty. Furthermore, it provides a set of recommendations based on the issues discussed. There are seven (7) initiatives in NIPA i.e. National Coordination Initiative, National Information Security Awareness & Competency Development, National Business Continuity Management, National Information Assurance, National Cyber Defence, Information Security Related Laws and Enforcement, and National Research & Development in Information Security. The implementation of the NIPA initiatives will bring up Malaysia in better position whilst securing the Critical National Infostructure (CNI) and Critical Infrastructure (CI) and protect the e-sovereignty of the nation.

ii) The development of a *National Information Security Policy Network* of which the key aspects of the framework's development is to look into these aspects; legislative & regulatory, institutional, technical, international and public-private cooperation. The proposal is under the review of the Ministry of Science, Technology and Innovation (MOSTI).

iii) Development of *Anti Spam Framework of Best Practices and Technical Guidelines* in which the objective is to recommend Anti-Spam Framework of Best Practices and Technical Guidelines. The working

group was established in July 2004 by NISER with the members are from various organisations such as government agencies, ISPs and Anti-Virus Solutions Providers, among others. The framework is expected to be the Malaysian version of best practices in handling Spam.

iv) Involvement in *Computer Emergency Response Team (CERT)* activities locally and internationally in which NISER has a global link with the Asia Pacific CERT (APCERT), European CERT and the US Continent CERT. MyCERT is also a member of Forum of Incident Response Security Team (FIRST), based in Carnegie Mellon University, USA.

v) Implementation of *Information Security Management System (ISMS)* pilot project, a programme that promotes ISMS Certification which is based on the British Standards Institute's (BSI) BS7799-2:2002. This programme is jointly conducted with SIRIM Berhad with the objective to enable local organisations to be certified with the Information Security Standard.

vi) *Information Security Awareness Programmes* that have been actively conducted by NISER which include ICT security training, ICT security surveys, and presentations/talks at local and international conferences and also local organisations.

vii) Working Groups in *Information Security Standard* where NISER is closely working with SIRIM in developing standards related to information security in Malaysia. NISER has been participating in the development of Information Security Standards developed by various standard bodies such as ISO/IEC (ISC'G/TC5/WG1). Other areas being participated are Security Evaluation Criteria (ISC'G'/TC5/WG3) and Business Continuity Management (ISC'G'/TC5/WG4).

viii) *Information Sharing Forum (ISF)* is being set up by the Malaysian Communications and Multimedia Commission (MCMC) in July 2004 in which NISER is one of the active members. The objectives of ISF are to bring together the relevant parties into a single forum to share their experiences and expertise for the benefit of the Malaysian network infrastructure; and to establish effective information sharing mechanism.

Conclusion

Cyber security is a national e-sovereignty challenge which needs to be approached in comprehensive manner. It cannot be done single handedly but requires partnership between all parties or users including public, private and other Internet communities. The culture of security should be the way of life while an integrated policy framework is needed to face the new wave of threats to information and technology. This also includes international cooperation to allow a global and coordinated approach for solving the common problems and transfer of know-how.

(ISC)2® PARTNERS WITH NISER TO OFFER INFORMATION SECURITY EDUCATION AND CERTIFICATION IN MALAYSIA

NISER supports (ISC)2 in declaring 2005 the 'Year of the Information Security Professional'

Kuala Lumpur, 12 January 2005 – The International Information Systems Security Certification Consortium, Inc. [(ISC)2]; the non-profit international leader dedicated to educating, qualifying and certifying information security professionals worldwide, today announced an agreement with the National ICT Security and Emergency Response Centre (NISER), Malaysia, to offer information security education and certification exams to candidates in Malaysia.

Lt Col Husin Jazri continued, "Heavily IT dependent organizations in Malaysia need highly qualified information security professionals to secure their IT environments. The country, however, is facing a lack of cyber training spaces that produce competent and certified information security professionals. NISER has taken a proactive approach to filling the gaps. NISER has extended its service by providing a platform for information security professionals to move one step further through certification."

As an affiliate of (ISC)2, NISER will play a major role in promoting and hosting the Certified Information Systems Security Professional (CISSP®) CBK® Review Seminars, based on a compendium of industry best practices and the CISSP certification examination. There are currently over 70 professionals in Malaysia holding (ISC)2 certifications. In June 2004, the CISSP was accredited as meeting the ANSI ISO/IEC 17024 standard for the certification of professionals, the only information technology credential to have this accreditation.

Lt Col Husin Jazri was also invited by (ISC)2 to become one of the members of its Asian Advisory Board. The volunteer advisory board advises the (ISC)2 executive management team on information security policies and trends and makes recommendations regarding professional certification programs offered to the information security workforce in Asia.

Why CISSP® Certification?

The CISSP Certification is an independent and objective measure of professional expertise and knowledge within the information security profession. In June 2004, the International Organization for Standardization's (ISO) United States representative, ANSI (American National Standards Institute), has granted certification accreditation in the area of information security under ISO/IEC 17024 for CISSP credential.

If you plan to build a career in information security- one of today's most visible professions - and if you have at least four full years of experience, then CISSP Certification should be your next career goal.

How CISSP® benefits you?

The CISSP® credential is a key differentiator in the selection process for information security positions, new assignments or promotions. When you achieve the CISSP® designation:

- You indicate you have measured up to a globally accepted professional and ethical standard.
- You have recognition and acceptance as a career professional.
- Your career opportunities are significantly enhanced.
- You have demonstrated knowledge of and competence in the 10 domains of the Information system security common body of knowledge (CBK).
- You possess an internationally recognized credential.

How CISSP® benefits your organization ?

Organizations staffed with CISSPs gain a competitive edge. Because the personnel protecting their data are the best in the business, these organizations demonstrate to customers, suppliers, and employees alike, the importance they place on security. Additionally, the CISSP® designation reflects a properly and consistently trained IT professional staff.

The Official (ISC)2 CISSP® CBK® Review Seminar
Most practitioners specialize in only one or two of the CBK domains, and typically have varying degrees of knowledge in the others. Knowledge of all 10 domains is required to pass the exam. For this reason (ISC)2® has developed this intensive, five-day review seminar that will broaden your understanding of all 10 domains and that will help you succeed on the CISSP exam.

The Seminar provides:
- extensive work from CISSPs, (ISC)2 Instructors and Subject Matter Experts in developing material and presentation;
- 100% revised, updated or new material;
- a practice exercise with 100 questions that are representative of the actual exam;
- a personal critique of your results to help you focus on the topics where you need more study;
- a comprehensive student guide that addresses all materials covered by the course.

The course material, covering the 10 CISSP domains of the CBK, is redesigned and updated for every Review Seminar to reflect the latest information system security issues, concerns, and countermeasures. The following domains are covered in the seminar modules.

- Security Management Practices
- Security Architecture and Models
- Access Control Systems and Methodology
- Application Development Security
- Operations Security
- Physical Security
- Cryptography
- Telecommunications, Network, and Internet Security
- Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
- Law, Investigations, and Ethics

For more information on CISSP, please visit our website at **http://www.niser.org.my/cissp** or call 603-86577042.

Upcoming ICT Security Related Events

1. The First Information Security Practice and Experience Conference (ISPEC 2005)
   Shangri-La's Rasa Sentosa Resort , Singapore, 11 - 14 April 2005

2. Cisco Security Summit 2005
   Sheraton Subang Jaya, Malaysia, 19 April 2005

3. DRI Asia 2005
   Suntec City, Singapore, 27 - 29 April 2005

4. IT GOVERNANCE 2005
   Sheraton Subang Jaya, Malaysia, 10 - 11 May 2005

5. SANS Security Bootcamp
   Melbourne, Australia, 27 June - 2 July 2005

6. SYMPOSIUM ON SECURITY AND ASIA NETWORKING 2005
   Singapore, 18 - 19 August 2005

7. The 8th Information Security Conference (ISC'05)
   Singapore, 20 - 23 September 2005

8. CardEx Asia 2005 & Smart Labels 2005
   PWTC, Kuala Lumpur, 17 - 19 May 2005

9. E-Security 2005 Expo & Forum
   Mines Resort City, Kuala Lumpur, 7 - 10 September 2005

10. The 4th International Workshop for Applied PKI (IWAP'05)
    Singapore, 23 September 2005

11. International Conference on Cryptology in Malaysia (Mycrypt 2005)
    PWTC, Kuala Lumpur, 28 September to 1 October 2005

12. E-Secure Malaysia 2005 Conference
    PWTC, Kuala Lumpur, 28 September to 1 October 2005

NISER 2005 TRAINING CALENDAR

MAY 2005

Date	Title	Venue	Price
03 – 04	Security Awareness	To be determined	RM 750.00

JUNE 2005

Date	Title	Venue	Price
06th	Business Continuity Planning (BCP) 100	To be determined	RM 850.00
07 – 08	Business Continuity Planning (BCP) 200	To be determined	RM 1,450.00
09 – 10	Business Continuity Planning (BCP) 300	To be determined	RM 1,450.00
21 – 22	Information Security Management System (ISMS)	To be determined	RM 750.00

JULY 2005

Date	Title	Venue	Price
12 – 14	Incident Response and Handling	To be determined	RM 1,070.00

AUGUST 2005

Date	Title	Venue	Price
09 – 10	Security Awareness	To be determined	RM 750.00

SEPTEMBER 2005

Date	Title	Venue	Price
05th	Business Continuity Planning (BCP) 100	To be determined	RM 850.00
06 – 07	Business Continuity Planning (BCP) 200	To be determined	RM 1,450.00
20 – 21	Information Security Management System (ISMS)	To be determined	RM 750.00

NOTE : For further details, please visit our website at :

http://www.niser.org.my/training.html

REPORTING INCIDENTS TO MyCERT

Tel	**:**	**60 3 8996 1901**
Fax	**:**	**60 3 8996 0827**
Via email	**:**	**mycert@mycert.org.my**
Via SMS	**:**	**019-2813801 (24x7)**
Via online	**:**	**http://www.mycert.org.my/report/form_report.html**

Join MyCERT's *mailing list* for updates and alerts.
Log on to the website to join this free service.

http://www.mycert.org.my

MyCERT
Malaysian Computer Emergency Response Team

NISER
National ICT Security and Emergency Response Centre