Protection against Hacking - Technique / Tools

A newsletter for IT Professionals

Issue 11

I. Background of Protection against Hacking

Introduction to Hacking

In order to protect the universities' information systems against malicious attacks, IT professionals should obtain a basic understanding of the common hacking methodology and learn to think from the perspective of a black-hat hacker.

Hacking Methodology

The hacking process can be summarised into the following five phases.

1 Information Gathering

This phase includes reconnaissance and footprinting. It is the preparatory phase to gather as much information as possible prior to an attack. In this phase, the attacker tries to find and exploit a loophole by identifying patterns of behavior of people or systems. Non-intrusive methods are used here to create a map of an organisation's network and systems.

- Target system
- Network architecture
- Application type
- Operating system and version
- Server type
- Physical location

2 Scanning and Enumeration

In the second phase of hacking, attackers identify target systems' IP addresses and determine whether a system is on the network and available.
This phase helps identify known security loopholes according to system and service version, and determines a user account or system account for potential use in hacking the target system. Most account privileges can then be escalated to allow the account with more access than it was previously granted.

Reference:
http://en.wikipedia.org/wiki/Hacker_(computer_security)
http://www.eccouncil.org/CEH.htm

I. Background of Hacking Protection (cont'd)

3 Gaining Access

In this phase, hackers exploit vulnerabilities exposed during the reconnaissance and scanning phase. They might gain access through different paths such as direct access to a personal computer, the local area network (LAN), or the Internet. Common examples of vulnerabilities include stack-based buffer overflows, denial of service and session hijacking, of which the main objective is to gain the ownership of the system. Once a system has been hacked, the hacker possesses the control and can use that system as they wish.

4 Maintaining Access

Hackers keep the access for future exploitation and attacks after gaining access. They may even harden the system and secure their exclusive access with backdoors, rootkits, and trojans to prevent other hackers. Once the hacker owns the system, they can use it as a base to launch additional attacks, in which the compromised system is also known as zombies.

5 Covering Tracks

After all attacks, hackers would remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms to protect themselves. Examples of activities during this phase of the attack include steganography, using a tunneling protocol and altering log files. The purpose is to avoid detection by security personnel to continue using the compromised system and remove evidence of hacking to avoid legal action.

Hacking Protection Techniques

In response to various hacking activities, the following are some recommended protection techniques that a university should use to lower the risk of exploitation by the black-hat hackers.

- **Security Infrastructure**

  One of the most common infrastructures for enforcing information security is the firewall, which aims at restricting the access of inbound and outbound traffic through configuration of rule sets.

  Stringent controls on physical access to the servers of a University system are not enough to protect the system itself. A lot of hacker's attacks come remotely from an external or internal network. Therefore a secure infrastructure is essential to lower the risk of remote attacks and better protect the University system.

- **Intrusion Detection System**

  Intrusion Detection System (IDS) protects a network by collecting information from a variety of systems and network sources, and then analysing the information for possible security problems. It provides real-time monitoring and analysis of user and system activity.

Reference:
http://en.wikipedia.org/wiki/Hacker_(computer_security)
http://www.eccouncil.org/CEH.htm

I. Background of Hacking Protection (cont'd)

In general, there are two types of IDS, namely Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS). Network Intrusion Detection System (NIDS) monitors multiple hosts by examining network traffic at the network boundaries. Host Intrusion Detection System (HIDS) can monitor one host by analysing application logs, file system modifications such as password file and access control lists. Here are some common examples of the functionalities of IDS:

- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching of known attacks
- Abnormal activity analysis
- Operating system audit

- **Code Review**

  For any self-developed applications such as web applications, an independent code review on the programs should be conducted separately from the application development in order to ensure no security flaw is revealed from the codes which are visible to the public, and correct error handling and input validation have been implemented in the code.

- **Security Patches**

  Many service providers, including software vendors and operating system providers, offer security patches when vulnerabilities of the software or the operating system were found. The installation of up-to-date security patches is very crucial since these vulnerabilities are usually well-known to the public, including the black-hat attackers.

Do Universities Need Hacking Protection?

Universities definitely need advanced protection against attacks, because they have a large pool of valuable data in their internal network. For instances, the research material and references of each faculty which contribute to the intellectual properties of the universities; the personal data being used in research and education; and sensitive information related to third party contractors.

Benefits that universities can obtain from appropriate hacking protection techniques include the following:

- Prevent leakage of sensitive data via hacking attacks
- Reduce cost of investigation and reputation damage / monetary loss
- Facilitate early risk detection and mitigation
- Increase trust from the senior management, staff , students, third party contractors and the public

Reference:
http://en.wikipedia.org/wiki/Intrusion_detection_system
http://www.eccouncil.org/CEH.htm

II. Risks of Hacking Protection in Universities

There are a number of risks universities should pay attention to when considering or implementing different hacking protection methodologies.

1 Excessive Reporting and False Positives

An improperly configured Intrusion Detection System (IDS) may generate significant number of false positives that overwhelm universities' IT security resources and obscure valid hits. Over-monitoring of data volume or keywords / data patterns can easily exhaust limited resources and result in delay or even interruption to service provision.

2 Improperly Configured Security Infrastructure

When a security infrastructure is not able to handle the amount of network traffic, due to either insufficient consideration of traffic volume during the design stage or increased network traffic over time, some network packets may be missed or dropped, allowing certain data to pass uninspected. It may render hacking protection ineffective when unauthorised transmission of sensitive data to external parties is ignored.

3 Conflicts with System Performance and Operations

Hacking protections, especially intrusion detection systems, can cause compatibility issues when conflicting with other systems and software. For example, some application software cannot run properly on encrypted hard drive. Applications errors or performance degradation are two common results of such conflicts. In worst case, the compatibility issues may cause the abnormal termination of other security controls and expose universities' information system to even great risks.

4 Over Protection against Hacking

Universities must pay extra attention to strike a balance between risk of exploitation and operational level. Otherwise, inadequately tuned security infrastructure may cause disruption of universities' operation, waste of staff or students' time, damage to relationship with external parties such as contractors and the public. E.g. blocking employees sending sensitive data to authorised external parties; disrupting normal e-mail services used by universities.

Reference:
JUCC IT newsletter Issue #5 – Data Leakage Protection
http://www.eccouncil.org/CEH.htm

III. Vulnerabilities of Hacking Protection

Common Types of Attacks

- **Vulnerability scanning**

  Hacker may initiate vulnerability scanning on target organisation's network to proactively identify the vulnerabilities of computer systems on a network. Hacker may obtain the operating system and version number, including service packs that may be installed, and identifies weaknesses or vulnerabilities in the operating system, on which certain hacking protection technologies are deployed.

- **Password cracking**

  Hacker may attempt to get password of an authorised user to gain access to the system with the username and password with authentication, which may render the hacking protections ineffective.

- **Trojans and backdoors**

  Trojans may sometimes be hidden in a software package of another program. Victims download the software package and install trojans onto their computer without notice. Once installed, trojans can run malicious programs on victim's computer, such as running commands remotely, intercepting keystrokes and so on. Backdoors created by Trojans also give hackers subsequent access to victims' computers.

- **Viruses and worms**

  The malicious codes from the hacker can be spread to victim's computer by a carrier programs, either via the form of viruses or worms. A virus code is infected on another normal program to spread itself. A worm is able to self-replicate and move from an infected computer to another victim's computer through network connection. If the hacking protection mechanisms are infected by viruses and worms, their abilities to defend against malicious attacks can be seriously impaired.

Recent Incident

HKEx Website Hacked

Trading in Hong Kong was disrupted on 10 August 2011 by a hacking incident on the Hong Kong Exchange website.

Shares of eight-listed companies were suspended from trade, including those of bourse operator Hong Kong Exchanges and Clearing, flag-carrier Cathay Pacific and banking giant HSBC.

Hong Kong Exchanges & Clearing CEO Charles Li said: "Our current assessment (is) that this is the result of a malicious attack by outside hacking.

See the article:
(http://www.channelnewsasia.com/stories/marketnews/view/1146230/1/.html)

III. Vulnerabilities of Hacking Protection (cont'd)

- **Denial of Service**

  Denial of service (DoS) is initiated by hackers to prevent legitimate users of a system from using it by different methods, such as flooding a network with traffic and preventing a particular individual from accessing a service. If a denial of service attack is posed upon an intrusion detection system, it is possible that the intrusion detection system is suspended and further exploitations can be generated against the Universities' network.

- **Inadequate Code Review**

  Inadequate Code Reviews performed for application can result in system vulnerabilities and allow various malicious attack attempts successfully made by hackers.

  Buffer overflow -- Hacker may send exceeding amount of information to a field variable in an application in order to cause an application error. The improper error handling of the application as the result of in adequate code reviews may lead to the execution of malicious commands after buffer overflow attack.

  SQL injection -- SQL injection is dangerous to any database server behind a web application if there are insufficient input validation mechanisms in place. Hacker may be able to dump, alter, delete or create information in a database by inserting deliberated SQL commands into the input.

  Cross-site scripting -- Web forms in the web pages of a web application may have a higher risk of being exploited by cross-site scripting (XSS) threat if malicious command entered into the web form is processed by the web application without being detected by its security function.

Relevant Material

Open Source Vulnerability Database (OSVDB)

Founded in August 2002 at the Black Hat and Defcon conferences, OSVDB was created to provide an independent and Open Source Vulnerability Database. The goal was to provide accurate, detailed, current and unbiased technical information about all types of vulnerabilities.

The project will promote greater, more open collaboration between companies and individuals, eliminate redundant works, and reduce expenses inherent with the development and maintenance of in-house vulnerability databases

See the article: (http://osvdb.org)

Reference:
http://www.eccouncil.org/CEH.htm
http://osvdb.org

IV. Hardening Steps for Hacking Protection

Hardening steps specific to each hacking category should be considered when planning the protection of the universities' systems against hacking.

Hardening Steps against Scanning and Enumeration

- **Firewall –** universities should examine the data of the packet, not just the TCP header, to carry out stateful inspections to detect the connection initiation traffic sent by port-scanning tools.

- **Open Required Ports Only –** universities should only open the ports required by service on their systems. The rest ports should be filtered or blocked. The TCP ports 135, 137,139, or 445 which are required for NetBIOS null session access should be closed to prevent null session attacks.

Hardening Steps against System Hacking

- **Two-Factor Authentication** – it is a good practice to require two (or more) forms of identification (such as the actual smart card and a password) when validating a user. An example of such authentication method is RSA Secure ID, which utilises a user defined password combined with the temporary password generated by a security token. However, universities should keep regular communication with the vendor of two-factor authentication mechanisms to timely patch the authentication systems with latest updates in response to any known vulnerabilities (e.g. attack on RSA using zero-day flash exploit in Excel)

- **Reinstall Operating System –** when you detect a trojan or backdoor program. Critical data should be backed up and the operating system and applications from a trusted source can be reinstalled afterwards. A well-documented automated installation procedure and trusted restoration media should be implemented in the University.

- **MD5 Checksum Utility –** is a 128-bit value, like the file's fingerprint, ensuring their integrity. Tools, such as Tripwire, implement MD5 checksums to identify files infected with malicious programs.

Hardening Steps against Web Application Attacks

- **Default Accounts** - rename the administrator account, and use a strong password.

- **Boundary Check** - perform bounds checking on input to web forms and query strings to prevent buffer overflow or malicious input attacks.

- **Remote Access** - disable remote administration functionalities.

- **Error Handling** - use a script to map unused file extensions to a 404 ("File not found") error message.

- **Legal Notice** - add a legal notice to the site to make potential attackers aware of the implications of hacking the site.

Reference:
http://www.eccouncil.org/CEH.htm
http://news.cnet.com/8301-27080_3-20051071-245.html

V. Summary

Recently, hacker communities from all over the world have been actively attacking different organisations including governmental or commercial entities. E.g. attacks on PlayStation Network (PSN), FBI, CIA and US Senate's high security networks by "Lulz". Universities as a role model to society could easily become a target of the hackers. Therefore, technical knowledge of the hacking methodology, application of adequate protection techniques, and awareness of security trends are increasingly important to provide confidence to the users and the owners of the systems and data maintained by universities.

Techniques used for protection against hacking activities can be powerful once they are properly implemented and used by personnel with sufficient knowledge of hacking. Universities should pay close attention to the appropriateness of the security measures and resources in place for protecting against hacking activities to avoid any adverse impact on achieving information security objectives.