­­­­­­­­­­­

UHMT1012 – GRADUATE SUCCESS ATTRIBUTES

ASSIGNMENT 3

(ACADEMIC REPORT)

SECTION : 43 - COMPUTER NETWORK AND SECURITY

GROUP : 01

SUB GROUP MEMBER :

|  |  |  |
| --- | --- | --- |
| NO. | NAME | STUDENT ID |
| 1 | CHA ZHI YE | A20EC0022 |
| 2 | LEE WAN FU | A20EC0066 |

LECTURER’S NAME : DR. NORHAIDA BTE MOHD SUAB

**ABSTRACT**

In the last decade, the progress of internet technologies has led to a significant increase in security and privacy issues for users. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. Factors affecting the safety of network is complex, for to do a good job of network security is a systematic work, has the high challenge. In this paper, we are trying to study and explores important security measures related to different network scenarios, so that a fully secured network environment could be established among the masses of users in computer networks.

**KEYWORDS**

Network Security; Security Attacks; Hackers; Cryptography; Strategies; Principle.

**INTRODUCTION**

Nowadays, the application of computer network has extended to every corner of the world and areas, is an unprecedented impact on people's work and life, as well as electric power, transportation, and has increasingly become an integral part of people's life. A home or small office may only require basic security while large businesses may require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. For years, IT professionals have built barriers to prevent any unauthorized entry that could compromise the organization’s network. Computer network security has become a global concern. Computer network and information security technology is the core issue of the computer and network systems for effective protection. Network security protection involves very wide range, from a technical level, mainly including data encryption, identity authentication, intrusion detection and intrusion protection, virus protection and virtual private networks (VPN). Computer network security by adopting various

technical and management measures, make the normal operation of the network system, to ensure the availability, integrity and privacy of network data. So, to establish the purpose of network security protection is to ensure that the data transmission and exchange through the network, not happen such as add, modify, loss and leak.

**TYPES OF ATTACKS**

Networks are subject to attacks from malicious sources. And with the advent and increasing use of internet attach is most commonly growing on increasing. A system must be able to limit damage and recover rapidly when attacks occur. There are some more types of attack that are also essential to be considered:

1. Passive Attack

This type of attack includes attempts to break the system by using observed data. One of the example of the passive attack is plain text attacks, where both plain text and cipher text are already known to the attacker. The attributes of passive attacks are as follows:

1. Interception: attacks confidentiality such as eavesdropping, “man-in-the-middle” attacks.
2. Traffic Analysis: attacks confidentiality, or anonymity. It can include trace back on a network, CRT radiation
3. Active Attack

This type of attack requires the attacker to send data to one or both of the parties, or block the data stream in one or both directions. The attributes of active attacks are as follows:

1. Interruption: attacks availability such as denial-of-service attacks.
2. Modification: attacks integrity.
3. Fabrication: attacks authenticity.
4. Distributed Attack

This type of attack requires the adversary introduce code, such as a Trojan horse or back-door program, to a “trusted” component or software that will later be distributed to many other companies and users. Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

1. Insider Attack

This type of attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access. It can affect all computer security elements and range from stealing sensitive data to injecting Trojan viruses in a system or network. Insiders also may affect system availability by overloading computer/network storage or processing capacity, leading to system crashes.

1. Close-in Attack

This type of attack requires attacker physically close to the target system. It consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. One popular form of close in attack is social engineering. In a social engineering attack, the attacker compromises the network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

1. Spyware Attack

This type of attack is a serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. And this capture information is maliciously used as the legitimate user for that particular kind of work.

1. Phishing Attack

This type of attack requires the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information,

the hacker records the username and password and then tries that information on the real site.

1. Hijack Attack

This type of attack requires the hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accidently.

1. Spoof Attack

This type of attack requires the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

1. Password Attack

This type of attack requires the attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks:

1. Dictionary attack: uses a word list file, which is a list of potential passwords.
2. Brute-force attack: tries every possible combination of characters.
3. Hybrid attack.

1. Exploit Attack

This type of attack requires the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.

1. Buffer Overflow

This type of attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

**THE APPLICATION OF THE STRATEGY FOR NETWORK SECURITY**

**TECHNOLOGY**

Security is the security of the network to survive, only safe and secure, network can realize its own value. The development of network security technology as people network practice and development, it involves technical is very wide, the main techniques such as authentication, encryption, firewall and intrusion detection is an important defense of network security.

1. VPN

VPN is the latest to solve the problem of information security, one of the most successful technology subject, a virtual private network (VPN) technology is on the public network to establish dedicated network, make the data through the security of encryption "pipe" in the public network. To build on the public communication network VPN there are two kinds of mainstream mechanism, these two mechanisms for routing filtration technology and tunnel technology. The current VPN mainly adopts the following four technology to ensure safe: tunnel technology, encryption technology, key management technology and user identity authentication technology and equipment. Among them, several popular techniques for the PPTP, L2TP tunnel and IPsec VPN tunnel mechanism should be able to have different levels of technology security services, the security services including different intensity of source identification, data encryption, etc. VPN have several classification methods, such as the access into the shuttle VPN and dial-up VPN; According to the tunnel protocol can be divided into the second and third layer; According to a way can be divided into sponsored by the client and the server.

1. Firewall

Firewalls are important means to ensure network security, network management applications though the use of technology, packet filtering technology and agent technology, effectively control network access permissions, comprehensive data to external restrictions and discrimination. Meanwhile, the firewall can make the internal network structure concealed, the external network to the internal network access to be limited in order to ensure the security of the internal network. In short, the firewall plays separated, analysis and its restricted hole.

1. Driving Security to the Hardware Level

To further optimize performance and increase security, Intel develop platforms also include several complementary security technologies built into multiple platform components, including the processor, chipset, and network interface controllers (NICs). These technologies provide low-level building blocks upon which a secure and high performing network infrastructure can be sustained. These technologies include Virtualization Technology, Trusted Execution Technology and Quick Assist Technology.

1. Intrusion Detection System

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. The typical antivirus software product is an example of an intrusion detection system. The systems used to detect bad things happening are referred to generically as intrusion detection systems. Intrusion detection in corporate and government networks is a fast-growing field of security research; this growth has been prompted by the realization that many systems make no effective use of log and audit data.

1. Data Encryption

Information technology is the key encryption technology to achieve information security, help strengthen security, through a particular encryption algorithm translated the important plaintext ciphertext, so unauthorized users can not directly read the raw data, even if the data file is lost or stolen, as long as difficult to crack the key, so it will not lead to the leakage of confidential information, which greatly ensure information security.

1. Authentication

Authentication should include at least verification protocol and license agreement. A variety of network applications and computer systems are needed to confirm the legality through authentication, and then determine its personal data and specific permissions. For authentication system, the legitimate user’s identity is easy to be someone else pretending to be its most important technical indicators. User being impersonated user may not only damage their own interests, but also may harm the interests of other users or the entire system. Therefore, authentication is the basis of authorization control. Only valid identity authentication, to ensure the effective implementation of access control, security audit, intrusion prevention and other security mechanisms.

1. Access Control

Security policy and security model based on access control body set access permissions, such as to the identity of the user, password authentication, in order to gain the true identity of the user, to facilitate tracing network behavior. Combined with network licensing, issuing access permits the use of effective passwords and other means to prevent unauthorized users on the network information resources maliciously modified or used. Care must be take to select a password which enhance the security of the password strength and change them regularly to ensure information security.

1. Dynamic Endpoint Modeling

Observable's security solution, represents a profoundly new way to look at IT security. It models each device on your network, so you can understand normal behavior and quickly take action when a device starts acting abnormally. There's no need to install agents on the devices, or attempt to use deep-packet inspection, giving you a powerful solution to overcome these new security challenges.

1. Mobile Biometrics

Biometrics on mobile devices will play a bigger role in authenticating users to network services, one security executive predicted. Biometrics emerging on mobile endpoints, either as applications that gather users’ behaviors or as dedicated features on mobile endpoints that scan personal features. For example, the iPhone 5s finger scan, will emerge in 2014, if these features are open and extensible, it could lead to real innovation in ensuring the identities of remote users.

**CONCLUSION**

Computer network security has become an important issues of network development at this stage. To ensure the network information security, we must comprehensive use of various protection strategy, integrating the advantages, cooperate with each other. Not just simply using a certain protective measures because it is no guarantee that the network information security. The key for building a secure network is to define what security means to your need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. There are different kinds of attacks on the security policies and also growing with the advancement and the growing use of internet. Therefore, we must depart from security threats through the use of advanced security technology and software technology to effectively monitor potential threats and timely warning to prevent malicious behavior. Network security work, is still a need in daily work point guard and will largely reduce network security hidden danger, to protect the normal use of the network.

**ACKNOWLEDGMENT**

We would like to express our special thanks of gratitude to our lecturer Dr. Norhaida Bte Mohd Suab who gave us the golden opportunity to do this wonderful project on the topic Computer Network and Security, which also helped us in doing a lot of classes and we came to know about so many new things. Secondly, we would also like to thank our parents and friends who helped us a lot in finishing this project within the limited time. We are making this project not only for marks but to also increase our knowledge.

**REFERENCES**

1. A beginner’s guide to network security, CISCO Systems [Online] available: <http://www.cisco.com/warp/public/cc/so/neso/sqso/ beggu_pl.pdf>
2. Importance of Network Security [Online] available: <http://www.content4reprint.com/computers/security/importance-of-network-security-system.html>
3. Predictions and Trends for Information, Computer and Network Security [Online] available:<http://www.sans.edu/research/security-laboratory/article/2140>
4. Network Security Types of attacks [Online] available: <http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html>
5. Securing the Intelligent Network [Online] available: <http://www.trendmicro.co.in/cloud-content/us/pdfs/security-intelligence/white-papers/wp_idc_network-overwatch-layer_threat-mngmt.pdf>
6. Network security needs big data [Online] available: <http://www.computerworld.com/article/2851517/network-security-needs-big-data.html>
7. CLOUD SECURITY ALLIANCE Big Data Analytics for Security Intelligence [Online] available: <https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf>