Network Security

Megha Verma **;** Palak Sharma ; Neha Sundriyal ; Jyoti Chauhan
III Semester, Department of Computer Science & Engineering Dronacharya College of Engineering, Gurgaon-123506, India
Email Id: megha.16093@ggnindia.dronacharya.info;
Email Id: palak.16109@ggnindia.dronacharya.info
Email Id: neha.16101@ggnindia.dronacharya.info
Email Id: jyoti.16078@ggnindia.dronacharya.info

ABSTACT :
Android is Linux based mobile OS which is being used by popular smart phone brand like Samsung ,LG ,HTC ,Sony Xperia and many other. Kitkat OS is 4.4 version of this android which was released on October 31, 2013 .This paper will contain detailed study of Android 4.4: Kitkat OS, pros and cons of kitkat. It will cover step wise development of android OS up to kitkat. Contrast of kitkat from old android OS, IOS and Windows phone OS, details review of technical background of kitkat OS.

Keywords-

Kitkat; Android 4.4; smart phone

I.INTRODUCTION

Network Security is the process of taking physical and software preventative measures to protect the networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

II.Why is network security needed?

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies. The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites;

a closed network does not allow a connection to public networks. Because they have no Internet connectivity, networks designed in this way can be considered safe from Internet attacks. However, internal threats still exist.

Also, many threats today are spread ove the internet and the most commom ones include:

- Viruses, worms, and Torjan horses
- Spyware and Adware
- Zero-day attacks or the zero-hour attacks
- Hacker attacks
- Denial of services attack
- Data interception and theft

With the development of large open networks, security threats have increased significantly in the past 20 years. Hackers have discovered more network vulnerabilities, and because you can now download applications that require little or no hacking knowledge to implement, applications intended for troubleshooting and maintaining and optimizing networks can, in the wrong hands, be used maliciously and pose severe threats.

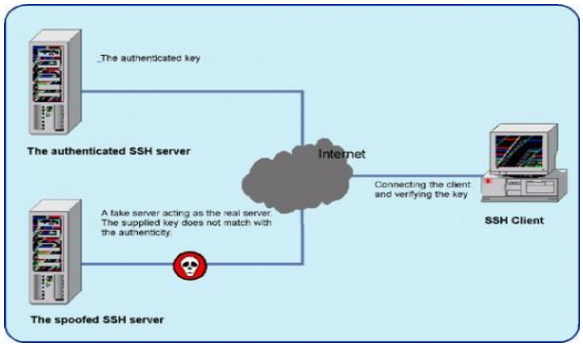
III.Types of Attacks

Types of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. There are five types of attack :

1. Spoofing
2. Sniffing Attack
3. Mapping (Eavesdropping)
4. Hijacking (Man in the middle attack)
5. Torjan Attack

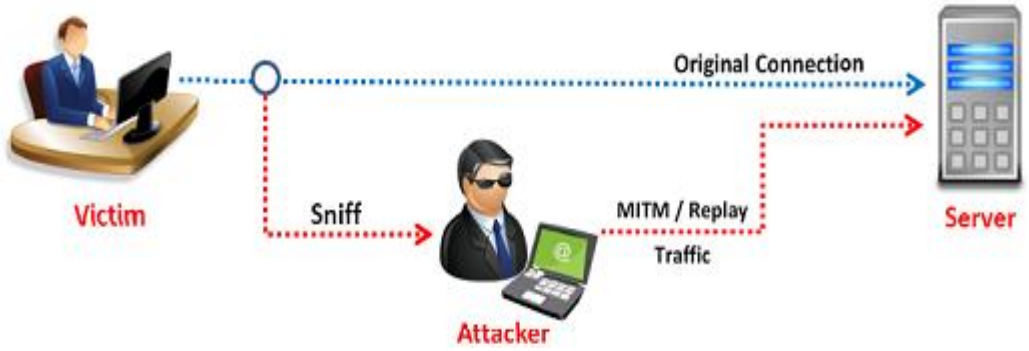
1. Spoofing (Identity spoofing or IP Address Spoofing)-

Any internet connected device necessarily sends IP datagrams into the network. Such internet data packets carry the sender's IP address as well as application-layer data. If the attacker obtains control over the software running on a network device, they can then easily modify the device's protocols to place an arbitrary IP address into the data packet's source address field. This is known as IP spoofing, which makes any payload appear to come from any source. TYhe countermeasure for spoofing is ingress filtering. Routers usually perform this to check the IP address of incoming datagrams and determine whether the source addresses that are known to be reachable via that interface. If the source address is not in the valid range, then such packets will be discarded.



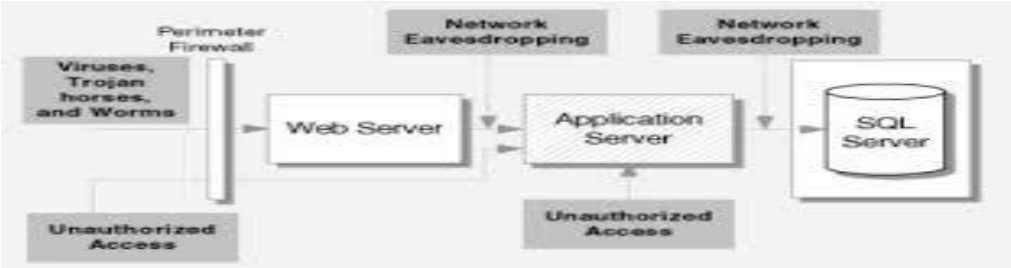
2. Sniffing Attack-

Packet sniffing is a form of wire-tap applied to computer networks instead of phone networks. It came into vogue with Ethernet, which is known as a "shared medium" network. This means that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus see everyones traffic



3. Mapping (Eavesdropping)-

Before attacking a network, attackers would like to know the IP address of machines on the network, the operating systems they use, and the services that they offer. With this information, their attacks can be more focused and are less likely to cause alarm. The process of gathering this information is known as mapping.
In general, the majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise.



4. Hijacking (Man-in-the-middle attack-

A technique used to gain unauthorized access to computers, whereby the intruder sends a message to the computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniqueses to find an IP address of a trusted host and then change the packet headers so that it appears that the packets are coming from that host. Newer routers and firewall arrangements can offer protection against IP spoofing. Man-in-middle attacks are like someone assuming your identity in order to read your message. The other person might belive its you to keep the exchange going on and also to gain more information.vh7

5. **Torjan Attack-**

Torjan horse attacks pose one of the most serious threats to computer security. If you were referred here you may have not onlt been attacked but mayalso be attacking others unknowingly. These are programs that look like ordinary software, but actually perform unintended or malicious actions behind the scenes when launched. Most remote control spyware programs are of this type. The number of trojan techniques are only limited by the attacker's imagination. A torjanizes file will look, operate, and appear to be the same size as the compromised system file. One only protection is early use of a *cryptographic checksum* or *binary digital signature* procedure.

IV. IMPORTANCE OF NETWORK SECURITY

The purpose of network security is essentially to prevent loss, through misuse of data. There are a number of potential pitfalls that may arise if network security is not implemented properly. Some of these are: High image clarity, large detector Portable lightweight and fast.

1. Breaches of confidentiality: Each business will identify with the need to keep certain critical information private from competitor eyes.
2. Data destruction: Data is a very valuable commodity for individuals and enterprises alike. It is a testament to its importance when the proliferation of backup technology available today is considered. Destruction of data can severely cripple the victim concerned.
3. Data manipulation: A system break-in may be easily detectable, as some hackers tend to leave tokens of their accomplishment. However, data manipulation is a more insidious threat than that. Data values can be changed and, while that may not seem to be a serious concern, the significance becomes immediately apparent when financial information is in question.

V. CONCLUSION

Hence we can conclude that network security is very essential in a network to prevent loss or misuse of data. There are various kind of network security attacks which include: Spoofing, Sniffing Attack, Mapping (Eavesdropping), Hijacking (Man in the middle attack) and Torjan Attacks. The best approach to implement good network security is to be prepared of the attcks before hand. It can be done in four steps: Ensuring components are well guarded, constant monitoring network activity, assessing the vulnerabilities of network security policies and also enhancing on the basis of collection of data and using it for better safeguards building. It is important to keep in mind that a constant review and maintenance is required for a good network security stratergy.

VI .REFERENCES

1. Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network security: private communication in a public world*. Prentice Hall Press.

2. William, S., & Stallings, W. (2006). *Cryptography and Network Security, 4/E*. Pearson Education India.

3. Stallings, W. (1995). *Network and internetwork security: principles and practice* (Vol. 1). Upper Saddle River, NJ: Prentice Hall.

4. Forouzan, B. A. (2007). *Cryptography & Network Security*. McGraw-Hill, Inc..

5. Heberlein, L. T., Dias, G. V., Levitt, K. N., Mukherjee, B., Wood, J., & Wolber, D. (1990, May). A network security monitor. In *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on* (pp. 296-304). IEEE.

6. Carman, D. W., Kruus, P. S., & Matt, B. J. (2000). Constraints and approaches for distributed sensor network security (final). *DARPA Project report,(Cryptographic Technologies Group, Trusted Information System, NAI Labs)*, *1*, 1.