There are basically two major types of this destructive category reports example

Law, Security

- Introduction:

Network security forms the basis of safe and private data management in modern computer networks. Network security is the elementary problem of today’s computer and communication networks in the presence of vast variety of spams, viruses and internet threats. Network security provides the solution to such problems of privacy violation and unauthorized access to personal and confidential data by implementing the laws and rules which reduce security violation significantly. Network security evolution is a continuous process which has evolved since the invention of first virus and it will keep on evolving as new types of viruses are developed and discovered. This report will explain briefly about network security, its protocols and standards. Network security architecture is also explained in brief words. This research work will help in understanding the concepts and working of network security in short time. At the end of report, few questions are given in order to test the knowledge obtained in this report.

- Network Security:

Network security is set of rules and regulations adapted by the network administrator in order to observe and restrict unauthorized access, modify, misuse of the network resources. It also include the authorization of access to data for some particular users. It is solely done by the network administrator. Most common practice is to assign an ID with a unique username and password through which a user can access to data and software. Effective network security protects the integrity, usability and privacy of the network and data. Networks can be public or private depending upon the requirement of the job. For example a network within a

company should be private while on the other hand some networks may allow the public access as well.

1. 1 Network security concepts:

First step regarding network security is the “ authentication”. As discussed earlier, most common method through which is the username and password. It is sometimes called “ one-factor authentication” since it requires only one field to authenticate the username i. e. “ password”. With “ two-factor” authentication the user may require the usage of some personal device like mobile, Usb dongle, or an ATM card. Three-factor authentication is something the user “ is”, for example it may require the fingerprint swap or retinal scan. As soon as the authentication is done, “ Firewall” comes into action and enforces the policies, for example, which services are allowed be accessed for this particular user. Although firewall is effective but it sometimes lag in preventing the flow of the harmful contents like Trojans and computer worms on the network. For this purpose Antivirus software (AV) and Intrusion prevention system (IPS) are used that tackles above mentioned malware. Also “ encryption” could be used in order to maintain privacy in the communication between 2 users. Honeypots, for example “ decoys” are often deployed in the network for observation and as an early-warning tools. Attackers are distracted from the legitimate servers through the use of these honeypots. Honeypots divert the attacker and urge the attacker to spend time on the decoy server while the actual data is kept safe on the real server. Just like a honey pot, “ honeynet” is also deployed. Its purpose is to invite the attacker and study their method of attack. This information can be really helpful in order to increase the network security.

Typically, a honeynet contains more than one honeypots. Virtual private networks (VPNs) is also an option for providing secure remote access to users.

No single solution fits for all the possible problems or threats. Multiple layers of security are required as a backup so that if one fails the other stands. All this can be accomplished through both software and hardware. Software should be updated and managed on regular intervals n order to protect from potentially emerging threats. All the above mentioned components like antivirus, anti-spyware, firewall, and VPNs ideally work together which results in minimized maintenance and improved security.

- Types of Network Security:

In this era of fast growing technology, networks are growing rapidly to fulfill the growing demands. Every single person is linked with networks in one or the other way. They are connected to wired or wireless networks. For these growing demands the security has been a major concern in networks to secure data, as every user wants to secure the data and are reluctant to use services of any ISP if the network is not secure enough. In recent years there is some serious developments in network security domain.

The broadcast nature of wireless networks poses some serious concerns over security, confidentiality and reliability. There are also some issue of broadcast storms and coding attacks generated by a malicious user resulting in chocking of network resources and denial of service. Similarly in cooperative domain the serious concerns may be raised over the authenticity of the relaying node. A malicious user may portray as a relay by broadcasting fake information resulting in changes in the routing table.

There are some algorithms that run on the Application level that guarantee end to end reliability and security. These algorithms include “ symmetric” and “ asymmetric” cryptographic systems. Assuming the nodes in the network have no restraint on computational power than these algorithms will work perfectly. Public or private key cryptography may be employed as per need to achieve our goals. However, in networks where we have nodes that are very limited in terms of processing power, we cannot run such computation intensive algorithms. Private Key cryptographic systems such as AES, DES of RC4 are very complex algorithms which cannot be run on such nodes. Similarly, private key cryptography also makes the use to a shared key between the communicating nodes which is also not considered to be a standard practice. However, on the other hand public key cryptographic systems use two keys, public and private, and are considered more secure.

“ Data encapsulation scheme” is a hybrid scheme in which if user A wants to send data to User B, it will obtain User B’s public key and generate a special private key from it. Using this special private key it will encrypt the data. Than User A will encrypt this special private key with User B’s public key and send both the encrypted pairs on the channel. On the recipient side, User B will use its own private key to de- crypt the Special Private Key, and then use this special key to decrypt the data. Here it will be impossible to derive the private key from the published public key and requires no initial key exchange mechanism as for symmetric cryptosystems.

- Common Issues of Network Security:

We have covered the enough background regarding network security. Now

we will move forward and list down some common known issues that are faced and need to be tackled as a network administrator.

3. 1Denial of Service:

Denial of service (DOS) is one of the toughest issue faced by the network to be address to. The reason behind being toughest is they are the easiest to launch, most of the time impossible to track, and request of the attacker can never be denied.

The logic behind DOC is simple; send requests to the machine more than it can handle. Attacker creates a connection just like all other users through a port. After all the connection creation formalities are done the malicious user starts sending the data requests by forging the header information and instantly drops the connection. Server or the main entity of the network goes into busy state. Malicious user creates another connection and sends request again. For example, if the server has the capacity of 20 connections at a time, the legitimate users will be denied of the services because the server is already busy facilitating the malicious connections. These attacks were quite common in 1996 to 1997 but now their popularity is decreasing. Following steps can be taken to reduce these attacks,

- Don’t run your visible-to-world servers closely to the capacity.
- Use filters to avoid fraudulent packets to enter into your network space
- Keep your security products up to date with latest patches and versions.

3. 2Unauthorized Access:

Term “ unauthorized access” is in fact a high level term and can refer to different number and types of attack. Main purpose of these attacks are to gain access to such resources that should not be provided to person without

permission. For example, a host can be a web server and it provides access to requested webpages. However it should not allow access to the command shell access without authenticating the user and his rights or privileges such as local administrator.

3. 3Executing Command Illicitly:

It is always objectionable that someone untrusted executes a command on your server machines. There are two basic types of the severity of this issue; Normal user access, in which the attackers just want the privileges of a common user like reading, copying, emailing the data. While in Administrator access the attacker wants to make configuration changes in the host domain as per his own desire that might include changing IP address or changing start-up script.

3. 4Confidentiality breaches:

This issue basically examines the threat model: “ what actually is the threat you are protecting yourself from”. There might be some information that could be destructive if it fell into hands of any competitor or enemy. In this case, compromise of a normal user’s account on a machine could be enough to cause the damage.

3. 5Destructive behavior:

- Data Diddling

This could be the worst type among this category because the attack is not immediately obvious. The attacker could be playing with numbers in the spread sheets or with the dates in your database records. He could be changing the account numbers of the auto-deposit bank checks. Once you find out any such problems you might need to start an auditory process but

the doubts will still be there regarding the numbers from that machine can how longer be trusted or how much far back you need to analyze the data for any potential changes done by the attacker.

- Data Destruction

Sometimes the attackers are simply psychopaths who just like to delete the stuff. Without any precautionary measure the damage done by such attack could be no less then destroying all the machines and databases as a result of accidental fire that destroys all the computing equipment.

- Network Security Architecture:

- Network Security Solutions:

- Network Security Protocols:

- Conclusion:

Network security is the key issue of modern networks and it is very important to resolve the issues of security in these networks in order to sustain privacy of confidential data. A large number of thefts are done through cybercrime today which can be reduced by implementing appropriate security protocols. This document briefly explains the problems and possible solutions to these problems in the form of network security protocols. Network security architecture is also explained in order to understand the workflow of network security issues. This report provides a brief explanation of basic concepts and issue of network security.

- Questions:

References: