There an advantage of using packet filtering

There are lots of detection system for networking in order to reduce the amount of threats and let the network run at full power. FirewallsFirewalls are intended to keep unauthorised access to a network or a computer.

You can enforce firewall in both software and hardware or even a combination of both. A firewall will monitor data packets coming in and out of the network it is protecting and will enforce the company's network security policy. It filters out the packets that look suspicious and do not meet the required security criteria. Many organisations use firewalls to keep their network safe from the internet. There are different types of firewall these are: Packet Filtering Firewall – This is one of the first firewalls to be created, it is a packet filtering firewall that will control what data can flow into and out of a network.

It is capable of rejecting or accepting data packets on a set user-defined rules known as ACLs. ACL's are lines of text, which will apply to each packet of data it receives, these lines of text give certain information to define what packet is acceptable and what packet is unacceptable. An advantage of using packet filtering firewalls are that it is flexible, anyone is able to customise the firewalls and enable it to operate with lots of distinct protocols and applications. Another advantage is that packet filtering firewalls aren't application-dependant and they and work at high speed as they don't have to execute extensive processing on the data packets. But with the advantages there are always a few disadvantages, and these are the fact that packet filtering firewalls are susceptible to security breaches due to the small amount of variables that is used in access control decisions, this is caused by an improper configuration.

Data filtering packet is also not able to prevent attacks that employ application-specific vulnerabilities. Stateful Inspection Packet Filtering Firewall – Stateful filtering tracks each connection that travels across the network. It’s initially intended to decline data packets that came from an untrustworthy source. Only packets that come from a known and trusted connection will be enabled to pass through the firewall.

The firewall will keep a state table (diary) of whoever was communicating and what they were doing. Thi can be very useful for when a problem happens within the network, since the firewall will be able to track the main source of the problem. Stateful Inspection Packet Filtering firewall can perform the same functions of a Packet Filtering Firewall. The advantage of this firewall is that it provides a security of a high level and it is scalable and transparent to users, furthermore it has the capability to track every communication channel, however it may need an expensive hardware for analysing the amount of data going through the system. Proxy Firewall – proxy firewalls is a highly secure protocol, but it also comes with the expense of speed and functionality. These firewalls are so secure because the data packets do not proxy, but instead the proxy acts as a mirror and creates a new network connection based on the request, which is unlike other firewalls. This can prevent direct connections, therefore it will be difficult for any attackers to discover the location of the network. When the proxy firewall receives the request, it looks it over for and suspicious information beforehand.

One of the advantages of using proxy firewalls is that it is the most secure firewall you can get, as they look at the information in the data packets up to

the application layer and break the connection between trusted and untrusted systems. But the disadvantage is the fact that proxy firewalls only supports limited amount of applications, they degrade traffic performance and slow the network down and the breaking of the connections that are untrusted could be bad. HoneyPotHoneyPot is a system where a computer or server is set up in the screened subnet or demilitarised zone in with the aim of luring attackers to the fake system other than the real production computer.

In order for the server to be attractive to the attackers the organisation would leave some ports open that are popular to attack. In order to make the HoneyPot look more believable then it’ll will need some security software, the software is easy to get through but it will still ensure the attacker that they have found right server. When an attacker tries to gain access to the fake server the organisation is able to view the situation and watching the attackers moves, so that they can make sure that an attack like the previous one will not happen again in the future by improving the overall security and preventing attacks to the real server.

A few administrators might even utilise detailed logs to obtain the attackers real identity and information to either attack back or to let the police know about the attack. HoneyPots are created in two different ways, one of them, known as the Actual Service HoneyPot is the more efficient method of creating HoneyPot, as they are actual computers and servers contain the required systems of the legitimate server but using counterfeit information, but this method can be very expensive to set up and buy the additional servers in order to protect the actual server. The less effective method is

called the Software Services HoneyPot, which can only trick the novice attackers.

This method is less expensive and can be useful for home networks or small business networks. Intrusion Detection System (IDS)IDS is used for detecting unauthorised entries and warn the administrator to act in response. IDS examines every outbound and inbound network activity and diagnose any mistrustful patterns which could prove to be somebody attempting to attack the system or network.

There are methods of IDS, these are known as: Network-based IDS (NIDS) and Host-based IDS (HIDS) – HIDS have preinstalled software anti-threat applications on all network computer which contains two way access to outside environments like the internet, essentially firewalls, antivirus software and spyware-detection programs. NIDS only has software installed at certain points, like servers that interface among the environment and the network segment to be protected. Passive and reactive IDS – Passive IDS will search for possible security threats and log all the information, then it signals alerts to the administrator of the network so that they can act in response in a suitable way. Reactive IDS responds to suspicious by logging the user that is being attacked off or by reprogramming the firewall actively to block any traffic from the source, this causes any contact with any source that seems untrustworthy.

Knowledge based IDS – most IDS that are extensively used are knowledge based. Knowledge based IDS implement the collected knowledge about different attacks and sensitive systems. As the IDS knows about the

vulnerabilities it will search for an attempt to expose the vulnerabilities. When an attempt has been made the IDS will set off an alarm which can warn the administrator of the network about the problem. Passive IDS vs Reactive IDSPassive IDS is only used for detection. Passive systems detects potential security breaches, then logs the information and signals the alerts.

Reactive IDS is used for responding to any suspicious activity that it has detected. When the suspicious activity is detected it logs off a users or either reprograms the firewall to block network traffic from the suspected malicious source. To conclude with comparison of Passive and Reactive IDS, i would note that the reactive IDS is more useful than passive, as it responds by itself and does not wait for the user to response and deals with the suspicious activity itself, whereas on passive IDS, the system waits for you to respond once finished alerting you.

File & Folder MonitoringFile Monitoring is software that monitors files and folders for folder size and specific file types, When monitoring the folder size, it Monitors increase and decrease in the size of the folder and the availability of a folder in the specified directory. Monitoring the folder also allows the software to keep track of every change made to the folders. When monitoring the specific file types it watched out for any changes made to the specific file (for example, .

log). Monitoring file types will also monitor the changes of size and age of a certain file in a folder and also keeps track of files and subfolders in a path. It is useful for detection since it enables users to see the difference in the file or folder sizes. AntivirusAnti-virus is a software that removes any malicious

software that can be harmful to a computer system by using the scan feature which scans your Hard Disk Drives. If a threat is found the software then quarantines the file. anti -virus also protects users from the internet by giving warning about the files that are about to be downloaded, allowing the user to be more aware and safe from the threats on the WWW (World Wide Web). Antivirus works well together with a firewall, since both firewall and Antivirus can keep the computer system protected and along with a fall back plan if any malicious packets or programs have been downloaded onto the system. The greatest and most obvious advantage to an up-to-date anti-virus software installed on a network or computer is that it can prevent many types of different viruses such as trojans, malware and spyware.

However it can take up a lot of memory a hard disk space another disadvantage is that it does not fully protect against every malicious software out there, so it is recommended that you also have a firewall along with the antivirusSpyware ProtectionSpyware protection is a utility software which prevents, detects and protects against any installations of spyware program as well as remove spyware programs if it were already installed onto the network or computer. The detection could be either rules-based or based on downloaded definition files that is recognised as active spyware program. FirewallAntivirusFile and Folder MonitoringComplexity Firewall is the best to use as it is certain ports so that access can be denied to any malware or users that will try to cause harm. Removes any malware detected within the computer. watches out for any changes to folders, subfolders and particular files. Access is controlled to and from the network. Has a scan feature that scans a Hard Disk Drive.

Monitors increase and decrease of file sizeThis is the most used common system that is used in networking. Very commonly used on computer systems to defend from malware. It is not used as often as firewall and antivirus.

You are able to make exclusions in your firewall for certain folders so that the firewall does not attack the packets that are friendly. A threat is quarantined once it has been found and lets do deal with it how you want. Checks availability of a folder in specified directory.

Allows you to remove access to users physically, therefore removing threats from harming the network. It protects users on the internet by giving warnings of certain files that you are downloading. This is useful for detection, since it lets you see the differences in sizes and files. Firewall HoneyPotsIDSFile & Folder MonitoringAntivirusOne of the simplest tasks performed by antivirus software is file scanning. This process compares the bytes in files with known signatures that are byte patterns indicative of a known malware. It represents the general approach of signature-based detection.

When new malware is captured, it is analyzed for unique characteristics that can be described in a signature. The new signature is distributed as updates to antivirus programs. Antivirus looks for the signature during file scanning, and if a match is found, the signature identifies the malware specifically. There are major drawbacks to this method, however: New signatures require time to develop and test; users must keep their signature files up to date; and new malware without a known signature may escape detection. The

ability of malware to change or disguise appearances can defeat file scanning. However, regardless of its form, malware must ultimately perform its mission. Thus, an opportunity will always arise to detect malware from its behavior if it is given a chance to execute. Antivirus software will monitor system events, such as hard-disk access, to look for actions that might pose a threat to the host.

Events are monitored by intercepting calls to operating system functions.

https://prezi.
com/ibtzgkrrqfu-/unit-32-networked-systems-security/http://timkingunit32.
blogspot. co. uk/2014/03/explain-operation-of-different-intruder.
htmlhttp://networksystemsecurity. blogspot. co. uk/2013/03/m1-explain-
operation-of-different. html http://searchsecurity. techtarget.
com/feature/Comparing-the-best-intrusion-prevention-systems