Security technologies essay

Network security has become a major concern to companies throughout the world, due to rapid growth of interest in the internet. This is in connection to the widely available information and tools needed to penetrate the security systems of corporate network. Consequently network administrators are spending more time and effort protecting their networks than on actual networks setup and administration following the increased focus on network security. The Security Administrators Tool for Analyzing Networks (SATAN) and the newly available scanning and intrusion defection packages and appliances, are tools that probe system vulnerabilities which assist attackers in their efforts, which administrators fail to provide a means to protect networks from all possible attacks since they only point out areas of weakness, it therefore leaves the administrator with the option of only keeping a breast of the large number of security issues confronting them in today's worldWhen an individual is connected to the internet from a private network, the individual network is connected to more than 50, 000 unknown networks and including all their users. At times, this can open connections or doors to many useful applications and provides great opportunities for information sharing, most or all private networks contain information that need not be shared with outside users on the internet, and given the fact that, not all internet users are involved in lawful activities. These two statements foreshadow the prime questions behind most security issues on the internet of most critical is protecting confidential information from those who do not explicitly need access to it and secondly protecting your network and its resources from malicious users and accidents that originate outside your network (wwwcisco.

om/univercd) On a network confidential information resides in two states, either on the physical storage media like the hard drive or memory or in a transit across the physical network wire in the form of packets. The two information states present multiple opportunities for attacks from users as well as those users on the internet. The second state are those users on the internet who are involved in security issues, namely; network packet snifters, IP spoofing password attacks, distribution of sensitive internal information to external sources and man-in-the middle attacks, represent the present opportunities which compromises the information on your network. In order to protect your information from the attacks, your concern/aim is to prevent the theft destruction, corruption, and introduction of information which causes irreparable damage to sensitive and confidential data (Clap ham, 2007). In a networked computer system communicate through a serial system where one information piece is sent after another, any large information is broken down into smaller pieces, and in either serial or parallel communication the information stream would be broken down into smaller pieces, and the overriding reason for this is that computers have limited intermediate buffers, and the smaller pieces called network packets. Several network applications distribute network packets in clear text, where the information sent across the network is not encrypted.

By encryption we mean that the information, or scrambling, of a message into an unreadable format by using a mathematical algorithm. Since network packets are not encrypted, they can be processed and understood by any application that can pick them up off the network and process them at the same time. Packets are identified and labeled by a network protocol, which

enables a computer to determine whether a packet is intended for it and Network protocol specifications like TCP/IP are widely published and as such a third party can easily interpret the network packets and develop a packet snifter, and the real threat today results from the numerous freeware and shareware packet snifters that are available, which do not require the user to understand anything about the underlying protocols. A packet snifter is a software application that uses a network adapter card in promiscuous mode to capture all network packets that are sent across a local area network (Brown, 2006). Several network applications distribute network packets in clear text, and therefore a packet shifter can provide an attacker with information, like the passwords and their account names.

With networked databases, a packet snifter can provide an attacker with information that is queried from the database, as well as the user account names and passwords used to access the database. But a problem is that user account names and passwords is that users often sense their login names and passwords across multiple applications. Majority of the users employ a single password for access to all accounts and applications and an application is run in client/server mode and authentication information is sent across the network in clear text, and this same authentication information is likely to be used again to gain access to other corporate access. The fact that attackers know and use human characteristics like the use of a single password for multiple accounts, they are often successful in gaining access to sensitive information.

In IP spoofing and denial of service attacks, an attacker outside your operating network pretends to a honest and trusted partner, and this is

mainly facilitated by the use of either IP address that falls within the range of IP addresses for your network, or by using an authorized external IP address that you trust and to which/whom you want to provide access to specified resources on your network. In normal cases, an IP spoofing attacks is limited to the injection of data or commands into an existing stream of data passed between a client and server application or a peer-to-peer network connection. In order to change all routing tables and for them to point to he spoofed IP address an attack must enable bidirectional communication, and if the attacker manages to change the routing tables to point to the spoofed IP address, the all the network packets hat are addressed to the spoofed address will be received and can reply just as any trusted user can. Another approach would be not to worry about receiving any response from the targeted host, and this is called a denial-of-service (DOS) attack. This occurs because the system receiving the requests becomes busy trying to establish a return communication path the initiation.

In technical terms, the targeted host receives a TCP-SYN and returns a SYN-ACK. It then remains in a waiting state, anticipating the completion of the TCP handshake that never happens, and each wait state uses system resources until eventually, the host cannot respond to other legitimate requests and like packet snifters IP spoofing and DOS attacks are not restricted to people who are external to the networkPassword attacks Several different methods can be implemented to use password attacks including brute-force attacks, Trojan horse programs, IP spoofing any packets shifters, but packet snifters and IP spoofing can yield user accounts and passwords, password attackers usually refer to repeated attempts to

identify a user account and/or password; these repeated attempts are called brute-force attacks. It is performed using a dictionary program that runs across the network and attempts to log in to a shared resource, like the server. When the attacker successfully gains access to a resource, that person has the same rights as the user whose account has been compromised to gain access to that resource. The attacker can create a back door for future access if the account has enough privilege without a concern of any status and password changes to the compromised user account.

At the core of a network security police is the controlling of the distribution of sensitive information majority of computer break-ins that organizations snifter are at the hands of disgruntled present or former employees. And at the core of these security breaches is the distribution of sensitive information to competitors or others that will use it to your advantages, an outside intruder can use password and IP spoofing attacks to copy information, and man in the middle attacks, requires that the attacker have access to network packets that come across networks. For instance your internet service provider (ISP) can gain access to all network packets transferred between your network and any other network and they are implemented using network packet snifters and routing ad also transport protocols. Most of this occurs in theft of information hijacking of an ongoing session to gain access to your internal network resources, traffic analysis to derive information about your network and its users, denial of service, corruption of transmitted data, and introduction of new information into network sessions.

Your highest and most important priority is to protect your information but protecting the integrity of your network is critical in your ability to protect the information contained in your network. A breach in the integrity of your network can be extremely costly in time and effort, and can at the same time open many avenues for continued attacks. The most commonly used methods to compromise the integrity of your network are network packet snifters, IP spoofing password attacks, denial-of-service attacks and application layer attacks. This is because when you consider what to protect within your network, you are concerned with maintaining the integrity of the physical network, your network software, any other network resources, and your reputation.

The integrity involves the verifiable identity of computers and users proper operation of the services that your network provides, and optimal network performance, all these concerns are important in maintaining a productive network environment (Chapman & Zwicky, (1995). Network packet snifters can yield critical system information, like the user account information and password. The attacker runs your network once the correct account information is obtained. In some worst scenarios/cases, the attacker gains access to a system level user account, which the attacker uses to create a new account that can be used at any time as a bulk door to get into your network and its resources; modifying system-critical files like the password for the system administrator account, the list of services and permissions on file servers, and the login details for other computers in the network that contain confidential information. They provide information about the topology of your network that many attackers find useful, at the same time a

network packet snifter can be modified to interject new information or change existing information in a packet, and this makes the attacker to cause network connections to that down prematurely, and as well in changing critical information within the packet, and what if the attacker meditates the information being transmitted to your accounting system, the effect can be costly at the same time very difficult to detect. A part from being used in other ways, IP spoofing can give access to user accounts and passwords, if or instance, an attack can emulate one of your internal users in ways that prove embarrassing for your organization, He/She could send e-mail message to business partners that appear to have originated from someone within your network organization, and they are easier when an attacker has a user account and password, but they are also possible by combining simple spoofing attacks with knowledge of messaging protocols, like in Telnet ting directly to the SMTP part on a system allows the attacker to insert bogus sender information.

As like packet snifters and IP spoofing attacks, a brute-source password attack also provides access to accounts what can be used to modify critical network files and services. In compromising your networks integrity an attacker modifies the routing tables for your network, and as such ensures that all network packets are routed to the attacker before they are transmitted to their final destination (Kinnagbe, Dressel, & OPdycke, 2007). Denial-et-service attacks are different from most other attacks because they are not targeted at gaining access to your network or the information on your network, but the attacks focus on making a service unavailable for normal use, which is typically accomplished by exhausting some resource

limitation on the network or within an operating system or application. When specific network server applications are involved, like the Hypertext Transfer Protocol (HTTP) servers or a File Transfer Protocol (FTP) server, the attacks focus on acquiring and keeping open all the available connections supported by that server, effectively lacking out valid users of the server or service. They can also be implemented using common internet protocols, like TCP and internet control message protocol (ICMP). Most denial of-service attacks exploit a weakness in the overall architecture of the system being attacked rather than a software buy or security hole.

Application layer attacks can be implemented using different methods, but the most common method is exploiting well-known weaknesses in software commonly found on servers, such as send mail, postscript, and FTP. By exploiting these weaknesses, attackers can gain access to a computer with the permissions of the account running the application, which is usually a privileged system level account. hen it comes to IT security, most enterprises have it really rough the same issues to deal with, Microsoft being not an exception, it is better to learn the given the fact that, Security in IT keeps on developing with technology and a technology solution is needed that provides the desired controls and monitoring in a centralized, cohesive fashion (Coggins et al. , 1997) Security technologies Microsoft® Managed Solutions (MMS), the Risk Management and Compliance team is charged with defining, monitoring, and correcting the risk posture of all MMS environments for both customer-facing services and infrastructure coordination for corporations. Of utmost important, we need security technologies that would

cover the three primary control types; preventive, detective, and corrective, and as well as provide auditing and reporting.

There are four main categories of security technology; risk management dashboard, anti-malware, network anomaly detection, and desired configuration management (Cheswick & Bellovin, 1998). Risk management dashboardIn my opinion, a risk management dashboard (RMD) is absolutely essential, it is the single most important technology to the operation of an IT security team because, Confidentiality, integrity, availability, and accountability (CIA2) risks in an enterprise are often monitored by disparate systems and processes with no single interface for data aggregation, correlation, and risk remediation and at the same time, regulates requirements specifying increasing difficult levels of enterprise data transparency, and there is no streamlined system to readily track policy from creation to enterprise execution. This is evidenced by common enterprise difficulties in data acquisition, correlation, assessment, remediation, and compliance, since data acquisition is hampered by an inability to aggregate and normalize data from disparate sources, data aggregation in and of itself is challenging, as it requires breaking out of the all too common soloed approach to gathering and reporting data; even where data aggregation is accomplished, normalization continues to pose an even bigger challenge because it is extremely difficult to establish the common framework needed to support the normalization of data. Without this normalization, it’s impossible to compare security and health-related events coming from different systems in a meaningful? way. In order to perform the needed automation, the risk management dashboard must have access to data

feeds from sources other than the four security technologies described inhere, for instance, a lot of non-security data can be used for determining overall risk posture and information like router logs, asset tracking, patch status, currently logged on users, performance reporting, and change management data, all provides relevant information to the incident investigator. Thus, the overall system needs access to all of this data and for the fact that we’re aware that even the most Microsoft-centric enterprise infrastructures include non-Microsoft technologies, so the RMD needs to accept feeds from non-Microsoft technologies trough a common interface.

The RMD is useful to administrators not on the security team, but since the dashboard encompasses a holistic view of the environment, the RMD can act as a central point for all staff to view current status. It may, for example, alert the messaging team about a denial of service attack at the SMTP gateway considering that, while this is a security incident to the risk management team, the messaging team will see it as an availability incident. Though the messaging team may not be responsible for fielding and resolving such an incident, they will at least want to be aware of incidents like this that affect the assets the team manages (Johansson, 2005). Anti-malware technologyThis technology is important for protecting your infrastructure against unforeseen threats hiding in code and user actions, currently; there are generally two separate types of tools to protect against malware: antivirus and anti-spy ware, since both effectively prevent, detect, and correct different types of infection. However, it’s only a matter of time before these two types of protection are unified into a single solution

and there will be just one anti-malware stack on a system; a thorough anti-malware solution needs to monitor in real-time and periodically scan.

It should centrally report known malware which includes viruses, spy ware, and root kits and other unknown malware based on typical risky behaviors. Robust anti-malware technology watches all the classic entry points like the file system, registry, shell, browser, e-mail, and connected applications through tight integration with the OS and various applications. It needs to cover more than just host security, also, watch common messaging and collaboration services where infected files often pass through, such as Share Point® and instant messaging, it therefore goes without saying that anti-malware is not useful without updates, since the system must keep its signature and removal systems updated to stay ahead of the latest threats. Network Anomaly Detection While anti-malware keeps an eye on systems, network anomaly detection (NAD) monitors the common pathways, watching for well-known indicators of suspicious behavior and reporting this information to the RMD for remediation. Suspicious behaviors can be well-known attack traffic like a worm or denial of service and any other data that fits a certain pattern such as U.

S. Social Security numbers that is being sent via e-mail, and despite the best efforts in IT management, large enterprise networks inevitably encounter an occasional malware incident. The fact that NAD can provide an early warning system that can help accelerate remediation, the NAD data-monitoring capabilities, and the ability to identify and stop sensitive information from being leaked are weak, and as such handy tools provides protection for information in an environment concerned about data leaks and regulatory

compliance. The major weakness of NAD is, NAD must constantly adapt to the latest set of threats and sensitive data types or its value is greatly diminished, a good NAD system should understand enough about the actual anomalies to minimize the number of false positives being reported, otherwise, administrators may ignore the reports coming from NAD, assuming that each is just another false alarm (Chen, 2006).

Whether it is build it in-house or bought from a reputable vendor, the dashboard is essential, acting as your team’s primary tool for incident response; Anti-malware is also essential, in helping to protect against the threats that multiply daily; Network anomaly detection is on the verge of changing from just malware signatures and host intrusion detection to include data leakage discovery and the last function can help to prevent the next well-publicized network breach, considering that Desired Configuration Management, while still new and not mentioned here, mighty soon be a mainstay for monitoring and maintaining configurations, regardless of who provides these tools, you must have at least one for each of these four categories, preferably RMD in my opinion. The inside story From this observation, we’ve seen so far, no single vendor including Microsoft included offers a single holistic solution that addresses each of the above observations and therefore, it is up to you find the selection of products that will suit your specific needs; an insight is provided as to what you need to consider, what you should be looking to achieve, and what the ideal solution will do for you. When defining a security policy for your organization, it is important to strike a balance between keeping your network and resources immune from attack and making the system so difficult to negotiate for

legitimate purposes that hinders productivity. This means you must walk a fine line between closing as many doors as possible without encouraging trusted users to try to circumvent the policy because it is too complex and time consuming to use, and allowing internet access from an organization poses the most risk to that organization.

Most important, to stress is that attacks may not be restricted to outside unknown parties, but may be initiated by internal users as well and knowing how the components of your network functions and interacts is the first step to knowing how to protect them.