Network Security Attacks: Reconnaissance Attacks And Ways To Prevent Them

Introduction

In today’s world of technology, a massive amount of information or data is stored in cyberspace. It’s because people can access stored information in a fraction of seconds compared to the tedious process of collecting information in the late 20 century. Cybersecurity protects computer systems from hardware, software, or electronic data being theft or damaged. A computer network is a collection of computers that are attached together to share resources. Coming to the topic of network security it is a very wide word to come to the subject of network security. It implies protecting data stored or information travelling across a network. The practice of network security is to prevent and protect corporate networks from unlawful intrusion. Security of the network has three main objectives: confidentiality, integrity, accessibility. Confidentiality implies ensuring that private data remains personal. Integrity ensures the accuracy of the information. This implies that information must be protected against unauthorised changes or destruction by a safety specialist. Accessibility ensures that information is available to the organization whenever necessary. This means protecting the network from anything, including energy outages, that would render it inaccessible.

The word hacker initially referred to someone who was able to write an ingenious piece of software. In reality, a specific smart piece of programming was intended by the sentence' a good hack.' However, outside the hacking community, anyone trying to access a computer network illegally is called a hacker. Hacking often involves becoming intimate with the details of existing software to provide the hacker with the knowledge necessary to attempt an unauthorized system break-in However, those who adhere to the original definition of the term hacker wanted to separate themselves from those who carry out illegal actions, i.e. the term cracker. There are many kinds of hackers in the globe today, such as White Hat, Black Hat, Grey Hat, Script Kiddies, Green Hat, Blue Hat, Red Hat, State / Nation Sponsored, Hacktivists and Whistle-blowers.

Aims

Whilst there are many different types of proposed solutions to the weaknesses in Network security, they all share a similar aim. The primary aim of network security is to effectively secure the integrity, confidentiality and availability of the assets belonging to each individual client. Harrington (2005) has argued that network security is a continuous process of protecting the confidentiality of information that should stay private. Security threats are deliberate and accidental and can come from outside or within an organization. Network security attacks are illegal acts against private, corporate or government IT resources to delete, alter or steal sensitive data. As more businesses allow workers to access data from their smartphones, networks are vulnerable to data theft and the destruction of data or networks. There are many types of network attacks they are

Reconnaissance Attacks

These attacks are general knowledge collection attacks. Such attacks can take place for both theoretical and physical approaches. It is suggested that if data is collected through network surveys or social engineering or external monitoring, such attacks can also be avoided (Britt,2019). Most Common examples of these attacks include social engineering, packet sniffing, port scanning, ping sweeping, phishing and online information queries. We may explore these further by splitting them into two groups, logical and physical.

Logical Reconnaissance refers to anything that is performed in the electronic world and does not allow a human being to perform a reconnaissance assault on the other hand. Port scans and ping sweeps, for instance, are two ways for finding both if the system is put in place and what it is searching for on the network. An illustration of a port scan return would be the detection of an IP address reacting to HTTPS traffic on port 443. This helps the attacker to know that they can attempt HTTPS-oriented exploitation.

In addition, here we can see requests for information on the Internet. These are often referred to as whois queries. All domains registered to independent businesses belong to a domain supplier, as all these domains must be controlled. The dilemma is the patenting name of the product where organization A wishes to use a given domain and organization B already owns that domain. Britt (2019) states that these domain administration systems perform the transfer and retention of domain names from creation to exhaustion. These domain hosting services normally provide a large amount of information about an entity which includes points of contact and contact details. All of this makes it easy to collect information if you approach an organization with legitimate information about persons of interest.

Physical Reconnaissance Crosses the boundaries of what is managed by the network administrator. There are things that will never be properly protected like areas, as well as security features such as mantraps, cameras, door locks and guards. For instance, bank security may be restricted in the ability to stop an incredibly well-organized heist attempts to do what the security staff has planned for but the simple fact that the bank has security measures in place provides the opportunity to dissuade the lowest to mid-level offenders who would make the attempt. This is the same concept that applies to most physical security steps for the safety of the network. Reconnaissance, as we have known, is the compilation of data from all kinds of available sources. (Britt, 2019). If the surveyor is unable to easily access the content, it can fully discourage the collection or push it into a more rational domain. Either one of these solutions for the surveyor would be helpful to the networking staff as it pushes visibility into a more manageable circumstance.

Solution

There is really a small attempt to do this type of attack, as some specifics and companies confidential information has to be out there. Nonetheless, through preparation and basic corrective steps, preventive measures can be taken to stop this from becoming more severe. Try to reduce the details you have written about the firm's contact details. Change banner returns to banner-grabbing attacks so that the data is confined to the hacker. Good user training is the first and perhaps the only protection against social engineering(Harrington, 2005). If all data is needed to contact the network manager or company representative, make sure that they are educated on how to detect social engineering attacks. This learning needs to be extended to all staff, as anyone is at risk of revealing corporate secrets if the social engineer is confident

enough.

Reference list

1. Britt, A. (2019). 3 Types of Network Attacks to Watch Out For. [online] The State of Security. Available at: https://www.tripwire.com/state-of-security/vulnerability-management/3-types-of-network-attacks/ [Accessed 27 Sep. 2019].
2. Harrington, J. (2005). Network security (pp. 1-33). Amsterdam: Elsevier.
3. What are Network Security Attacks? | Akamai. (2019). Retrieved 4 October 2019, from https://www.akamai.com/us/en/resources/network-attacks.jsp