Nehru E- Journal
A Journal of Nehru Arts and Science College (Autonomous)
Journal Home Page: http://nehrucolleges.net/jo.html
ISSN: 2349-9052

Research Article
Vol 5 issue 1(2017)
(Jan - July 2017)

TOUR ON CURRENT ISSUES OF NETWORK SECURITY AND POSSIBLE SOLUTIONS

N.Karthik, Asst. Professor,
Department of IT & CT
Nehru Arts and Science College, Coimbatore 641 105, India

Keywords:

network security

Abstract

In today’s industry, too many people continue to do the same mistakes with their network security over and over again. It seems that we just learning our lesson. It was Einstein who once said, “You cannot solve problems by using the same kind of thinking that we used when we created them, ”it means that, if a dilemma arises, you can’t fix it and keep it fixed without changing your methods. We all seem to fall into one or more of these habits over time, In order to remind what we need to look for; here is some common network security issues and solutions.

INTRODUCTION

CURRENT ISSUES AND SOLUTIONS

1. Non-complex Access to Passwords

Most network system administrators are open to an “old school” exploit known as brute forcing. To correct this network security password vulnerability, they have implemented “CAPTCHA Technology.” A common type of CAPTCHA[2] requires the user to type letters or digits from a distorted image that appears on screen, which is commonly used to prevent unwanted internet bots from accessing websites and networks. This technology has given network security administrators a false sense of security, in regard to counter brute forcing.

The solution for this problem, is obviously to create complex password. The complex password consists of seven or more characters combined with at least three numbers and one special character (capital letters, @ or # signs, etc.). Network security administrators should require the creation of complex passwords as well as implement a password expiration system to help remind users to change their passwords often. A restriction on how soon a password can be reused is also another handy precaution. In that way someone isn’t cycling between two different passwords in every month.

2. Server Application or Software Expiry

Companies constantly release patches to ensure that your system is not vulnerable to new public threats. Hackers consistently release new threats and exploits your network if these patches are not in place. A simple solution is to ensure your system administrator is regularly informed of new threats and updating your applications on a monthly basis.

3. Web Secret Collectors - Cookies

Although cookies do not carry viruses and cannot install malware on the host computer, the tracking of cookies is commonly used to compile records of individuals’ browsing histories. Unencrypted cookies are a major network security issue because they can open your system to XSS (Cross Site Scripting) vulnerability and that is a major privacy concern. With ‘Open Cookies’ anyone can access to any login data cookies (saved password sessions) on the network, and that creates a major vulnerability on your network security system.

The solution is to ensure your entire network cookies are encrypted and have an encoded expiration time. Your network administrator should also force users to re-login at any time they are accessing sensitive directories in your network.

4. Plain Index as Hashing

Hashing is used to index and retrieve items in a database. Plain Hashes are used in many encryption algorithms. A Salt (which is another type of encryption) is added to Hashes make a lookup table assisted Directory Attack (or Brute-Force) impractical or extremely difficult, provided the Salt is large enough. Basically, an attacker wouldn't be able to use a pre-computed look up table to assist in exploiting your network, because that make a whole new level of complexity to your network security system.

Even if an attacker gains access and compromises your database (table), it will still be very difficult for the attacker to retrieve the information. The best way to ensure safety in regard to Hashes is, your network administrator has to hide the Salt (or encryption key). If not the hacker is able to gain access to your Salt encryption and they can access your network system. Salt all of your Hashes. If there is no Salt there is void security.

5. Share hosting

If you are running a legitimate business and have a website with access to your internal network, Shared Hosting is not the way to go! A shared web hosting service is the one where many websites reside on one web server connected to the Internet.

Each site sits on its own partition, or section or space on the server, to keep it separate from other sites. This is generally, the most economical option for hosting, because people share the overall cost of server maintenance. To put it clear think of this way, shared hosting is like sharing a house with other people, and if someone break into your roommate's bedroom or any other area of the home for that matter, they can also access your own room!

This same concept is applied to Shared Hosting. When an attacker is inside one area of the shared server, it's almost they have a skeleton key that fits all of the locks. The best solution is to have dedicated Server Hosting and/or Secured Cloud Hosting.

Conclusion

Network security is not only mean starting with authenticating, it is commonly with a username and a password. It also requires multifactor authentication. For example, performed in story of ATM and three factor authentications such as fingerprint systems which follow strong policies such as what services are allowed to be accessed by the network users. An anomaly-based intrusion detection system may also monitor the network like wire shark traffic and logged for audit purposes. Later high-level analysis which can detect active network attackers from malicious insiders. Thus communication between two hosts using a network may be encrypted to maintain privacy.

References

1. A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco

2. Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

3. "Dark Reading: Automating Breach Detection For The Way Security Professionals Think". October 1, 2015.