Global Scientific JOURNALS

GSJ: Volume 10, Issue 3, March 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

BRUTE FORCE ATTACK DETECTION AND PREVENTION ON A NETWORK USING WIRESHARK ANALYSIS AND FILE ZILL

UWIMANA ROBERT

Email: uwirobert@gmail.com

Faculty of Computing and Information Sciences, University of Lay Adventists of Kigali

Abstract

Brute-force attacks are a prevalent phenomenon that is getting harder to successfully detect on a network level due to the increasing volume and encryption of network traffic and the growing ubiquity of high-speed networks. Although research in this field has advanced considerably, there still remain classes of attacks that are undetectable. Since no security measure can guarantee that an attacker will not succeed eventually, intrusion detection techniques should be applied to detect anomalous behavior early and minimize its impacts on network performance caused by the intruders. This research proposed an intrusion detection technique in which the node (server) uses a monitoring software application to monitor the traffic flow on the network and collects relevant statistics about it. By analyzing and comparing the traffic information, the administrator will be able to indicate if an attack is performed or not.

KEYWORDS: Brute- Force, Wireshark, network, FTP Server.

Introduction

Information and network systems can be open to attacks even if some finest technological measures such as firewall and anti-virus are put in place. The reason is that information security is not limited to some of technological aspect but also other detection techniques which give accurate analysis. Brute force attacks are used for detecting login credentials using random combinations of username and passwords. This research demonstrates a technique by which brute force attacks on FTP servers can be detected using technological analysis such as Wireshark, FileZilla Server and client which in turns helps packets analyzers in decision making (Kirandeep, 2013).

Since no security measure can guarantee that an attacker will not succeed eventually, intrusion detection techniques should be applied to detect anomalous behavior early and minimize its impacts on network performance caused by the intruders. This research proposed an intrusion detection technique in which the node(server) uses a monitoring software application to monitor the traffic flow on the network and collects relevant statistics about it. By analyzing and comparing the traffic information, the administrator will be able to indicate if any attack is performed or not (Mohammed, 2017).

Review of Literature

In recent years, network security research started focusing on flow-based attack detection in addition to the well-established payload-based detection approach. Instead of only looking for malicious activity in the actual packet data, network Flows are also considered for analysis. This is not surprising since the amount of data one has to fight with is drastically reduced and the attacks visible inflow data tend to complement the attacks that we strive to find in network payload. We propose a detection technique and shed light on the shortcomings inherent to the flow-based attack detection approach. This research aims at demonstrating a technique by which brute force attacks on FTP servers can be detected using Wireshark Analysis. The research seeks to realize the following objectives:

- ✓ Response Codes Logged in attempts
- ✓ Nature of End-Product with the number of login attempts.
- ✓ Information on the initiator of the attack.

Related Studies

Several studies have identified areas of vulnerability in information assets of organizations using some detection methods or techniques, however my research seeks to look at securing network data from the point of detection technique using Wireshark in conjunction with FTP server. (Smith, 2004) conducted a test to show how data are insecure in organizations. He performed an information security review of publicly accessible servers of the GIAC enterprise. The methodology he used was to examine the public servers from both the network perspective as well as from the local host perspective. The findings of the assessment include:

- ✓ Operating systems are not up to date with the latest system updates and security updates.

- ✓ The apache server is vulnerable to attacks and is running default configuration □ The Domain Name System (DNS) server has not been locked down.
- ✓ The File Transfer Protocol (FTP) server authenticates users using insecure methods.
- ✓ The mail server authenticates users in clear-text when encrypted methods are available.

The conclusion was that the information assets of the organization are vulnerable data and information are insecure.

A similar test was carried by Honeywell (Industrial IT Solutions, 2012) in an attempt to help AmerChem company better understand their current cyber security situation, the potential risks associated with that current status, and a proposed path put forward to remediate any issues. The scope of the audit was all cyber assets at the AmerChem facility. In total, thirty-nine (39) servers and workstations were audited. The findings were that Cyber assets have not been patched since their installation dates; Default Guest accounts are enabled on a number of cyber assets; There are early indications of hard drive failure on one cyber asset; One cyber asset is connected to both the process control network and the business network, and Cyber assets are not up to date, or do not have any malicious software prevention solution in place.

(Silver, 2013), James and al. and (Anita, G., Kavita, K. and Kirandeep, K. , 2013)have followed the same trend on concentrating vulnerability evaluation on hardware aspect of information assets and using some detection mechanisms but then again the Wireshark detection factor is short of which this research will address. Studies have been undertaken to identify some of the weaknesses and vulnerabilities in most commonly used cryptographic algorithms. Though studies on cryptosystems vulnerabilities and this research are related, one is purely technical and some software based detections and the other focuses on the Wireshark aspect of detection.

One of the major areas of information security weakness discussed in literature is on database vulnerabilities. Here again, the vulnerabilities are software and hardware related. The human factor has been glossed over. Shulman (2006), outlines ten vulnerabilities associated with database infrastructures but none of them talked about the activities end users do that make information systems vulnerable to attacks and some other effective detection technique to these attacks. I

n today's businesses, database technologies are needed more than before and with the increasing usage of the internet for business, threats or risks to these databases are growing. (Lamar, 2014) opines that database attacks are prevalent these days because of the following vulnerabilities: Vulnerabilities in Operating Systems like Windows, UNIX and Linux and their services associated with the databases could create a loophole for illegal access which may lead to a Denial of Service (DoS) attack. Database rootkits: A database rootkit is a program or a procedure that is hidden inside the database and that gives the administrator special privileges to be able to access data in the database. Sometimes the rootkits turn off alerts prompted by Intrusion Prevention Systems (IPS) which could be disastrous.

Weak authentication: Weak authentication models permit attackers to use tactics like social engineering and brute force to get hold of database login details of users. Weak audit trails: A weak audit logging method in a database server is risky to an institution particularly in retail, financial, healthcare, and other businesses with strict regulatory observance. PCI, SOX, and HIPAA are rules that require extensive logging of actions and also generate events when something goes wrong. In order to resolve issues when something goes wrong, logging to critical transactions in a database must be done in an automated way. Audit trails work as the last line of database defence and can sense any violation. Audit trails can help trace back the violation to a particular period and a particular user.

This research will add to the literature by looking at a different angle to information systems detection mechanisms, thus, targeting only the use of Wireshark to detect brute force attacks. Finally, Firewall vulnerabilities have also been discussed in the literature. Firewalls guard a trusted network from an untrusted network by filtering traffic by following a designated security policy. Different firewalls are being used today and they are one of the sources of security vulnerabilities. (Kamara, 2010)) give a taxonomy to understand firewall vulnerabilities in the framework of firewall implementations as it is not practical to study and test each firewall for all possible problems. They examined firewall attributes, and cross-reference each firewall operation with causes and effects of flaws in that operation, evaluating twenty recognized flaws with existing firewalls.

The outcome of their investigation is a set of matrices that demonstrate the distribution of firewall vulnerabil causes and sand effects over firewall operations. These matrices are beneficial in circumventing and perceiving unforeseen hitches during both firewall implementation and firewall testing. Firewalls can be software or hardware and vulnerability studies in them are classified according to the vulnerabilities in the software, the hardware, and vulnerabilities due to misconfiguration (Kashefi, 2013). But the loyalty of the networks is a matter of concern. Since no security measure can guarantee that an attacker will not succeed eventually, intrusion detection techniques should be applied to detect anomalous behavior early and minimize its impacts on network performance caused by the intruders. We have proposed an intrusion detection technique in which the node (server) uses a monitoring software application to monitor the traffic flow on the network and collects relevant statistics about it. By analyzing and comparing the traffic information, the administrator will be able to indicate if any attack is performed or not.

Wireshark is an open-source protocol analyzer designed by Gerald Combs that runs on Windows and Unix platforms. Originally known as Ethereal, its main objective is to analyze traffic as well as analyzing communications and resolving network problems. Wireshark implements a range of filters that facilitate the definition of search criteria and currently supports over 1100 protocols (version 1.4.3), all with a simple and intuitive front-end that enables you to break down the captured packets by layer. Wireshark "understands" the structure of different networking protocols, so you are able to view the fields of each one of the headers and layers of the packets being monitored, providing a wide range of options to network administrators when performing certain traffic analysis tasks.

Methodology

Research Methodology is the process used to collect information and data for the purpose of making business decisions.

Techniques

It is practical methods or skills applied to particular tasks identified as part of the research. It is increasingly common for researchers and academics to combine multiple techniques within a single research project (Mixed-Mode Data Collection). This approach helps to reduce mistakes and inconsistencies that can arise. Therefore, the following techniques are preferred to be used:

Interview

An interview is generally a qualitative research technique that involves asking open-ended questions to converse with respondents and collect elicit data about a subject. The interviewer is most cases is the subject matter expert who intends to understand respondent opinions in a well planned and executed series of questions and answers.

Documentation

This is the main method used while collecting secondary data from files and official documents at case study institutions relevant to this work. Consulting documentation about system security in our carrier, news articles on the internet, reading books, and different documents related to the use of ICT to secure information or data from unauthorized access. Documentation is the evidence provided for information and ideas borrowed from others.

Observation

It is a social research technique that involves the direct observation of phenomena in their natural setting. Therefore, when doing research, you have to observe the existing system on your own in order to master how it operates.

Data collection

Data collection is a process of collecting information from all the relevant sources to find answers to the research problem, test the hypothesis and evaluate the outcomes. It can be divided into two categories: secondary methods of data collection (published in books) and primary methods of data collection which in turn divided into quantitative (based on mathematical My reach is electricity power theft detection EUL Rwanda is innovative and contributing because it will involve all types of the customers of electricity i.e those with normal payments history and those caught in electricity theft Scenario. As the reduction of electricity fraud in Rwanda can reduce the cost of electricity in Rwanda and help the EUCL in power distribution of the whole country, the research can be helpful not only for EUL but also for the whole Nation (Rwanda). I will share my experience from knowledge discovery with ECUL officials that will help them to investigate the suspicious scenario in electricity customers and identify the non-trusted customers.

Conclusion

Successful implementation of **Bruteforce detection** will increase the confidentiality of the information provided on the KAYONZA District website since the admin will be able to detect and block illegal access done by someone who repeatedly tries to log in with a different username or password. Thus, this study on its successful deployment would have great importance to the users as they know that sensitive information should not be violated by any one out of the system.

References

Anita, G., Kavita, K. and Kirandeep, K. . (2013). *Vulnerability assessment and penetration testing. International Journal of Engineering Trends and Technology 4 (13).* Unate Staye: F5 Networks, Inc.

Dennis, W. T. (2009). *System Analysis and Design with UML.* United States: 222 Rosewood Drive.

Industrial IT Solutions. (2012). *Integrated Secutrity.* Bangalore: Honeywell International Inc

Kirandeep, K. (2013). Vulnerability assessment and penetration testing. *International Journal of Engineering Trends and Technology 4 (13).* , 8.

Lamar, A. (. (2014, March 18). *Types of threats to database security*. Retrieved August 07, 2019, from http://www.brighthub.com/computing/smb-security/articles/61402.aspx

Mohammed, M. A. (2017). BRUTE FORCE ATTACK DETECTION AND PREVENTION ON A NETWORK. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH* , 2.

Silver. (2013). *Vulnerability assessment and penetration testing.*

Smith, R. D. (2004). *PUBLIC SERVERS.* Unated State: SANS Institute.

BIODATA

Robert UWIMANA Student at Master of Science in Information Technology, University of Lay Adventists of Kigali. Email: uwirobert@gmail.com

Tel: 0786473209

Dr. Papias NIYIGENA, PhD; Lecturer at University of Lay Adventists of Kigali.