ABSTRACT

Brute-force attacks are a prevalent phenomenon that is getting harder to successfully detect on a network level due to increasing volume and encryption of network traffic and 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 any 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 antivirus are put in place. The reason is that information security is not limited to some of the technological aspect but also other detection techniques which gives 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 Wireshark Analysis. 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 in flow 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.

LITERATURE SURVEY

Several studies have identified areas of vulnerability in information assets of organizations using some detection methods or techniques, however our 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:
A similar test was carried by Honeywell’s 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 is 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 et al. (2009), Philip et al. (2003) and Anita, Kavita and Kiraandeep (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.

In 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 (2012) 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 of 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 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 et al. (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 vulnerability causes.
and 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, et al, 2013).

But the loyalty of the networks is the matter of concerned. 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.

WHY WIRESHARK?
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
This research employed an experimental approach

Experiment:
The purpose of this test was to display or exhibit how brute force attacks on FTP servers can be detected alongside using Wireshark analysis. The method used was: brute force attack.

Brute Force Attack
Brute force attempts were made to reveal how Wireshark could be used to detect and give accurate login attempts to such attacks. To do this, the admin ftpserver interface was accessed.

FTP server (Filezilla server), which is an open source (third party) software, was used for the test. The Filezilla FTP server was found to be running on port 21.

Figure 1
Figure 1 above represents the initial interface of the filezilla FTP server when launched and logged on.
Creating the directory
Go to:
- edit and click on groups
- on groups interface click on shared folders
- click on "Add" and choose where you would want to save Accounts

To Create a Group:
- Select the directory created
- under Groups at the right-side, click "Add"
- Enter the group name and click "ok"
Now Give the Group the necessary Permissions and click okay to save
Figure 4 Creating Users in the FTP Server

To Add a User:
- Hover the mouse pointer to Edit on the FileZilla FTP Server and click on users
- Click on "Add" and enter the name of the user
- At the drop down menu are the various Groups Created.
- Assign the user to the appropriate groups and click "ok"
- Now check the Password Box and Enter the password of the user
- Click okay to save settings

Lab Components
- Hardware
  - Windows system with FTP Server.
  - Windows system.
  - Switch
- Software
  - Wireshark

FTP server was downloaded and installed onto the server.

Installation and setup for FTP server
- Run the exe installer
- Select admin port and remember this port
- Launch FileZilla Server Interface
- Enter port from above, enter (new) password for administration, click ok/connect
- Create a user and/or group with permissions to a home directory.
- Add additional directory and set the alias name to display within home directory (e.g. /Alias Name)

Complete
User accounts with administrative rights were created on the ftp server
These accounts do perform different administrative tasks

Lab Setup
- The lab topology used is shown below.
RESULTS FROM EXPERIMENT

Brute Force Attack
The experiment also found out that the system is vulnerable to brute force attacks. A brute force attack is a trial-and-error method used to obtain information such as a user password or personal details. In this attack a software (Filezilla ftp client) was used to generate a large number of consecutive guesses as to the value of the desired data.

FTP Analysis after incorrect password
- Wireshark is started on the FTP server.
- A FTP connection is initiated from the FTP client (attacker system) to the FTP server. The command `ftp 192.168.2.2` is provided on Windows.
- After the above command is initiated, the username and password to log into the system is provided.
- To analyze the behavior of incorrect password on the server, a wrong password is provided to connect to the server.
- Wireshark is filtered for FTP traffic. The screenshot is shown in the following slide.
Wireshark Analysis of FTP with incorrect password

When the incorrect password is sent from the client, the FTP server responds with ‘Login Incorrect’ message.

FTP servers respond with a specific response code which is 530 when the login is incorrect which is shown in the previous slide.

This response code can be used for detecting incorrect login attempts on the server.

Brute force detection technique

FTP servers respond with a specific response code which is 530, when an incorrect password is provided.

Wireshark filter can be used to monitor packets which have the specific FTP code.

This would provide details on the number of login attempts made by a specific IP address, which would help to analyze a brute force attack.

Brute force simulation

Wireshark is started on the FTP server.

Multiple login attempts with incorrect username and password is initiated from the attacker system (192.168.2.5) to the server.

The Wireshark on the server is filtered with the code `ftp.response.code==530`, which would filter all incorrect login attempts on the server.

The screenshot is shown in the following slide.
Using Wireshark Filter for Brute Force Detection

- It can be observed that Frame no 111, 1062, 1085 responds with the 530 error message.
- If the number of incorrect login attempts exceeds 3, it indicates a brute force attack.
- The destination IP address would also provide information on the initiator of the attack, which in this case is 192.168.2.5.
No single indicator is certain, but these are all logical possibilities:

- Many failed log-ins from the same IP address. This is a particularly strong sign (though if the attacker is using a botnet, IP addresses will obviously vary).
- Logins with multiple username attempts emerging from the same IP address
- Logins for a single account coming from many different IP addresses
- Failed login attempts from alphabetically sequential usernames or passwords

What to do after Detecting a Brute Force Attack

The FileZilla FTP Server has a feature called “Automatic ban”. However, the automatic ban mechanism could only work after we enabled it first.

But this feature is not sufficient mechanism since an attacker can change his/her IP to start a new attack.

The best way to do this is to disable the user accounts being brute forced.

Process:

- Click on “Edit”
- Hover to users and click on it
- Select the accounts that is being attacked
- Uncheck the Enable account and click “Ok”

The process of disabling the user accounts is shown in the figure below.
FINDINGS

Human factor vulnerabilities in information security
The following are human factor vulnerabilities that emerged during the experiments. These threats and vulnerabilities include acts performed without intent or malicious purpose by an authorized user (respondents). When people use information systems, sometimes improper usage happens. Inexperience, improper training, and the making of incorrect assumptions are just a few circumstances that can cause these vulnerabilities.

Lack of mechanism to lock users after several login attempts
The system seems to have a weak lock out mechanism or none at all. This was apparent during the experiment when several passwords were gathered through brute force attack. A measure such as blocking a user after several attempts can be used to allay brute force password guessing attacks. In such measures, accounts are usually blocked after three to five unsuccessful login attempts and can only be unblocked after a given period of time, through an unlock system, or intercession by an administrator. Account lockout systems should offer a balance between protecting accounts from illegal access and guarding users from being denied authorized access.

Leaving computers unattended to
Computers which have been left idle and unattended to can pose a threat to data as do other threats. This gives room to unauthorized accesses which can facilitate access to sensitive data and email messages.

This study shows that majority of the respondents (55.43%) will leave their computers idle when leaving the work premises. Again, majority of them (67.39%) will leave their computers unattended to when attending meetings and 81.52 % will not log off their computers when visiting the washroom. These actions put data at risk especially the risks of insider attacks associated with employees leaving their PCs unattended with active sessions running. A significant number of unauthorized access events may occur when someone sits down at another user's computer.

Connecting to networks outside the corporate infrastructure
Connecting to a private or a public network other than the corporate network infrastructure can pose a serious threat to data when the device used to connect is compromised. A device which has been compromised could be used as a gateway to a corporate infrastructure. Workers who connect their mobile devices to the home network could expose their devices to attacks, as the devices are outside the perimeter of the more secured corporate network. One of the IT personnel interviewed states that attackers could launch a silent attack against any device connected outside a corporate’s network when it is inactive pending the device to connect back to the corporate network.
Remote worker security
One of the dangerous ways of exposing data to attacks is by forwarding them to home. This activity can turn all of the security measures in an institution into a completely useless process. Workers have the tendency to move a non-finished work to their devices and personal computers at home so that they could work on it later at home. This is quite risky because often personal computers and devices are less secured compared to the corporate ones. While business operations become more and more dispersed and online, mobile workers increase the potential threat for data. One of the IT professionals indicated that improper handling of data such as moving files from an office device to a home computer that does not have proper IT security measures attracts information theft.

CONCLUSION
The research has established that despite the fact that technology is important in the information security framework, some detection technology alone was not enough to keep an organization secure from data breaches. Wireshark analysis needed to be factored in to make the security framework holistic.

Again, the research revealed that it is not enough to say that the role of people is to run the applications. People can either be the weakest or the strongest link in the security framework and therefore should compensate for the deficiencies in the available security technology. Therefore, there is the need to bring IT and human security together under a true information security management system.

Moreover, the increasing reliance on some technological components of information security, makes securing information system increasingly challenging. Quite a number of the security problems emanate from humans because humans have the tendency to show their unethical attitudes when using information systems. Humans are therefore critical part that, when ignored, could affect information security efficiency.

Improving security using technical means is important for organizations conducting business online as well as for organizations that are at the same time seeking to realize their missions and goals. However, implementing technical measures does not guarantee a more secure environment. All sorts of human factors can severely affect the management of security in personal and organizational setting.

Therefore, security is in the aspect of FTP servers needs more and better detection technique such as Wireshark analysis to enable us put better security measures in place.

Recommendations
We recommend that administrators must use Wireshark to analyze the network traffic in order to be able to read information about every packet.

Administrators must disable a user account instead of putting a lock on an account for a period of time. Disabling the account would prevent access to the account forever unless the authorized user of the account sees the administrator for reactivation.

Based on the findings of the study, it is recommended that for the human factor in information security be managed effectively, the following should be taken into consideration:

- Security awareness: Security consciousness and education are some of the most successful measures to mitigate the human factor threats to information security. In that regard, any information security plan should include a needs assessment that entails collecting information on the existing processes, the knowledge that is required of workers, and the cracks in the current information security.
- Endpoint Security: Quite a number of information in institutions is not centralized. Where there are centralized systems, information is often shared among workers and copied to different devices. Endpoint security is the notion that each device in an organization needs to be secured. It is recommended that sensitive information on portable devices like laptops and tablets should be encrypted. In addition, removable storage such as DVD drives and USB ports may be blocked if they are considered to be a major threat path for malware infections or data leakage. To secure endpoints, one needs extensive planning like applying policies that state that only certain computers like laptops can connect to particular networks. Usage of wireless (WiFi) access points should also be restricted.
ACKNOWLEDGMENT

The authors wish to acknowledge the efforts of all the sources of reference for this work.

REFERENCE


CITE AN ARTICLE