ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

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

Mustapha Adamu Mohammed*, Ashigbi Franlin Degadzor, Botchey Francis Effrim, Kwame Anim Appiah

[*] Department of Computer Science, Koforidua Technical University, Koforidua, Ghana
Department of Computer Science, Koforidua Technical University, Koforidua, Ghana
Department of Computer Science, Koforidua Technical University, Koforidua, Ghana
Department of Computer Science, Koforidua Technical University, Koforidua, Ghana

DOI: 10.5281/zenodo.802797

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.

LETERATURE 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:

- 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 and data and information are insecure.

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 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 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.

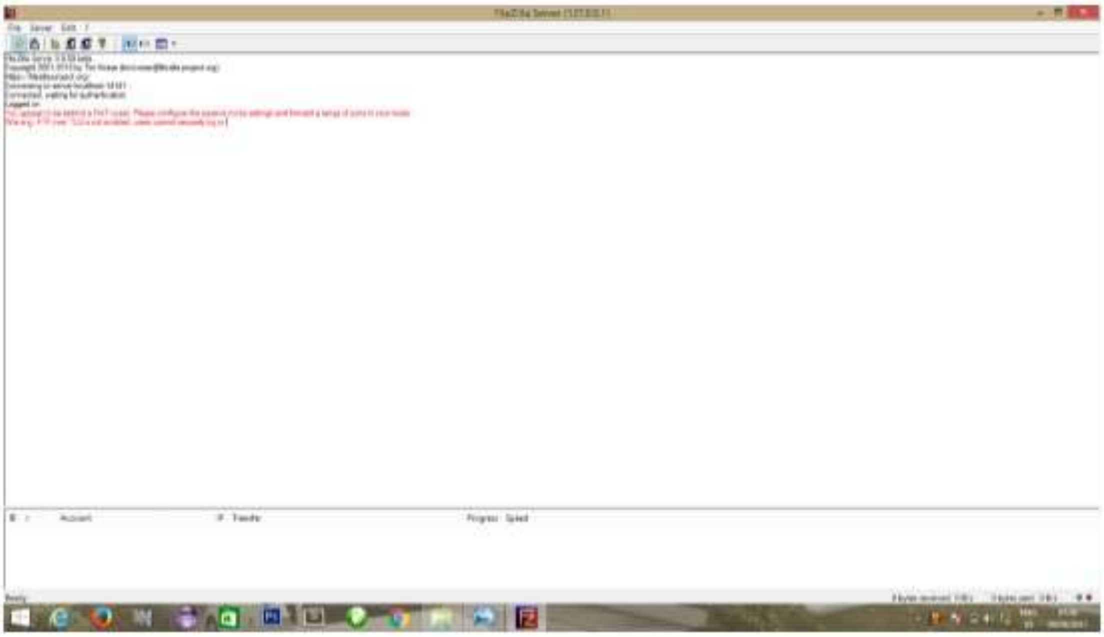


Figure 1 FTP Server (Filezilla Server) Interface

Figure 1 above represents the initial interface of the filezilla FTP server when launched and logged on.

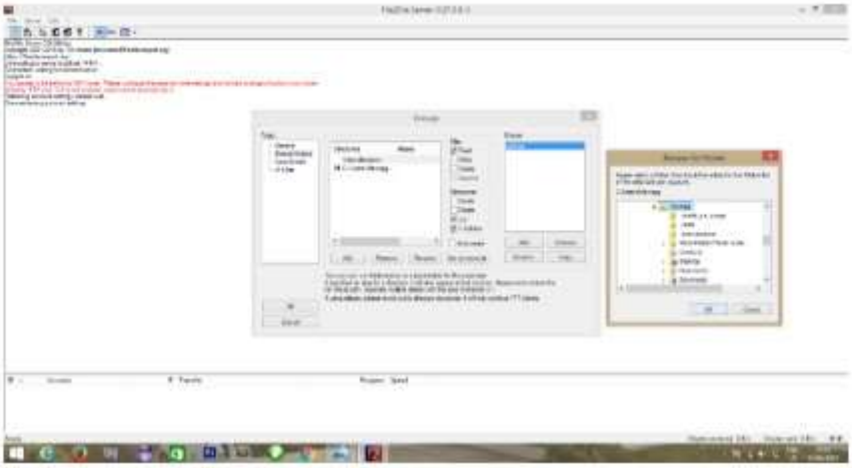
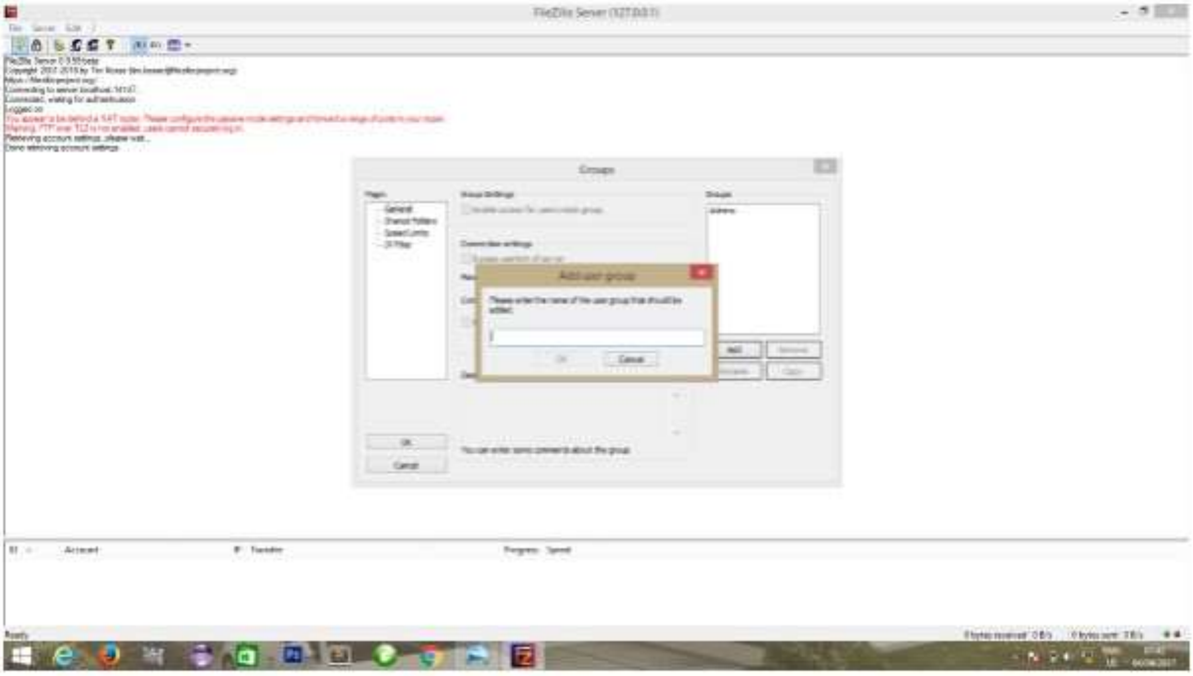


Figure 2 Creating a Directory for User Accounts

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 you Accounts



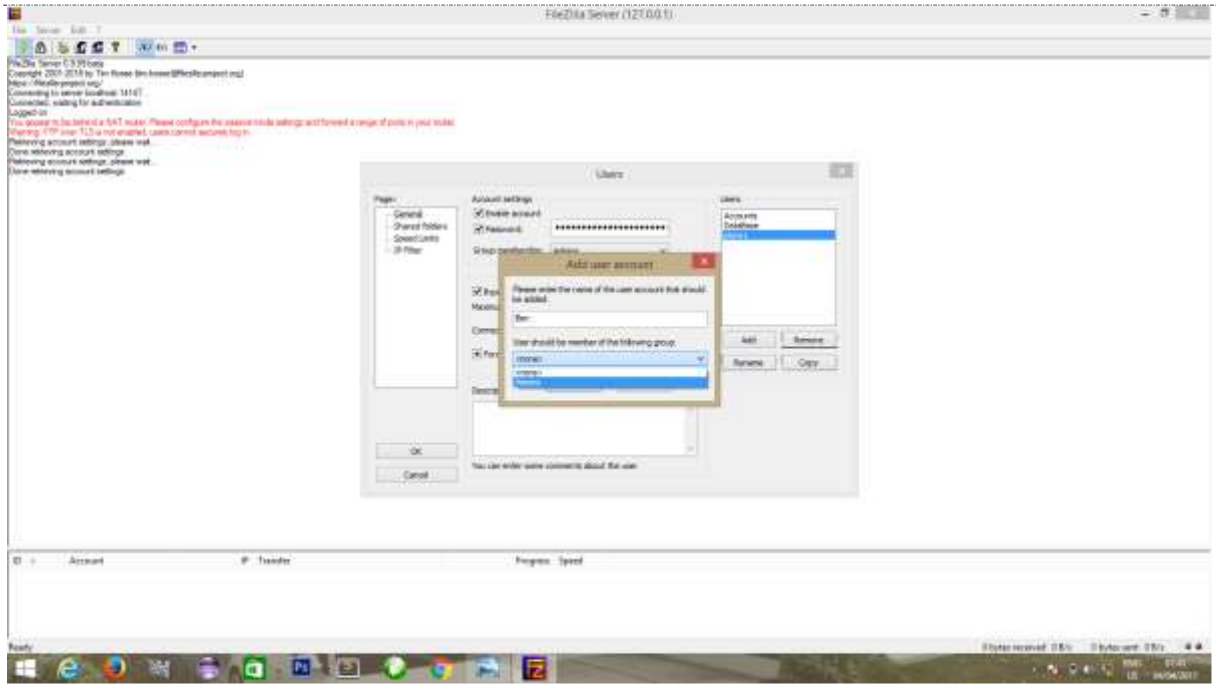
```
FileZilla Server 0.9.59 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router.
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving account settings, please wait...
Done retrieving account settings.
```

Figure 3 Creating Groups to Categorized Users

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



```
FileZilla Server 0.9.59 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router.
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
```

Users

Account settings
☑ Enable account
☑ Password: ••••••••••••••••••••••

Add user account

Please enter the name of the user account that should be added.

Ben

User should be member of the following group:

<none>

You can enter some comments about the user

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.

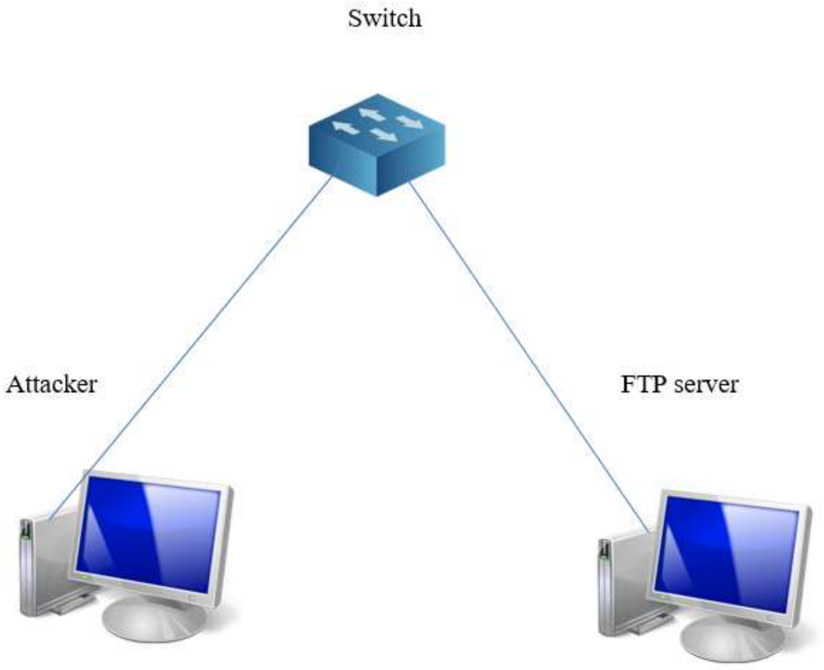


Figure 5 Setup of the lab used for experiment

Windows	
Windows with FTP server And wireshark	
Ip: 192.168.2.5	ip: 192.168.2.2
Mask: 255.255.255.0	Mask: 255.255.255.0

We chose windows for both server and attacker system

- The PC's were connected to the switch and configured with the IP addresses as shown in the previous slide.
- The PC with the IP address, 192.168.2.5 was used as the attacker's system. The PC with the IP address, 192.168.2.2 served as the FTP server.
- Net-Kit FTP server was installed along with wireshark on the FTP server system. (Any FTP server which is compatible on windows was used.)

RESULTS FROM EXPERIMENT

Brute Force Attack

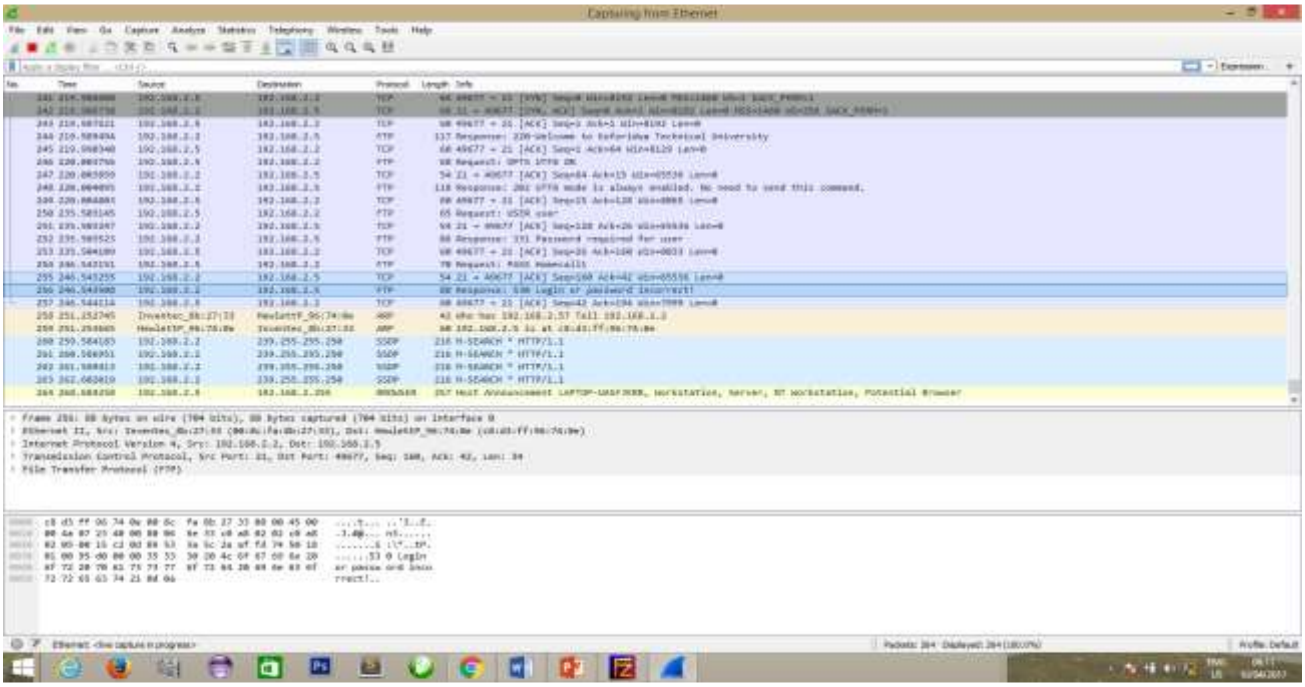
The experiment also found out that the system is vulnerable to brute force attacks. A brute force attack is a trial-and-error method used to obtain information such as a user password or personal details. In this attack a software (Filezilla ftp client) was used to generate a large number of consecutive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

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Wireshark Analysis of FTP with incorrect password


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Ethernet: <live capture in progress>
Packets: 264 · Displayed: 264 (100.0%)
Profile: Default

```
No.   Time        Source              Destination         Protocol  Length Info
  241 219.988888  192.168.2.5         192.168.2.2         TCP       66 49677 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  242 219.988758  192.168.2.2         192.168.2.5         TCP       66 21 → 49677 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  243 219.987021  192.168.2.5         192.168.2.2         TCP       60 49677 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
  244 219.989494  192.168.2.2         192.168.2.5         FTP      117 Response: 220-Welcome to Kafrelsheikh Technical University
  245 219.998340  192.168.2.5         192.168.2.2         TCP       60 49677 → 21 [ACK] Seq=1 Ack=64 Win=8129 Len=0
  246 220.003756  192.168.2.5         192.168.2.2         FTP       68 Request: OPTS UTF8 ON
  247 220.003959  192.168.2.2         192.168.2.5         TCP       54 21 → 49677 [ACK] Seq=64 Ack=15 Win=65536 Len=0
  248 220.004095  192.168.2.2         192.168.2.5         FTP      118 Response: 202 UTF8 mode is always enabled. No need to send this command.
  249 220.004881  192.168.2.5         192.168.2.2         TCP       60 49677 → 21 [ACK] Seq=15 Ack=128 Win=8065 Len=0
  250 235.583145  192.168.2.5         192.168.2.2         FTP       65 Request: USER user
  251 235.583247  192.168.2.2         192.168.2.5         TCP       54 21 → 49677 [ACK] Seq=128 Ack=26 Win=65536 Len=0
  252 235.585525  192.168.2.2         192.168.2.5         FTP       88 Response: 331 Password required for user
  253 235.584189  192.168.2.5         192.168.2.2         TCP       60 49677 → 21 [ACK] Seq=26 Ack=160 Win=8033 Len=0
  254 246.543191  192.168.2.5         192.168.2.2         FTP       70 Request: PASS [illegible]
  255 246.543255  192.168.2.2         192.168.2.5         TCP       54 21 → 49677 [ACK] Seq=160 Ack=42 Win=65536 Len=0
  256 246.543900  192.168.2.2         192.168.2.5         FTP       88 Response: 530 Login or password incorrect!
  257 246.544214  192.168.2.5         192.168.2.2         TCP       60 49677 → 21 [ACK] Seq=42 Ack=194 Win=7999 Len=0
  258 251.252745  Inventec_8b:27:33   HewlettP_96:74:0e   ARP       42 Who has 192.168.2.5? Tell 192.168.2.2
  259 251.258865  HewlettP_96:74:0e   Inventec_8b:27:33   ARP       60 192.168.2.5 is at c8:d3:ff:96:74:0e
  260 259.584185  192.168.2.2         239.255.255.250     SSDP     216 M-SEARCH * HTTP/1.1
  261 260.584951  192.168.2.2         239.255.255.250     SSDP     216 M-SEARCH * HTTP/1.1
  262 261.588413  192.168.2.2         239.255.255.250     SSDP     216 M-SEARCH * HTTP/1.1
  263 262.602419  192.168.2.2         239.255.255.250     SSDP     216 M-SEARCH * HTTP/1.1
  264 268.588250  192.168.2.5         192.168.2.255       BROWSER  257 Host Announcement LAPTOP-U[illegible], Workstation, Server, NT Workstation, Potential Browser

> Frame 256: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
> Ethernet II, Src: Inventec_8b:27:33 (00:8c:fa:8b:27:33), Dst: HewlettP_96:74:0e (c8:d3:ff:96:74:0e)
> Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.2.5
> Transmission Control Protocol, Src Port: 21, Dst Port: 49677, Seq: 160, Ack: 42, Len: 34
> File Transfer Protocol (FTP)

0000  c8 d3 ff 96 74 0e 00 8c  fa 8b 27 33 08 00 45 00   ....t.....'3..E.
0010  [illegible]                                          [illegible]
0020  [illegible]                                          [illegible]
0030  [illegible]                                          ......53 0 Login
0040  [illegible]                                          or passw ord inco
0050  72 72 65 63 74 21 0d 0a                              rrect!..
```

Figure 6: Wireshark analysis of FTP on incorrect password

Wireshark Analysis of FTP with incorrect password

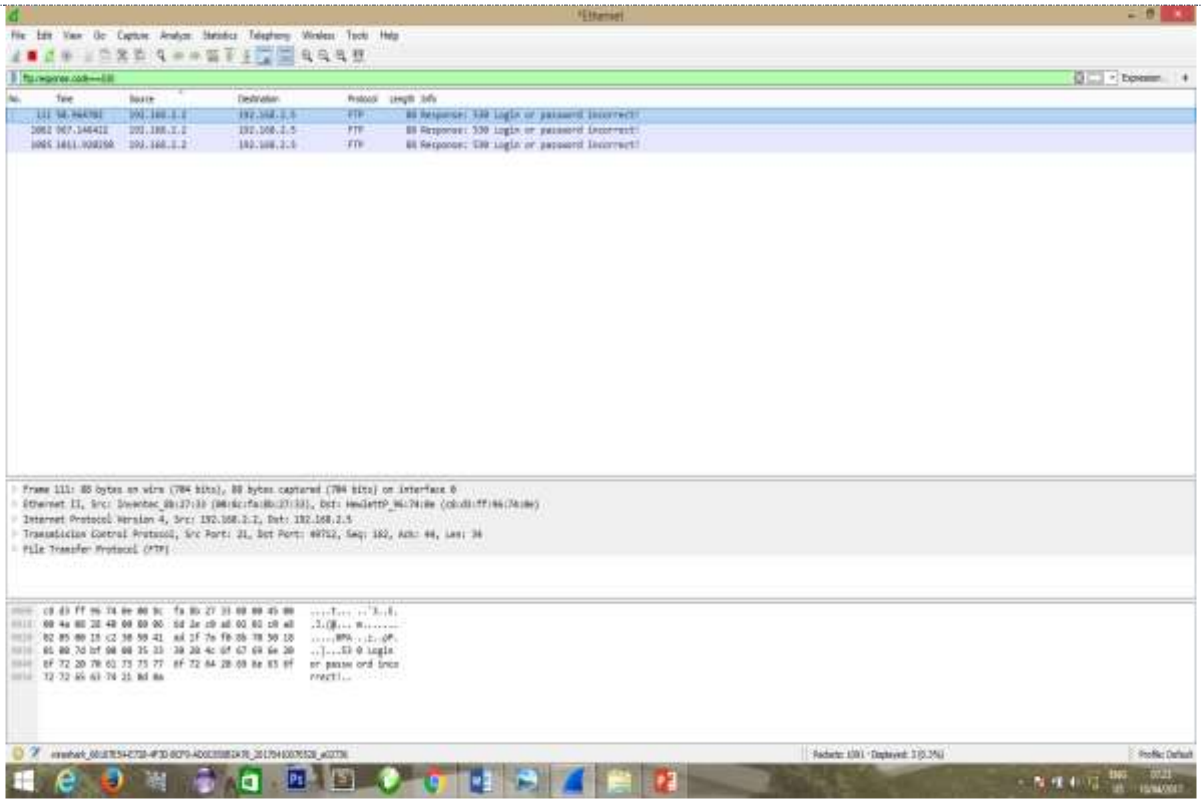
- When the incorrect password is sent from the client, the FTP server responds with 'Login Incorrect' message.
- FTP servers respond with a specific response code which is 530 when the login is incorrect which is shown in the previous slide.
- This response code can be used for detecting incorrect login 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.

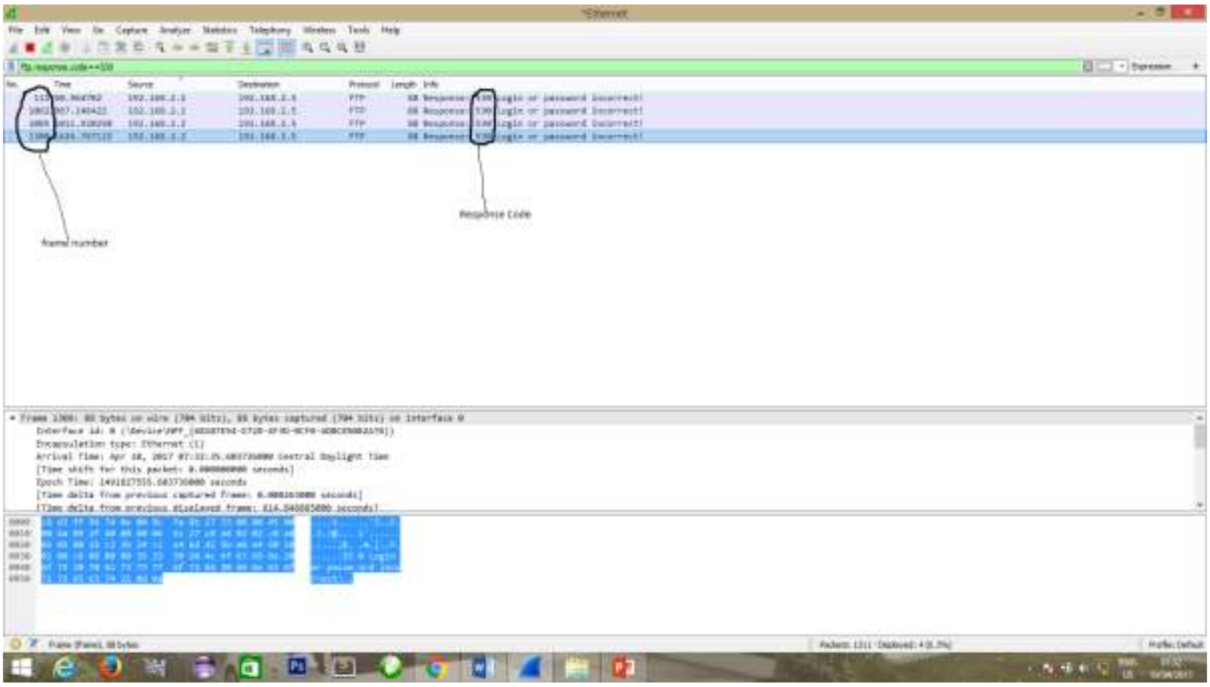


```
ftp.response.code==530

No.   Time          Source        Destination   Protocol Length Info
  111 58.964782     192.168.2.2   192.168.2.5   FTP      88 Response: 530 Login or password incorrect!
 1062 967.146422    192.168.2.2   192.168.2.5   FTP      88 Response: 530 Login or password incorrect!
 1085 1611.928298   192.168.2.2   192.168.2.5   FTP      88 Response: 530 Login or password incorrect!

> Frame 111: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
> Ethernet II, Src: Inventec_8b:27:33 (00:8c:fa:8b:27:33), Dst: HewlettP_96:74:8e (c8:d3:ff:96:74:8e)
> Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.2.5
> Transmission Control Protocol, Src Port: 21, Dst Port: 49752, Seq: 182, Ack: 44, Len: 34
> File Transfer Protocol (FTP)

0000  c8 d3 ff 96 74 8e 00 0c  fa 8b 27 33 08 00 45 00   ....t... ..'3..E.
0010  00 4a 08 28 40 00 80 06  6d 2e c0 a8 02 02 c0 a8   .J.(@... m.......
0020  02 05 00 15 c2 58 59 41  ad 1f 7a f8 8b 78 50 18   .....XYA ..z..xP.
0030  01 00 7d bf 00 00 35 33  30 20 4c 6f 67 69 6e 20   ..}...53 0 Login 
0040  6f 72 20 70 61 73 73 77  6f 72 64 20 69 6e 63 6f   or passw ord inco
0050  72 72 65 63 74 21 0d 0a                            rrect!..

wireshark_[illegible]    Packets: 1091 · Displayed: 3 (0.3%)    Profile: Default
```

Figure 7 Wireshark filter for brute force detection interface

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.



```
ftp.response.code==530

No.   Time          Source        Destination   Protocol Length Info
  111 58.964782     192.168.2.2   192.168.2.5   FTP      88 Response: 530 Login or password incorrect!
 1062 967.146422    192.168.2.2   192.168.2.5   FTP      88 Response: 530 Login or password incorrect!
 1085 1611.928298   192.168.2.2   192.168.2.5   FTP      88 Response: 530 Login or password incorrect!
 1308 1626.707118   192.168.2.2   192.168.2.5   FTP      88 Response: 530 Login or password incorrect!

v Frame 1308: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
    Interface id: 0 (\Device\NPF_{[illegible]})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 18, 2017 07:32:35.[illegible] Central Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1492[illegible] seconds
    [Time delta from previous captured frame: 0.000[illegible] seconds]
    [Time delta from previous displayed frame: 14.[illegible] seconds]

Frame (frame), 88 bytes    Packets: 1311 · Displayed: 4 (0.3%)    Profile: Default
```

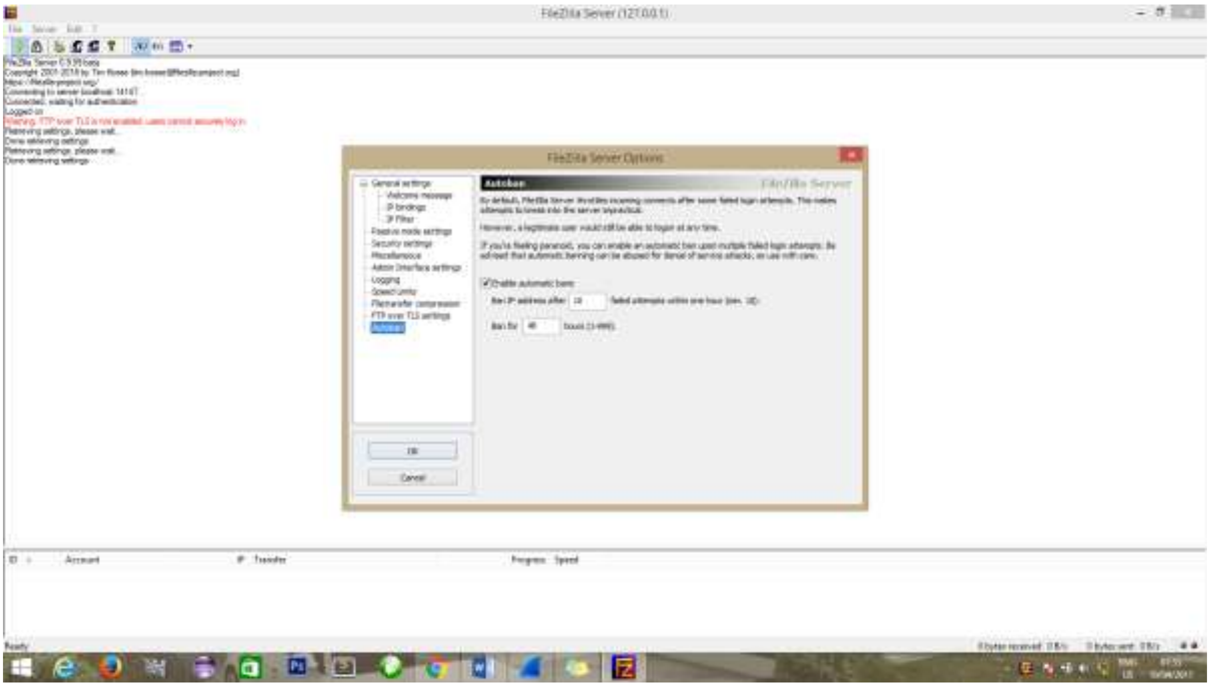
Figure 8 Frame number and response codes of Wireshark analysis

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.



```
FileZilla Server 0.9.59 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving settings, please wait...
Done retrieving settings
Retrieving settings, please wait...
Done retrieving settings
```

By default, FileZilla Server throttles incoming connects after some failed login attempts. This makes attempts to break into the server impractical.

However, a legitimate user would still be able to login at any time.

If you're feeling paranoid, you can enable an automatic ban upon multiple failed login attempts. Be advised that automatic banning can be abused for denial of service attacks, so use with care.

☑ Enable automatic bans

Ban IP address after 10 failed attempts within one hour (def. 10)

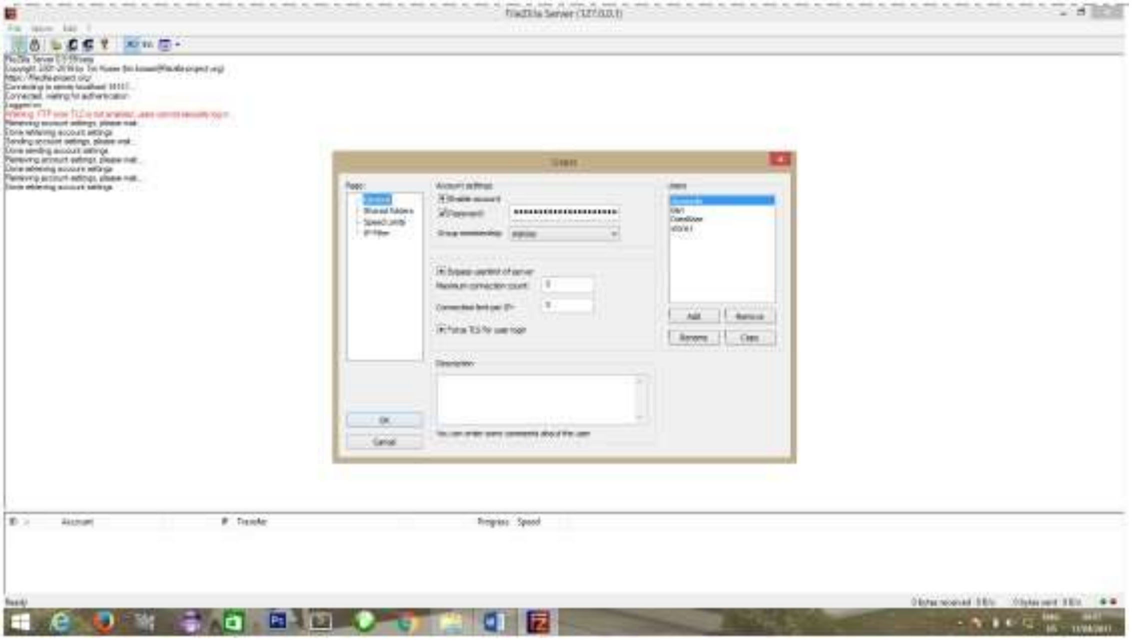
Ban for 48 hours (1-999)

Figure 9 Initiating the Auto Ban mechanism

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.



```
FileZilla Server [illegible]
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving account settings, please wait...
Done retrieving account settings
Sending account settings, please wait...
Done sending account settings
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
```

Figure 10 Disabling a user account (after an attack is been detected)

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 gate way 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. This allows the attacker to gain access to the network from the inside because the network will consider the devices as trusted ones as they are already associated with the 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.

ACKNOWLEDMENT

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

REFERENCE

[1] Anita, G., Kavita, K. and Kirandeep, K. (2013), Vulnerability assessment and penetration testing. *International Journal of Engineering Trends and Technology* 4 (13).
[2] Honeywell's Industrial IT solutions (2012), Amerchem cyber security vulnerability assessment
[3] James, A. K., Barton P. M., Eduardo, C. and Elisa, H. (2009), "First principles vulnerability assessment," (http://research.cs.wisc.edu/mist/VA.pdf), (accessed 2014 February 21)
[4] Kashefi, I., Kassiri, M., and Shahidinijad, A. (2013), A survey of on security issues in firewall: a new approach for classifying fire wall vulnerabilities. *Internationla Journal of Engineering Researh and Applications (IJERA)* 3 (2). pp. 585-591
[5] Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F., and Frantzen M. (2010), "Analysis of vulnerabilities in internet firewalls," (https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf), (accessed 2014 March).
[6] Lamar, A. (2012) "Types of threats to database security," (http://www.brighthub.com/computing/smb-security/articles/61402.aspx), (accessed 2014 March 18)
[7] Mitnick, K.D. and Simon, W.L. (2002). The Art of Deception: Controlling the Human Element, Indianapolis: Wiley Publishing Inc.
[8] Shulman, A. (2006), Top ten database security threats. Foster City, CA: Imperva Inc.
[9] Silver, P. (2013), Vulnerability assessment with application security. WA: F5 Networks, Inc.
[10] Smith, R. D. (2004), Public servers' vulnerability assessment report. Swansea: SANS Institute

CITE AN ARTICLE

Mohammed, M. A., Degadzor, A. F., Effrim, B. F., & Appiah, K. A. (2017). BRUTE FORCE ATTACK DETECTION AND PREVENTION ON A NETWORK USING WIRESHARK ANALYSIS. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 6*(6), 26-37. doi:10.5281/zenodo.802797