A Firewall based Hands-on Approach for Enhancing the Comprehension of FTP Traffic Filtering in Information Security Education

Zouheir Trabelsi
College of Information Technology, UAE University
United Arab Emirates
trabelsi@uaeu.ac.ae

ABSTRACT: *Network traffic filtering is an important topic in information security education at both undergraduate and graduate levels, and constitutes a major part of a general course on network security. Lectures on network traffic filtering cover mostly network packet filtering, mainly IP, TCP, UDP and ICMP packets, as well as common network services filtering, such as web and email services. In contrast to most common network services, FTP (File Transfer Protocol) is considered an unusual network service and requires special filtering mechanisms. FTP is an unusual service in that it uses two communication channels, called the Command channel (also known as the Control channel), and the Data channel. However, most common network service uses one communication channel for exchanging both command and data traffic.*

With the objective of enhancing information security education, this paper discusses what fundamental concepts the students need to know about the filtering of the unusual FTP network traffic. Also, to allow students to acquire hands-on skills on FTP traffic filtering using firewall technology, a set of comprehensive hands-on lab exercises are described. The paper does so in the hope that it will encourage the teaching of FTP network traffic filtering using a hands-on approach, when offering courses on network security. Finally, the paper discusses the effect of using a hands-on approach while teaching FTP traffic filtering concepts, on the students' grading performance and learning outcomes.

Keywords: Firewall, FTP traffic, Packet filtering, TCP/IP protocols, Course learning outcomes.

Received: 13 February 2016, Revised 15 March 2016, Accepted 19 March 2016

1. Introduction

Information security programs offer courses that cover various security fields, including mainly network security, cryptography, database and distributed systems security, software security, computer forensics, biometrics, operating systems security, cyber law, and ethical hacking. Usually, network security is a complicated course to teach requiring extensive hands-on experience to fully develop the students knowledge base [1]. The network security field covers typically network packet and service filtering, firewalls, network traffic analysis, network attacks, VPN (Virtual Private Network), and intrusion detection and prevention topics. All these security topics are included in NSTISSI 4011 [2] and CNSSI 4013 [3], which are required by the USA National

S-ecurity Agency to certify an institution as a National Center of Academic Excellence in Information Assurance Education (CAE/IAE).

Commonly, information security classes require both the preparation of regular lectures to teach students the fundamental security concepts, and the development of hands-on laboratory exercises. The courseware should be designed in a way that the laboratory exercises bring to students effective operational experiences on the use and implementation of security techniques and solutions, in additional to the regular lectures that explain the fundamental security concepts and mechanisms. In fact, a security education curriculum that does not give the students the opportunity to experiment in practice with security techniques cannot prepare them to be able to protect efficiently the confidentiality, integrity, and availability of computer systems and assets.

Nowadays, the need to use a practice and application oriented approach in information security education is paramount [4]. In fact, with the increase of information security programs, a number of laboratory experiments and laboratory-based courses have been developed for information security education [5-11]. However, even though, network packet and service filtering, is an import topic in information security education at both undergraduate and graduate levels, and constitutes a major part of a general course on network security, there are few hands-on approach based textbooks and academic papers that discuss the security concepts relative to this topic [1, 12-13]. Hence, to contribute to fill the aforementioned void in network service filtering education, and with the objective of enhancing information security education, this paper discusses what the students need to know about the fundamental security concepts relative to FTP service filtering. In addition, the paper describes a set of comprehensive hands-on lab exercises to allow students to acquire hands-on skills on FTP network traffic filtering using firewall technology. In contrast to most common network service, FTP is considered an unusual network service and requires special filtering mechanisms. FTP is an unusual service in that it uses two communication channels, called the Command channel (also known as the Control channel), and the Data channel. However, most common network services (such as web, telnet, and email) use one communication channel between the client and server, for exchanging both command and data traffic.

The rest of the paper is organized as follows: Section 2 introduces the required background regarding network service filtering concepts. Section 3 discusses what students need to know about FTP traffic filtering. Section 4 presents two models of lecture exercises that can be offered to students during lecture time. Section 5 discusses the effect of using a hands-on approach while teaching FTP traffic filtering concepts, on the students' grading performance and learning outcomes. Finally, Section 6 concludes the paper.

2. Background

2.1 TCP based network service

This paper assumes that the user has basic knowledge about TCP/IP protocols [14], the TCP three-way handshake mechanism, common Internet services [15], and network packet filtering using firewall technology [16].

In computer networking, there are many types of network services. A network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server architecture based on application layer network protocols, such as HTTP (for web) and FTP (for file and data transfer).

Commonly, the controls of the access to network services, is based on a set of filtering rules which reflect and enforce the organization's security policy [15]. In fact, the concept of network service filtering consists of determining whether the network packets relative to a particular service are allowed to enter or exit a network by comparing the packet's payload data and/or some fields' values located in the packets' headers to predefined values. Service and packet filtering technology is found in operating systems, firewalls, intrusion detection systems, and as a security feature for most routers and of some advanced switches. Within a network, the firewall is typically the first filtering device that encounters packets that attempt to enter an organization's network from the outside, and it is typically the last device to see exiting packets. It is the firewall's job to make filtering decision on every packet that crosses it: either to let it pass, or to drop it.

Filtering rules related to TCP bi-directional services (such as HTTP) have to allow both traffic directions to cross the firewall. TCP based network services are based on client-server architecture. That is, a TCP session has a client which is the computer that initiates the session, and a server which is the computer hosting the service. For example, the filtering rule shown in Table

1 allows bi-directional http traffic between the Web clients with IP addresses 192.168.1.1/24 and the Web server with the IP address 192.168.2.2/32 to across the firewall.

Direction	Source IP	Destination IP	Protocol	Source port	Destination port	Action
Client-to-Server	*192.168.1.1/24*	*192.168.2.2/32*	TCP	Any	80 (HTTP)	Allow

Table 1. A filtering rule to allow bi-directional HTTP traffic

2.2 TCP based network service filtering rules

When a client system attempts to establish a TCP connection to a system providing a service (the server), the client and server exchange firstly a sequence of messages to establish the TCP connection. This process is known as the three-way handshake. That is, the client begins by sending a SYN (synchronization) message to the server. The server then acknowledges the SYN message by sending a SYN-ACK (acknowledgment) message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then opened, and the service-specific data can be exchanged between the client and the server.

In a TCP session, if we consider only the SYN and ACK flags, there are only four types of exchanged TCP packets, as shown in Figure 1:

- Client-to-server packet: TCP packet with the flag SYN set, and the flag ACK unset.
- Server-to-client packet: TCP packet with the flags SYN and ACK set.
- Client-to-server packet: TCP packet with the flag SYN unset, and the flag ACK set.
- Server-to-client packet: TCP packet with the flag SYN unset, and the flag ACK set.

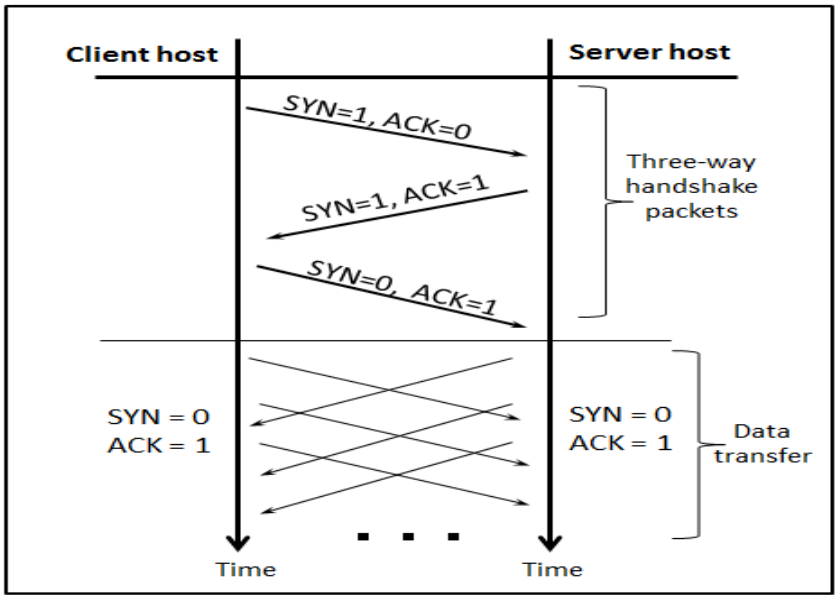


Figure 1. The types of packets exchanged in a TCP connection

Consequently, to allow TCP bi-directional service traffic, the firewall should allow the above four types of TCP packets to pass through. For example, using the TCP SYN and ACK flags, Table 2 lists the appropriate filtering rules that allow Web clients with IP addresses 192.168.1.1/24 and a Web server with the IP address 192.168.2.2/32 to across the firewall.

Rule	Direction	Source IP	Destination IP	Protocol	Source port	Destination port	SYN	ACK	Action
R1	Client-to-Server	*192.168.1.1/24*	*192.168.2.2/32*	TCP	Any	80	1	0	Allow
R2	Server-to-Client	*192.168.2.2/32*	*192.168.1.1/24*	TCP	80	Any	1	1	Allow
R3	Client-to-Server	*192.168.1.1/24*	*192.168.2.2/32*	TCP	Any	80	0	1	Allow
R4	Server-to-Client	*192.168.2.2/32*	*192.168.1.1/24*	TCP	80	Any	0	1	Allow

Table 2. An example of filtering rules using the SYN and ACK flags

3. FTP Network Traffic Filtering

3.1 Fundamental Concepts

FTP is a service that is based on TCP client-server architecture. In contrast to common TCP based network services, FTP is an unusual service in that it uses two communication channels, called the Command channel (also known as the Control channel), and the Data channel, as shown in Figure 2. In the case of most common TCP network services, there exists only one communication channel between the client and the server, to send commands and exchange data. FTP service utilizes two ports at the server side, a Command port (21) and a Data port (usually 20 or 1024-65535). In addition, FTP offers two connection modes namely, the Active FTP mode (also kwon as the Normal FTP mode), and the Passive FTP mode. The following subsections describe the two modes.

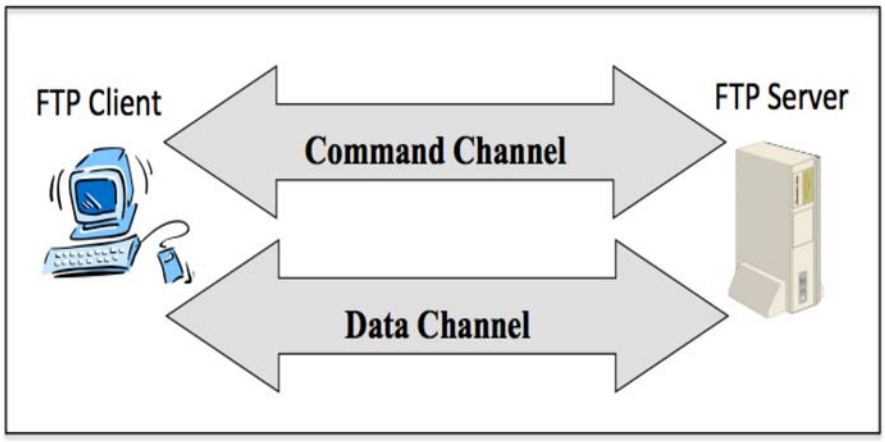


Figure 2. The two communication channels (Command channel and Data channel) of FTP service

3.1.1 Active FTP mode

In Active FTP mode, the FTP client connects from a random port (X > 1023) to the FTP server's command port, port 21. Then, the client starts listening to port X+1 and sends the command "PORT X+1" to the server. The value "X+1" represents the port number of the Data channel at the client side. The server will then initiate the Data channel. That is, the server connects back to the client's specified data port from its local data port, which is port 20 or a random port (Y > 1023).

Figure 3 shows the two TCP channels of an Active FTP connection. In step 1 of Figure3, the FTP client's command port (X > 1023) contacts the server's command port (21) and sends the command PORT (X+1). In step 2, the server then sends an ACK back to the client's command port. In step 3, the server initiates a connection on its local data port (Y) to the data port (X+1) specified earlier by the client. Finally, the client sends an ACK back as shown in step 4.

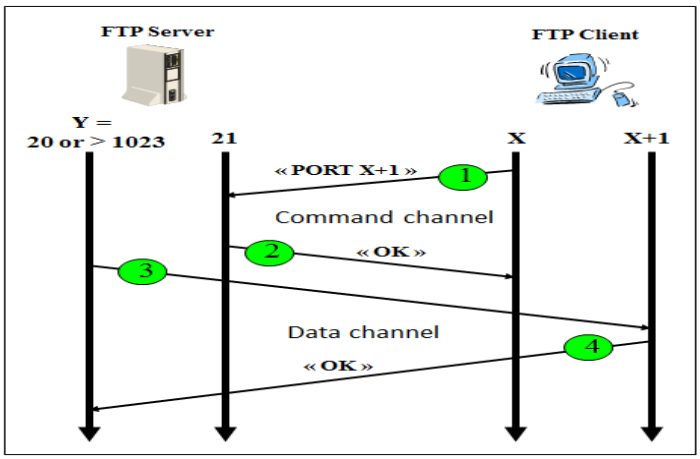


Figure 3. Command and Data channels of an Active FTP connection

3.1.2 Active FTP traffic filtering rules

To allow Active FTP traffic passes through the firewall, filtering rules should be implemented to allow the traffic of both the Command and the Data channels. Figure 4 shows the different TCP packets exchanged in an Active FTP session. The Command session is initiated by the FTP client, while the Data session is initiated by the FTP server.

In addition, since FTP uses TCP based channels, then for each channel, four filtering rules are required to allow the corresponding traffic to pass through the firewall. For example, if the FTP client is an internal host and the FTP server is an external host, then tables 3 and 4 list all the necessary filtering rules for the Command and Data channels, respectively.

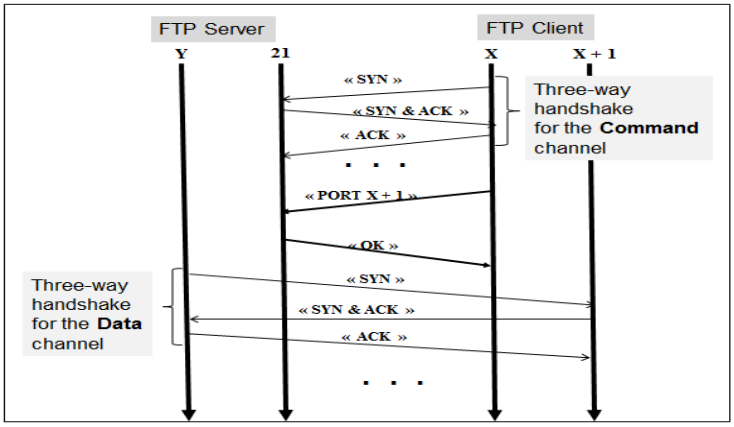


Figure 4. TCP packets used to initiate the channels of an Active FTP session

Direction	Source IP	Destination IP	Protocol	Source port	Destination port	SYN	ACK	Action
Outgoing	FTP client	FTP server	TCP	1024-65535	21	1	0	Allow
Incoming	FTP server	FTP client	TCP	21	1024-65535	1	1	Allow
Outgoing	FTP client	FTP server	TCP	1024-65535	21	0	1	Allow
Incoming	FTP server	FTP client	TCP	21	1024-65535	0	1	Allow

Table 3. Filtering rules for the Command channel in an Active FTP session

Direction	Source IP	Destination IP	Protocol	Source port	Destination port	SYN	ACK	Action
Incoming	FTP server	FTP client	TCP	20, 1024-65535	1024-65535	1	0	Allow
Outgoing	FTP client	FTP server	TCP	1024-65535	20, 1024-65535	1	1	Allow
Incoming	FTP server	FTP client	TCP	20, 1024-65535	1024-65535	0	1	Allow
Outgoing	FTP client	FTP server	TCP	1024-65535	20, 1024-65535	0	1	Allow

Table 4. Filtering rules for the Data channel in an Active FTP session

3.1.3 Filtering rules implementation for Active FTP traffic

Most firewalls include predefined filtering rules to allow and support Active FTP traffic. However, for educational purpose, to implement manually the filtering rules shown in tables 3 and 4, the firewall should allow manipulating the values of the TCP flags while creating a filtering rule. For example, Jetico Personal Firewall [17] offers such a capability, and allows specifying the values of most fields in packets while creating filtering rules. As an example, using Jetico Personal Firewall's GUI interface, Figure 5 shows the implementation of the height filtering rules of tables 3 and 4, required to allow Active FTP traffic. We assume that the IP addresses of the internal FTP client and the external FTP server are 192.168.1.101 and 192.168.1.104, respectively. The default security policy is "Deny All".

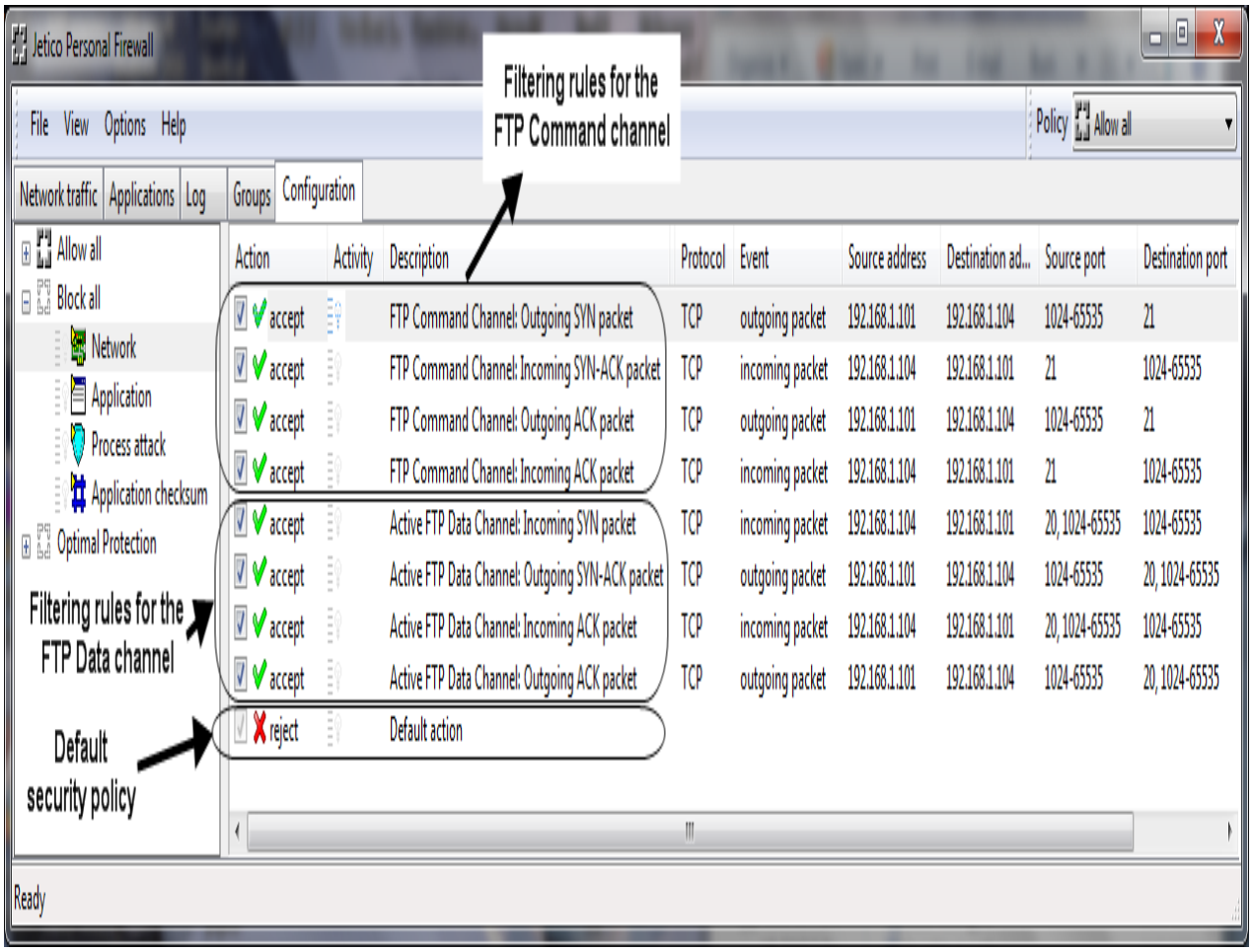


Figure 5. Filtering rules implementation for Active FTP session using Jetico Personal Firewall's GUI interface

As an example, Figure 6 shows the detailed contents of the first filtering rule of an Active FTP session. The filtering rule allows outgoing SYN packets for the Command channel.

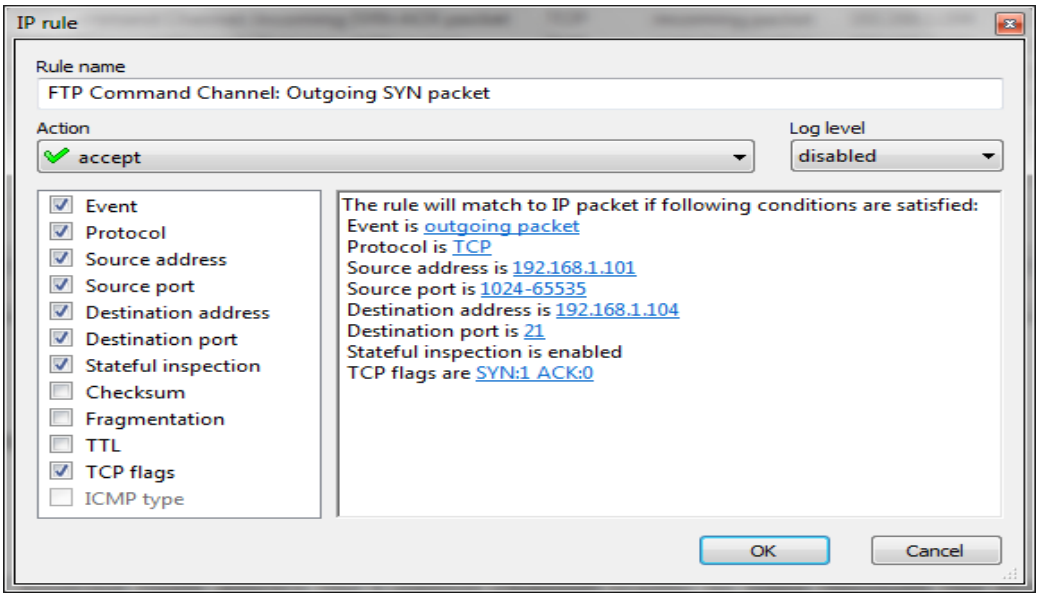


Figure 6. A filtering rule for allowing outgoing SYN packets for the Command channel

3.1.4 Security Issue with Active FTP mode

Commonly, in a TCP client-server session, client hosts initiate the session. However, in an Active FTP session, the FTP client initiates the Command session, and the FTP server initiates the Data session. This is a major security issue, since for the firewall, outside hosts are allowed to initiate TCP sessions on internal hosts. This type of connection is usually blocked since it allows malicious external hosts to generate attacks against the internal hosts. That is, in an Active FTP session, a malicious host can exploit the filtering rules corresponding to the Data channel to establish TCP connections with the internal hosts. This vulnerability would allow the malicious host to easily attack the internal hosts. Denial of Service (DoS) attacks or remote controlled program based attacks (such as Trojan horses) are examples of attacks that malicious hosts can perform against the internal hosts. Therefore, Active FTP is beneficial to the FTP server admin, but detrimental to the client side admin.

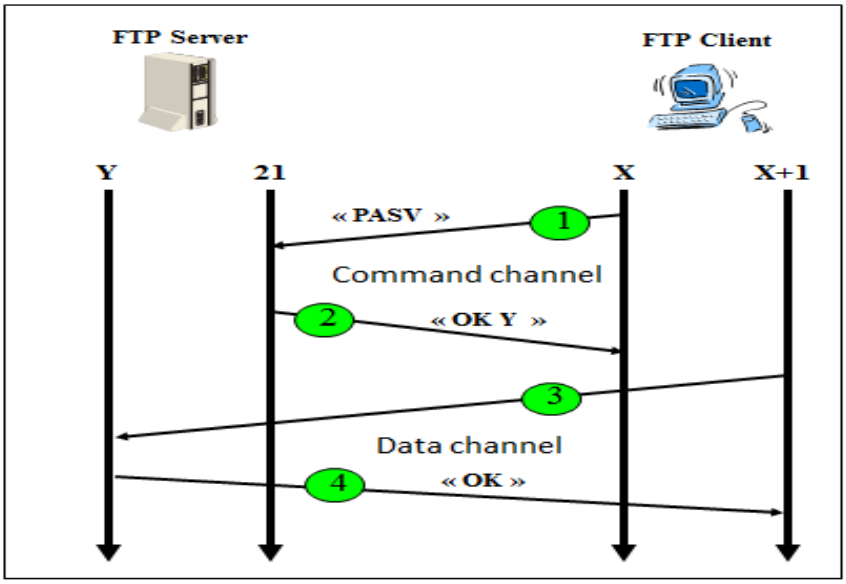


Figure 7. Command and Data channels of a Passive FTP connection

3.1.5 Passive FTP Mode

In order to resolve the security issue with the Active FTP mode, a different method for FTP connections was developed. This is known as Passive FTP mode. In this mode, the FTP client initiates both the Command and Data channels, hence solving the security issue with the Active FTP mode. The FTP client uses the command "PASV" to tell the server that the FTP session will be in Passive mode.

Figure 7 shows the two TCP channels of a Passive FTP connection. When opening an FTP connection, the client opens two random ports locally (X > 1023 and X+1). The first port contacts the server on port 21, then the client issues the "PASV" command (Step 1). The result of this is that the server then opens a port Y (20 or a random port (Y > 1023)) and sends the command "PORT Y" back to the client (Step 2). The client then initiates the connection from port "X+1" to port Y on the server to transfer data (Step 3). Finally, in Step 4, the server sends back an ACK to the client's data port.

3.1.6 Passive FTP Traffic Filtering

To allow Passive FTP traffic passes through the firewall, filtering rules should be implemented to allow the traffic of both the Command and the Data channels. Figure 8 shows the different TCP packets exchanged in a Passive FTP session. The Command and Data sessions are both initiated by the FTP client.

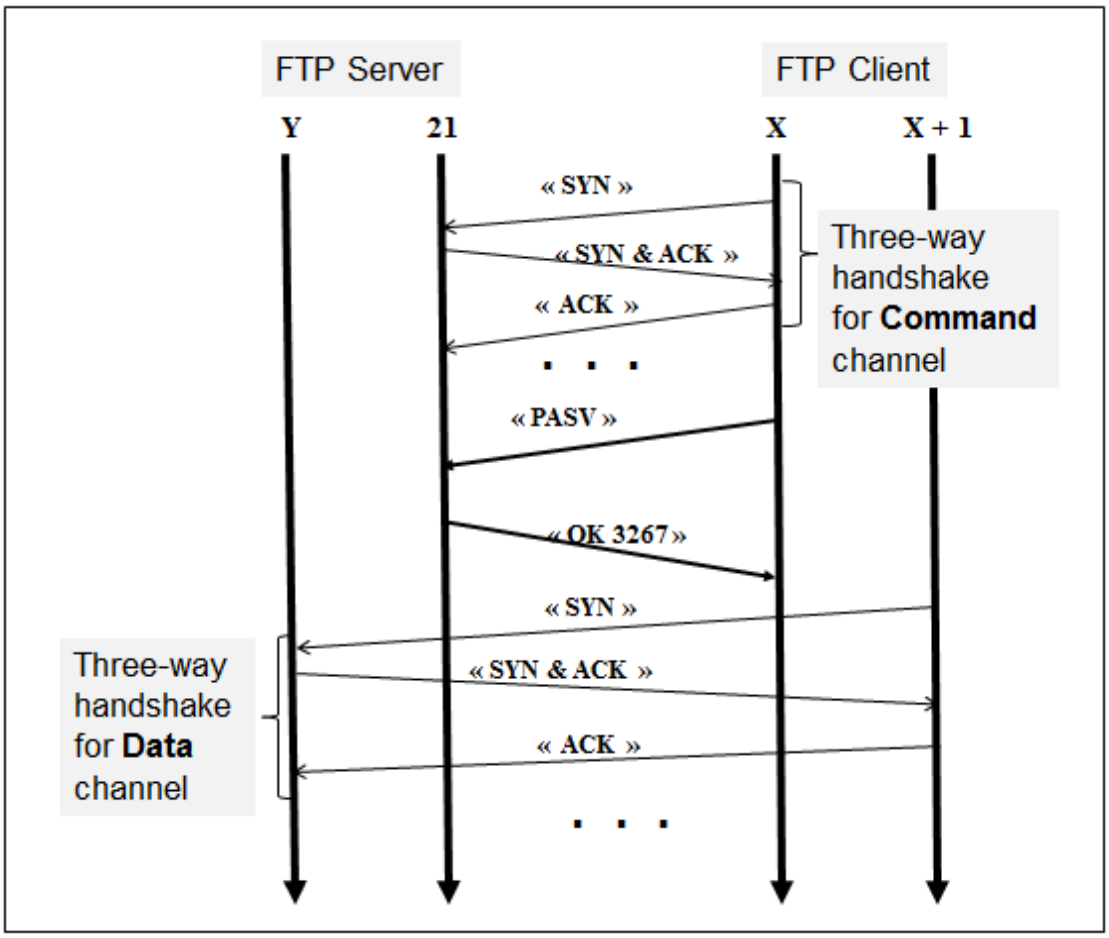


Figure 8. TCP packets used to initiate a Passive FTP session

In addition, since FTP uses TCP based channels, then for each channel, four filtering rules are required to allow the corresponding traffic to pass through the firewall. For example, if the FTP client is an internal host and the FTP server is an external host, then Table 5 lists all the filtering rules for the Command and Data channels, respectively.

Direction	Source IP	Destination IP	Protocol	Source port	Destination port	SYN	ACK	Action
Outgoing	FTP client	FTP server	TCP	1024-65535	21, 20, 1024-65535	1	0	Allow
Incoming	FTP server	FTP client	TCP	21, 20, 1024-65535	1024-65535	1	1	Allow
Outgoing	FTP client	FTP server	TCP	1024-65535	21, 20, 1024-65535	0	1	Allow
Incoming	FTP server	FTP client	TCP	21, 20, 1024-65535	1024-65535	0	1	Allow

Table 5. Filtering rules for the Command and Data channels in a Passive FTP session

3.1.7 Filtering rules implementation for Passive FTP traffic

As an example, using Jetico Personal Firewall's GUI interface, Figure 9 shows the implementation of the four filtering rules of Table 5, required to allow Passive FTP traffic.

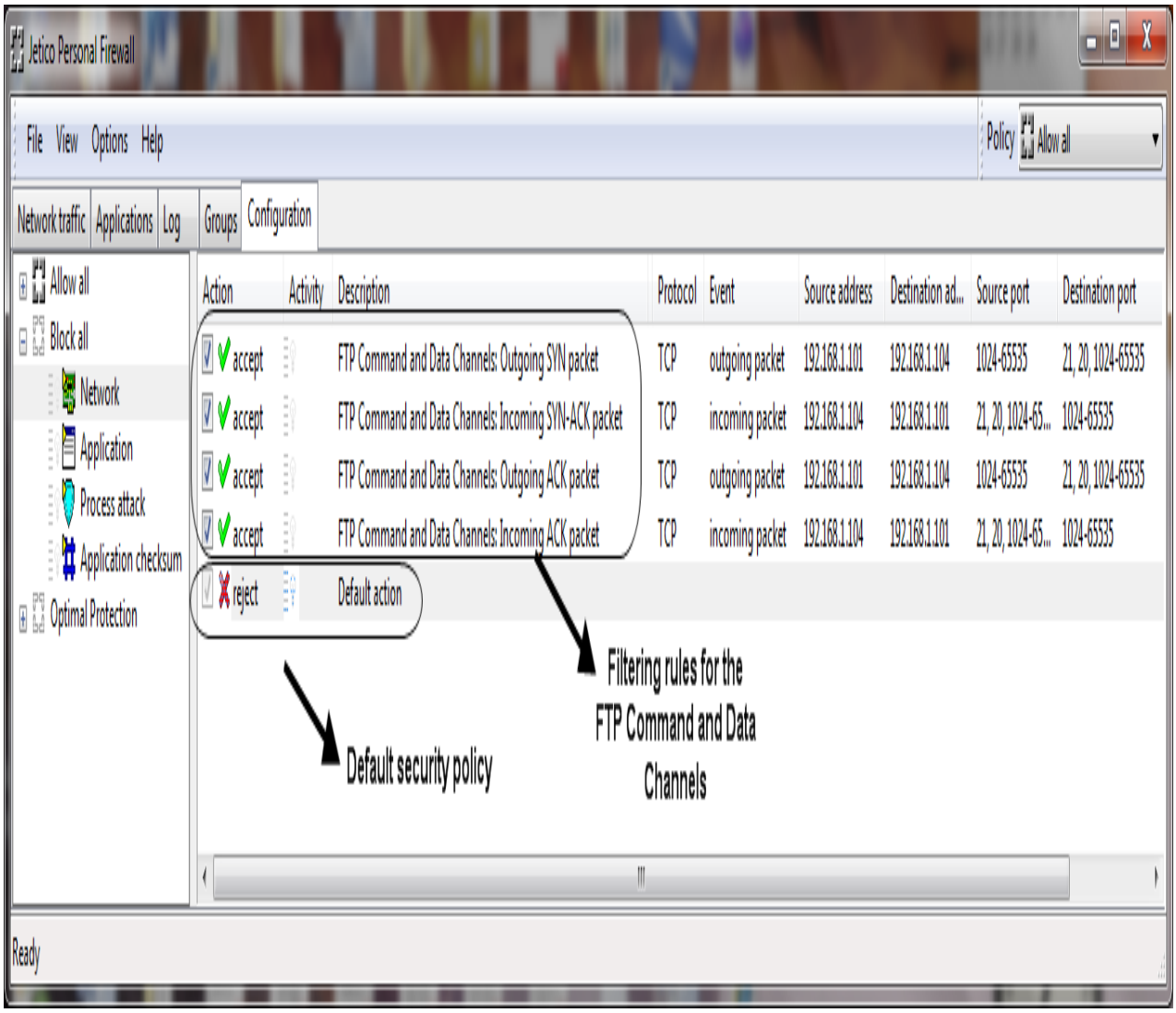


Figure 9. Filtering rules implementation for Passive FTP session using Jetico Personal Firewall's GUI interface

Figure 10 shows the details of the first filtering rule in a Passive FTP session. The filtering rule allows outgoing SYN packets for both Command and Data channels.

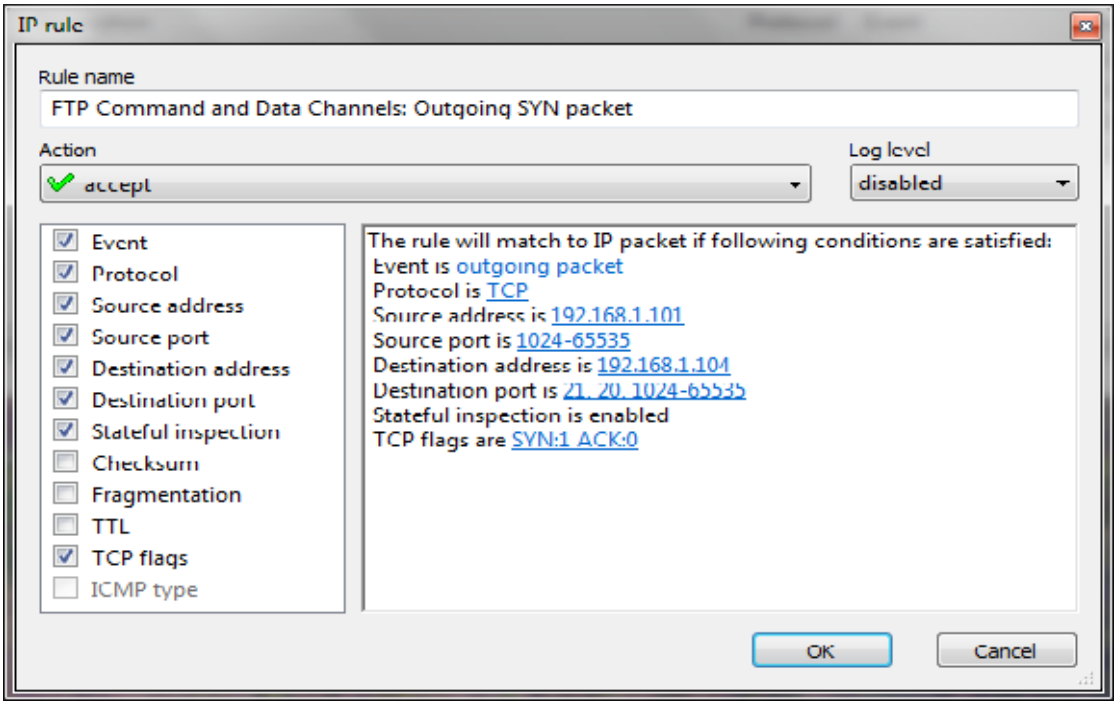


Figure 10. Filtering rule for allowing outgoing SYN packets for the Command and Data channels

3.1.8 Security Issue with Passive FTP mode

It is unquestionable that the Passive mode is a more secure mode compared to the Active mode. However, the major security issue with the Passive mode is that FTP client hosts are allowed to initiate connection to high numbered ports on the FTP server. This may open up a whole range of security problems on the FTP server side. However, since admins of FTP servers will need to make their servers accessible to the greatest number of clients, they will almost certainly need to support passive FTP session. In fact, the security issue with the Passive mode can be minimized by using FTP servers that allow admins to specify a limited port range for the FTP servers to use. In addition, firewalls will block any port which does not belong to that range. Therefore, Passive FTP is beneficial to the client, but detrimental to the FTP server admin.

On the other hand, the use of FTP Passive mode within a network involves supporting and troubleshooting clients which do (or do not) support Passive FTP mode. In addition, nowadays, users prefer to use their web browsers as FTP clients. If the firewall is configured to allow only Passive FTP mode, then the browsers should be configured to connect in FTP Passive mode. This requires additional support work and troubleshooting clients. For example, Figure 11 shows how to change Internet Explorer 11 to connect to a FTP server in Passive mode.

3.2. Hands-on lab exercise

The learning objective of this hands-on lab exercise is for students to better anatomize the concept of Active and Passive FT modes through the sniffing and analyzing of FTP traffic.

3.2.1 Part #1: Active FTP session traffic sniffing

The following experiment describes how to sniff and analyze the packets of an Active FTP session. The experiment consists of the following steps:

- Step 1: Configure a Web browser (or a FTP client tool, such as LeapFTP tool [18]) as an Active FTP client (This is the default setting for most Web browser and FTP clients).
- Step 2: Connect to a FTP server using the Active FTP mode and sniff the session packets, using a sniffer tool, such as CommView Sniffer [19].

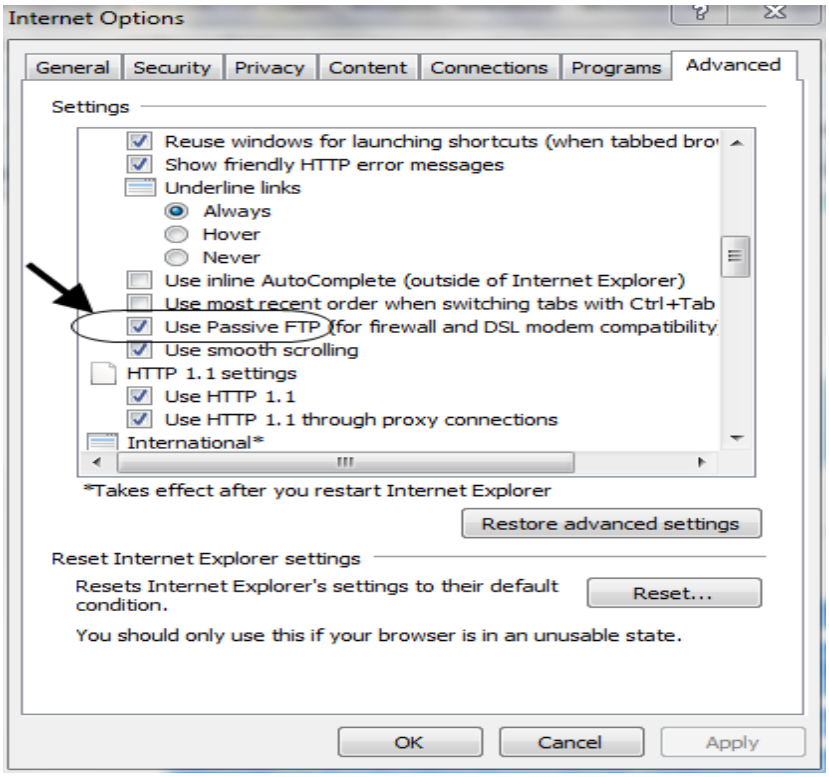


Figure 11. Configuring Internet Explorer 11 to connect in Passive FTP mode

- Step 3: Analyze the Active FTP session packets
- Step 4: Identify the Command and Data channels' ports of the FTP session, as shown in Figure 3. That is:
    - o X is the client port number for the Command channel
    - o (X +1) is the client port number for the Data channel.
    - o Y is the server port number for the Data channel.

For example, Figure 12 shows the TCP packet number 19 of the Command channel in the Active FTP session that includes the port number for the Data channel (PORT X+1). The packets shown in Figure 12 have been captured by CommView sniffer tool.

The FTP header of packet 19 contains the command "PORT", the IP address of the host hosting the FTP client, and the value of the port (X + 1) of the Data channel at the client side.

3.2.2 Part #2: Passive FTP session traffic sniffing

The following experiment describes how to sniff and analyze the packets of a Passive FTP session. The experiment consists of the following steps:

- Step 1: Configure a Web browser (or a FTP client) as a Passive FTP client
- Step 2: Connect to the FTP server and sniff the session packets.
- Step 3: Analyze the Passive FTP session packets
- Step 4: Identify the Command and Data channels' ports of the Passive FTP session, as shown in Figure 7. That is:
    - o X is the client port number for the Command channel.
    - o X+1 is the client port number for the Data channel.

o Y is the server port number for the Data channel.

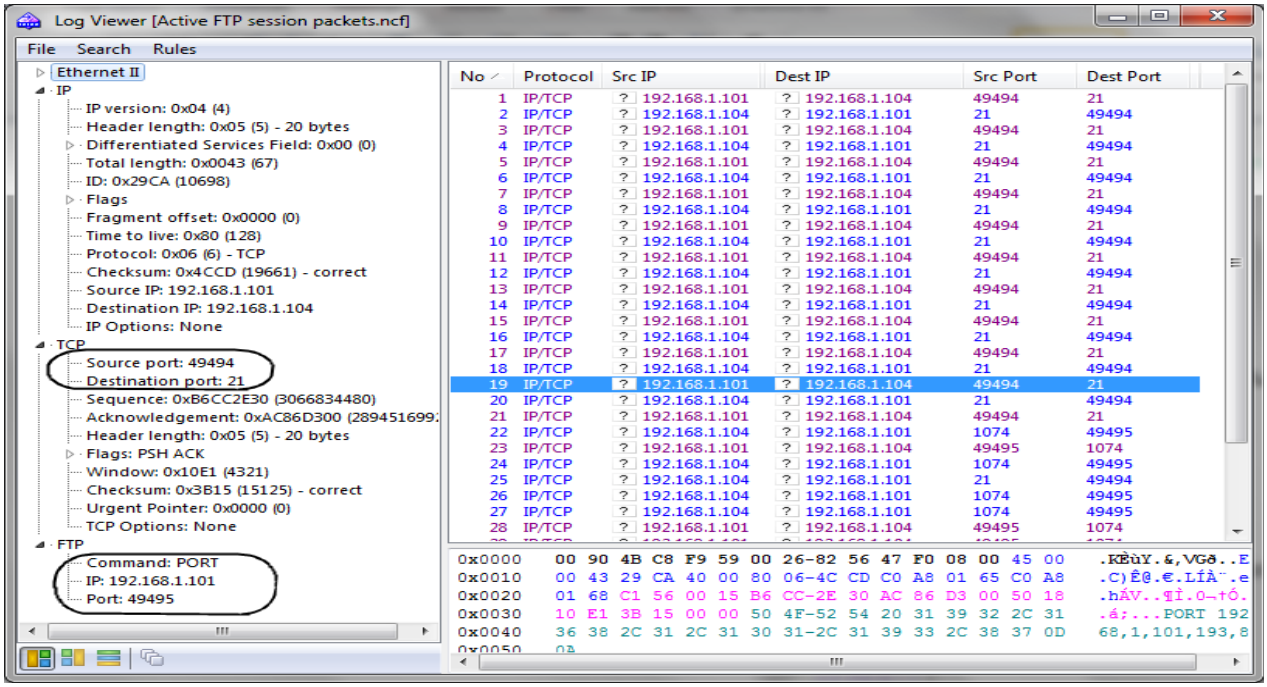


Figure 12. The TCP packet of the Command channel that includes the FTP client port number for the Data channel (PORT X+1)

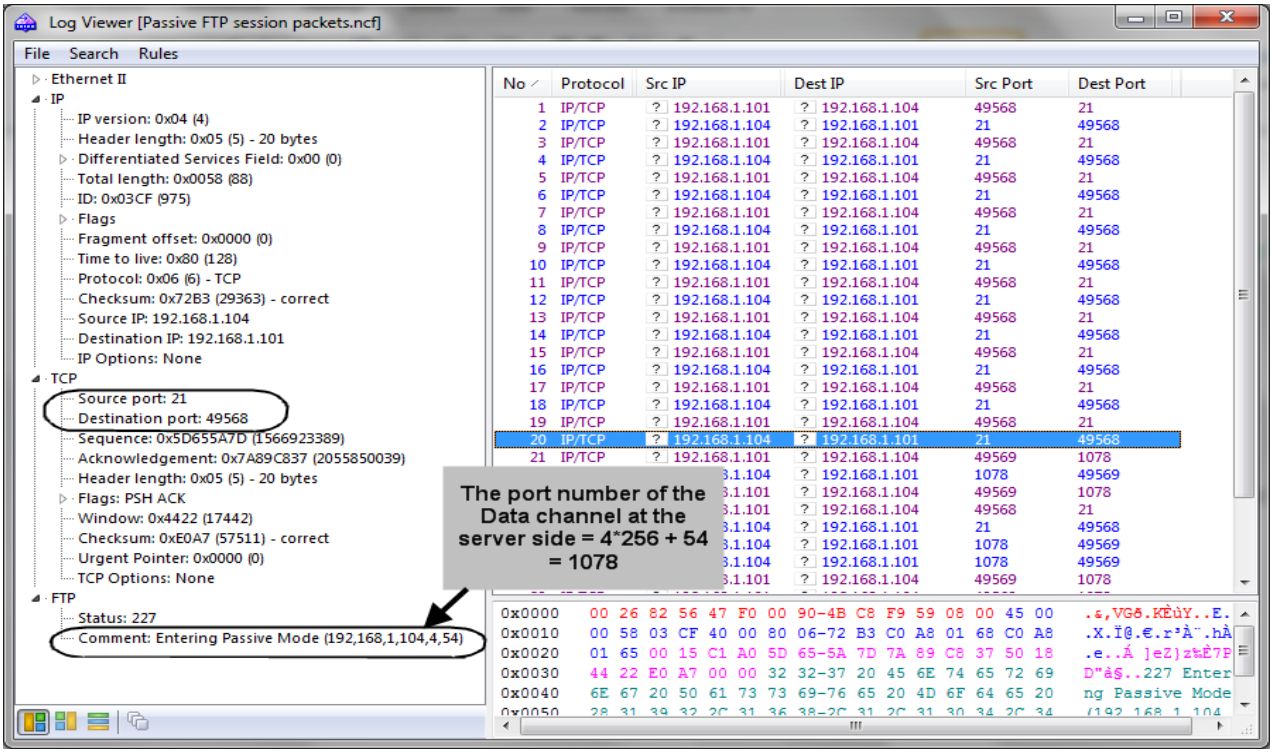


Figure 13. The TCP packet that includes the port number of the Data channel at the server side

For example, Figure 13 shows the TCP packet number 20 of the Command channel in the Passive FTP session that sends the port number of the Data channel at the server side. The format of the PORT command is formatted as a series of six numbers separated by commas. The first four octets are the FTP server's IP address while the last two octets comprise the port that will be used for the data connection. To find the actual port, multiply the fifth octet by 256 and then add the sixth octet to the total. Thus, in the example below the port number is ((4*256) + 54), or 1078.

4. Models of Lecture Exercises

This section provides example models of exercises that can be offered to students during lectures on FTP traffic filtering.

1. Exercise 1

In this exercise, students are asked to write the appropriate firewall filtering rules for the following security policy.

Question:

We assume that your LAN network is protected by a firewall, and you want to allow your internal hosts to communicate with the external FTP server (With IP address: IP-2), using only the FTP PASSIVE mode (The Normal mode should be denied). Also, we assume that the port number of the Data channel at the server side is 20. The default security policy is "Deny All".

Write the appropriate firewall filtering rules for this security policy.

Solution:

Rule	Direction	Protocol	Source IP	Destination IP	Source Port	Destination Port	SYN	ACK	Action
FTP Command and Data Channels									
R1	Outgoing	TCP	LAN	IP-2	Any	20, 21	1	0	Allow
R2	Incomimg	TCP	IP-2	LAN	20, 21	Any	1	1	Allow
R3	Outgoing	TCP	LAN	IP-2	Any	20, 21	0	1	Allow
R4	Incomimg	TCP	IP-2	LAN	20, 21	Any	0	1	Allow
Deny FTP Normal mode									
R5	Incomig	TCP	IP-2	LAN	21	Any	1	0	Deny
Default Security Policy									
Default	Any	Any	Any	Any	Any	Any	Any	Any	Deny

2. Exercise 2

In this exercise, students are asked to identify the mode of a given FTP session (Normal or Passive mode) by analyzing the Command and Data channels' packets.

Question:

We assume that the following packets belong to a FTP session.

(1) Write the details of the packets (Packet number, Source IP, Destination IP, Source port, Destination port, and TCP flags) corresponding to the Command and Data channels of the FTP session, using the chronological order.

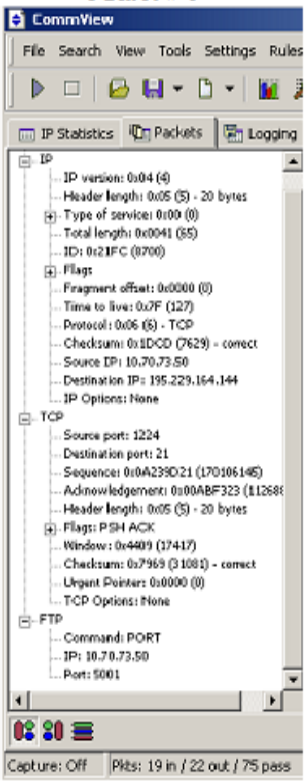
(2) Indicate the mode of the FTP session (Normal or Passive), and justify your answer.

Solution:

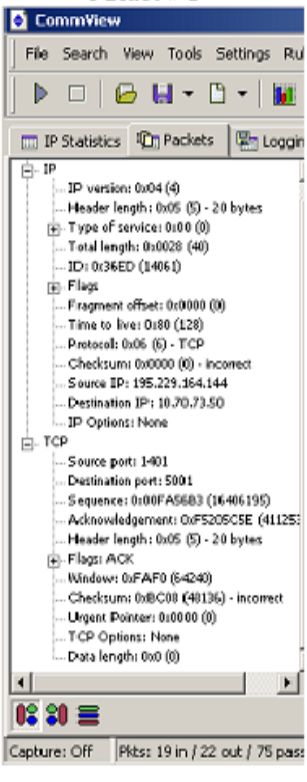
(1) Figure 14 summarizes the chronological order of the packets of the Command and Data channels of the FTP session. In addition, Table 6 shows the details of the packets corresponding to the Command and Data channels of the FTP session.

(2) The mode of the FTP session is the Normal mode, since the FTP server initiated the Data channel, as shown in Packet #7.

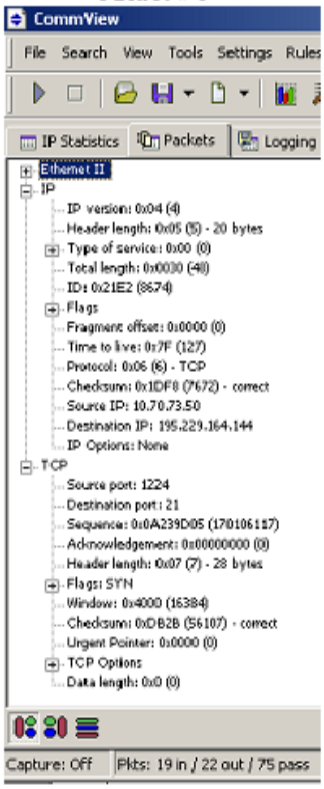
Packet # 1



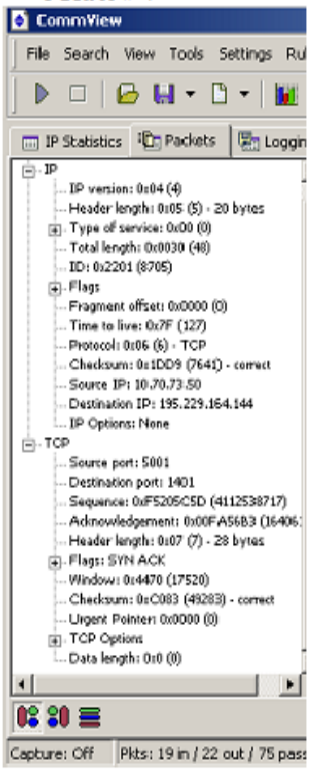
Packet # 2



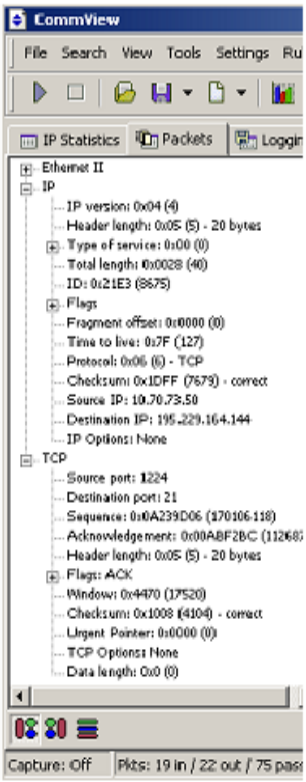
Packet # 3



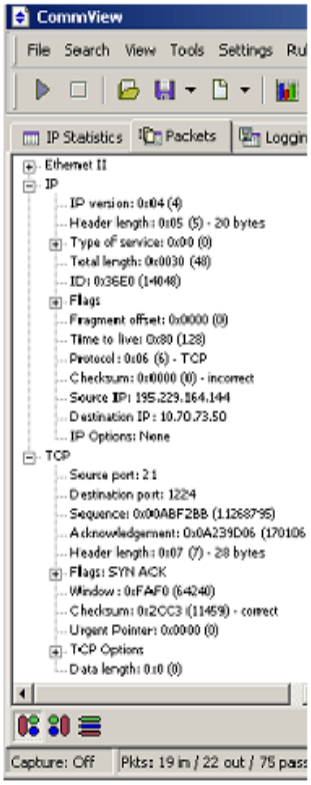
Packet # 4



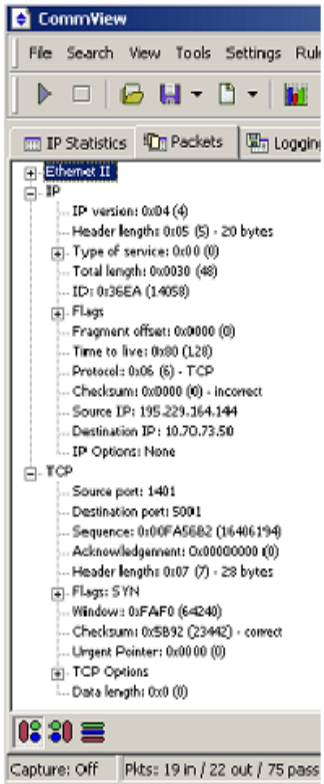
Packet # 5



Packet # 6



Packet # 7



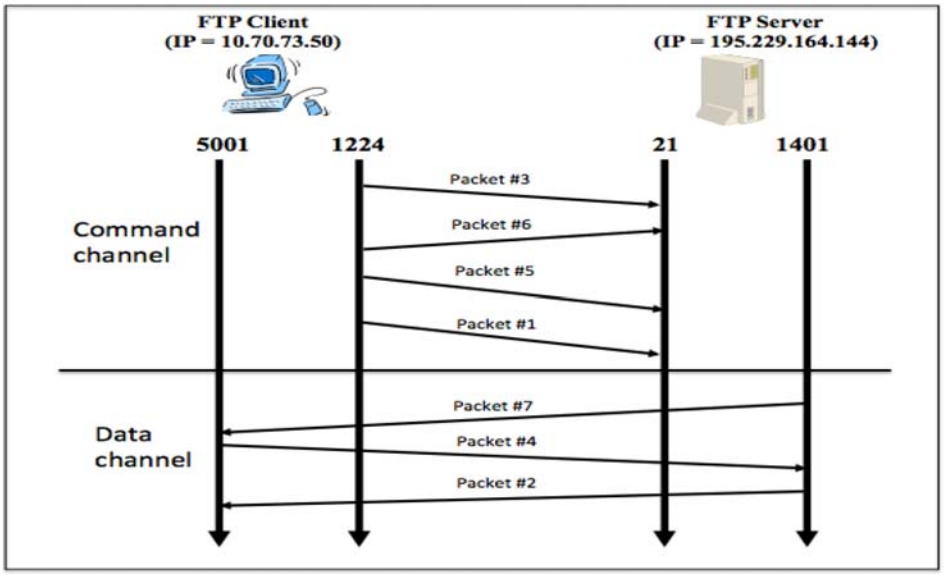


Figure 14. The chronological order of the Command and Data channels' packets

Packet number	Source IP	Destination IP	Source Port	Destination Port	SYN	ACK	PSH	RST	URG	FIN
FTP Session's Command Channel										
Packet #3	10.70.73.50	195.229.164.144	1224	21	1	0	0	0	0	0
Packet #6	195.229.164.144	10.70.73.50	21	1224	1	1	0	0	0	0
Packet #5	10.70.73.50	195.229.164.144	1224	21	0	1	0	0	0	0
Packet #1	10.70.73.50	195.229.164.144	1224	21	0	1	1	0	0	0
FTP Session's Data Channel										
Packet #7	195.229.164.144	10.70.73.50	1401	5001	1	0	0	0	0	0
Packet #4	10.70.73.50	195.229.164.144	5001	1401	1	1	0	0	0	0
Packet #2	195.229.164.144	10.70.73.50	1401	5001	0	1	0	0	0	0

Table 6. The details of the Command and Data channels' packets

5. Evaluation

5.1 Learning Outcomes Evaluation Process

The discussed security concepts on FTP traffic filtering have been covered in our Network Border Control course (SECB 358) since the academic year 2008/2009. The course covers mainly network packet and services filtering, firewall technology, stateless and stateful firewalls, firewall based network architectures, and VPN.

SECB358 course has five learning outcomes (COs), as shown in Table 7, which describe what students can do as a results of their educational experiences. The active verbs of the learning outcomes have been selected using the Bloom's taxonomy for student learning outcomes [20]. The SECB358 course is designed in such as way that students will develop basic learning skills and acquire foundation knowledge in the earliest lectures of the course.

As they move to more advanced topics, they develop higher-order learning skills and more advanced understanding of the field of network packet and service filtering, firewalls and VPN. This development change can be described in terms of the increasingly sophisticated behaviors represented at higher levels in Bloom's taxonomy.

On the other hand, eight course topics were identified and mapped to SECB358 course's leaning outcomes. FTP traffic filtering is among these course topics. Also, four assessment tools have been selected to assess the achievements of the leaning

Outcome	Level of Bloom's Taxonomy
CO1: Describe TCP/IP protocols and network services	Understanding (2)
CO2: Explain common security threats	Understanding (2)
CO3: Practice configuration of firewalls and VPNs	Application (3)
CO 4: Design firewall filtering rules for different network architectures and services	Synthesis (5)
CO 5: Evaluate different types of network architectures	Evaluation (6)

Table 7. Mapping SECB358 course learning outcomes to Blooms Taxonomy

outcomes including quizzes, midterm exam, final exam, and hands-on lab exercise reports. Throughout the semester, the course coordinator collects the assessment data, and by the end of the semester, the collected assessment data are mapped to the leaning outcomes. The achievement level of each leaning outcome is then calculated in terms of mean and standard deviation using (1) and (2).

$$\mu(CO_i) = \frac{\sum \mu_t \times n_t}{\sum_t n_t} \quad (1)$$

$$\sigma(CO_i) = \sqrt{\frac{\sum_t \sigma_t^2 \times n_t}{\sum_t n_t}} \quad (2)$$

where μ_t and σ_i denote respectively the normalized mean, and standard deviation of the students' marks when assessment tool t is used, and n_t denotes the number of students. After calculating the achievement level for each leaning outcome, the course coordinator discusses the assessment results with the faculty members who taught the course, and then decides on the needed recommendations to address any discovered shortcoming.

5.2 Students' Comprehension of FTP Traffic Filtering

This section discusses the effect of introducing the hands-on lab exercises on the students' comprehension of FTP traffic filtering. In fact, during the 2008/2009 and 2009/2010 academic years, students enrolled in the SECB358 course were not offered any hands-on lab exercise on FTP traffic filtering. Only the theoretical security concepts were described during the lecture time along with a limited number of class exercises. However, starting from fall 2010, the course coordinator decided to offer the hands-on lab exercises proposed in this paper as a corrective action to improve the leaning outcomes achievement levels.

To evaluate the students' comprehension of FTP traffic filtering, one quiz and one midterm exam's question are offered to students each semester. The quiz and midterm exam's question are directly mapped to the learning outcome CO4, which is directly concerned with network packet and services filtering and firewall filtering rule design. The data collected relative to the quiz and midterm exam's question are used to assess the achievement of CO4, along with other data collected from other assessment tools.

It is important to mention that the same teachers were involved with the pre and post lab classes, as well as the offered quizzes and midterm exam questions.

Figure 15 shows the students average grades for the quiz and the midterm exam's question. It clearly shows that starting from 10/11 academic year, the students' average grade has started improving. This is mainly due to the fact that the offered hands-on lab exercises allowed students to better anatomize and assimilate the taught security concepts on FTP traffic filtering. The students have learned better with the hands-on lab exercises, which had a positive effect on their performance. For example, in case of the quiz, introducing the hands-on lab exercises improved the students' average grade by 8.9% from 78 to 85 and maintained the improvement for the following two academic years. Consequently, this improvement in students grading performance would contribute positively on the achievement of the learning outcome CO4.

It is important to mention that there was a decrease in 2012/2013 in student performance compared to the two previous years during which the hands-on lab exercises have been also offered. This is not a major issue, since we got an increase during 2012/2013 academic year compared to the academic years during which the hands-on lab exercises have not been offered.

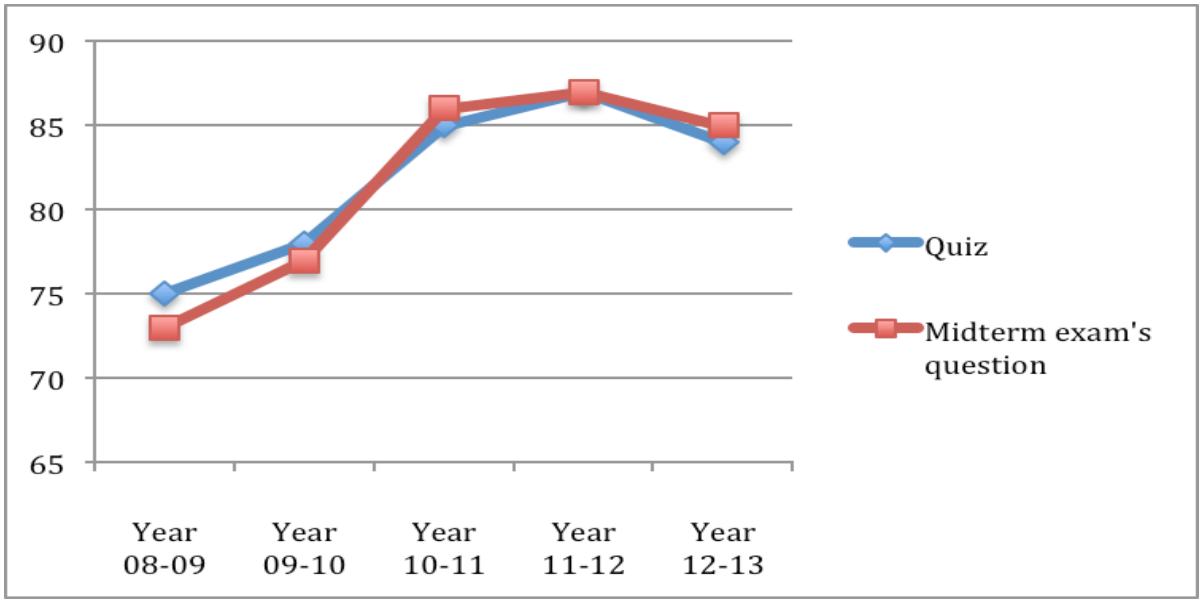


Figure 15. Student performance in the quiz and midterm exam's question on FTP traffic filtering before and after introducing the hands-on lab exercises

5.3 Student's Survey

In order to evaluate how effective the students think the lectures and hands-on lab exercises are and measure their satisfaction level, we solicited students' opinions using an anonymous survey at the end of each semester for three consecutive academic years (From Fall 2010 to Spring 2013). Precisely, the purpose of the survey is to assess how closely the hands-on exercises mapped to our lectures from students' point of view and if students have learned more about FTP traffic filtering after taking the hands-on lab exercises.

The survey consists of questions in three categories: the hands-on lab exercises, the relevance between the lecture and hands-on lab exercises, and the overall impact of the lecture and hands-on lab exercises on students. The survey's questions contains positive statements about the lectures and hands-on lab exercises, and were presented using a five-point Likert scale. Students were asked to rate the statement based on a scale from 1 (strongly disagree) to 5 (strongly agree).

5.4 Results analysis

Table 4 shows a summary of the results of the anonymous survey that was administered to 95 students who over there academic years had participated in the hands-on lab exercises. In general, students gave favorable evaluation, as shown in Table 7. The averages of all survey items are between 4.0 and 4.77 with standard deviations from 0.6 to 1.06. This result shows that students mostly either agree or strongly agree with the positive statement about the lecture's contents and the hands-on lab exercises on FTP traffic filtering. Among the three categories, the "Hands-on lab exercises" category has the highest average (4.77) and the "Overall impact of the lecture and the hands-on lab exercises on students" category has the lowest average (4.0). This result shows that students are satisfied with the hands-on lab exercises on FTP traffic filtering, but are less certain about the overall impact of the lectures and the hands-on lab exercises on their career.

The results of the survey showed that students mostly either agree or strongly agree that the hands-on lab exercises to be useful and helped them better understand the underlying theoretical security concepts associated with FTP traffic filtering. The survey also revealed that students mostly are strongly interested in similar hands-on lab exercises in other security classes, and would strongly recommend the exercises to other students.

However, the survey item number 3 in the category "Overall impact of the lectures and hands-on lab exercises on students" has received the lowest average but with the highest standard deviation. This result shows that some students are less inspired by the class in terms of pursuing a future career in information security. We believe that this is due probably to the fact that the students are not giving enough importance to their professional career at this time of their study, or lack professional experience that allows them to answer adequately this survey item.

In addition, the results of the survey indicate that students enjoyed the classes when the hands-on lab exercises are combined as a part of the class activities. We found that the offered hands-on lab exercises made the course more interesting and informative to students. The hands-on lab exercises allow students to understand the course topic better than lectures alone. Students often raised questions whenever they encounter problems that prevent them from completing the exercises but they do not usually ask questions during a lecture. Overall, it is clear that the survey's results allow to recommend information security educators to incorporate hands-on lab exercises into their courseware whenever possible.

Survey Item	Item Average	Item Standard Deviation
Hands-on lab exercises (Average = 4.77, Standard deviation = 0.67)		
1. I enjoyed the hands-on lab exercises on FTP traffic filtering.	4.9	0.7
2. I think the hands-on lab exercises on FTP traffic filtering are easy to follow and straightforward.	4.7	0.9
3. I have better understanding regarding the lecture topic on FTP traffic filtering after finishing the corresponding lab exercises.	4.8	0.6
4. I will definitely recommend the hands-on lab exercises to others.	4.7	0.5
The relevance between the lecture and hands-on lab exercises (Average = 4.72, Standard deviation = 0.6)		
1. The combination of the lectures and hands-on lab exercises makes the class more interesting and informative than a class with only lectures.	4.8	0.7
2. The hands-on approach based lecture improved my knowledge in FTP traffic filtering.	4.6	0.5
3. I know better about putting security concepts being taught in practice after finishing the related hands-on lab exercises.	4.6	0.9
4. The hands-on lab exercises stimulate my further interests in learning the technology and theories/concepts behind the security solutions.	4.8	0.6
5. I will be interested in taking other security classes that blend in hands-on lab exercises with lectures.	4.8	0.5
Overall impact of the lecture and hands-on lab exercises on students (Average = 4.0, Standard deviation = 1.06)		
1. The lectures and hands-on lab exercises improved my knowledge and skills in the area of network security.	4.2	0.8
2. After taking the lectures on FTP traffic filtering, I am even more interested in the network traffic filtering area than I did.	4.2	0.9
3. After taking the lectures on FTP traffic filtering, I am even more interested in having a career in the information security area, particularly in the network security area, than I did.	3.6	1.5

Table 7. Summary of the results from the courseware questionnaire

6. Conclusion

The importance of experimental learning in information security education has long been recognized in the learning theory literature. Hence, to enhance information security education throughout experimental learning, this paper discussed an educational approach that combines information security practice with theory, for teaching FTP traffic filtering in network security related courses. This experience should help information security educators in planning their information security courses and in

bringing more interesting and informative learning environment to the students. In addition, such a hands-on approach would contribute considerably to better prepare the students to work as security administrators with better chances of landing jobs than students without these hands-on skills.

The discussed security courseware has three unique features. First, regarding the implementation of the discussed hand-on lab exercises, it is simple to setup the lab environment for both the instructor and the students. Second, the hands-on lab exercises packages are adaptable in a limited budget and are portable to most computer laboratories in universities. Third, each hands-on lab exercise is closely tied to a related security concept or principle, on FTP traffic filtering.

In addition, the paper has presented an evaluation learning process and survey instrument that allow to assess the student learning outcomes, and measure students' feedbacks and satisfaction levels regarding the lecture contents and hands-on lab exercises. Using the proposed learning process and survey instrument, we found evidence that students learned better about the FTP traffic filtering concepts after introducing the hands-on lab exercises.

References

[1] Gavas, Efstratios., O'Brien, Keith (2012). Teaching Network Security Using VITAL, *In*: Proceedings of the 16th Colloquium for Information Systems Security Education, p. 116-121, Florida June 11 - 13, 2012.

[2] NSTISS (1994). National Training Standard for Information Systems Security (InfoSec) Professionals, NSTISS June 20 1994.

[3] CNSS (2004). National Information Assurance Standard for System Administrators (SAs), Committee on National Security Systems March 2004.

[4] Chen, Li-Chiou., Lin, Chienting (2007). Combining Theory with Practice in Information Security Education, *In*: Proceedings of the 11th Colloquium for Information Systems Security Education, MA, June 4-7, 2007.

[5] Yuan, Dongqing., Zhong, Jiling (2008). A lab implementation of TCP SYN flood attack and defense. *In*: SIGITE '08 Proceedings of the 9th ACM SIGITE Conference on Information Technology Education (SIGITE '08), p. 57-58, Cincinnati, Ohio, USA, October 16-18, 2008.

[6] Trabelsi, Zouheir (2011). Hands-on Lab Exercises Implementation of DoS and MiM Attacks using ARP Cache Poisoning. Proceedings of the 2011 Information Security Curriculum Development Conference, (InfoSecCD 2011), p. 74-83, Kennesaw, GA, USA, September 30 - October 01, 2011.

[7] Trabelsi, Zouheir (2012). Switch's CAM Table Poisoning Attack: Hands-on Lab Exercises for Network Security Education, *In*: Proceedings of the Fourteenth Australasian Computing Education Conference (ACE2012), p. 113-120, Melbourne, Australia, January 30 - February 3, 2012.

[8] O'Leary, Mike (2006). A Laboratory Based Capstone Course in Computer Security for Undergraduates, *In*: Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education (SIGCSE'06), Houston, Texas, USA, March 3–5, 2006.

[9] Wagner, Paul J., Wudi, Jason M. (2004). Designing and Implementing a Cyberwar Laboratory Exercise for a Computer Security Course. ACM SIGCSE Bulletin, 36 (1) March 2004.

[10] Yuan, Xiaohong mattews, David., Wright, Omari., Xu, Jinsheng., Yu, Huiming (2010). Laboratory exercises for wireless network attacks and defenses, *In*: Proceedings of the 14th Colloquium for Information Systems Security Education, p. 115-123, Baltimore, Maryland, USA, June 7-9, 2010.

[11] Murray, William Hugh. (2008). What the Graduate Needs to Know about Cryptography, *In*: Proceedings of the 12th Colloquium for Information Systems Security Education, p. 153-157, Dallas, TX, USA, June 2 - 4, 2008.

[12] Trabelsi, Zouheir., Hayawi, Kadhim (2012). Arwa Al Braiki, Sujith Samuel Mathew, Network Attacks and Defenses: A Hands-on Approach, CRC Press, Auerbach Publications, 2012.

[13] Trabelsi, Zouheir (2012). Teaching Stateless and Stateful Firewall Packet Filtering: A Hands-on Approach, *In*: Proceedings of the 16th Colloquium for Information Systems Security Education, p. 95-102, Florida, USA, June 11-13, 2012.

[14] Fall, Kevin R., Stevens, W. Richard (2011). TCP/IP Illustrated. Volume 1: The Protocols (2nd Edition), Addison-Wesley Professional, 2011.

[15] Tibbs, Richard., Oakes, Edward (2006). Firewalls and VPNs: Principles and Practices, Prentice Hall, 2006.

[16] Zwicky D, Elizabeth ., Cooper, Simon., Chapman D, Brent (2000). Building Internet Firewalls, O'Reilly Media; Second Edition edition, 2000.

[17] Jetico Personal Firewall, http://www.jetico.com

[18] LeapFTP tool, http://www.leapware.com

[19] CommView Network Monitor and Analyzer tool, http://www.tamos.com

[20] Anderson, L. W., Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. New York: Longman.