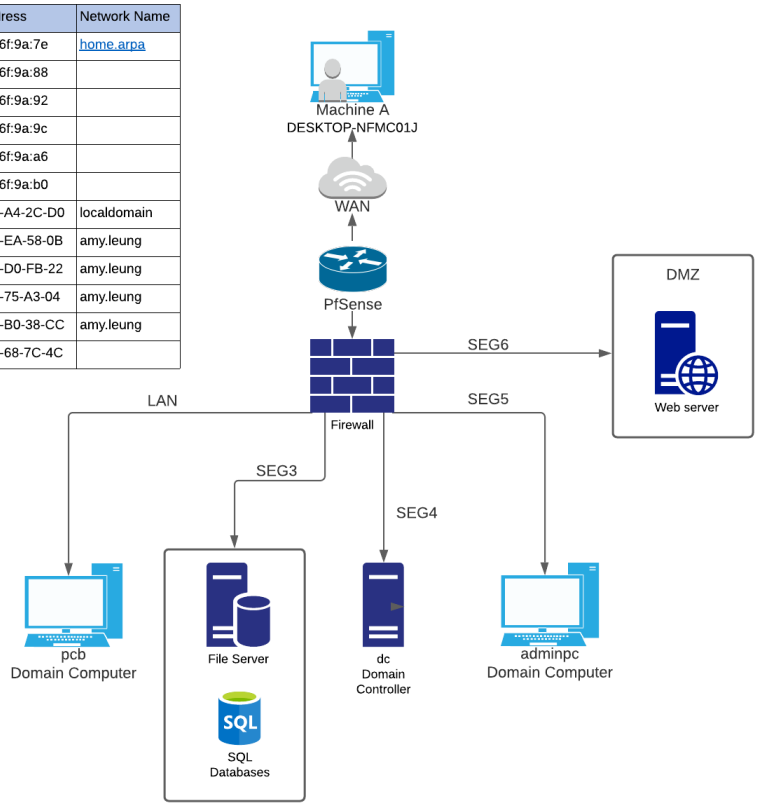
Network Topology

Device Name	Interface	IP Address	MAC Address	Network Name
pfsense	WAN	192.168.1.128 /24	00:0c:29:6f:9a:7e	home.arpa
	LAN	192.168.2.1/24	00:0c:29:6f:9a:88	
	SEG3	192.168.3.1/24	00:0c:29:6f:9a:92	
	SEG4	192.168.4.1/24	00:0c:29:6f:9a:9c	
	SEG5	192.168.5.1/24	00:0c:29:6f:9a:a6	
	SEG6	192.168.6.1/24	00:0c:29:6f:9a:b0	
DESKTOP-NFMC01J	WAN	192.168.1.129 /24	00-0C-29-A4-2C-D0	localdomain
pcb	LAN	192.168.2.30/24	00-0C-29-EA-58-0B	amy.leung
fileserver	SEG3	192.168.3.25/24	00-0C-29-D0-FB-22	amy.leung
dc	SEG4	192.168.4.30/24	00-0C-29-75-A3-04	amy.leung
adminpc	SEG5	192.168.5.30/24	00-0C-29-B0-38-CC	amy.leung
webserver	SEG6	192.168.6.25/24	00-0C-29-68-7C-4C	

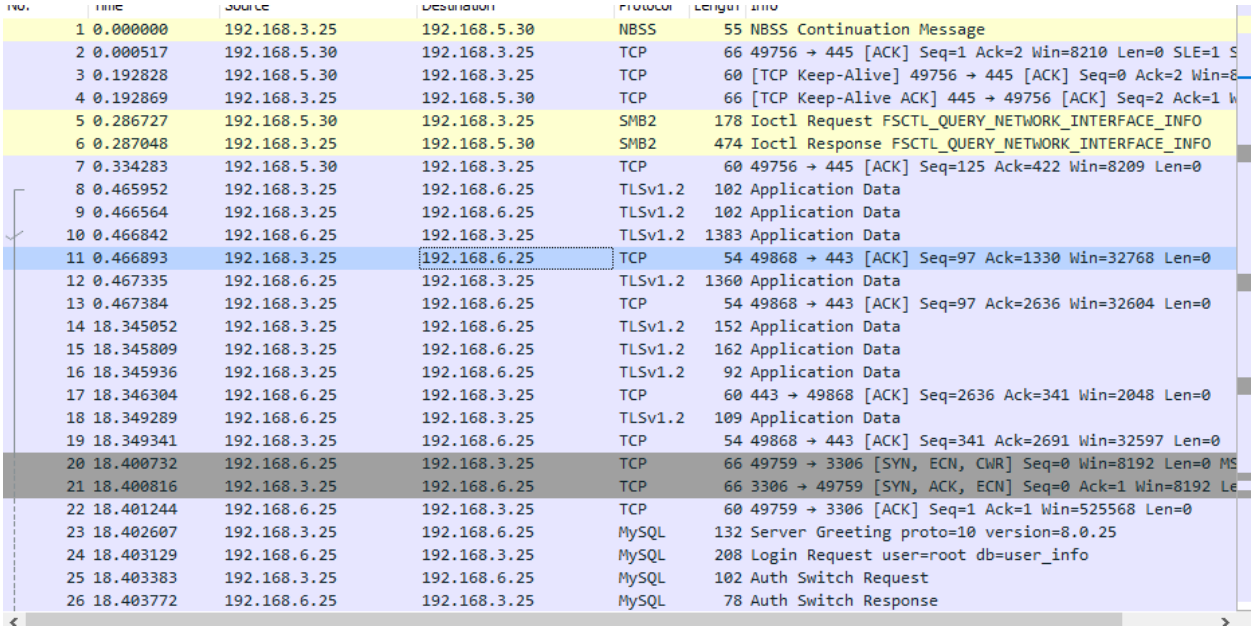


This is the IT Security Final project

A. Accessing internal website

As background, I am accessing the webserver site (192.168.6.25) using the fileserver (192.168.3.25).

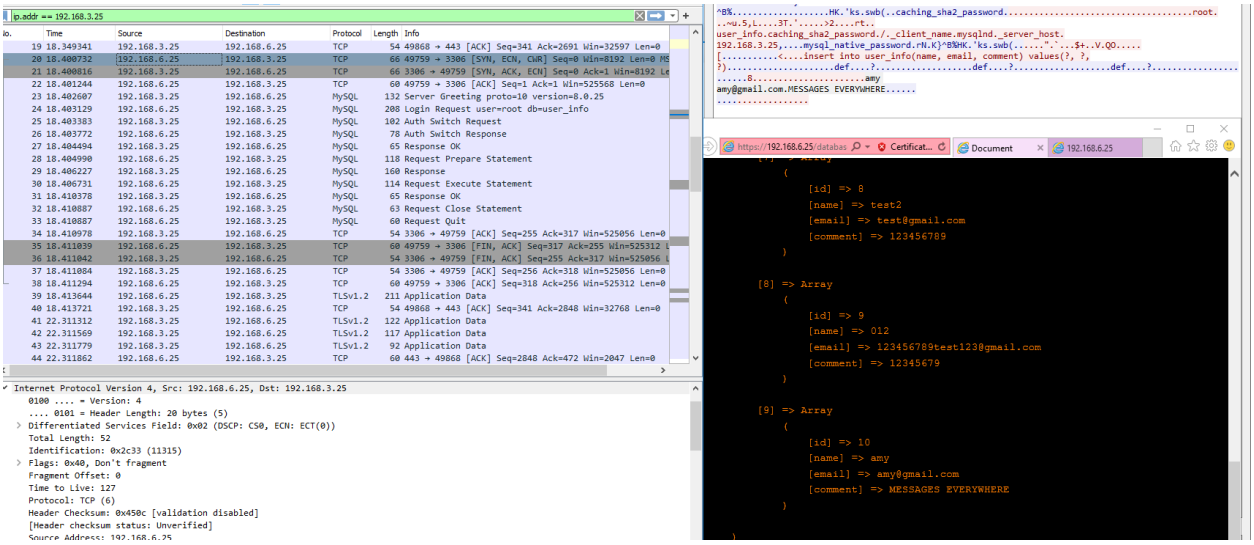
SC#1 – screenshot of accessing the webserver site



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.3.25	192.168.5.30	NBSS	55	NBSS Continuation Message
2	0.000517	192.168.5.30	192.168.3.25	TCP	66	49756 → 445 [ACK] Seq=1 Ack=2 Win=8210 Len=0 SLE=1 S
3	0.192828	192.168.5.30	192.168.3.25	TCP	60	[TCP Keep-Alive] 49756 → 445 [ACK] Seq=0 Ack=2 Win=8
4	0.192869	192.168.3.25	192.168.5.30	TCP	66	[TCP Keep-Alive ACK] 445 → 49756 [ACK] Seq=2 Ack=1 W
5	0.286727	192.168.5.30	192.168.3.25	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
6	0.287048	192.168.3.25	192.168.5.30	SMB2	474	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
7	0.334283	192.168.5.30	192.168.3.25	TCP	60	49756 → 445 [ACK] Seq=125 Ack=422 Win=8209 Len=0
8	0.465952	192.168.3.25	192.168.6.25	TLSv1.2	102	Application Data
9	0.466564	192.168.3.25	192.168.6.25	TLSv1.2	102	Application Data
10	0.466842	192.168.6.25	192.168.3.25	TLSv1.2	1383	Application Data
11	0.466893	192.168.3.25	192.168.6.25	TCP	54	49868 → 443 [ACK] Seq=97 Ack=1330 Win=32768 Len=0
12	0.467335	192.168.6.25	192.168.3.25	TLSv1.2	1360	Application Data
13	0.467384	192.168.3.25	192.168.6.25	TCP	54	49868 → 443 [ACK] Seq=97 Ack=2636 Win=32604 Len=0
14	18.345052	192.168.3.25	192.168.6.25	TLSv1.2	152	Application Data
15	18.345809	192.168.3.25	192.168.6.25	TLSv1.2	162	Application Data
16	18.345936	192.168.3.25	192.168.6.25	TLSv1.2	92	Application Data
17	18.346304	192.168.6.25	192.168.3.25	TCP	60	443 → 49868 [ACK] Seq=2636 Ack=341 Win=2048 Len=0
18	18.349289	192.168.6.25	192.168.3.25	TLSv1.2	109	Application Data
19	18.349341	192.168.3.25	192.168.6.25	TCP	54	49868 → 443 [ACK] Seq=341 Ack=2691 Win=32597 Len=0
20	18.400732	192.168.6.25	192.168.3.25	TCP	66	49759 → 3306 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MS
21	18.400816	192.168.3.25	192.168.6.25	TCP	66	3306 → 49759 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Le
22	18.401244	192.168.6.25	192.168.3.25	TCP	60	49759 → 3306 [ACK] Seq=1 Ack=1 Win=525568 Len=0
23	18.402607	192.168.3.25	192.168.6.25	MySQL	132	Server Greeting proto=10 version=8.0.25
24	18.403129	192.168.6.25	192.168.3.25	MySQL	208	Login Request user=root db=user_info
25	18.403383	192.168.3.25	192.168.6.25	MySQL	102	Auth Switch Request
26	18.403772	192.168.6.25	192.168.3.25	MySQL	78	Auth Switch Response

Directed to mo.11 is the beginning of when we are accessing the site. You can see that I am sending a TCP packet that has a ACK flag to the port 443. The port 443 is for sites with an ssl certificate, because I built the site with ssl the ports we are looking for is 443 as opposed to port 80 (which is more unsecure).

SC#2 – Screenshot of the form being submitted to the fileserver



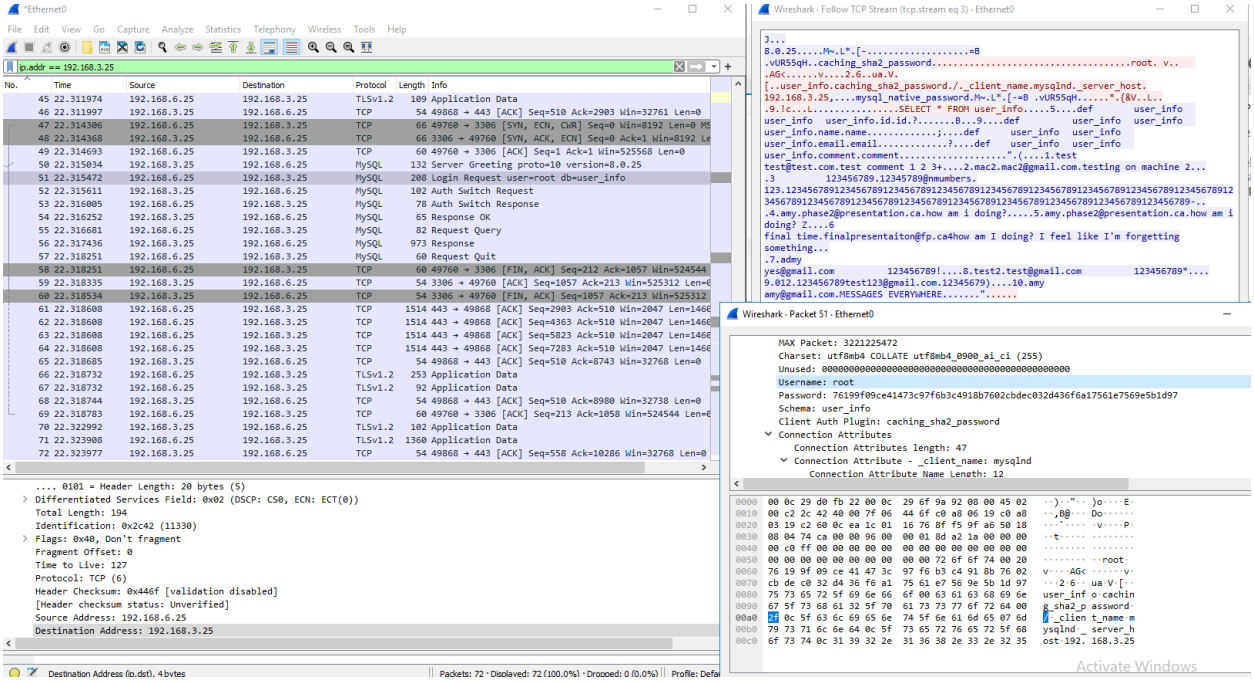
No.20 is when the form is being submitted to the database, we can see that the webserver is accessing the fileserver. When following the data stream we can see that there is information being inserted into the table. The data is being inserted into the table user_info, in the order of name, email, comment. In particular the “amy amy@gmail.com.MESSAGES EVERYWHERE” is indicative that it is being sent to the database.

From the screenshot we can conclude that the order of values being sent to the use_info table is:

User_info	
name	Amy
email	amy@gmail.com
comment	MESSAGES EVERYWHERE

No.36 is when we see that the handshake is finished because of the FIN flag.

SC#3 – Screenshot of the form values being retrieved from the fileserver



The above Screenshot shows the form values being retrieved from the database. when following the TCP stream for packet 47 we can see that we SQL code I particular we can see SELECT * FROM user_info, this means that from the table user_info select the following data. The following data is defined by user_info.id.id, user_info.name.name, user_info.email.email, and user_info.comment.comment. We can then see all of the values entered using the website form.

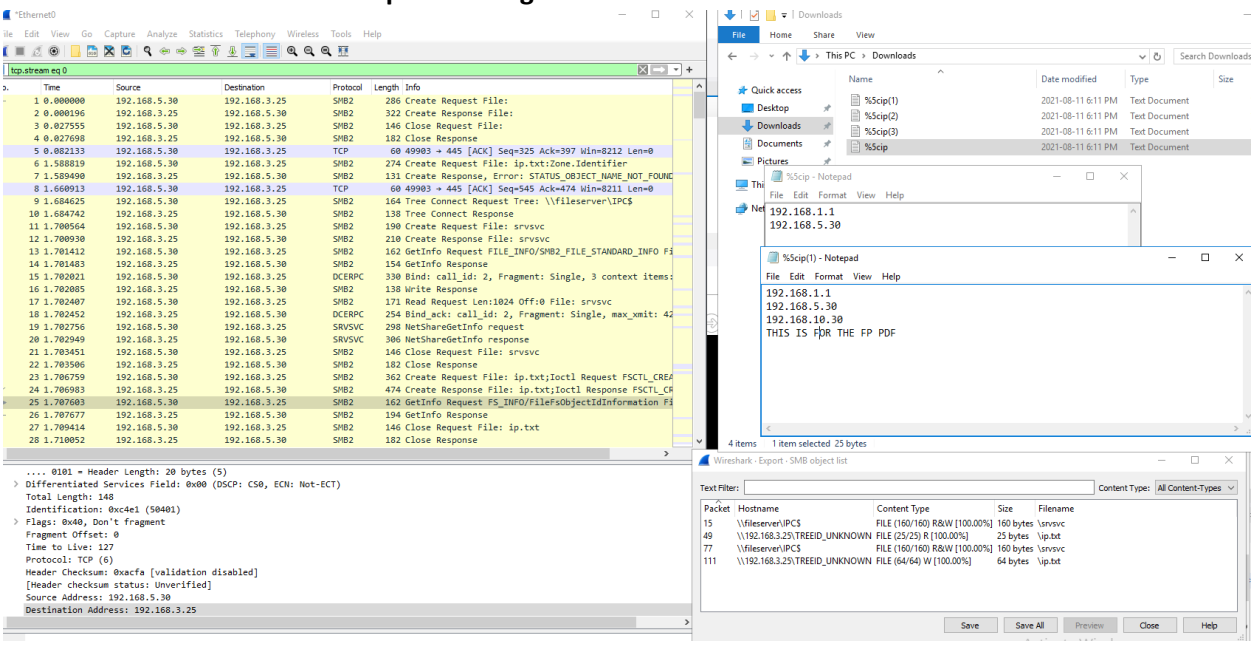
This could be potentially problematic because we can get the MySQL username in this case which is root which can be seen in packet 51. The password is encrypted using SHA2, but it can be cracked if we compare hash strings of known passwords. In an enterprise it would be better to have a more complex password.

Being able to see the data also means that individuals can steal private and personal data. For example, if the table was instead user_info.password.password, user_info.address.address, user_info.dob.dob, etc. then this means someone can potentially steal data and use sql injections.

B. Accessing document on fileserver

As background I am accessing the fileserver (192.168.3.25) using the adminpc (192.168.5.30) as Annie Hanson

SC#4 – screenshot of the adminpc accessing a file on the file server

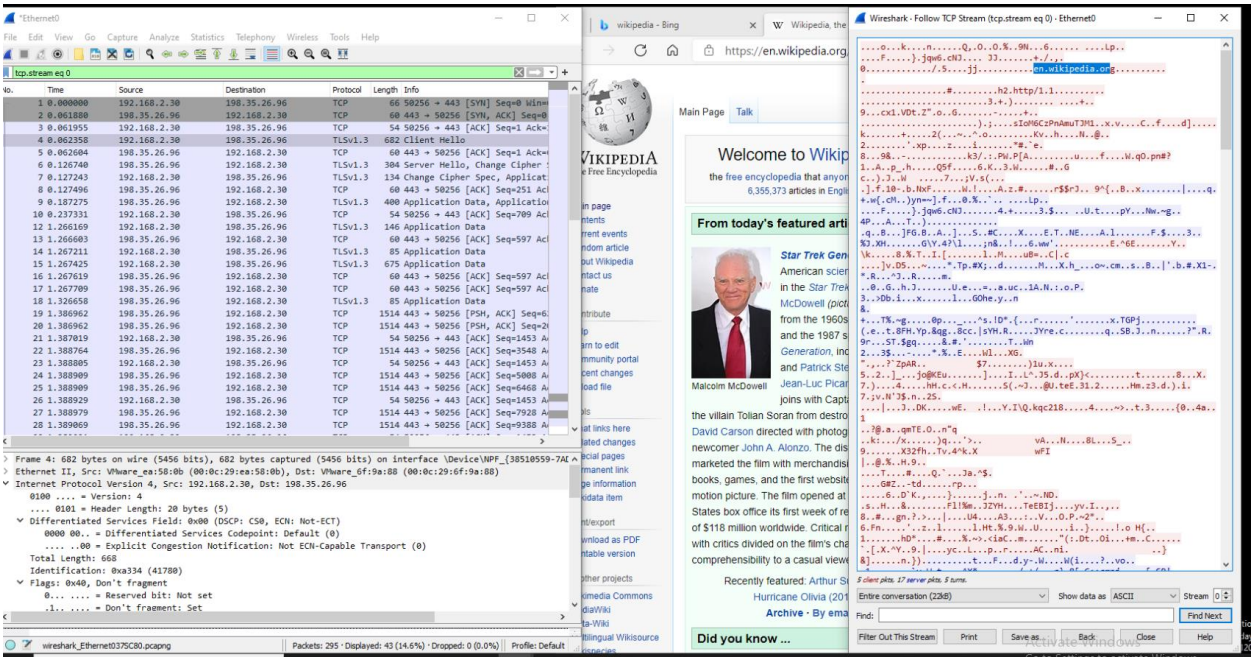


Above we can see an abundance of information. If we follow the streams of any of the packets most of the data that we can see is ineligible for humans. However we can see that the adminpc creates a request file, the request files and its response is what gives the adminpc allowance to work in those files requested. We can also see the server of what we are trying to reach which is \\fileserver\IPC$. we can also see that there is a request file for ip.txt in packet no.23 what this means is that adminpc is trying to get access to ip.txt. So the file server sends a GetInfo Request to verify if the adminpc has appropriate permissions. When the GetInfo Response is finished the request and response is then closed, and now the adminpc has access to the file.
We can also export files, in the example above we exported all of the files. When opening %5cip(1) we can see the new text added which is:
“192.168.10.30
This is for the FP PDF”
What this means is that we can see the file before edits and after edits.

C. Accessing the internet website

To access the internet website I am going to use pcb to access the site www.youtube.com

SC#5 – screenshot of pcb accessing the internet site wikipedia.com



Packet no.3 shows pcb accessing the Wikipedia site. When packet no.3 is followed we can see that en.wikipedia.com is being accessed. The reason for the sizable pcap file is because of the loading of resources. The pcap file has 295 packets, and while the site was loading it needed to access the images, links, etc. which took longer than usual.