Cyber security and digital forensics

One technique that can be used is port scanning(avast software n.d). Port scanning allows a user to gain information about a remote machine through its ip address. It relays to us what ports are currently open on the remote machine and the services that are running. A tool that utilizes this is called nmap. You can also use different types of scans to acquire different types of information. One such scan is the default TCP SYN scan. This is a common and useful scan as it can scan thousands of ports in a short time and won’t be restricted by firewalls put in place. Furthermore it is covert when it comes to scanning because it doesn’t complete the three way handshake instead we wait and analyse the response sent by the remote machine to determine the state of the port. It also displays clearly whether a port is open, filtered or closed. Another scan is the TCP connect scan. This is used when the SYN scan isn’t available. The difference between this scan and the SYN scan is that with this scan we complete the three way handshake and establish a direct connection to the remote machine. Preferably, it would be better to use a SYN scan instead. This is because TCP scans require more packets to be sent in order to gain the same amount of information as a SYN scan because they complete the three way handshake. This in turn makes it more time consuming. Furthermore the connection that is made it’s most likely going to be detected by any ids that are running. The connection will be logged into the system and an administrator would be able to view these log attempts and act accordingly. Making the reconnaissance mission not as covert as you would want.

Another useful technique is fingerprinting(Jeremy Faircloth,2017). By using this technique we can try and figure out what type of software is being used to provide the service on the remote machine, and the current version of the service. Furthermore it tells us what ports are opened or closed. To add on it's possible to make an estimated guess about the type of operating system that's running on the remote machine. This is because when we send tcp and udp requests, each operating system responds differently to that request. By utilizing a tool like nmap, we can analyse all the responses that are received and compare it to nmaps operating system database where it displays to us details about the operating system if it's found a match.

Another useful technique is banner grabbing(Ajay Saranjam,2021). Banner grabbing is a technique used to gain knowledge about a computer system on a network and enumerate the services and software running on its open ports and the current version. It also tells us the operating system. By gaining this information from the banner, it can be used to exploit any known vulnerabilities on the os or service version that is running. Banner grabbing works by sending a request to the remote machine which initializes a connection and then analyzing the response that the remote machine sends back. The response will be a banner message that contains information about the remote machine. There are two types of banner grabbing called passive and active. With active banner grabbing your connection is logged into the remotes machine system. This can be a problem as it could get picked up by any intrusion detection system that's setup and alerts the machine. Passive however allows for the same information to be obtained without having to create a direct connection to the remote machine making it less detectable and more ideal for gathering information secretly.

One way to mitigate information exposure is to ensure that all systems are updated regularly(universal class). Installing the release of patches ensures that any vulnerabilities in the previous version of the os can’t be exploited by hackers to try and retrieve confidential information.

Another step to prevent information exposure would be to ensure all unnecessary ports are closed(Hartwig,2015). This is because a third party can use port scanning to determine what services are running and the OS you have. This in turn means they can exploit any vulnerabilities known to it and check the level of security to find exploits. By closing the ports it means less information gets exposed about that port that can be exploited.

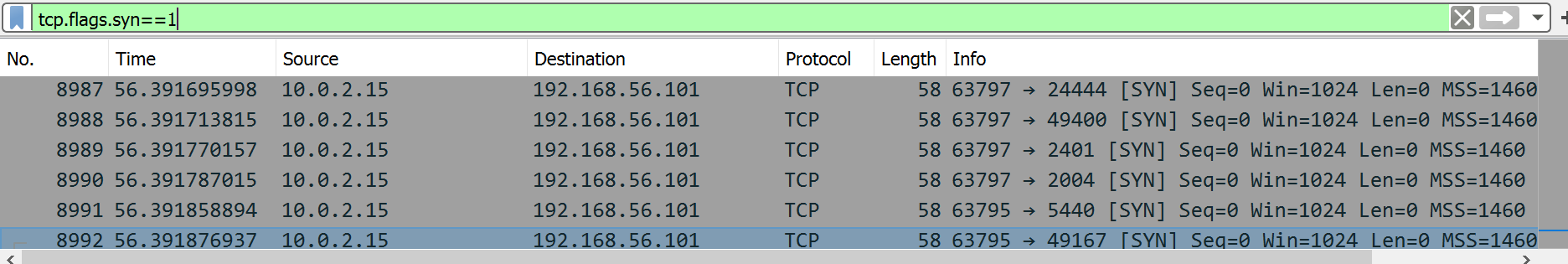
Another useful mechanism would be the implementation of firewalls(forcepoint). Firewalls can mitigate information exposure because it monitors ingoing and outgoing traffic within the system and can filter packets going in and out. Within a firewall you can specify what network traffic is allowed to be transmitted and which network traffic is blocked. Which In turn allows you to specify who can access your ports and who can’t . This can be effective against port scanning because it can block unauthorized third parties from trying to connect to your ports. This reduces the exposure of information as someone who isn't included in the firewall rules will not be permitted to retrieve information from your system or ports as they wont respond to the requests, and in turn can't gain any information that they can exploit to harm your system.

Another mitigating technique would be disabling the apache banner(sucun). By default if someone performed banner grabbing, your system would display details such as the type of server it is, the operating system and the version number. By changing the settings so that this information doesn't get presented to a third party, it means a hacker would have less knowledge about what type of server they're trying to break into making it more difficult for them.

Another technique to mitigate information exposure would be checking system logs regularly(Glover n.d). The actions that are happening on your system will be logged into files. These files can be checked by an administrator to see if there's any unusual activity happening on the system. This can be used against os fingerprinting because if someone has made numerous attempts to fingerprint your system, by identifying these attempts as early as possible, appropriate measures can be taken in order to reduce the amount of data being exposed.

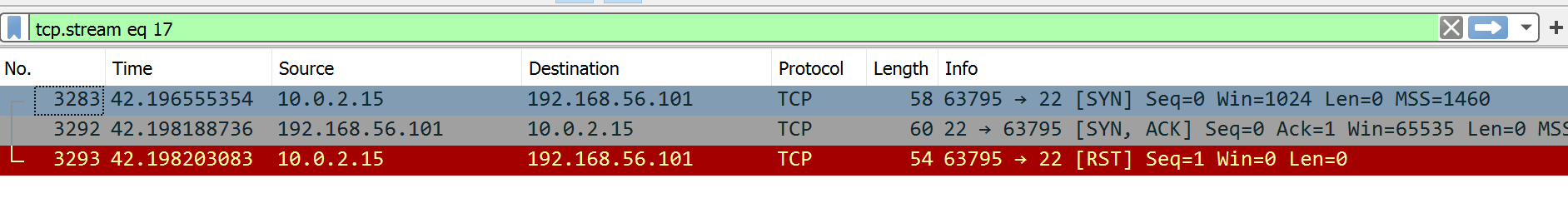
Firstly I want to identify if there has been any attempts of a stealth or full scan to a system.

**ftp**



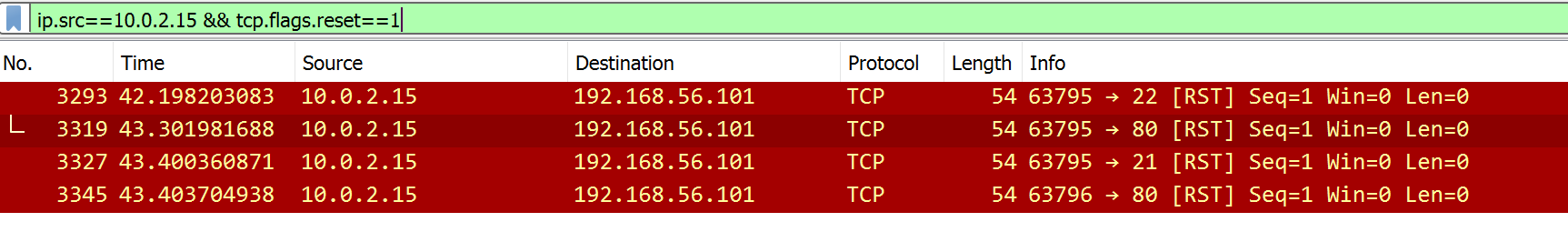
In the above screenshot I filtered out the packets to show which source ip is trying to establish a connection to another ip. I found that the ip 10.0.2.15 was sending a lot of syn packets to 192.168.56.101 in a short amount of time. This indicates that ip 10.2.15 is possibly an attacker trying to gain information from ip 192.168.56.101

To further analyse the communication that's being passed I followed the tcp stream of one of the packets in the screenshot below.

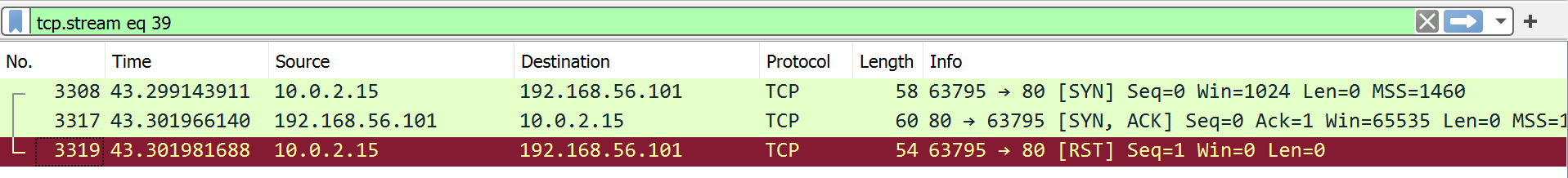


From analysing this I can see that ip 192.168.56.101 has responded to the syn request with an acknowledgement and synchronization flag. This response tells me that the port 22 is open and listening. The source ip then responds by terminating the communication by sending a reset packet. Based on the flow of communication, the source ip has used a TCP stealth half scan on the system. Port 22 is responsible for SSH which is used for encryption over a network.

I wanted to see if the source ip 10.0.2.15 had found out about any other ports that were opened. I used the filter in the screenshot below to determine this.



From this screenshot I can ascertain that port 80 was opened as well. Just to make sure I followed the stream in the screenshot below.



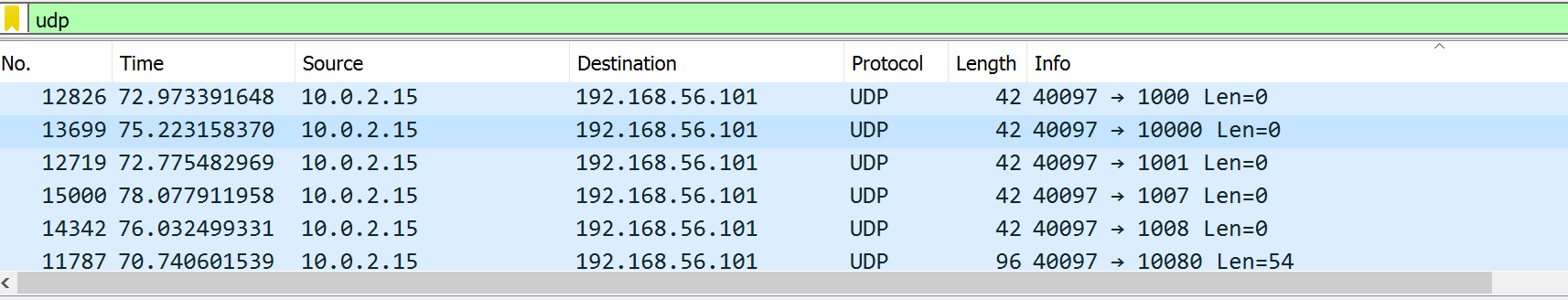
This follows the stealth scan procedure.

The source ip 10.0.2.15 mac address is in the screenshot below.

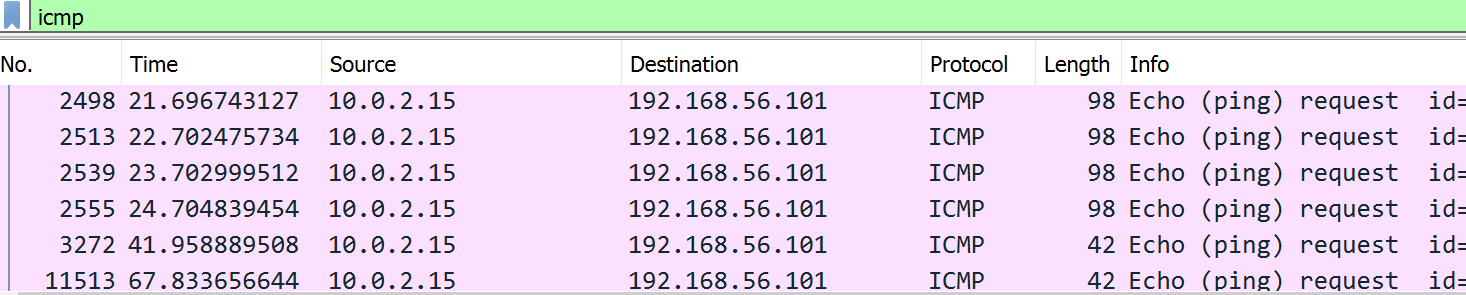


**Udp**

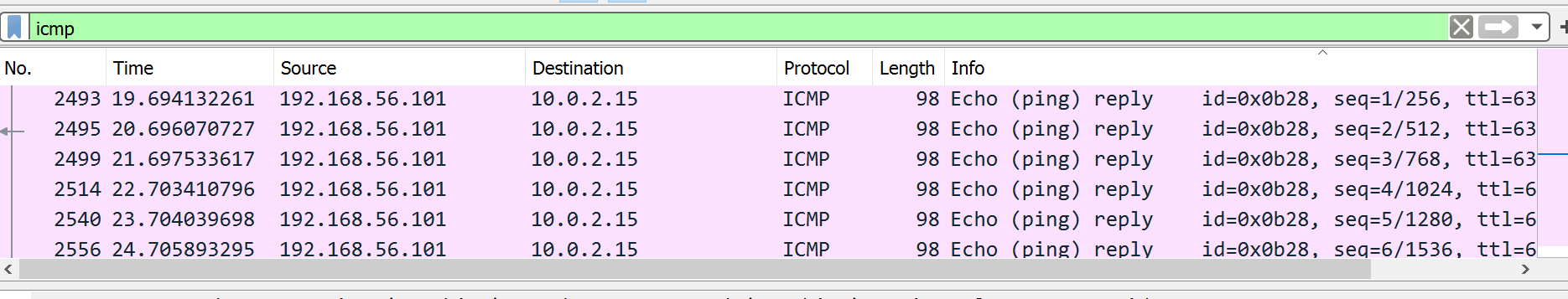
Udp scans are different from tcp scans as there is no three way handshake and doesn’t give responses in the same way tcp does. So we can only make a guess as to whether the ip 10.0.2.15 was able to connect to the remote machine using a udp scan.



In the screenshot above we can see the source ip 10.0.2.15 attempting to use the udp protocol to establish a connection to the remote machine. Because the source ip 10.0.2.15 isn’t receiving a response back, it means either the port is open or the port is being filtered. This is less reliable than tcp because it’s not definitive. However using other protocols we can gain a more definitive answer as to whether the attacker was able to make a connection.

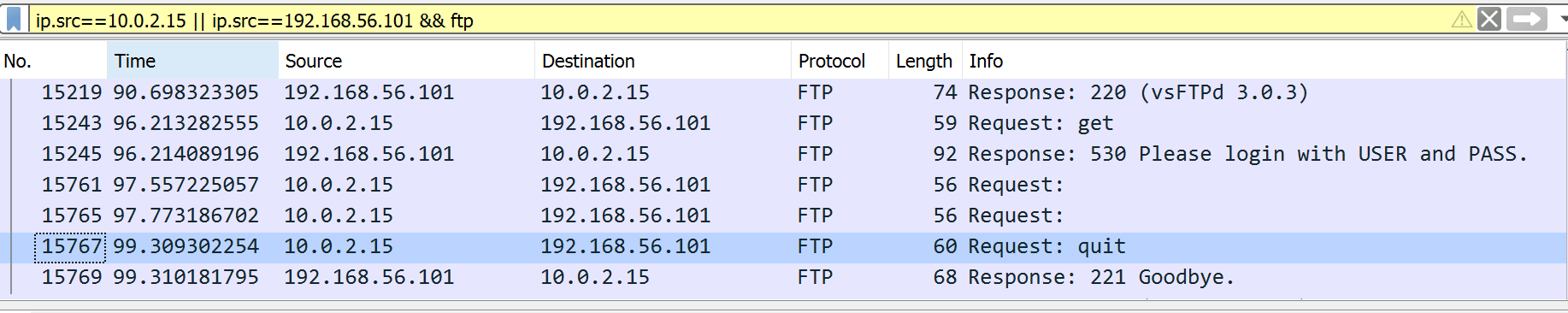


Above we can see that the source ip 10.0.2.15 used the Icmp protocol to try and check for a connection.

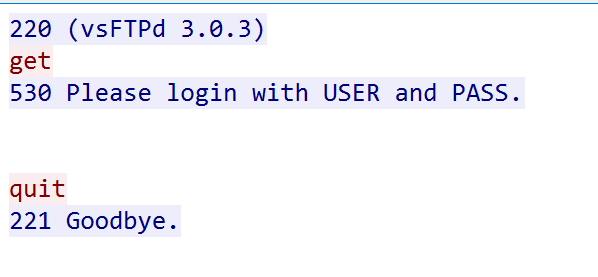


From this screenshot it shows that the remote machine replied with an echo ping. This indicates that the source ip 10.0.2.15 has a route to the machine and possibly connectivity.

**Ftp**



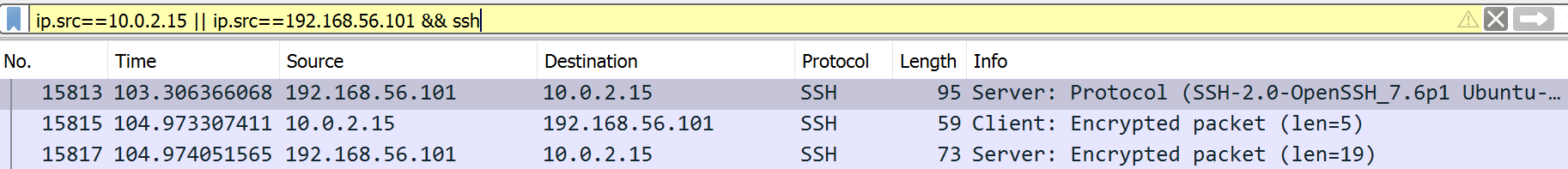
After the port scan the source ip 10.0.2.15 was attempting to log into the ftp server but was unsuccessful.



From following the 3035 stream I captured this.The screenshot above indicates that the source ip 10.0.2.15 had no idea as to the appropriate username and password so decided to quit.

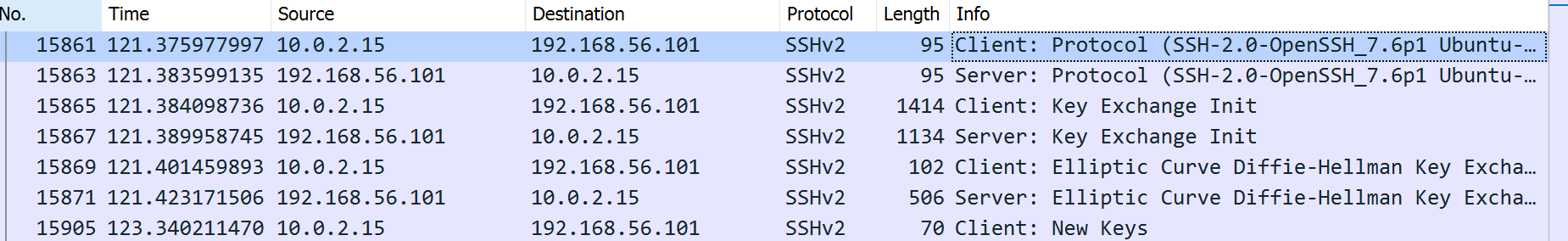
**Ssh**

At this time the source ip 10.0.2.15 attempted to access the ssh server. From the screenshot below it seems they intercepted some encrypted packets but it's unclear as to what exactly happened with the packets and whether the source ip 10.0.2.15 was able to retrieve information or not. This is because ssh is encrypted.

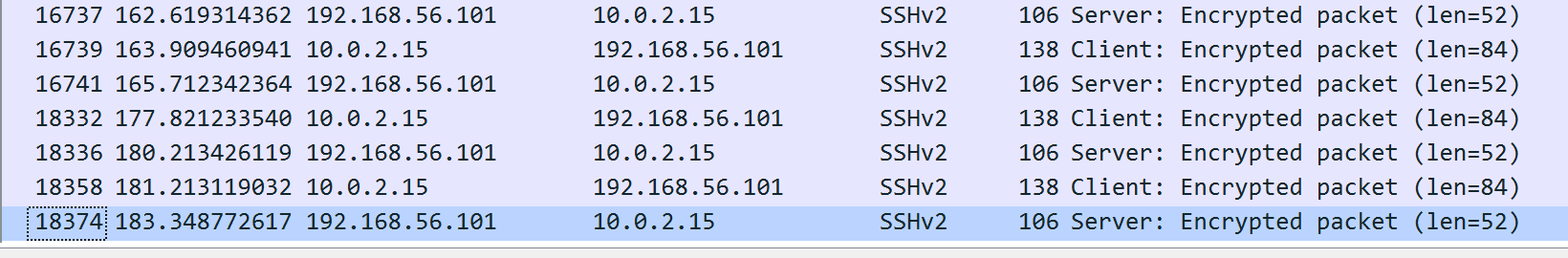


**Sshv2**

At this time the source ip 10.0.2.15 is initiating the sshv2 protocol. Furthermore it appears that the software running the service is an old version of ssh. It also appears to be running on ubuntu. From the screenshot below, the source ip 10.0.2.15 is using the elliptic curve diffie-hellman key exchange algorithm. They seem to be exchanging a key with the remote server in order to generate a new secure key that the attacker can use to communicate.

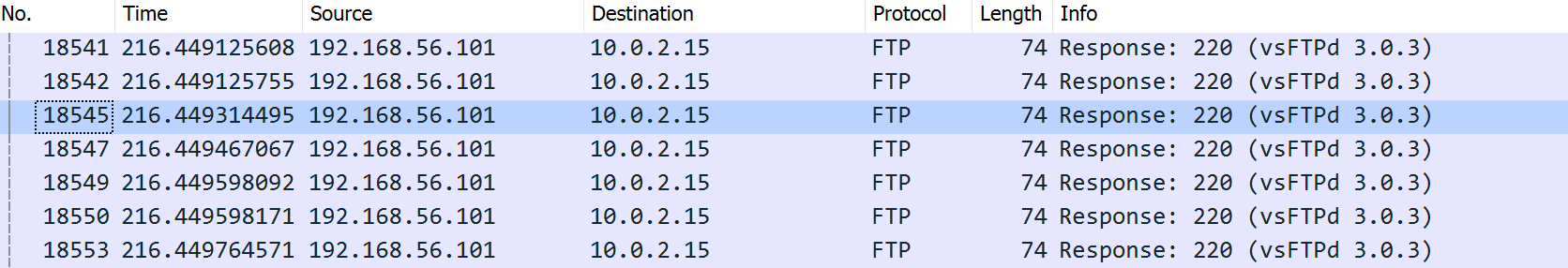


In the screenshot below the source and the remote machine then began to exchange encrypted packets between each other.

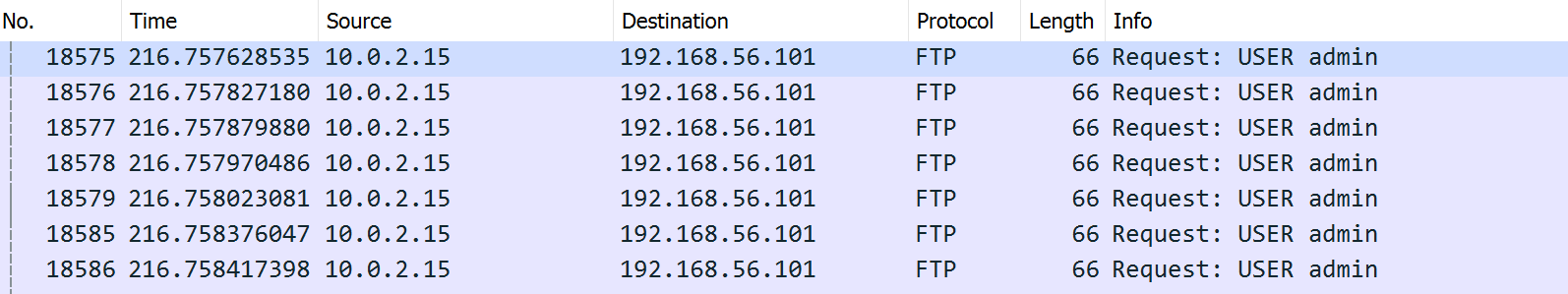


Because the source ip 10.0.2.15 is a participant in the ssh communication, they should be able to decrypt the packets using the new key.

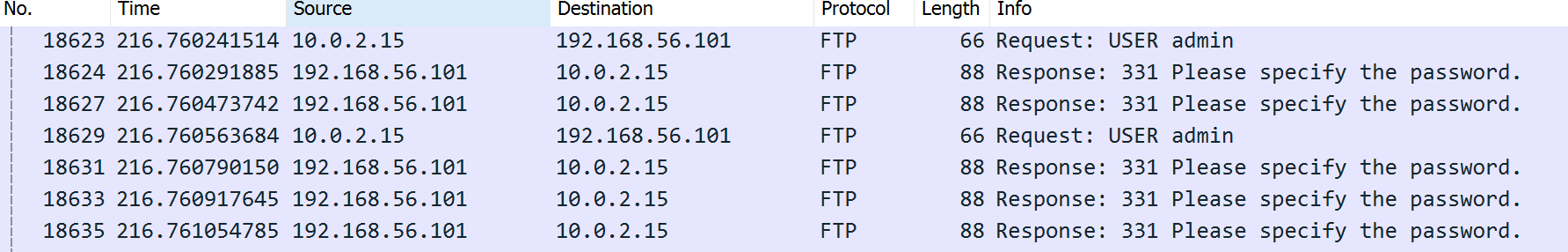
**Ftp bruteforce**

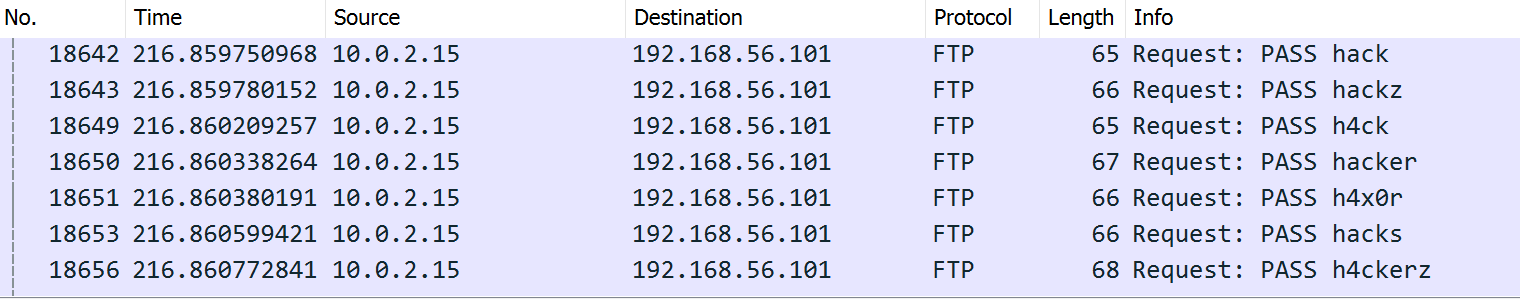
At this point in time the source ip 10.0.2.15 has attempted a brute force attack.

In the screenshot above the software running the service seems to be vsFTPd 3.0.3.

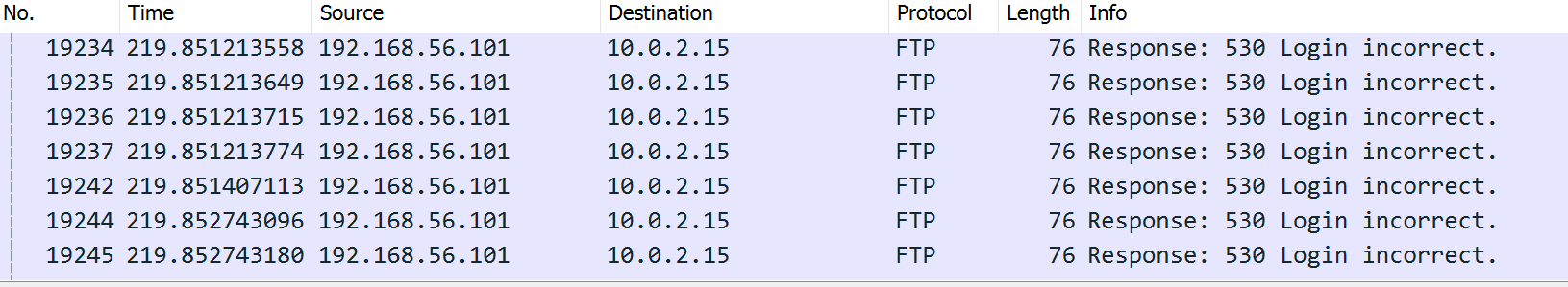


In this screenshot we see the source ip 10.0.2.15 making numerous attempts to log in using the username admin.





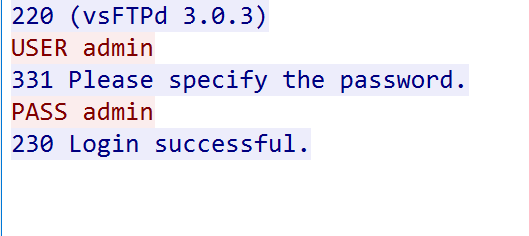
In the above screenshots the source ip 10.0.2.15 makes numerous attempts to log in using the potential passwords that they managed to obtain.



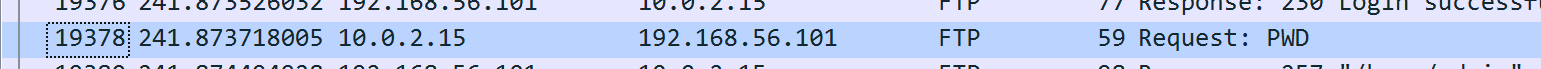
In this screenshot I can see that most of the passwords were wrong.



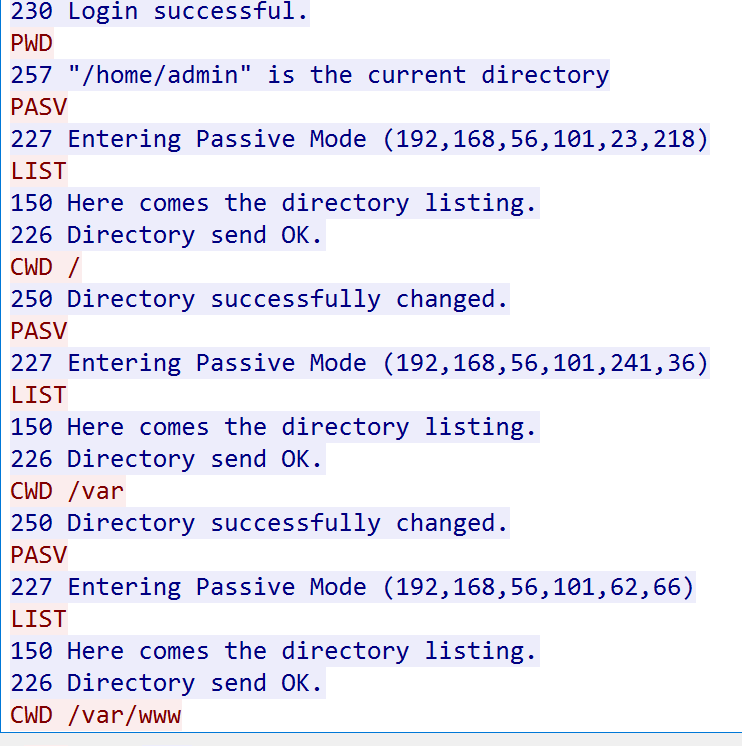
However in this screenshot the source ip 10.0.2.15 has entered the correct password and was able to log in.

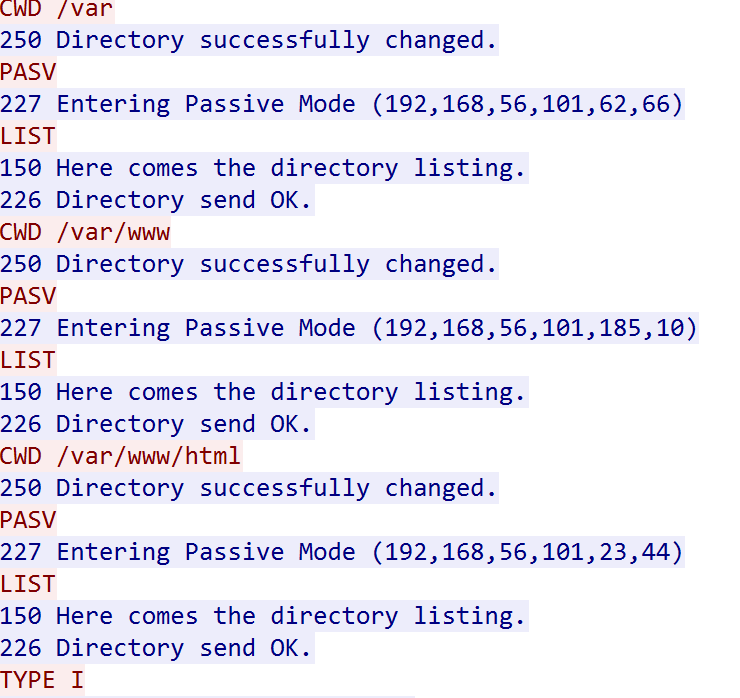


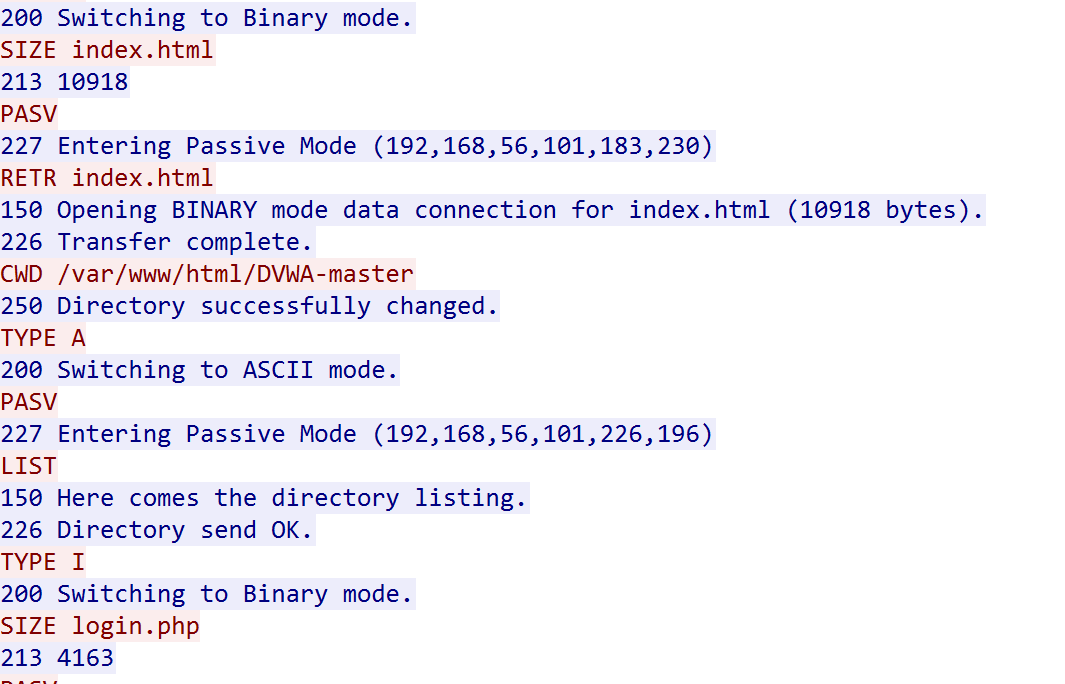
From following the tcp stream i can see that the correct username was admin and the correct password was admin.

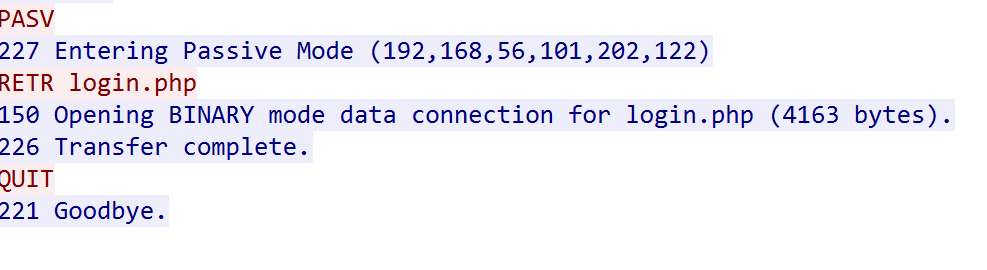


To see the actions that the source ip 10.0.2.15 took after they logged in I followed the tcp stream of the packet. What I can gather is the attack used the pwd command to check the current directory.

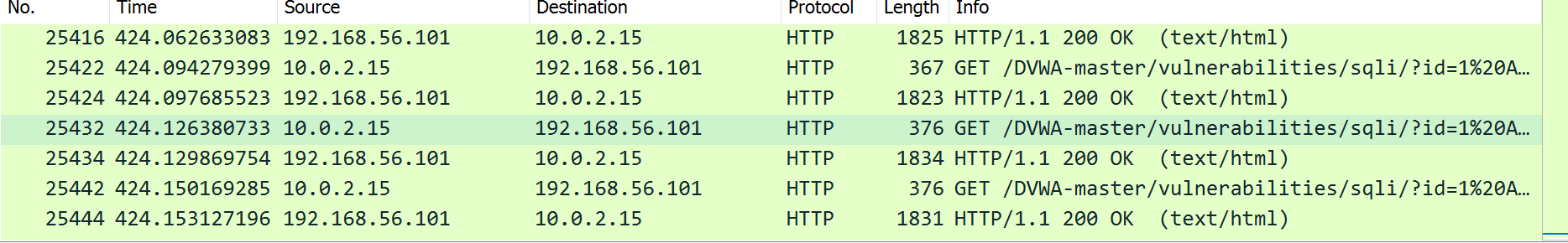








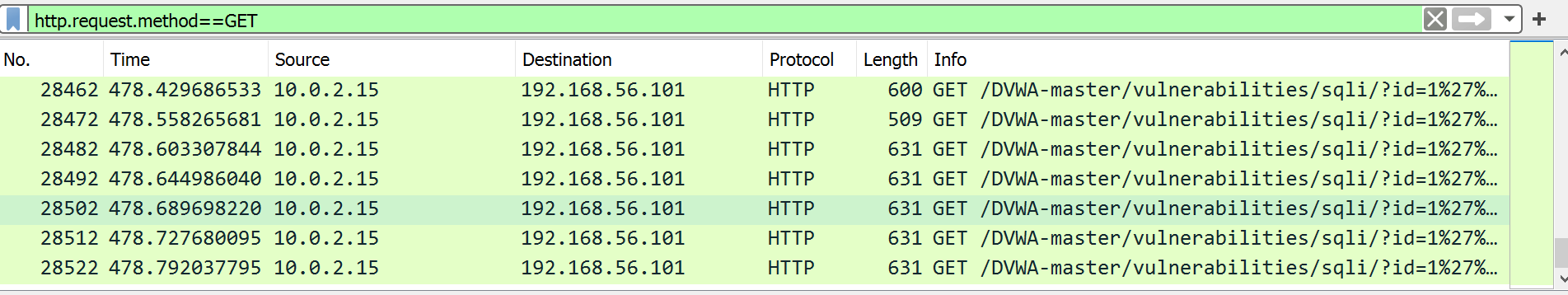
To summarise the screenshots above, the source ip 10.0.2.15 navigated their way through the directories. they connected to the server using a passive ftp connection. This means the source ip 10.0.2.15 is the one that establishes a connection to the server's 21 port by sending the PASV command. The source ip 10.0.2.15 also connected to another random port on the server from which data transfers would be made. When the source found the index.html file under the /var/www/html directory, they converted it into binary format and then downloaded the data to themselves. They then navigated to the var/html/www/dvwa-master directory and located the login.php file. This was converted into ascii and also downloaded to themselves through the binary connection. Once both files were retrieved the source ip 10.0.2.15 used the quit command to exit. The login.php file contained the source code for the login page details and the index.html file contained the source code for the website.

****

From the screenshot above, the source ip 10.0.2.15 has attempted an sql injection against the remote servers html page. They used the get method in order to request the data from the DVWA-master/vulnerabilities directory. The server then responds to these requests by displaying in html format the information from the database.



In this screenshot the source ip 10.0.2.15 uses this session id in order to authenticate themselves so that they can interact with the servers webpage.

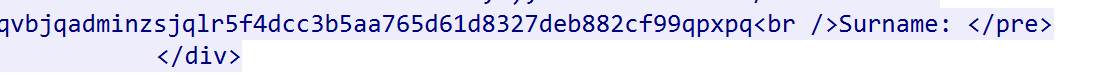


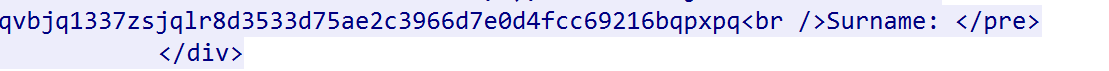
In the screenshot above I used the filter in order to find the ip addresses that were using the get method. I then scrolled down and followed the http stream of the last five packets.



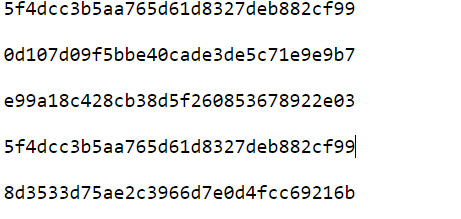








Inside those streams I saw the sql injections alongside the normal content of the page. What I could gather was that the usernames were being concatenated. The ip address 10.0.2.15 was able to obtain the following usernames : smith,pablo,gordon,admin,1337. A hashing algorithm was used to encrypt the passwords.



By making the hashes unsalted i used a hash cracker and was able to retrieve the passwords as well. They were md5 hash type. Passwords:password,letmein,abc123,password and charley.

**references**

Avast software [What is port scanning and how does it work? | Avast](https://www.avast.com/en-gb/business/resources/what-is-port-scanning)

Jeremy Faircloth,scanning and enumeration,[Active Fingerprinting - an overview | ScienceDirect Topics](https://www.sciencedirect.com/topics/computer-science/active-fingerprinting)

Ajay Saranjam,banner grabbing,[Banner Grabbing: In 3 Easy Points (jigsawacademy.com)](https://www.jigsawacademy.com/blogs/cyber-security/banner-grabbing/)

Forcepoint,what is a firewall,[What is a Firewall? Defined, Explained, and Explored | Forcepoint](https://www.forcepoint.com/cyber-edu/firewall)

Chris Hartwig, why closing unused server ports is critical to cyber security,december 15th 2015,[Why Closing Unused Server Ports is Critical to Cyber Security (getcryptostopper.com)](https://blog.getcryptostopper.com/why-closing-unused-server-ports-is-critical-to-cyber-security)

Sucun,disable server banners,[Disable Server Banners | Sucuri Docs](https://docs.sucuri.net/warnings/hardening/disable-server-banners/)

Gary Clover,the importance of log management,security metrics,[The Importance of Log Management (securitymetrics.com)](https://www.securitymetrics.com/blog/importance-log-management)

Universal class,the procedure of installing security patches to protect your computer,[The Procedure of Installing Security Patches to Protect Your Computer | UniversalClass](https://www.universalclass.com/articles/computers/the-procedure-of-installing-security-patches-to-protect-your-computer.htm)