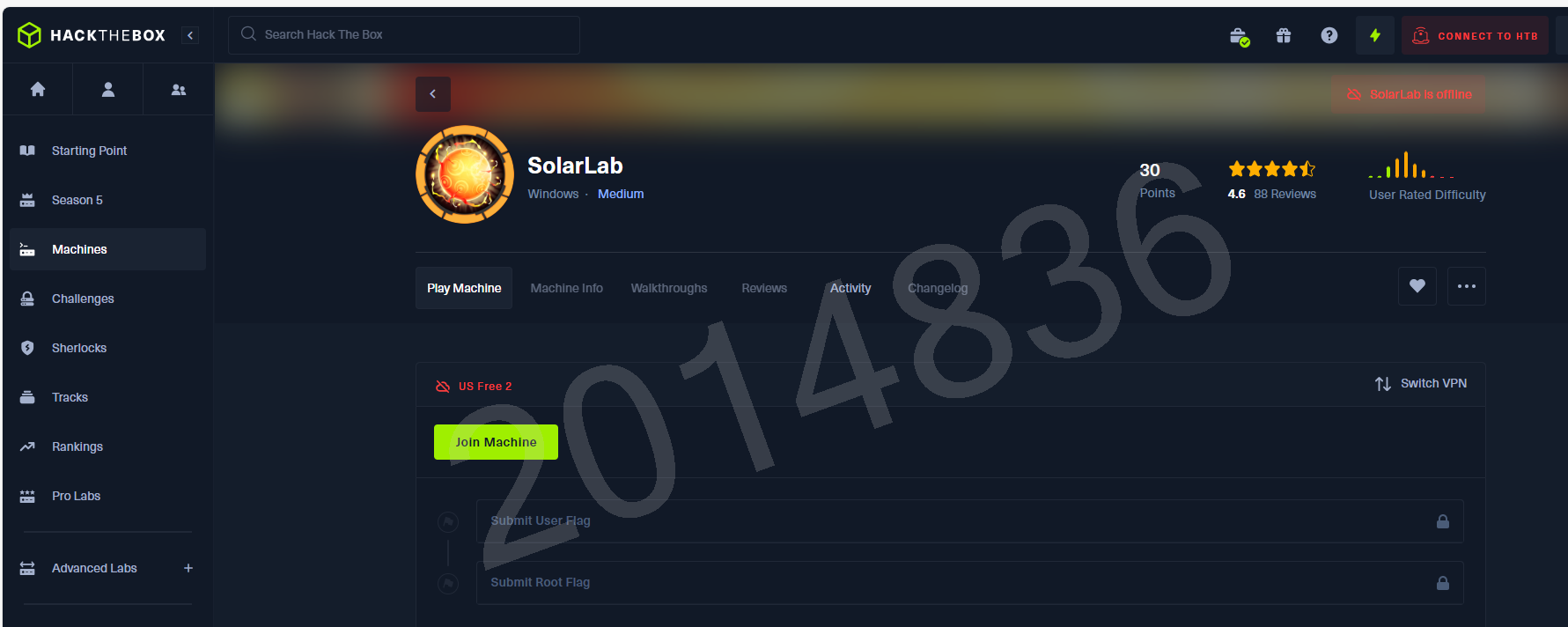
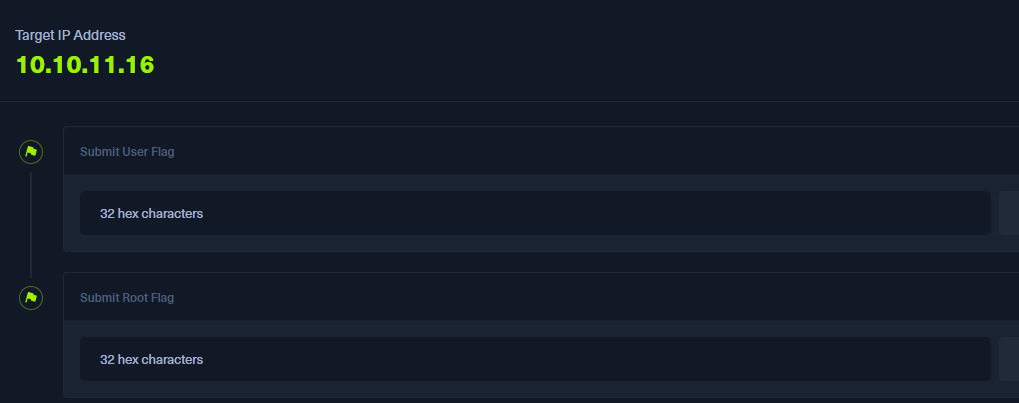
**Penetration Testing - Handson Exercise:**

* The Candidate would need to create an account in Hackthebox site if they don’t have one (https://www.hackthebox.com/)
* Navigate to **Machines** and choose either **SolarLab or Runner** Machine and complete any one of the exercises.

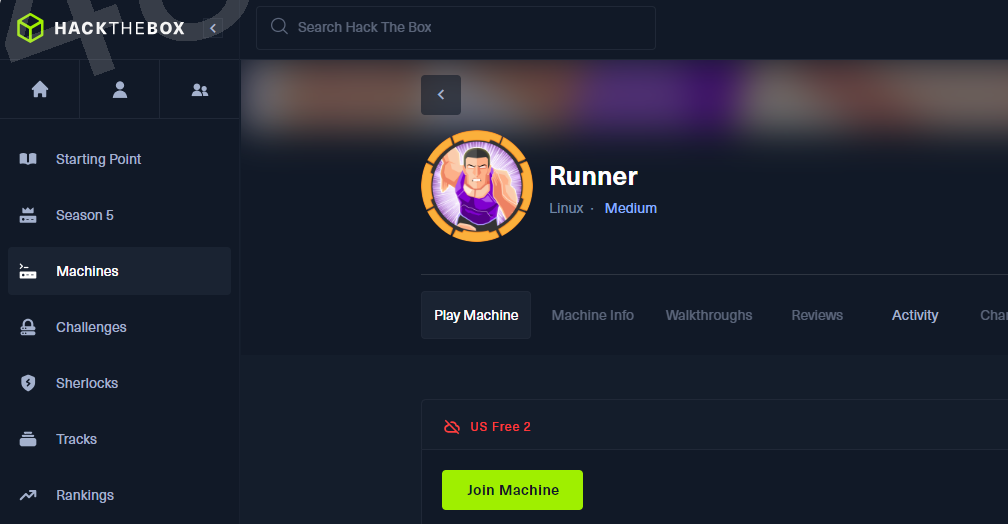
1. Screenshot of **SolarLab** Machine



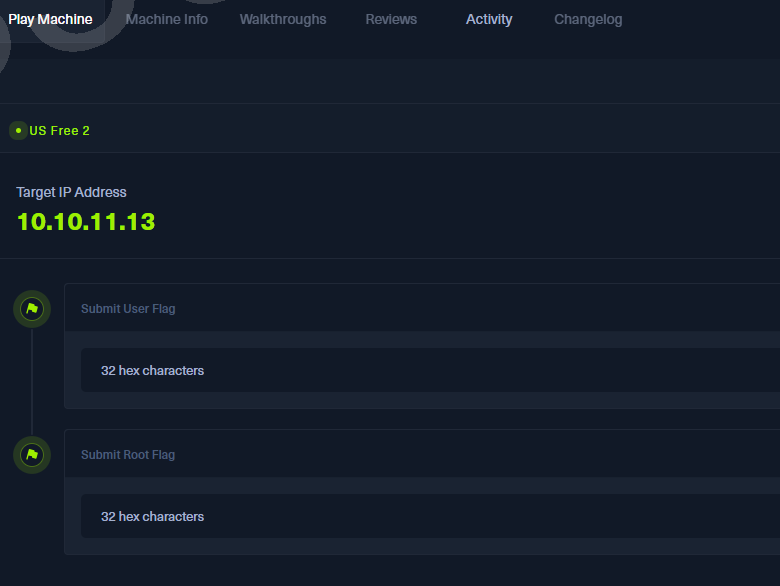
**Target IP**



2. Screenshot of **Runner** Machine



**Target IP**



**Expectation:**

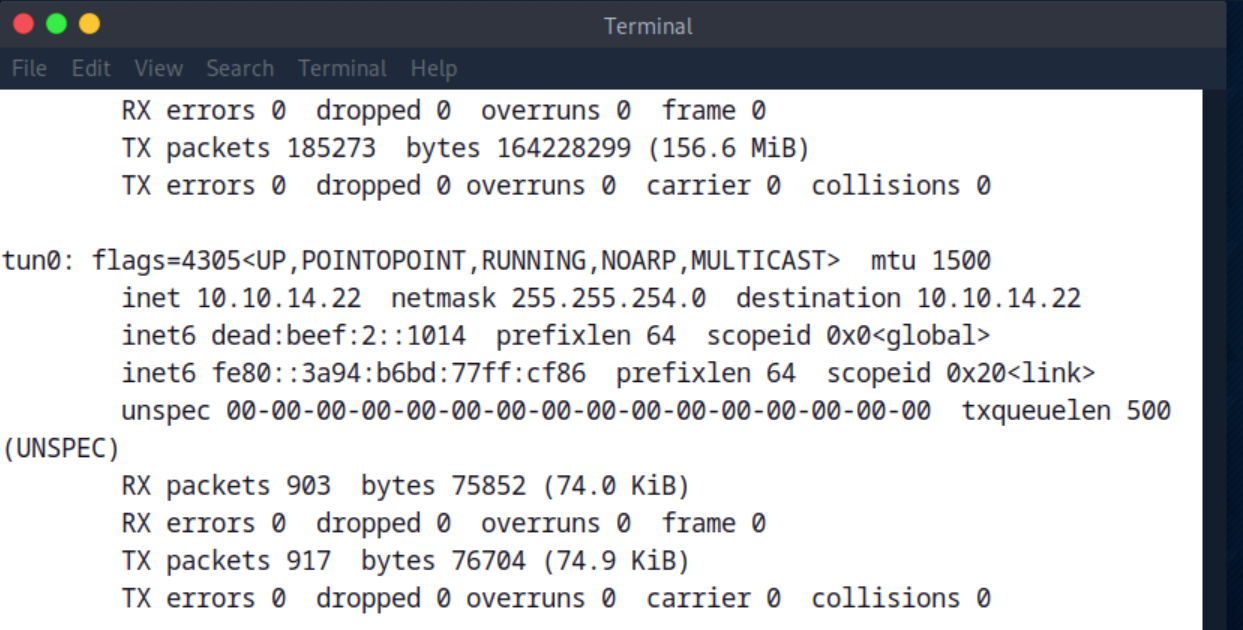
Detailed report on the step-by-step procedure taken to complete the exercise along with the screenshots.

**Screenshot of Hack the box IP:** A computer screen shot of a program

Description automatically generated

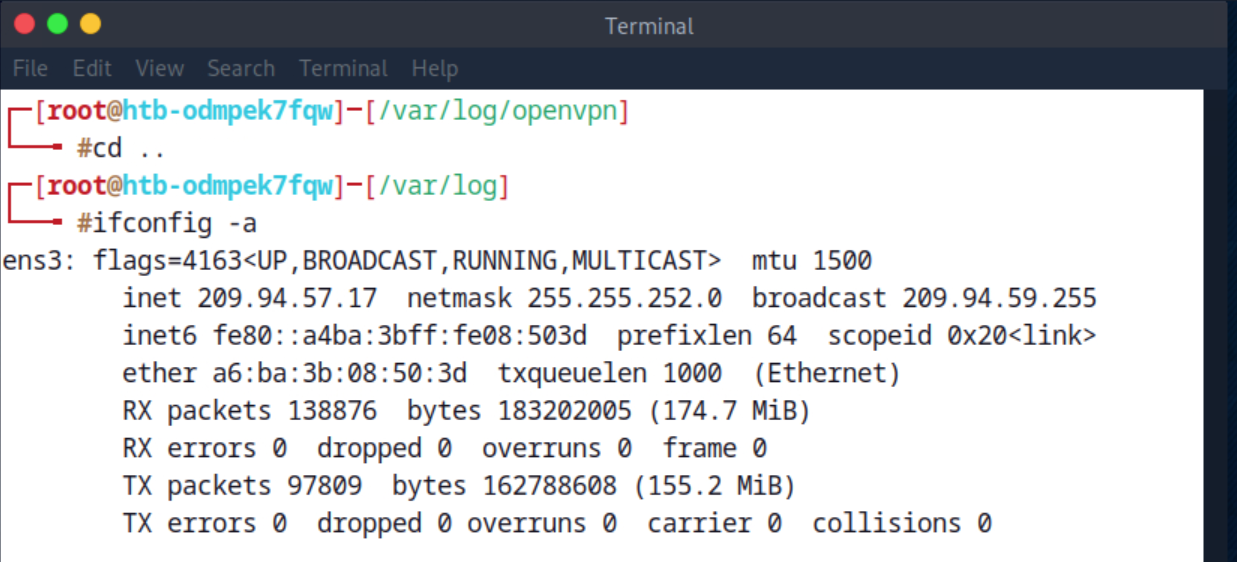
**Screenshot of System flag:** A cartoon of a wizard pointing at a wand

Description automatically generated



**Screenshot of User Flag:** A cartoon of a wizard pointing at a wand

Description automatically generated



Completion Screenshot: A screenshot of a computer program

Description automatically generated

**Below is the capture without able to connect to Runner VM.**

─[us-free-2]─[10.10.14.95]─[balaio2003@htb-wordtpkrqr]─[~/Desktop]

└──╼ [★]$ sudo openvpn starting\_point\_balaio2003.ovpn

2024-07-22 07:06:50 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.

2024-07-22 07:06:50 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.

2024-07-22 07:06:50 OpenVPN 2.6.3 x86\_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]

2024-07-22 07:06:50 library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 2.10

2024-07-22 07:06:50 DCO version: N/A

2024-07-22 07:06:50 TCP/UDP: Preserving recently used remote address: [AF\_INET]38.46.224.104:1337

2024-07-22 07:06:50 Socket Buffers: R=[212992->212992] S=[212992->212992]

2024-07-22 07:06:50 UDPv4 link local: (not bound)

2024-07-22 07:06:50 UDPv4 link remote: [AF\_INET]38.46.224.104:1337

2024-07-22 07:06:50 TLS: Initial packet from [AF\_INET]38.46.224.104:1337, sid=89cd9769 e97c5912

2024-07-22 07:06:50 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority

2024-07-22 07:06:50 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: us-starting-point-1-dhcp Issuing CA

2024-07-22 07:06:50 VERIFY KU OK

2024-07-22 07:06:50 Validating certificate extended key usage

2024-07-22 07:06:50 ++ Certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server Authentication

2024-07-22 07:06:50 ++ Certificate has EKU (oid) 1.3.6.1.5.5.7.3.2, expects TLS Web Server Authentication

2024-07-22 07:06:50 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication

2024-07-22 07:06:50 VERIFY EKU OK

2024-07-22 07:06:50 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=us-starting-point-1-dhcp

2024-07-22 07:06:50 Control Channel: TLSv1.3, cipher TLSv1.3 TLS\_AES\_256\_GCM\_SHA384, peer certificate: 256 bit ED25519, signature: ED25519

2024-07-22 07:06:50 [us-starting-point-1-dhcp] Peer Connection Initiated with [AF\_INET]38.46.224.104:1337

2024-07-22 07:06:50 TLS: move\_session: dest=TM\_ACTIVE src=TM\_INITIAL reinit\_src=1

2024-07-22 07:06:50 TLS: tls\_multi\_process: initial untrusted session promoted to trusted

2024-07-22 07:06:51 SENT CONTROL [us-starting-point-1-dhcp]: 'PUSH\_REQUEST' (status=1)

2024-07-22 07:06:51 PUSH: Received control message: 'PUSH\_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,explicit-exit-notify,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::11eb/64 dead:beef:2::1,ifconfig 10.10.15.237 255.255.254.0,peer-id 16,cipher AES-256-CBC,protocol-flags cc-exit tls-ekm dyn-tls-crypt,tun-mtu 1500'

2024-07-22 07:06:51 OPTIONS IMPORT: --ifconfig/up options modified

2024-07-22 07:06:51 OPTIONS IMPORT: route options modified

2024-07-22 07:06:51 OPTIONS IMPORT: route-related options modified

2024-07-22 07:06:51 OPTIONS IMPORT: tun-mtu set to 1500

2024-07-22 07:06:51 net\_route\_v4\_best\_gw query: dst 0.0.0.0

2024-07-22 07:06:51 net\_route\_v4\_best\_gw result: via 194.113.72.1 dev ens3

2024-07-22 07:06:51 ROUTE\_GATEWAY 194.113.72.1/255.255.252.0 IFACE=ens3 HWADDR=a6:ba:3b:08:2c:50

2024-07-22 07:06:51 GDG6: remote\_host\_ipv6=n/a

2024-07-22 07:06:51 net\_route\_v6\_best\_gw query: dst ::

2024-07-22 07:06:51 sitnl\_send: rtnl: generic error (-101): Network is unreachable

2024-07-22 07:06:51 ROUTE6: default\_gateway=UNDEF

2024-07-22 07:06:51 TUN/TAP device tun1 opened

2024-07-22 07:06:51 net\_iface\_mtu\_set: mtu 1500 for tun1

2024-07-22 07:06:51 net\_iface\_up: set tun1 up

2024-07-22 07:06:51 net\_addr\_v4\_add: 10.10.15.237/23 dev tun1

2024-07-22 07:06:51 net\_iface\_mtu\_set: mtu 1500 for tun1

2024-07-22 07:06:51 net\_iface\_up: set tun1 up

2024-07-22 07:06:51 net\_addr\_v6\_add: dead:beef:2::11eb/64 dev tun1

2024-07-22 07:06:51 net\_route\_v4\_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1

2024-07-22 07:06:51 sitnl\_send: rtnl: generic error (-17): File exists

2024-07-22 07:06:51 NOTE: Linux route add command failed because route exists

2024-07-22 07:06:51 net\_route\_v4\_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1

2024-07-22 07:06:51 sitnl\_send: rtnl: generic error (-17): File exists

2024-07-22 07:06:51 NOTE: Linux route add command failed because route exists

2024-07-22 07:06:51 add\_route\_ipv6(dead:beef::/64 -> dead:beef:2::1 metric -1) dev tun1

2024-07-22 07:06:51 net\_route\_v6\_add: dead:beef::/64 via :: dev tun1 table 0 metric -1

2024-07-22 07:06:51 Initialization Sequence Completed

2024-07-22 07:06:51 Data Channel: cipher 'AES-256-CBC', auth 'SHA256', peer-id: 16, compression: 'lzo'

2024-07-22 07:06:51 Timers: ping 10, ping-restart 120

2024-07-22 07:06:51 Protocol options: explicit-exit-notify 1, protocol-flags cc-exit tls-ekm dyn-tls-crypt

**Below is the IP info and ping to runner VM’s IP of 10.10.11.13.**

┌─[us-free-2]─[10.10.14.95]─[balaio2003@htb-wordtpkrqr]─[~]

└──╼ [★]$ ip a

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid\_lft forever preferred\_lft forever

inet6 ::1/128 scope host noprefixroute

valid\_lft forever preferred\_lft forever

2: ens3: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000

link/ether a6:ba:3b:08:2c:50 brd ff:ff:ff:ff:ff:ff

altname enp0s3

inet 194.113.74.60/22 brd 194.113.75.255 scope global dynamic ens3

valid\_lft 84027sec preferred\_lft 84027sec

inet6 fe80::a4ba:3bff:fe08:2c50/64 scope link

valid\_lft forever preferred\_lft forever

3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UNKNOWN group default qlen 500

link/none

inet 10.10.14.95/23 scope global tun0

valid\_lft forever preferred\_lft forever

inet6 dead:beef:2::105d/64 scope global

valid\_lft forever preferred\_lft forever

inet6 fe80::323b:c970:d38b:8ef4/64 scope link stable-privacy

valid\_lft forever preferred\_lft forever

4: tun1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UNKNOWN group default qlen 500

link/none

inet 10.10.15.237/23 scope global tun1

valid\_lft forever preferred\_lft forever

inet6 dead:beef:2::11eb/64 scope global

valid\_lft forever preferred\_lft forever

inet6 fe80::7841:d21d:da43:74d6/64 scope link stable-privacy

valid\_lft forever preferred\_lft forever

┌─[us-free-2]─[10.10.14.95]─[balaio2003@htb-wordtpkrqr]─[~]

└──╼ [★]$ ping 10.10.11.13

PING 10.10.11.13 (10.10.11.13) 56(84) bytes of data.

64 bytes from 10.10.11.13: icmp\_seq=1 ttl=63 time=8.66 ms

64 bytes from 10.10.11.13: icmp\_seq=2 ttl=63 time=8.57 ms

64 bytes from 10.10.11.13: icmp\_seq=3 ttl=63 time=8.87 ms

64 bytes from 10.10.11.13: icmp\_seq=4 ttl=63 time=8.96 ms

64 bytes from 10.10.11.13: icmp\_seq=5 ttl=63 time=8.74 ms

64 bytes from 10.10.11.13: icmp\_seq=6 ttl=63 time=8.91 ms

64 bytes from 10.10.11.13: icmp\_seq=7 ttl=63 time=8.85 ms

64 bytes from 10.10.11.13: icmp\_seq=8 ttl=63 time=8.78 ms

64 bytes from 10.10.11.13: icmp\_seq=9 ttl=63 time=8.92 ms

64 bytes from 10.10.11.13: icmp\_seq=10 ttl=63 time=8.66 ms

^C

--- 10.10.11.13 ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9014ms

rtt min/avg/max/mdev = 8.572/8.790/8.958/0.125 ms

┌─[us-free-2]─[10.10.14.95]─[balaio2003@htb-wordtpkrqr]─[~]

└──╼ [★]$

Below is the exit code

^C2024-07-22 07:28:44 event\_wait : Interrupted system call (fd=-1,code=4)

2024-07-22 07:28:44 SIGTERM received, sending exit notification to peer

2024-07-22 07:28:44 SENT CONTROL [us-starting-point-1-dhcp]: 'EXIT' (status=1)

2024-07-22 07:28:45 delete\_route\_ipv6(dead:beef::/64)

2024-07-22 07:28:45 net\_route\_v6\_del: dead:beef::/64 via :: dev tun1 table 0 metric -1

2024-07-22 07:28:45 Closing TUN/TAP interface

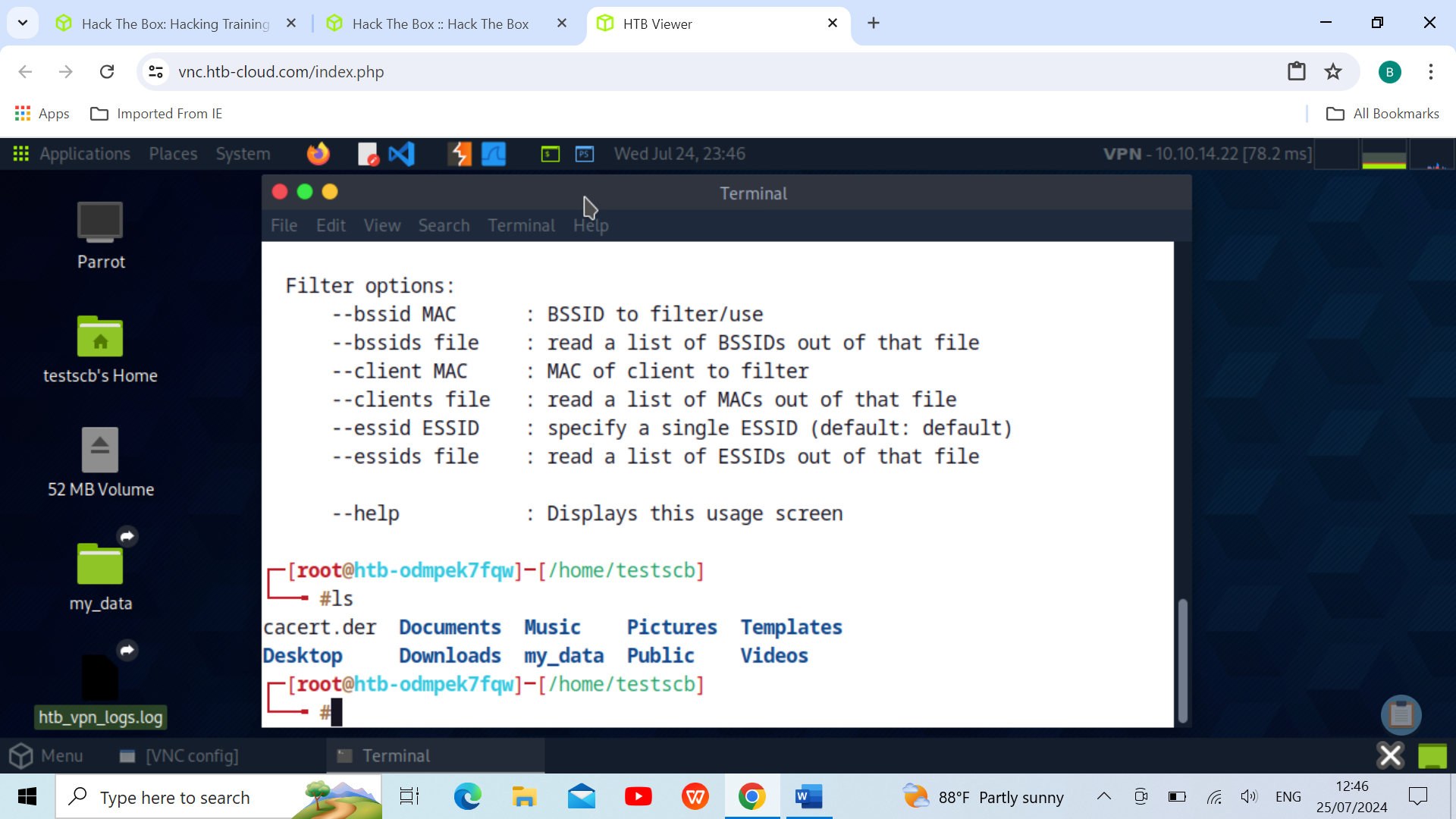
2024-07-22 07:28:45 net\_addr\_v4\_del: 10.10.15.237 dev tun1

2024-07-22 07:28:45 net\_addr\_v6\_del: dead:beef:2::11eb/64 dev tun1

2024-07-22 07:28:45 SIGTERM[soft,exit-with-notification] received, process exiting

┌─[us-free-2]─[10.10.14.95]─[balaio2003@htb-wordtpkrqr]─[~/Desktop]

└──╼ [★]$



**Vulnerability of errors in the system logs**

┌─[root@htb-odmpek7fqw]─[/var/log]

└──╼ #cat \*.\* | grep error

2024-07-25 05:05:49.334+0000 INFO Logging config in use: File '/etc/neo4j/user-logs.xml'

2024-07-25 05:05:49.350+0000 INFO Starting...

2024-07-25 05:05:50.042+0000 INFO This instance is ServerId{302e3b80} (302e3b80-b759-4d31-aae4-91db3c3c7e15)

2024-07-25 05:05:51.038+0000 INFO ======== Neo4j 5.21.0 ========

2024-07-25 05:05:52.243+0000 INFO Anonymous Usage Data is being sent to Neo4j, see <https://neo4j.com/docs/usage-data/>

2024-07-25 04:14:19,255 - subp.py[DEBUG]: Unexpected error while running command.

2024-07-03 12:54:05 install liberror-perl:all <none> 0.17029-2

2024-07-03 12:54:05 status half-installed liberror-perl:all 0.17029-2

2024-07-03 12:54:05 status unpacked liberror-perl:all 0.17029-2

2024-07-03 12:54:15 configure liberror-perl:all 0.17029-2 <none>

2024-07-03 12:54:15 status unpacked liberror-perl:all 0.17029-2

2024-07-03 12:54:15 status half-configured liberror-perl:all 0.17029-2

2024-07-03 12:54:15 status installed liberror-perl:all 0.17029-2

2024-07-03 13:14:51 install libgpg-error-dev:amd64 <none> 1.46-1

2024-07-03 13:14:51 status half-installed libgpg-error-dev:amd64 1.46-1

2024-07-03 13:14:51 status unpacked libgpg-error-dev:amd64 1.46-1

2024-07-03 13:14:52 configure libgpg-error-dev:amd64 1.46-1 <none>

2024-07-03 13:14:52 status unpacked libgpg-error-dev:amd64 1.46-1

2024-07-03 13:14:52 status half-configured libgpg-error-dev:amd64 1.46-1

2024-07-03 13:14:52 status installed libgpg-error-dev:amd64 1.46-1

2024-07-03 13:48:07 install liberror-prone-java:all <none> 2.18.0-1

2024-07-03 13:48:07 status half-installed liberror-prone-java:all 2.18.0-1

2024-07-03 13:48:08 status unpacked liberror-prone-java:all 2.18.0-1

2024-07-03 13:48:08 configure liberror-prone-java:all 2.18.0-1 <none>

2024-07-03 13:48:08 status unpacked liberror-prone-java:all 2.18.0-1

2024-07-03 13:48:08 status half-configured liberror-prone-java:all 2.18.0-1

2024-07-03 13:48:08 status installed liberror-prone-java:all 2.18.0-1

[2024-07-07T10:50:33.596Z] [ warning] [vmsvc] [442] SOCKET failed to create socket, error 97: Address family not supported by protocol

[2024-07-03T20:38:04.980Z] [ message] [desktopEvents] [99273] Emitting tcs\_de\_xioerror due to X I/O error.

[2024-07-03T20:50:19.754Z] [ message] [desktopEvents] [2448] Emitting tcs\_de\_xioerror due to X I/O error.

[2024-07-05T11:26:37.611Z] [ message] [desktopEvents] [2283] Emitting tcs\_de\_xioerror due to X I/O error.

[2024-07-05T12:09:57.308Z] [ message] [desktopEvents] [1880] Emitting tcs\_de\_xioerror due to X I/O error.

(WW) warning, (EE) error, (NI) not implemented, (??) unknown.

(WW) warning, (EE) error, (NI) not implemented, (??) unknown.

2024-07-25 05:05:52.274+0000 INFO Bolt enabled on localhost:7687.

2024-07-25 05:05:52.792+0000 INFO HTTP enabled on localhost:7474.

2024-07-25 05:05:52.792+0000 INFO Remote interface available at http://localhost:7474/

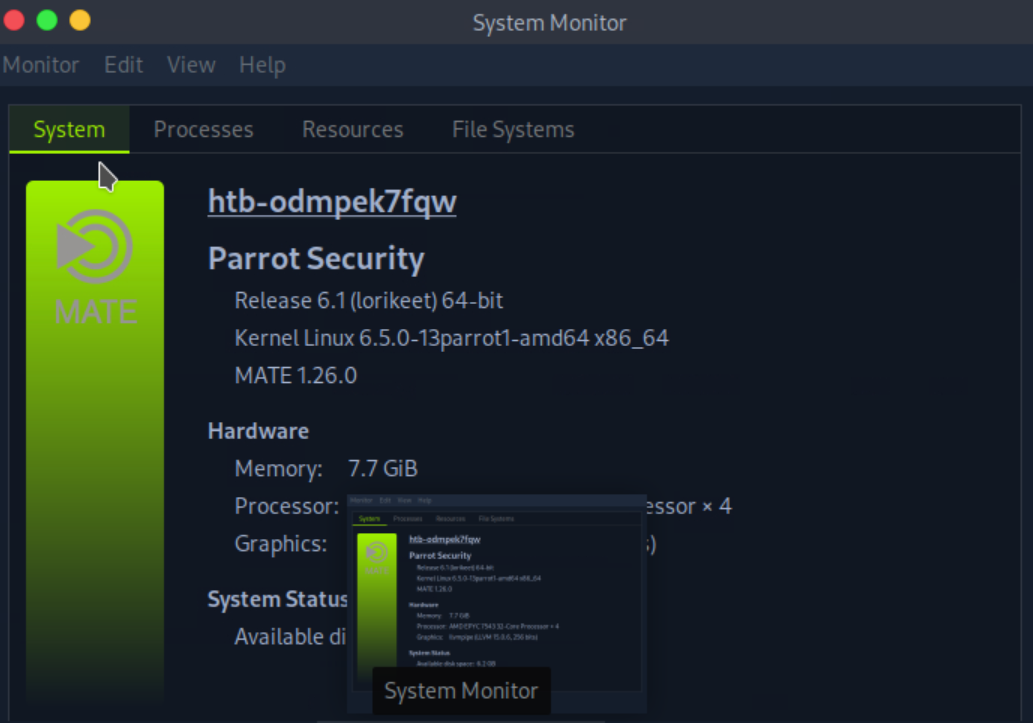
2024-07-25 05:05:52.794+0000 INFO id: 8D677D728406D8A2AC662657BC5360FEF0CD31DE3F2FACB4852830D175612C94

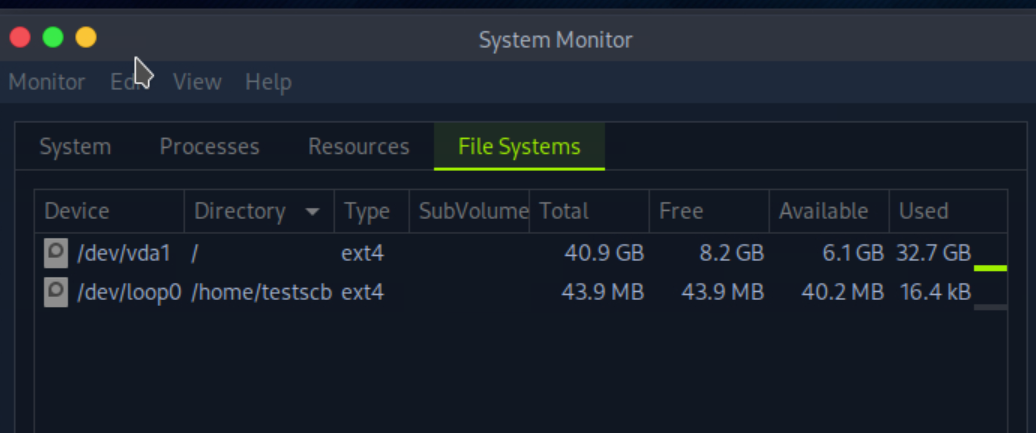
2024-07-25 05:05:52.794+0000 INFO name: system

2024-07-25 05:05:52.795+0000 INFO creationDate: 2024-07-03T20:49:02.392Z

2024-07-25 05:05:52.795+0000 INFO Started.

**System and Capacity of Resources used in the system**





**Vulnerability and the impact to the system**

┌─[root@htb-odmpek7fqw]─[~]

└──╼ #**aircrack-ng -u**

Vendor = AMD

Model = AMD EPYC 7543 32-Core Processor

Features = MMX,SSE,SSE2,SSE3,SSSE3,SSE4.1,SSE4.2,AES-NI,AVX,AVX2

Hypervisor = Yes (Virtualization detected)

Hyper-Threading = Yes

Logical CPUs = 128

Threads per core= 1

CPU cores = 128 (4 total)

SIMD size = 8 (256 bit)

SIMD size in use= 8 (256 bit)

─[root@htb-odmpek7fqw]─[~]

└──╼ #**unix-privesc-check standard**

Assuming the OS is: linux

Starting unix-privesc-check v1.4 ( http://pentestmonkey.net/tools/unix-privesc-check )

This script checks file permissions and other settings that could allow

local users to escalate privileges.

Use of this script is only permitted on systems which you have been granted

legal permission to perform a security assessment of. Apart from this

condition the GPL v2 applies.

Search the output below for the word 'WARNING'. If you don't see it then

this script didn't find any problems.

############################################

Recording hostname

############################################

htb-odmpek7fqw

############################################

Recording uname

############################################

Linux htb-odmpek7fqw 6.5.0-13parrot1-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.5.13-1parrot1 (2023-12-19) x86\_64 GNU/Linux

############################################

Recording Interface IP addresses

############################################

ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 209.94.57.17 netmask 255.255.252.0 broadcast 209.94.59.255

inet6 fe80::a4ba:3bff:fe08:503d prefixlen 64 scopeid 0x20<link>

ether a6:ba:3b:08:50:3d txqueuelen 1000 (Ethernet)

RX packets 395998 bytes 203935697 (194.4 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 282393 bytes 485614674 (463.1 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 595721 bytes 493892157 (471.0 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 595721 bytes 493892157 (471.0 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500

inet 10.10.14.22 netmask 255.255.254.0 destination 10.10.14.22

inet6 dead:beef:2::1014 prefixlen 64 scopeid 0x0<global>

inet6 fe80::3a94:b6bd:77ff:cf86 prefixlen 64 scopeid 0x20<link>

unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)

RX packets 4129 bytes 346836 (338.7 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 4158 bytes 348876 (340.6 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

############################################

Checking if external authentication is allowed in /etc/passwd

############################################

No +:... line found in /etc/passwd

############################################

Checking nsswitch.conf for addition authentication methods

############################################

Neither LDAP nor NIS are used for authentication

############################################

Checking for writable config files

############################################

Checking if anyone except root can change /etc/passwd

Checking if anyone except root can change /etc/group

Checking if anyone except root can change /etc/fstab

Checking if anyone except root can change /etc/profile

Checking if anyone except root can change /etc/sudoers

Checking if anyone except root can change /etc/shadow

############################################

Checking if /etc/shadow is readable

############################################

Checking if anyone except root can read file /etc/shadow

############################################

Checking for password hashes in /etc/passwd

############################################

No password hashes found in /etc/passwd

############################################

Checking account settings

############################################

Checking for accounts with no passwords

############################################

Checking library directories from /etc/ld.so.conf

############################################

############################################

Checking sudo configuration

############################################

-----------------

Checking if sudo is configured

WARNING: Sudo is configured. Manually check nothing unsafe is allowed:

root ALL=(ALL:ALL) ALL

ALL ALL=(ALL) NOPASSWD: ALL

-----------------

Checking sudo users need a password

WARNING: Some users can use sudo without a password:

ALL ALL=(ALL) NOPASSWD: ALL

############################################

Checking permissions on swap file(s)

############################################

Checking if anyone except root can change /swapfile

Checking if anyone except root can read file /swapfile

Checking if anyone except root can change /dev/vda5

Checking if anyone except root can read file /dev/vda5

############################################

Checking programs run from inittab

############################################

File /etc/inittab not present. Skipping checks.

############################################

Checking postgres trust relationships

############################################

No postgres trusts detected

############################################

Checking permissions on device files for mounted partitions

############################################

############################################

Checking cron job programs aren't writable (/etc/crontab)

############################################

Crontab path is /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

Processing crontab run-parts entry: 17 \* \* \* \* root cd / && run-parts --report /etc/cron.hourly

Checking if anyone except root can change /etc/cron.hourly

Checking directory: /etc/cron.hourly

No files in this directory.

Processing crontab run-parts entry: 25 6 \* \* \* root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }

Checking if anyone except root can change /etc/cron.daily;

Processing crontab run-parts entry: 47 6 \* \* 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }

Checking if anyone except root can change /etc/cron.weekly;

Processing crontab run-parts entry: 52 6 1 \* \* root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }

Checking if anyone except root can change /etc/cron.monthly;

Processing crontab entry: 17 \* \* \* \* root cd / && run-parts --report /etc/cron.hourly

ERROR: Can't find absolute path for cd. Skipping.

Processing crontab entry: 25 6 \* \* \* root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }

Checking if anyone except root can change /bin/test

Processing crontab entry: 47 6 \* \* 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }

Checking if anyone except root can change /bin/test

Processing crontab entry: 52 6 1 \* \* root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }

Checking if anyone except root can change /bin/test

############################################

Checking cron job programs aren't writable (/var/spool/cron/crontabs)

############################################

No user crontabs found in /var/spool/cron/crontabs. Skipping checks.

############################################

Checking cron job programs aren't writable (/var/spool/cron/tabs)

############################################

Directory /var/spool/cron/tabs is not present. Skipping checks.

############################################

Checking inetd programs aren't writable

############################################

File /etc/inetd.conf not present. Skipping checks.

############################################

Checking xinetd programs aren't writeable

############################################

Directory /etc/xinetd.d not present. Skipping checks.

############################################

Checking home directories aren't writable

############################################

Processing /etc/passwd line: root:x:0:0:root:/root:/bin/bash

Checking if anyone except root can change /root

Processing /etc/passwd line: daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

Checking if anyone except daemon can change /usr/sbin

Processing /etc/passwd line: bin:x:2:2:bin:/bin:/usr/sbin/nologin

Checking if anyone except bin can change /bin

Processing /etc/passwd line: sys:x:3:3:sys:/dev:/usr/sbin/nologin

Checking if anyone except sys can change /dev

Processing /etc/passwd line: sync:x:4:65534:sync:/bin:/bin/sync

Checking if anyone except sync can change /bin

Processing /etc/passwd line: games:x:5:60:games:/usr/games:/usr/sbin/nologin

Checking if anyone except games can change /usr/games

Processing /etc/passwd line: man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

Checking if anyone except man can change /var/cache/man

Processing /etc/passwd line: lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

Checking if anyone except lp can change /var/spool/lpd

Processing /etc/passwd line: mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

Checking if anyone except mail can change /var/mail

Processing /etc/passwd line: news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

Checking if anyone except news can change /var/spool/news

Processing /etc/passwd line: uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

Checking if anyone except uucp can change /var/spool/uucp

Processing /etc/passwd line: proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

Checking if anyone except proxy can change /bin

Processing /etc/passwd line: www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

Checking if anyone except www-data can change /var/www

Processing /etc/passwd line: backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

Checking if anyone except backup can change /var/backups

Processing /etc/passwd line: list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

Checking if anyone except list can change /var/list

Processing /etc/passwd line: irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin

Checking if anyone except irc can change /run/ircd

Processing /etc/passwd line: \_apt:x:42:65534::/nonexistent:/usr/sbin/nologin

Checking if anyone except \_apt can change /nonexistent

Processing /etc/passwd line: nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

Checking if anyone except nobody can change /nonexistent

Processing /etc/passwd line: systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin

Checking if anyone except systemd-network can change /

Processing /etc/passwd line: tss:x:100:107:TPM software stack,,,:/var/lib/tpm:/bin/false

Skipping user tss. They don't have a shell.

Processing /etc/passwd line: systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin

Checking if anyone except systemd-timesync can change /

Processing /etc/passwd line: messagebus:x:101:108::/nonexistent:/usr/sbin/nologin

Checking if anyone except messagebus can change /nonexistent

Processing /etc/passwd line: usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin

Checking if anyone except usbmux can change /var/lib/usbmux

Processing /etc/passwd line: dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin

Checking if anyone except dnsmasq can change /var/lib/misc

Processing /etc/passwd line: avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin

Checking if anyone except avahi can change /run/avahi-daemon

Processing /etc/passwd line: fwupd-refresh:x:106:115:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin

Checking if anyone except fwupd-refresh can change /run/systemd

Processing /etc/passwd line: saned:x:107:117::/var/lib/saned:/usr/sbin/nologin

Checking if anyone except saned can change /var/lib/saned

Processing /etc/passwd line: geoclue:x:108:118::/var/lib/geoclue:/usr/sbin/nologin

Checking if anyone except geoclue can change /var/lib/geoclue

Processing /etc/passwd line: polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin

Checking if anyone except polkitd can change /nonexistent

Processing /etc/passwd line: rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin

Checking if anyone except rtkit can change /proc

Processing /etc/passwd line: colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin

Checking if anyone except colord can change /var/lib/colord

Processing /etc/passwd line: gnome-initial-setup:x:111:65534::/run/gnome-initial-setup/:/bin/false

Skipping user gnome-initial-setup. They don't have a shell.

Processing /etc/passwd line: Debian-gdm:x:112:121:Gnome Display Manager:/var/lib/gdm3:/bin/false

Skipping user Debian-gdm. They don't have a shell.

Processing /etc/passwd line: sshd:x:113:65534::/run/sshd:/usr/sbin/nologin

Checking if anyone except sshd can change /run/sshd

Processing /etc/passwd line: lightdm:x:114:122:Light Display Manager:/var/lib/lightdm:/bin/false

Skipping user lightdm. They don't have a shell.

Processing /etc/passwd line: strongswan:x:115:65534::/var/lib/strongswan:/usr/sbin/nologin

Checking if anyone except strongswan can change /var/lib/strongswan

Processing /etc/passwd line: pulse:x:116:123:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin

Checking if anyone except pulse can change /run/pulse

Processing /etc/passwd line: nm-openvpn:x:117:125:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin

Checking if anyone except nm-openvpn can change /var/lib/openvpn/chroot

Processing /etc/passwd line: nm-openconnect:x:118:126:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin

Checking if anyone except nm-openconnect can change /var/lib/NetworkManager

Processing /etc/passwd line: debian:x:1001:1001:Debian:/home/debian:/bin/bash

Checking if anyone except debian can change /home/debian

Processing /etc/passwd line: arpwatch:x:105:127:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh

Checking if anyone except arpwatch can change /var/lib/arpwatch

Processing /etc/passwd line: inetsim:x:119:128::/var/lib/inetsim:/usr/sbin/nologin

Checking if anyone except inetsim can change /var/lib/inetsim

Processing /etc/passwd line: postgres:x:120:129:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash

Checking if anyone except postgres can change /var/lib/postgresql

Processing /etc/passwd line: miredo:x:121:65534::/var/run/miredo:/usr/sbin/nologin

Checking if anyone except miredo can change /var/run/miredo

Processing /etc/passwd line: ntpsec:x:122:130::/nonexistent:/usr/sbin/nologin

Checking if anyone except ntpsec can change /nonexistent

Processing /etc/passwd line: redis:x:123:131::/var/lib/redis:/usr/sbin/nologin

Checking if anyone except redis can change /var/lib/redis

Processing /etc/passwd line: \_gvm:x:124:132::/var/lib/openvas:/usr/sbin/nologin

Checking if anyone except \_gvm can change /var/lib/openvas

Processing /etc/passwd line: mysql:x:125:133:MySQL Server,,,:/nonexistent:/bin/false

Skipping user mysql. They don't have a shell.

Processing /etc/passwd line: tcpdump:x:126:135::/nonexistent:/usr/sbin/nologin

Checking if anyone except tcpdump can change /nonexistent

Processing /etc/passwd line: stunnel4:x:993:993:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin

Checking if anyone except stunnel4 can change /var/run/stunnel4

Processing /etc/passwd line: neo4j:x:127:136:neo4j,,,:/var/lib/neo4j:/bin/bash

Checking if anyone except neo4j can change /var/lib/neo4j

Processing /etc/passwd line: \_rpc:x:128:65534::/run/rpcbind:/usr/sbin/nologin

Checking if anyone except \_rpc can change /run/rpcbind

Processing /etc/passwd line: statd:x:129:65534::/var/lib/nfs:/usr/sbin/nologin

Checking if anyone except statd can change /var/lib/nfs

Processing /etc/passwd line: htb:x:1000:1000:htb,,,:/home/htb:/bin/bash

Checking if anyone except htb can change /home/htb

Processing /etc/passwd line: testscb:x:1002:1002:,,,:/home/testscb:/bin/bash

Checking if anyone except testscb can change /home/testscb

############################################

Checking for readable sensitive files in home directories

############################################

Checking if anyone except root can read file /root/.ssh/authorized\_keys

Checking if anyone except root can read file /root/.bash\_history

Checking if anyone except debian can read file /home/debian/.ssh/authorized\_keys

Checking if anyone except htb can read file /home/htb/.bash\_history

Checking if anyone except testscb can read file /home/testscb/.bash\_history

############################################

Checking SUID programs

############################################

Skipping checks of SUID programs (it's slow!). Run again in 'detailed' mode.

############################################

Checking for Private SSH Keys home directories

############################################

############################################

Checking for Public SSH Keys home directories

############################################

WARNING: Public SSH Key Found in /root/.ssh/authorized\_keys

############################################

Checking for SSH agents

############################################

WARNING: There are SSH agents running on this system:

testscb 2967 2874 0 Jul24 ? 00:00:00 /usr/bin/ssh-agent /usr/bin/im-launch x-session-manager

############################################

Checking for GPG agents

############################################

No GPG agents found

############################################

Checking startup files (init.d / rc.d) aren't writable

############################################

Processing startup script /etc/init.d/README

Checking if anyone except root can change /etc/init.d/README

Processing startup script /etc/init.d/alsa-utils

Checking if anyone except root can change /etc/init.d/alsa-utils

Processing startup script /etc/init.d/anacron

Checking if anyone except root can change /etc/init.d/anacron

Processing startup script /etc/init.d/apache-htcacheclean

Checking if anyone except root can change /etc/init.d/apache-htcacheclean

Processing startup script /etc/init.d/apache2

Checking if anyone except root can change /etc/init.d/apache2

Processing startup script /etc/init.d/apparmor

Checking if anyone except root can change /etc/init.d/apparmor

Processing startup script /etc/init.d/arpwatch

Checking if anyone except root can change /etc/init.d/arpwatch

Processing startup script /etc/init.d/binfmt-support

Checking if anyone except root can change /etc/init.d/binfmt-support

Processing startup script /etc/init.d/cloud-config

Checking if anyone except root can change /etc/init.d/cloud-config

Processing startup script /etc/init.d/cloud-final

Checking if anyone except root can change /etc/init.d/cloud-final

Processing startup script /etc/init.d/cloud-init

Checking if anyone except root can change /etc/init.d/cloud-init

Processing startup script /etc/init.d/cloud-init-local

Checking if anyone except root can change /etc/init.d/cloud-init-local

Processing startup script /etc/init.d/console-setup.sh

Checking if anyone except root can change /etc/init.d/console-setup.sh

Processing startup script /etc/init.d/cron

Checking if anyone except root can change /etc/init.d/cron

Processing startup script /etc/init.d/cups

Checking if anyone except root can change /etc/init.d/cups

Processing startup script /etc/init.d/cups-browsed

Checking if anyone except root can change /etc/init.d/cups-browsed

Processing startup script /etc/init.d/darkstat

Checking if anyone except root can change /etc/init.d/darkstat

Processing startup script /etc/init.d/dbus

Checking if anyone except root can change /etc/init.d/dbus

Processing startup script /etc/init.d/docker

Checking if anyone except root can change /etc/init.d/docker

Processing startup script /etc/init.d/gdm3

Checking if anyone except root can change /etc/init.d/gdm3

Processing startup script /etc/init.d/hwclock.sh

Checking if anyone except root can change /etc/init.d/hwclock.sh

Processing startup script /etc/init.d/inetsim

Checking if anyone except root can change /etc/init.d/inetsim

Processing startup script /etc/init.d/ipsec

Checking if anyone except root can change /etc/init.d/ipsec

Processing startup script /etc/init.d/keyboard-setup.sh

Checking if anyone except root can change /etc/init.d/keyboard-setup.sh

Processing startup script /etc/init.d/kmod

Checking if anyone except root can change /etc/init.d/kmod

Processing startup script /etc/init.d/lightdm

Checking if anyone except root can change /etc/init.d/lightdm

Processing startup script /etc/init.d/mariadb

Checking if anyone except root can change /etc/init.d/mariadb

Processing startup script /etc/init.d/miredo

Checking if anyone except root can change /etc/init.d/miredo

Processing startup script /etc/init.d/neo4j

Checking if anyone except root can change /etc/init.d/neo4j

Processing startup script /etc/init.d/networking

Checking if anyone except root can change /etc/init.d/networking

Processing startup script /etc/init.d/nfs-common

Checking if anyone except root can change /etc/init.d/nfs-common

Processing startup script /etc/init.d/nmbd

Checking if anyone except root can change /etc/init.d/nmbd

Processing startup script /etc/init.d/ntpsec

Checking if anyone except root can change /etc/init.d/ntpsec

Processing startup script /etc/init.d/open-vm-tools

Checking if anyone except root can change /etc/init.d/open-vm-tools

Processing startup script /etc/init.d/openvpn

Checking if anyone except root can change /etc/init.d/openvpn

Processing startup script /etc/init.d/pcscd

Checking if anyone except root can change /etc/init.d/pcscd

Processing startup script /etc/init.d/plymouth

Checking if anyone except root can change /etc/init.d/plymouth

Processing startup script /etc/init.d/plymouth-log

Checking if anyone except root can change /etc/init.d/plymouth-log

Processing startup script /etc/init.d/postgresql

Checking if anyone except root can change /etc/init.d/postgresql

Processing startup script /etc/init.d/procps

Checking if anyone except root can change /etc/init.d/procps

Processing startup script /etc/init.d/ptunnel

Checking if anyone except root can change /etc/init.d/ptunnel

Processing startup script /etc/init.d/pulseaudio-enable-autospawn

Checking if anyone except root can change /etc/init.d/pulseaudio-enable-autospawn

Processing startup script /etc/init.d/rc

Checking if anyone except root can change /etc/init.d/rc

Processing startup script /etc/init.d/rcS

Checking if anyone except root can change /etc/init.d/rcS

Processing startup script /etc/init.d/redis-server

Checking if anyone except root can change /etc/init.d/redis-server

Processing startup script /etc/init.d/rpcbind

Checking if anyone except root can change /etc/init.d/rpcbind

Processing startup script /etc/init.d/rsync

Checking if anyone except root can change /etc/init.d/rsync

Processing startup script /etc/init.d/samba-ad-dc

Checking if anyone except root can change /etc/init.d/samba-ad-dc

Processing startup script /etc/init.d/saned

Checking if anyone except root can change /etc/init.d/saned

Processing startup script /etc/init.d/screen-cleanup

Checking if anyone except root can change /etc/init.d/screen-cleanup

Processing startup script /etc/init.d/smbd

Checking if anyone except root can change /etc/init.d/smbd

Processing startup script /etc/init.d/ssh

Checking if anyone except root can change /etc/init.d/ssh

Processing startup script /etc/init.d/stunnel4

Checking if anyone except root can change /etc/init.d/stunnel4

Processing startup script /etc/init.d/sudo

Checking if anyone except root can change /etc/init.d/sudo

Processing startup script /etc/init.d/sysstat

Checking if anyone except root can change /etc/init.d/sysstat

Processing startup script /etc/init.d/udev

Checking if anyone except root can change /etc/init.d/udev

Processing startup script /etc/init.d/ufw

Checking if anyone except root can change /etc/init.d/ufw

Processing startup script /etc/init.d/x11-common

Checking if anyone except root can change /etc/init.d/x11-common

Processing startup script /etc/init.d/xl2tpd

Checking if anyone except root can change /etc/init.d/xl2tpd

############################################

Checking if running programs are writable

############################################

------------------------

PID: 1

Owner: root

Program path: /usr/lib/systemd/systemd

Checking if anyone except root can change /usr/lib/systemd/systemd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1031

Owner: root

Program path: /usr/lib/xorg/Xorg

Checking if anyone except root can change /usr/lib/xorg/Xorg

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1035

Owner: root

Program path: /usr/sbin/agetty

Checking if anyone except root can change /usr/sbin/agetty

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1057

Owner: root

Program path: /usr/sbin/xl2tpd

Checking if anyone except root can change /usr/sbin/xl2tpd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 11

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 112541

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1130

Owner: root

Program path: /usr/sbin/lightdm

Checking if anyone except root can change /usr/sbin/lightdm

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1134

Owner: lightdm

Program path: /usr/lib/systemd/systemd

Checking if anyone except lightdm can change /usr/lib/systemd/systemd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1135

Owner: lightdm

Program path: /usr/lib/systemd/systemd

Checking if anyone except lightdm can change /usr/lib/systemd/systemd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1161

Owner: lightdm

Program path: /usr/bin/pipewire

Checking if anyone except lightdm can change /usr/bin/pipewire

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1164

Owner: lightdm

Program path: /usr/bin/wireplumber

Checking if anyone except lightdm can change /usr/bin/wireplumber

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1165

Owner: lightdm

Program path: /usr/bin/pipewire

Checking if anyone except lightdm can change /usr/bin/pipewire

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1166

Owner: lightdm

Program path: /usr/sbin/slick-greeter

Checking if anyone except lightdm can change /usr/sbin/slick-greeter

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1167

Owner: lightdm

Program path: /usr/bin/dbus-daemon

Checking if anyone except lightdm can change /usr/bin/dbus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1172

Owner: rtkit

Program path: /usr/libexec/rtkit-daemon

Checking if anyone except rtkit can change /usr/libexec/rtkit-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1185

Owner: lightdm

Program path: /usr/libexec/dconf-service

Checking if anyone except lightdm can change /usr/libexec/dconf-service

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1186

Owner: lightdm

Program path: /usr/libexec/gvfsd

Checking if anyone except lightdm can change /usr/libexec/gvfsd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 12

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1204

Owner: lightdm

Program path: /usr/libexec/gvfsd-fuse

Checking if anyone except lightdm can change /usr/libexec/gvfsd-fuse

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 122

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 13

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 135

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1350

Owner: lightdm

Program path: /usr/libexec/at-spi-bus-launcher

Checking if anyone except lightdm can change /usr/libexec/at-spi-bus-launcher

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 136

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1368

Owner: lightdm

Program path: /usr/bin/dbus-daemon

Checking if anyone except lightdm can change /usr/bin/dbus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 139362

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 14

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1477

Owner: root

Program path: /usr/libexec/upowerd

Checking if anyone except root can change /usr/libexec/upowerd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 15

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1502

Owner: lightdm

Program path: /usr/libexec/tracker-miner-fs-3

Checking if anyone except lightdm can change /usr/libexec/tracker-miner-fs-3

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 153

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 155

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 156

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 157

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 158

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1580

Owner: lightdm

Program path: /usr/libexec/gvfs-udisks2-volume-monitor

Checking if anyone except lightdm can change /usr/libexec/gvfs-udisks2-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 16

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1616

Owner: lightdm

Program path: /usr/libexec/gvfs-afc-volume-monitor

Checking if anyone except lightdm can change /usr/libexec/gvfs-afc-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 162

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1626

Owner: lightdm

Program path: /usr/libexec/gvfs-gphoto2-volume-monitor

Checking if anyone except lightdm can change /usr/libexec/gvfs-gphoto2-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1633

Owner: lightdm

Program path: /usr/libexec/gvfs-mtp-volume-monitor

Checking if anyone except lightdm can change /usr/libexec/gvfs-mtp-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1644

Owner: lightdm

Program path: /usr/libexec/gvfs-goa-volume-monitor

Checking if anyone except lightdm can change /usr/libexec/gvfs-goa-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 164817

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 164818

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 164858

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1658

Owner: lightdm

Program path: /usr/libexec/goa-daemon

Checking if anyone except lightdm can change /usr/libexec/goa-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 167504

Owner: testscb

Program path: /usr/libexec/gvfsd-network

Checking if anyone except testscb can change /usr/libexec/gvfsd-network

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 167545

Owner: testscb

Program path: /usr/libexec/gvfsd-dnssd

Checking if anyone except testscb can change /usr/libexec/gvfsd-dnssd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 167657

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 17

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 1743

Owner: lightdm

Program path: /usr/libexec/goa-identity-service

Checking if anyone except lightdm can change /usr/libexec/goa-identity-service

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 18

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 185320

Owner: root

Program path: /usr/sbin/sshd

Checking if anyone except root can change /usr/sbin/sshd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 185563

Owner: testscb

Program path: /usr/bin/bash

Checking if anyone except testscb can change /usr/bin/bash

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 185574

Owner: root

Program path: /usr/bin/sudo

Checking if anyone except root can change /usr/bin/sudo

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 185575

Owner: root

Program path: /usr/bin/bash

Checking if anyone except root can change /usr/bin/bash

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 186758

Owner: root

Program path: /usr/bin/dash

Checking if anyone except root can change /usr/bin/dash

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 19

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 20

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 204

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 205

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 21

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2105

Owner: root

Program path: /usr/sbin/lightdm

Checking if anyone except root can change /usr/sbin/lightdm

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2107

Owner: lightdm

Program path: /usr/libexec/at-spi2-registryd

Checking if anyone except lightdm can change /usr/libexec/at-spi2-registryd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 22

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2247

Owner: root

Program path: /opt/htb/pwnbox-insights

Checking if anyone except root can change /opt/htb/pwnbox-insights

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 23

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 25

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 26

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2602

Owner: \_rpc

Program path: /usr/sbin/rpcbind

Checking if anyone except \_rpc can change /usr/sbin/rpcbind

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 27

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2727

Owner: root

Program path: /usr/lib/systemd/systemd

Checking if anyone except root can change /usr/lib/systemd/systemd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2728

Owner: root

Program path: /usr/lib/systemd/systemd

Checking if anyone except root can change /usr/lib/systemd/systemd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2744

Owner: root

Program path: /usr/bin/pipewire

Checking if anyone except root can change /usr/bin/pipewire

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2745

Owner: root

Program path: /usr/bin/wireplumber

Checking if anyone except root can change /usr/bin/wireplumber

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2746

Owner: root

Program path: /usr/bin/pipewire

Checking if anyone except root can change /usr/bin/pipewire

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2749

Owner: root

Program path: /usr/bin/dbus-daemon

Checking if anyone except root can change /usr/bin/dbus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2767

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2768

Owner: root

Program path: /usr/sbin/sshd

Checking if anyone except root can change /usr/sbin/sshd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 277

Owner: root

Program path: /usr/lib/systemd/systemd-journald

Checking if anyone except root can change /usr/lib/systemd/systemd-journald

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 28

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2865

Owner: testscb

Program path: /usr/bin/perl

Checking if anyone except testscb can change /usr/bin/perl

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2866

Owner: testscb

Program path: /usr/bin/Xtigervnc

Checking if anyone except testscb can change /usr/bin/Xtigervnc

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2869

Owner: testscb

Program path: /usr/bin/dash

Checking if anyone except testscb can change /usr/bin/dash

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2873

Owner: testscb

Program path: /usr/bin/tigervncconfig

Checking if anyone except testscb can change /usr/bin/tigervncconfig

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2874

Owner: testscb

Program path: /usr/bin/mate-session

Checking if anyone except testscb can change /usr/bin/mate-session

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2899

Owner: testscb

Program path: /usr/bin/dbus-launch

Checking if anyone except testscb can change /usr/bin/dbus-launch

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 29

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2900

Owner: testscb

Program path: /usr/bin/dbus-daemon

Checking if anyone except testscb can change /usr/bin/dbus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2922

Owner: testscb

Program path: /usr/libexec/dconf-service

Checking if anyone except testscb can change /usr/libexec/dconf-service

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2951

Owner: testscb

Program path: /usr/bin/dbus-launch

Checking if anyone except testscb can change /usr/bin/dbus-launch

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2952

Owner: testscb

Program path: /usr/bin/dbus-daemon

Checking if anyone except testscb can change /usr/bin/dbus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2967

Owner: testscb

Program path: /usr/bin/ssh-agent

Checking if anyone except testscb can change /usr/bin/ssh-agent

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2984

Owner: testscb

Program path: /usr/bin/ibus-daemon

Checking if anyone except testscb can change /usr/bin/ibus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2988

Owner: testscb

Program path: /usr/libexec/gvfsd

Checking if anyone except testscb can change /usr/libexec/gvfsd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2993

Owner: testscb

Program path: /usr/libexec/gvfsd-fuse

Checking if anyone except testscb can change /usr/libexec/gvfsd-fuse

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2995

Owner: testscb

Program path: /usr/libexec/ibus-memconf

Checking if anyone except testscb can change /usr/libexec/ibus-memconf

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 2997

Owner: testscb

Program path: /usr/libexec/ibus-ui-gtk3

Checking if anyone except testscb can change /usr/libexec/ibus-ui-gtk3

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3006

Owner: testscb

Program path: /usr/libexec/ibus-extension-gtk3

Checking if anyone except testscb can change /usr/libexec/ibus-extension-gtk3

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3009

Owner: testscb

Program path: /usr/libexec/ibus-x11

Checking if anyone except testscb can change /usr/libexec/ibus-x11

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3012

Owner: testscb

Program path: /usr/libexec/ibus-portal

Checking if anyone except testscb can change /usr/libexec/ibus-portal

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3017

Owner: testscb

Program path: /usr/libexec/at-spi-bus-launcher

Checking if anyone except testscb can change /usr/libexec/at-spi-bus-launcher

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3022

Owner: testscb

Program path: /usr/bin/dbus-daemon

Checking if anyone except testscb can change /usr/bin/dbus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3034

Owner: testscb

Program path: /usr/libexec/xdg-desktop-portal

Checking if anyone except testscb can change /usr/libexec/xdg-desktop-portal

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3035

Owner: testscb

Program path: /usr/libexec/at-spi2-registryd

Checking if anyone except testscb can change /usr/libexec/at-spi2-registryd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3043

Owner: testscb

Program path: /usr/libexec/xdg-document-portal

Checking if anyone except testscb can change /usr/libexec/xdg-document-portal

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3048

Owner: testscb

Program path: /usr/libexec/xdg-permission-store

Checking if anyone except testscb can change /usr/libexec/xdg-permission-store

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 305

Owner: root

Program path: /usr/bin/udevadm

Checking if anyone except root can change /usr/bin/udevadm

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3057

Owner: root

Program path: /usr/bin/fusermount3

Checking if anyone except root can change /usr/bin/fusermount3

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 30617

Owner: root

Program path: /usr/sbin/cupsd

Checking if anyone except root can change /usr/sbin/cupsd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 30619

Owner: root

Program path: /usr/sbin/cups-browsed

Checking if anyone except root can change /usr/sbin/cups-browsed

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3062

Owner: testscb

Program path: /usr/libexec/xdg-desktop-portal-gnome

Checking if anyone except testscb can change /usr/libexec/xdg-desktop-portal-gnome

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 31

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3118

Owner: testscb

Program path: /usr/libexec/dconf-service

Checking if anyone except testscb can change /usr/libexec/dconf-service

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3129

Owner: testscb

Program path: /usr/bin/mate-screensaver

Checking if anyone except testscb can change /usr/bin/mate-screensaver

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3133

Owner: testscb

Program path: /usr/bin/gnome-keyring-daemon

Checking if anyone except testscb can change /usr/bin/gnome-keyring-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3140

Owner: testscb

Program path: /usr/bin/mate-settings-daemon

Checking if anyone except testscb can change /usr/bin/mate-settings-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3154

Owner: testscb

Program path: /usr/libexec/xdg-desktop-portal-gtk

Checking if anyone except testscb can change /usr/libexec/xdg-desktop-portal-gtk

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3159

Owner: testscb

Program path: /usr/bin/marco

Checking if anyone except testscb can change /usr/bin/marco

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 32

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3222

Owner: testscb

Program path: /usr/libexec/ibus-engine-simple

Checking if anyone except testscb can change /usr/libexec/ibus-engine-simple

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3223

Owner: testscb

Program path: /usr/bin/caja

Checking if anyone except testscb can change /usr/bin/caja

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3230

Owner: testscb

Program path: /usr/lib/x86\_64-linux-gnu/brisk-menu/brisk-menu

Checking if anyone except testscb can change /usr/lib/x86\_64-linux-gnu/brisk-menu/brisk-menu

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3236

Owner: testscb

Program path: /usr/libexec/gvfs-udisks2-volume-monitor

Checking if anyone except testscb can change /usr/libexec/gvfs-udisks2-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3246

Owner: testscb

Program path: /usr/libexec/gvfs-afc-volume-monitor

Checking if anyone except testscb can change /usr/libexec/gvfs-afc-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3258

Owner: testscb

Program path: /usr/libexec/gvfs-gphoto2-volume-monitor

Checking if anyone except testscb can change /usr/libexec/gvfs-gphoto2-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3263

Owner: testscb

Program path: /usr/libexec/gvfs-mtp-volume-monitor

Checking if anyone except testscb can change /usr/libexec/gvfs-mtp-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 32655

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3270

Owner: testscb

Program path: /usr/libexec/gvfs-goa-volume-monitor

Checking if anyone except testscb can change /usr/libexec/gvfs-goa-volume-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3281

Owner: testscb

Program path: /usr/libexec/goa-daemon

Checking if anyone except testscb can change /usr/libexec/goa-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3282

Owner: testscb

Program path: /usr/bin/nm-applet

Checking if anyone except testscb can change /usr/bin/nm-applet

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 33

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3300

Owner: testscb

Program path: /usr/libexec/goa-identity-service

Checking if anyone except testscb can change /usr/libexec/goa-identity-service

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3308

Owner: testscb

Program path: /usr/libexec/evolution-data-server/evolution-alarm-notify

Checking if anyone except testscb can change /usr/libexec/evolution-data-server/evolution-alarm-notify

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3310

Owner: testscb

Program path: /usr/bin/mate-volume-control-status-icon

Checking if anyone except testscb can change /usr/bin/mate-volume-control-status-icon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3316

Owner: testscb

Program path: /usr/bin/python3.11

Checking if anyone except testscb can change /usr/bin/python3.11

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3321

Owner: testscb

Program path: /usr/lib/mate-panel/notification-area-applet

Checking if anyone except testscb can change /usr/lib/mate-panel/notification-area-applet

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3322

Owner: testscb

Program path: /usr/lib/mate-panel/clock-applet

Checking if anyone except testscb can change /usr/lib/mate-panel/clock-applet

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3325

Owner: testscb

Program path: /usr/libexec/geoclue-2.0/demos/agent

Checking if anyone except testscb can change /usr/libexec/geoclue-2.0/demos/agent

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 34

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3442

Owner: testscb

Program path: /usr/bin/dbus-daemon

Checking if anyone except testscb can change /usr/bin/dbus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3450

Owner: testscb

Program path: /usr/libexec/dconf-service

Checking if anyone except testscb can change /usr/libexec/dconf-service

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3496

Owner: testscb

Program path: /usr/libexec/evolution-source-registry

Checking if anyone except testscb can change /usr/libexec/evolution-source-registry

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 35

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3505

Owner: testscb

Program path: /usr/bin/mate-panel

Checking if anyone except testscb can change /usr/bin/mate-panel

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3559

Owner: testscb

Program path: /usr/libexec/evolution-calendar-factory

Checking if anyone except testscb can change /usr/libexec/evolution-calendar-factory

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3579

Owner: testscb

Program path: /usr/libexec/evolution-addressbook-factory

Checking if anyone except testscb can change /usr/libexec/evolution-addressbook-factory

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3583

Owner: testscb

Program path: /usr/libexec/gvfsd-metadata

Checking if anyone except testscb can change /usr/libexec/gvfsd-metadata

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3600

Owner: testscb

Program path: /usr/lib/mate-panel/wnck-applet

Checking if anyone except testscb can change /usr/lib/mate-panel/wnck-applet

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3605

Owner: testscb

Program path: /usr/lib/mate-applets/command-applet

Checking if anyone except testscb can change /usr/lib/mate-applets/command-applet

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3607

Owner: testscb

Program path: /usr/lib/mate-applets/mate-multiload-applet

Checking if anyone except testscb can change /usr/lib/mate-applets/mate-multiload-applet

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 37

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3703

Owner: testscb

Program path: /usr/bin/python3.11

Checking if anyone except testscb can change /usr/bin/python3.11

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3880

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3881

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 39

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 3931

Owner: root

Program path: /usr/sbin/openvpn

Checking if anyone except root can change /usr/sbin/openvpn

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 4

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 4032

Owner: ntpsec

Program path: /usr/sbin/ntpd

Checking if anyone except ntpsec can change /usr/sbin/ntpd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 42

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 4245

Owner: testscb

Program path: /usr/libexec/gvfsd-trash

Checking if anyone except testscb can change /usr/libexec/gvfsd-trash

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 428

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 43

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 4345

Owner: testscb

Program path: /usr/bin/python3.11

Checking if anyone except testscb can change /usr/bin/python3.11

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 44

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 44849

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 44852

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 48

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 49

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 49664

Owner: root

Program path: /usr/bin/more

Checking if anyone except root can change /usr/bin/more

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 5

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 50

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 51

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 52

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 53

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 54

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 55

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 56

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 5771

Owner: testscb

Program path: /usr/libexec/gnome-terminal-server

Checking if anyone except testscb can change /usr/libexec/gnome-terminal-server

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 58

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 5801

Owner: testscb

Program path: /usr/bin/bash

Checking if anyone except testscb can change /usr/bin/bash

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 5811

Owner: root

Program path: /usr/bin/sudo

Checking if anyone except root can change /usr/bin/sudo

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 5812

Owner: root

Program path: /usr/bin/bash

Checking if anyone except root can change /usr/bin/bash

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 58483

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 59

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 6

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 60

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 61

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 615

Owner: root

Program path: /usr/sbin/dhclient

Checking if anyone except root can change /usr/sbin/dhclient

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 62

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 68

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 70

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 71

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 719

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 72

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 720

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 763

Owner: root

Program path: /usr/libexec/accounts-daemon

Checking if anyone except root can change /usr/libexec/accounts-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 766

Owner: avahi

Program path: /usr/sbin/avahi-daemon

Checking if anyone except avahi can change /usr/sbin/avahi-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 767

Owner: root

Program path: /usr/sbin/cron

Checking if anyone except root can change /usr/sbin/cron

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 768

Owner: messagebus

Program path: /usr/bin/dbus-daemon

Checking if anyone except messagebus can change /usr/bin/dbus-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 77

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 771

Owner: root

Program path: /usr/libexec/low-memory-monitor

Checking if anyone except root can change /usr/libexec/low-memory-monitor

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 777

Owner: polkitd

Program path: /usr/lib/polkit-1/polkitd

Checking if anyone except polkitd can change /usr/lib/polkit-1/polkitd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 778

Owner: root

Program path: /usr/libexec/power-profiles-daemon

Checking if anyone except root can change /usr/libexec/power-profiles-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 779

Owner: root

Program path: /usr/libexec/switcheroo-control

Checking if anyone except root can change /usr/libexec/switcheroo-control

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 780

Owner: root

Program path: /usr/lib/systemd/systemd-logind

Checking if anyone except root can change /usr/lib/systemd/systemd-logind

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 781

Owner: root

Program path: /usr/libexec/udisks2/udisksd

Checking if anyone except root can change /usr/libexec/udisks2/udisksd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 783

Owner: avahi

Program path: /usr/sbin/avahi-daemon

Checking if anyone except avahi can change /usr/sbin/avahi-daemon

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 8

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 81

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 836

ERROR: Can't find full path of running program:

Owner: root

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 841

Owner: root

Program path: /usr/sbin/NetworkManager

Checking if anyone except root can change /usr/sbin/NetworkManager

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 871

Owner: root

Program path: /usr/sbin/wpa\_supplicant

Checking if anyone except root can change /usr/sbin/wpa\_supplicant

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 872

Owner: root

Program path: /usr/sbin/ModemManager

Checking if anyone except root can change /usr/sbin/ModemManager

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 920

Owner: root

Program path: /usr/sbin/lightdm

Checking if anyone except root can change /usr/sbin/lightdm

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

------------------------

PID: 925

Owner: root

Program path: /usr/bin/containerd

Checking if anyone except root can change /usr/bin/containerd

/usr/bin/unix-privesc-check: 1076: [: standard: unexpected operator

┌─[root@htb-odmpek7fqw]─[~]

──╼ #

**Attack path of the route from the IP address**

└──╼ **[★]$ nmap -v -**A google.com.sg

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 01:19 CDT

NSE: Loaded 156 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 01:19

Completed NSE at 01:19, 0.00s elapsed

Initiating NSE at 01:19

Completed NSE at 01:19, 0.00s elapsed

Initiating NSE at 01:19

Completed NSE at 01:19, 0.00s elapsed

Initiating Ping Scan at 01:19

Scanning google.com.sg (142.250.64.67) [4 ports]

Completed Ping Scan at 01:19, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 01:19

Completed Parallel DNS resolution of 1 host. at 01:19, 0.00s elapsed

Initiating SYN Stealth Scan at 01:19

Scanning google.com.sg (142.250.64.67) [1000 ports]

Completed SYN Stealth Scan at 01:19, 21.05s elapsed (1000 total ports)

Initiating Service scan at 01:19

Initiating OS detection (try #1) against google.com.sg (142.250.64.67)

Retrying OS detection (try #2) against google.com.sg (142.250.64.67)

Initiating Traceroute at 01:19

Completed Traceroute at 01:19, 0.02s elapsed

Initiating Parallel DNS resolution of 8 hosts. at 01:19

Completed Parallel DNS resolution of 8 hosts. at 01:19, 0.11s elapsed

NSE: Script scanning 142.250.64.67.

Initiating NSE at 01:19

Completed NSE at 01:19, 5.01s elapsed

Initiating NSE at 01:19

Completed NSE at 01:19, 0.00s elapsed

Initiating NSE at 01:19

Completed NSE at 01:19, 0.00s elapsed

Nmap scan report for google.com.sg (142.250.64.67)

Host is up (0.0011s latency).

Other addresses for google.com.sg (not scanned): 2607:f8b0:4006:823::2003

rDNS record for 142.250.64.67: lga34s30-in-f3.1e100.net

All 1000 scanned ports on google.com.sg (142.250.64.67) are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: printer|webcam

Running (JUST GUESSING): Sharp embedded (94%), TRENDnet embedded (94%)

OS CPE: cpe:/h:sharp:ar-c260m cpe:/h:sharp:ar-m351n cpe:/h:trendnet:tv-ip100

Aggressive OS guesses: Sharp AR-C260M or AR-M351N printer (94%), TRENDnet TV-IP100 webcam (94%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 9 hops

TRACEROUTE (using proto 1/icmp)

HOP RTT ADDRESS

1 0.65 ms 209.94.56.1

2 0.72 ms 100.70.203.145

3 0.72 ms 172.24.250.30

4 0.69 ms 172.24.255.213

5 0.68 ms 172.24.255.253

6 1.03 ms core1-0-2-0.lga.net.google.com (198.32.160.130)

7 2.12 ms 192.178.106.113

8 2.19 ms 142.250.46.195

9 1.13 ms lga34s30-in-f3.1e100.net (142.250.64.67)

NSE: Script Post-scanning.

Initiating NSE at 01:19

Completed NSE at 01:19, 0.00s elapsed

Initiating NSE at 01:19

Completed NSE at 01:19, 0.00s elapsed

Initiating NSE at 01:19

Completed NSE at 01:19, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

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

Nmap done: 1 IP address (1 host up) scanned in 28.86 seconds

Raw packets sent: 2050 (93.148KB) | Rcvd: 16 (1.060KB)

┌─[eu-free-1]─[10.10.14.22]─[testscb@htb-odmpek7fqw]─[/root]

I have never used Parrot Linux in my working live, I always use Enterprise license linux which have the standard commands to do the testing and pentrations but this need more time to learn the Parrot linux kernel commands and the OS bash is totally different from standard linux.

Please provide more time like 2 weeks to really do a total test on this Simulation which need time to learn.