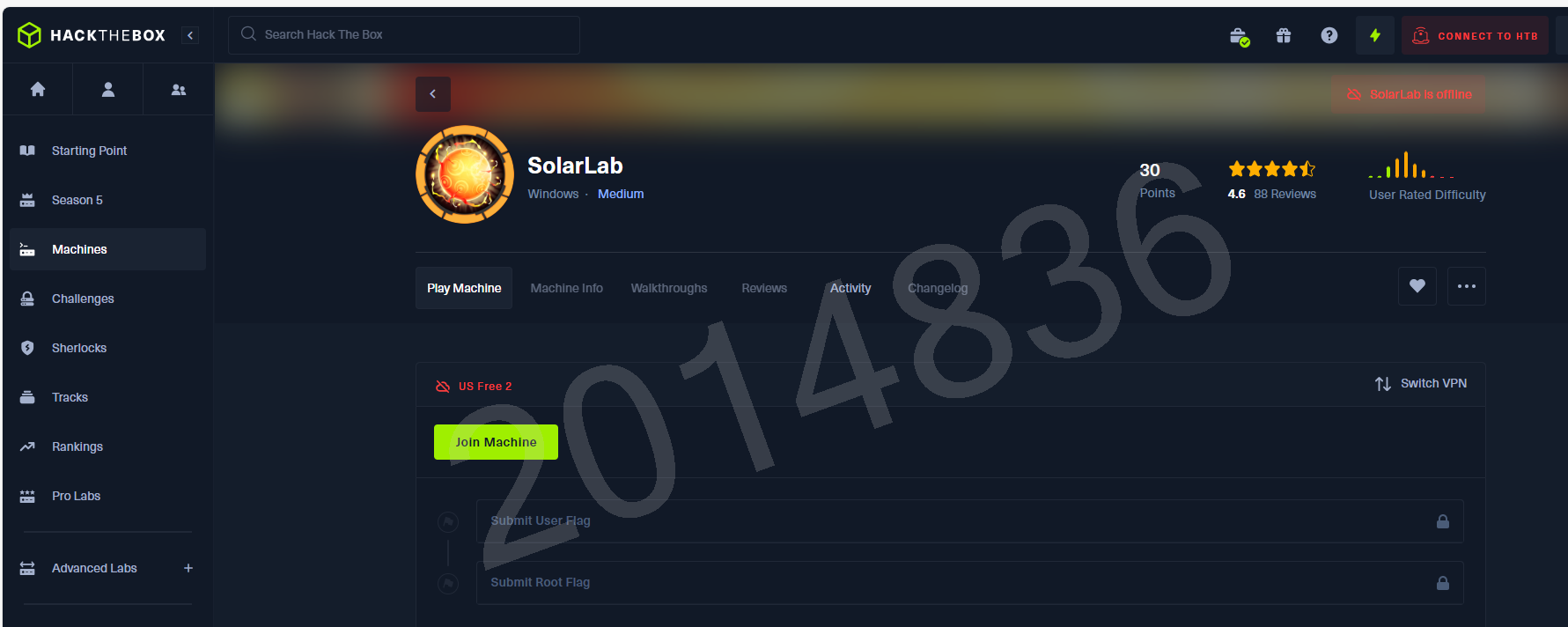
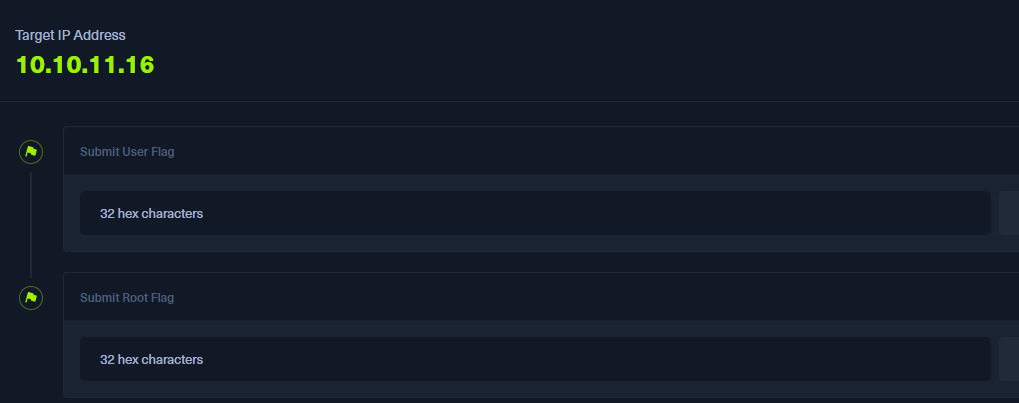
**Penetration Testing - Handson Exercise:**

* 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.

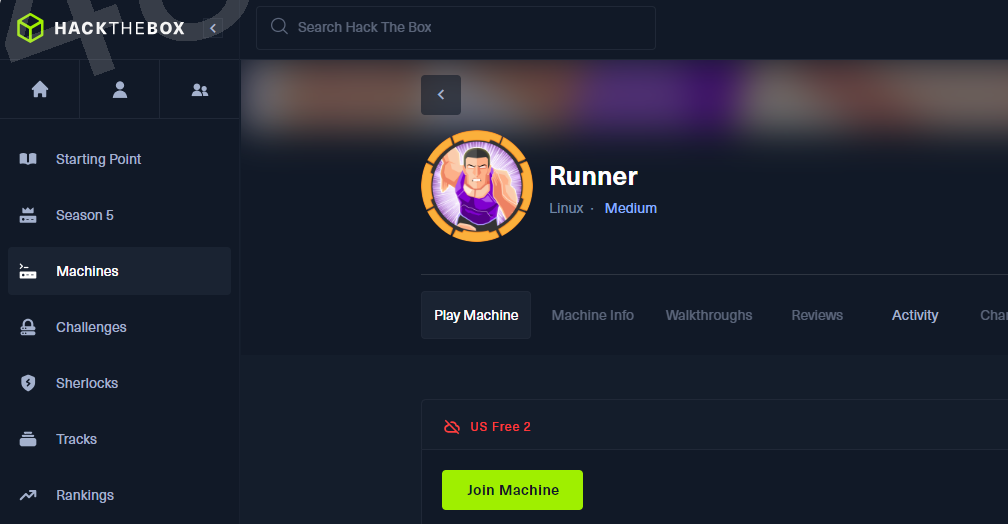
1. Screenshot of **SolarLab** Machine



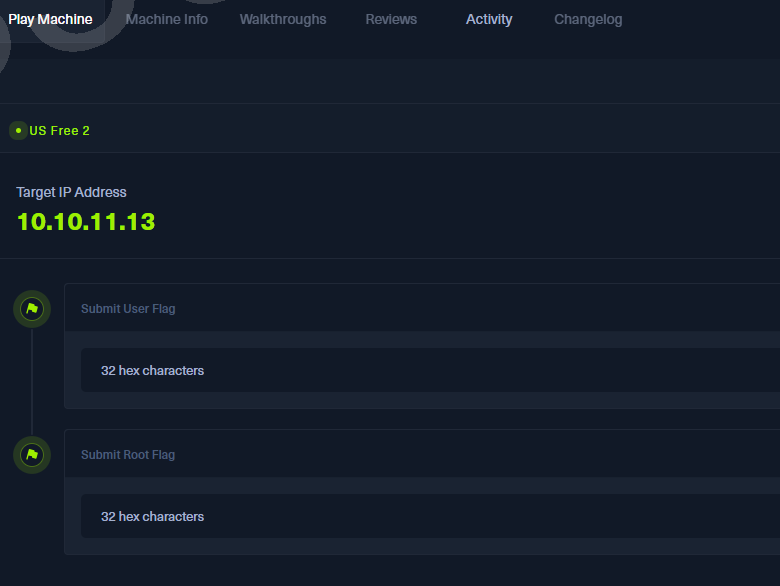
**Target IP**



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

Identify the vulnerability and explain the impact: Sent packets are not compressed

Create a attack path diagram with attack vector.

Identify the suitable mitigation plan and map it to benchmark standards

Create a report with apt screenshot/evidences, map the threats against MITRE framework

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]

└──╼ [★]$

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.