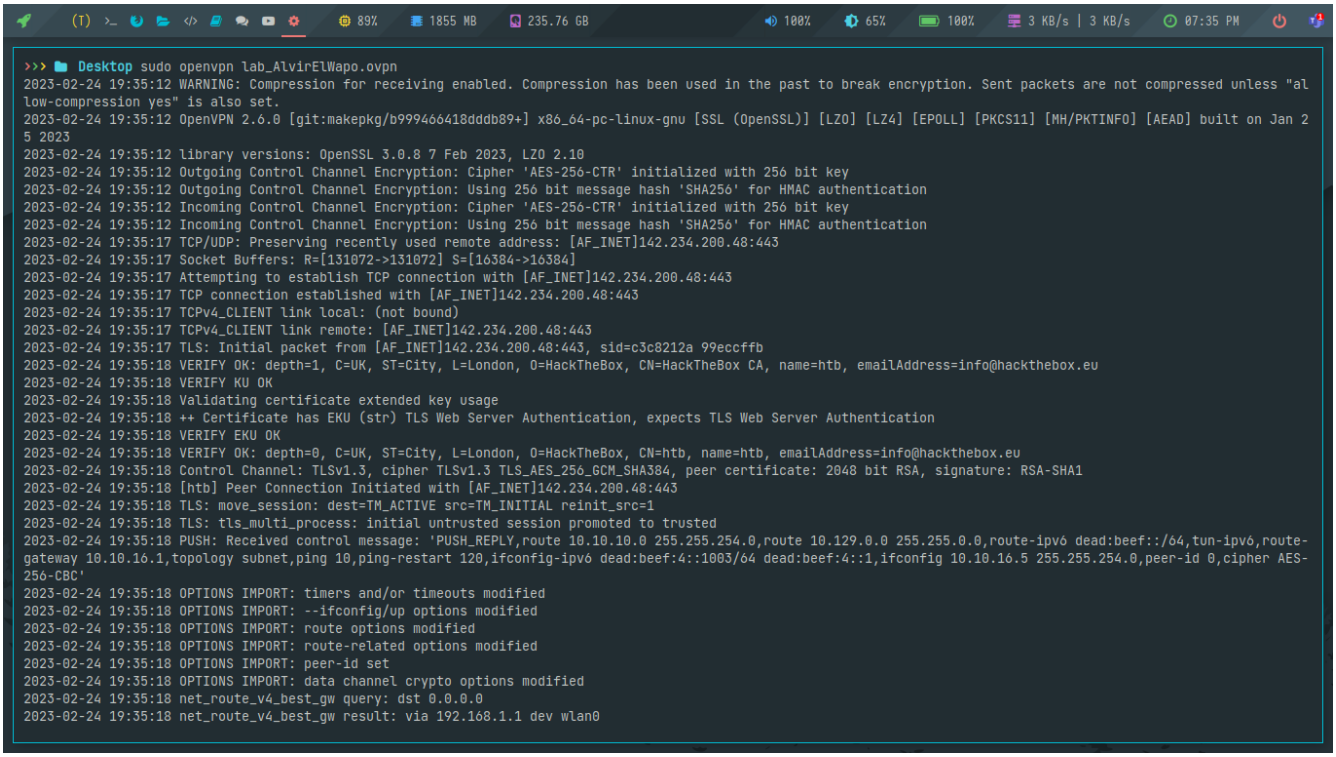
Universidad Autónoma del Estado de México
Unidad Académica Profesional Tianguistenco

Producto de Práctica Hydra

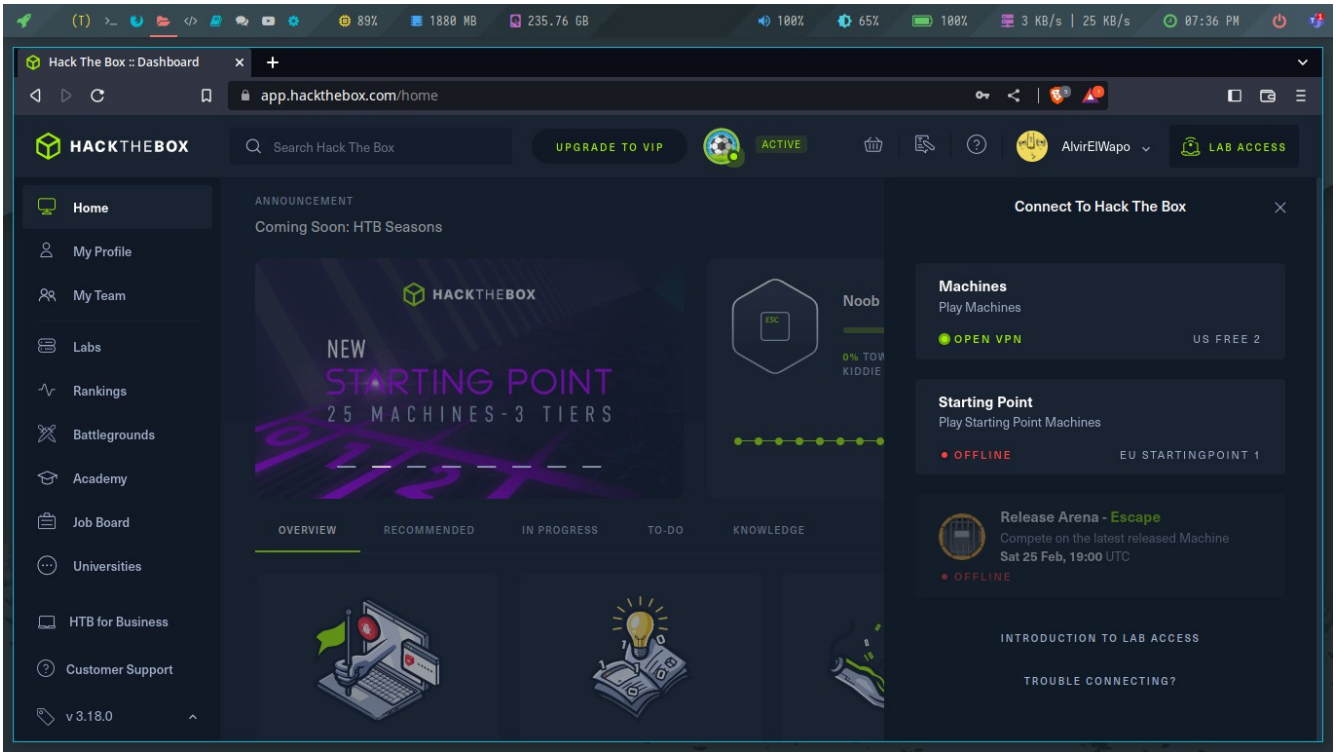
Seguridad Informática

Andrés Alvir Guzmán

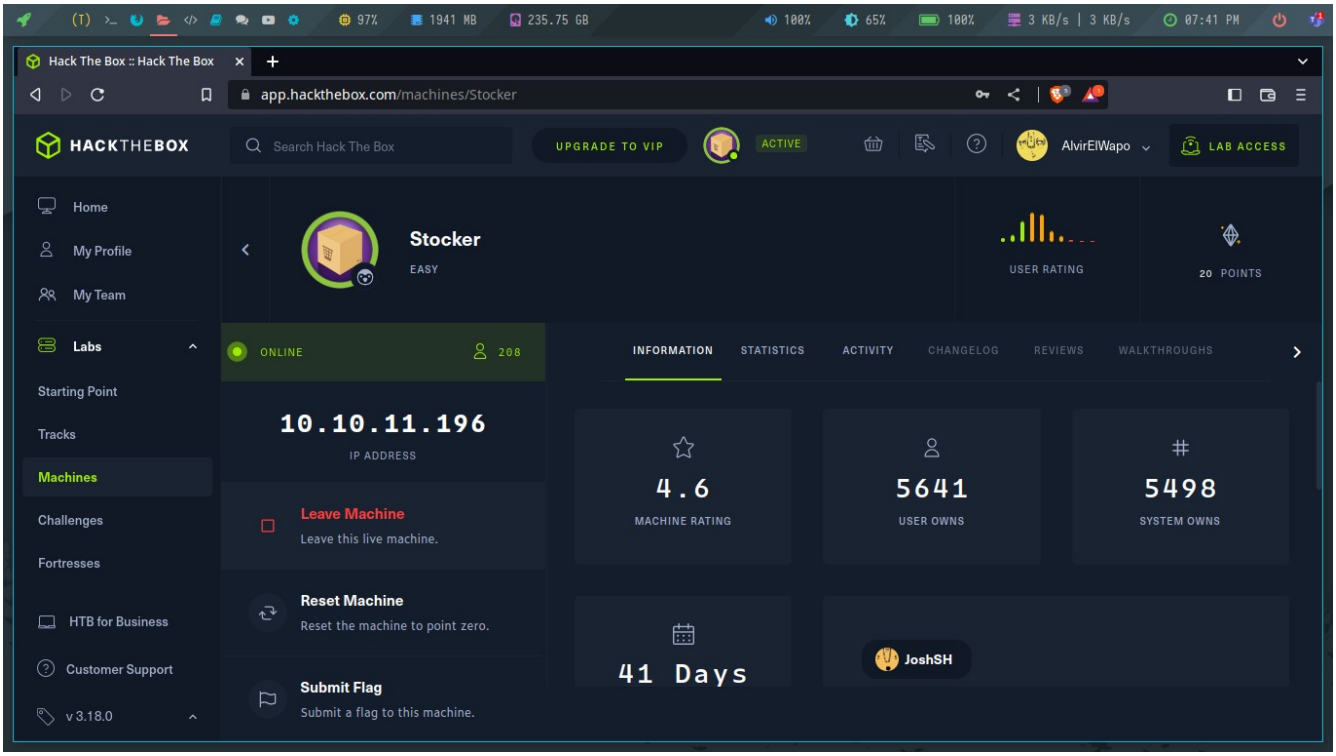
Primer paso: Acceder a la VPN de máquinas de Hack The Box:



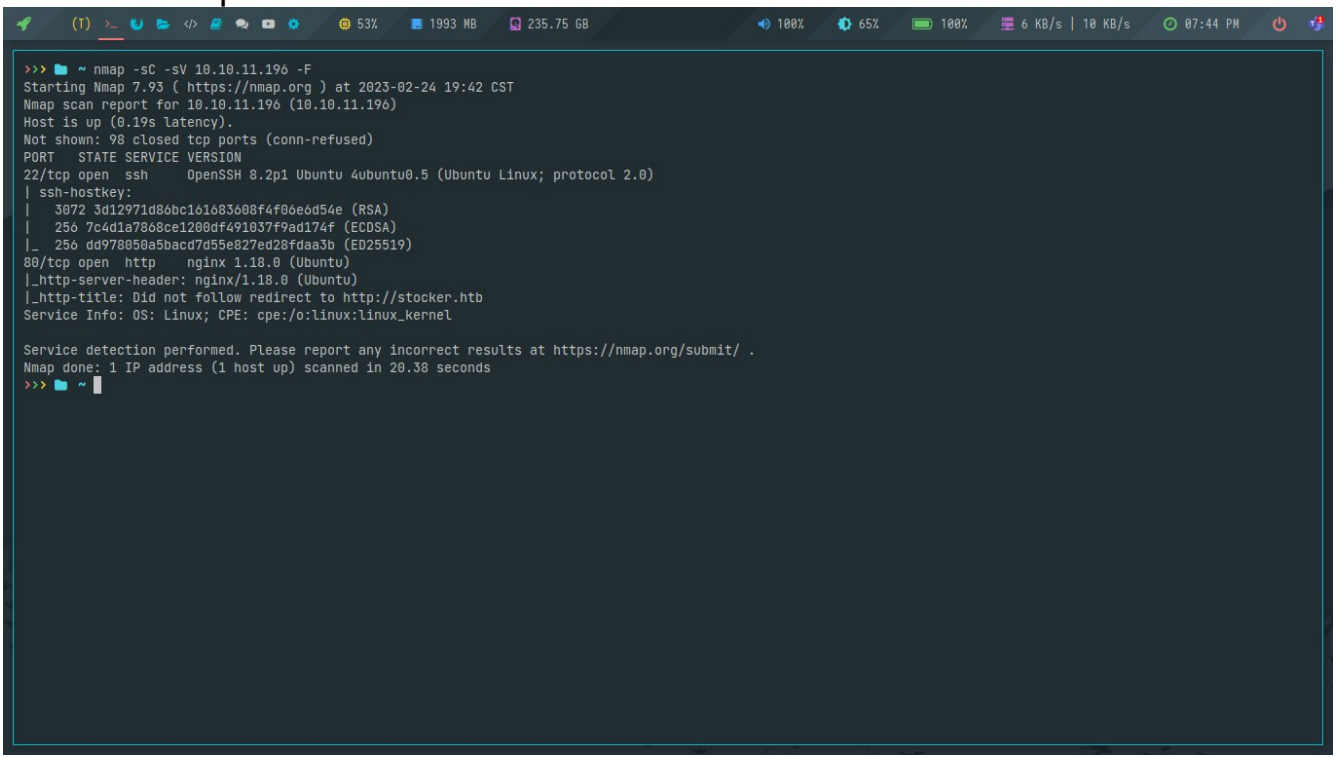
```
>>> Desktop sudo openvpn lab_AlvirElWapo.ovpn
2023-02-24 19:35:12 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2023-02-24 19:35:12 OpenVPN 2.6.0 [git:makepkg/b999466418dddb89+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jan 25 2023
2023-02-24 19:35:12 library versions: OpenSSL 3.0.8 7 Feb 2023, LZO 2.10
2023-02-24 19:35:12 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2023-02-24 19:35:12 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
2023-02-24 19:35:12 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2023-02-24 19:35:12 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
2023-02-24 19:35:17 TCP/UDP: Preserving recently used remote address: [AF_INET]142.234.200.48:443
2023-02-24 19:35:17 Socket Buffers: R=[131072->131072] S=[16384->16384]
2023-02-24 19:35:17 Attempting to establish TCP connection with [AF_INET]142.234.200.48:443
2023-02-24 19:35:17 TCP connection established with [AF_INET]142.234.200.48:443
2023-02-24 19:35:17 TCPv4_CLIENT link local: (not bound)
2023-02-24 19:35:17 TCPv4_CLIENT link remote: [AF_INET]142.234.200.48:443
2023-02-24 19:35:17 TLS: Initial packet from [AF_INET]142.234.200.48:443, sid=c3c8212a 99eccffb
2023-02-24 19:35:18 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2023-02-24 19:35:18 VERIFY KU OK
2023-02-24 19:35:18 Validating certificate extended key usage
2023-02-24 19:35:18 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2023-02-24 19:35:18 VERIFY EKU OK
2023-02-24 19:35:18 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2023-02-24 19:35:18 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RSA, signature: RSA-SHA1
2023-02-24 19:35:18 [htb] Peer Connection Initiated with [AF_INET]142.234.200.48:443
2023-02-24 19:35:18 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2023-02-24 19:35:18 TLS: tls_multi_process: initial untrusted session promoted to trusted
2023-02-24 19:35:18 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,tun-ipv6,route-gateway 10.10.16.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:4::1003/64 dead:beef:4::1,ifconfig 10.10.16.5 255.255.254.0,peer-id 0,cipher AES-256-CBC'
2023-02-24 19:35:18 OPTIONS IMPORT: timers and/or timeouts modified
2023-02-24 19:35:18 OPTIONS IMPORT: --ifconfig/up options modified
2023-02-24 19:35:18 OPTIONS IMPORT: route options modified
2023-02-24 19:35:18 OPTIONS IMPORT: route-related options modified
2023-02-24 19:35:18 OPTIONS IMPORT: peer-id set
2023-02-24 19:35:18 OPTIONS IMPORT: data channel crypto options modified
2023-02-24 19:35:18 net_route_v4_best_gw query: dst 0.0.0.0
2023-02-24 19:35:18 net_route_v4_best_gw result: via 192.168.1.1 dev wlan0
```



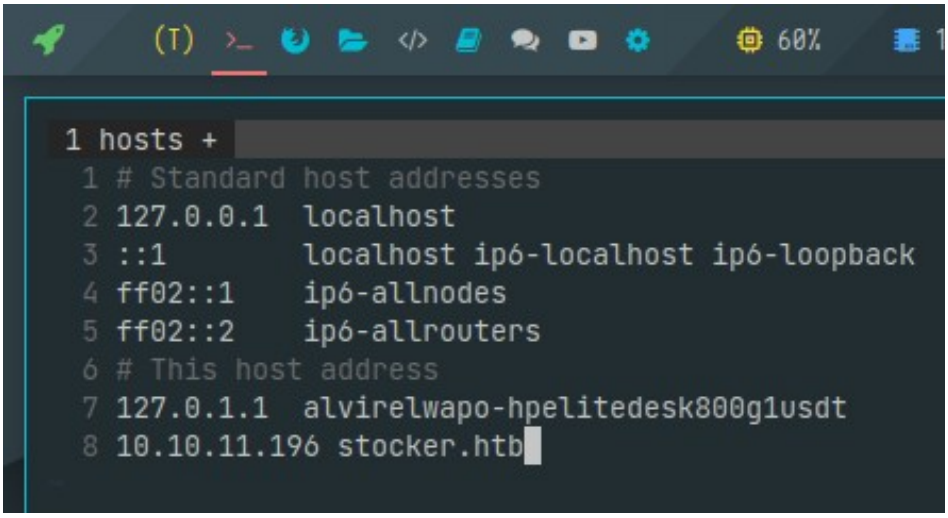
Paso 2: Iniciar la máquina seleccionada en la presentación

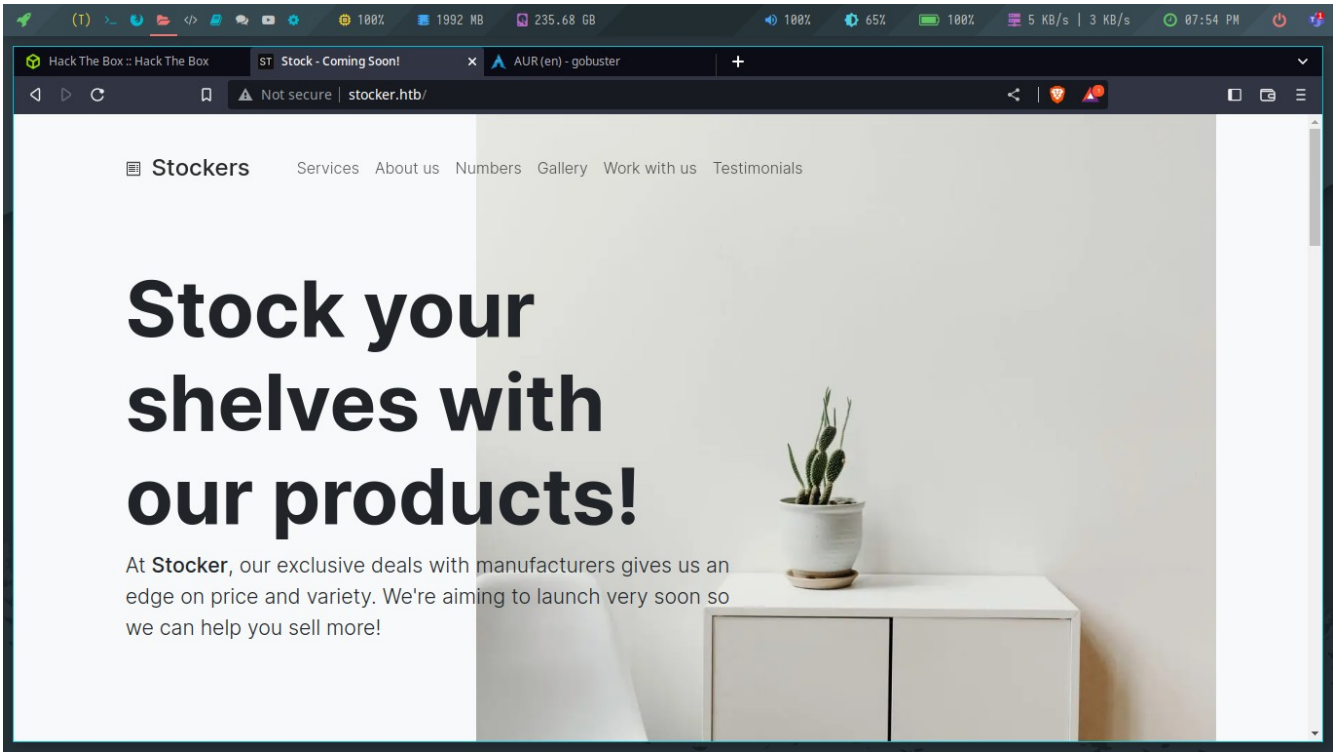


Paso 3: Nmap…

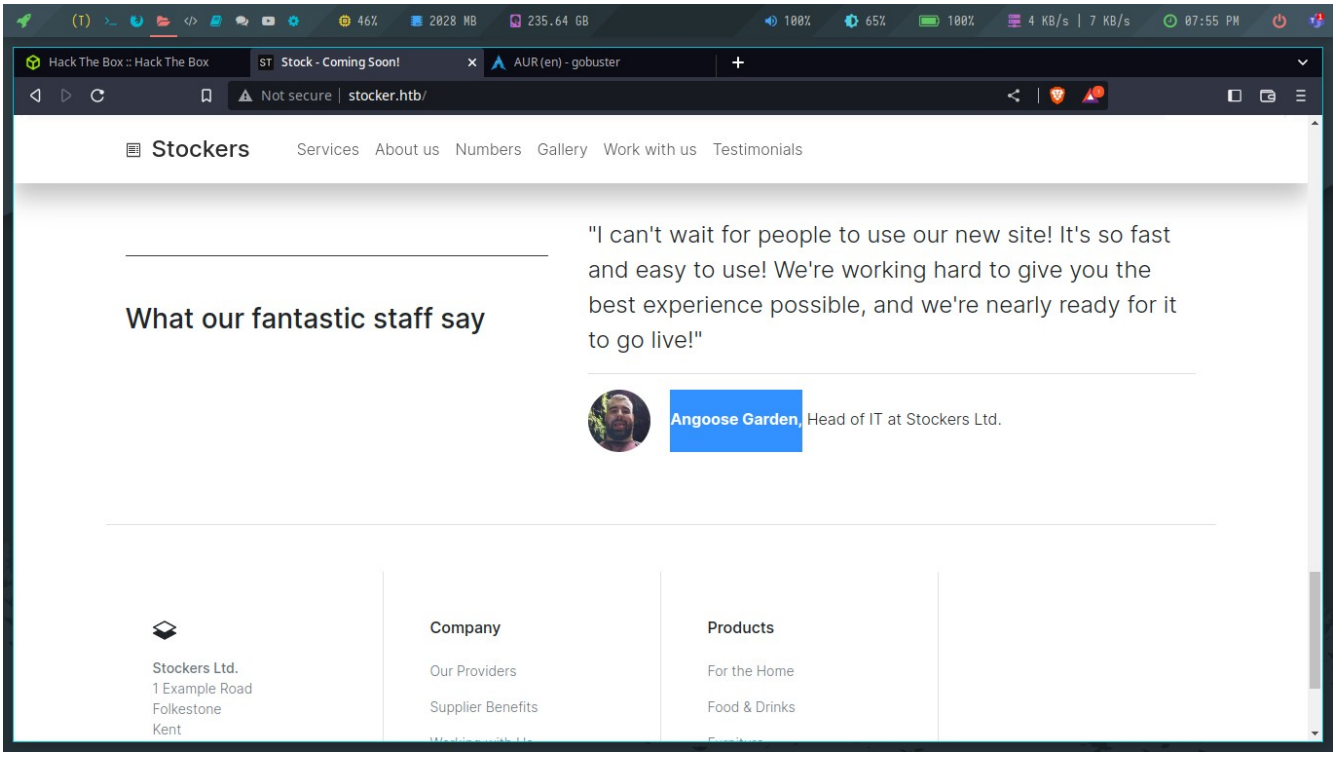


Paso 4: agregar el sitio que nos aparece a nuestro archivo /etc/hosts y encontrar un nombre de usuario.

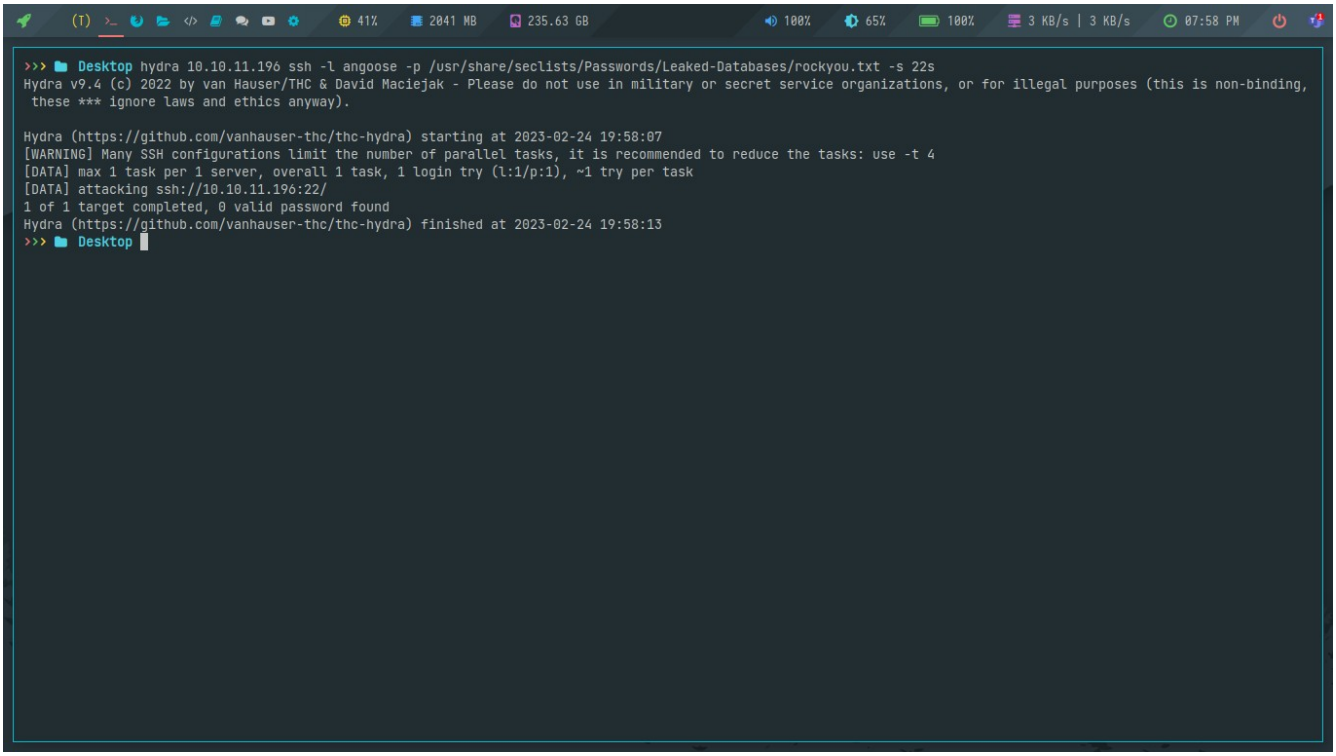




Listo! Tenemos acceso a la Página.



Paso 5 Realizar el ataque con ssh al usuario del dueño.



Y listo! Tenemos el ejemplo realizado de un ataque con hydra a un usuario SSH! Aunque no encontramos ninguna contraseña.