

Benjamin Suljevic 4AHITS

11.04.2024

Nmap

Nmap installieren:

sudo apt install nmap (auf Linux)

Mit nmap -sn sieht man alle Leute in seinem eigenen Subnetz die man pingen kann

-sn ... subnetzmask

```
PS C:\Users\bsulj> nmap -sn 172.18.8.0/22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-11 14:33 Mitteleuropäische Sommerzeit
Nmap scan report for 172.18.8.1
Host is up (0.0040s latency).
MAC Address: AC:71:2E:41:37:EA (Fortinet)
Nmap scan report for 172.18.8.21
Host is up (0.094s latency).
MAC Address: C8:B2:9B:47:EA:3C (Intel Corporate)
Nmap scan report for L32394.intra (172.18.8.46)
Host is up (0.11s latency).
MAC Address: 28:11:A8:CB:B0:92 (Intel Corporate)
Nmap scan report for DESKTOP-EPGFVVL.intra (172.18.8.50)
Host is up (0.058s latency).
MAC Address: C8:5E:A9:25:81:18 (Intel Corporate)
Nmap scan report for Luki.intra (172.18.8.53)
Host is up (0.012s latency).
MAC Address: 24:EE:9A:7D:62:61 (Intel Corporate)
Nmap scan report for DESKTOP-FOASM6G.intra (172.18.8.59)
Host is up (0.054s latency).
MAC Address: 1C:BF:C0:ED:9B:F7 (Chongqing Fugui Electronics)
Nmap scan report for LAPTOP-IR7JGHVE.intra (172.18.8.60)
Host is up (0.0030s latency).
MAC Address: C8:58:C0:D2:58:57 (Intel Corporate)
Nmap scan report for 172.18.8.67
Host is up (0.020s latency).
MAC Address: F4:26:79:7C:59:52 (Intel Corporate)
```

Um eine Ip Adresse zu scannen:

nmap

```
PS C:\Users\bsulj> nmap 172.18.10.186
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-11 14:44 Mitteleuropäische Sommerzeit
Nmap scan report for 172.18.10.186
Host is up (0.010s latency).
All 1000 scanned ports on 172.18.10.186 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 6A:3B:1D:0F:21:1B (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 8.55 seconds
```

Eine Domain scannen:

nmap <domain>

```
PS C:\Users\bsulj> nmap abc.at
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-11 14:47 Mitteleuropäische
Nmap scan report for abc.at (5.35.247.250)
Host is up (0.014s latency).
rDNS record for 5.35.247.250: hecustomer02.ynet.at
Not shown: 983 filtered tcp ports (no-response)
PORT      STATE SERVICE
1/tcp     open  tcpmux
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
106/tcp   open  pop3pw
110/tcp   open  pop3
113/tcp   closed ident
119/tcp   open  nntp
135/tcp   open  msrpc
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   closed submission
993/tcp   open  imaps
995/tcp   open  pop3s
8010/tcp  open  xmpp
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

Betriebssystem herausfinden:

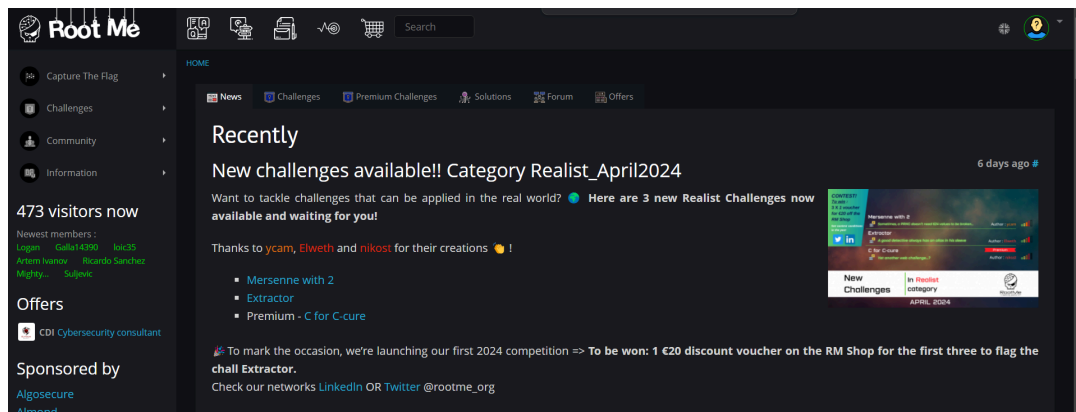
nmap <ip> -O

```
PS C:\Users\bsulj> nmap 192.168.166.247 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-11 15:11 Mitteleuropäische Sommerzeit
Nmap scan report for 192.168.166.247
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.166.247 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 70:66:55:5E:53:1B (AzureWave Technology)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.68 seconds
```

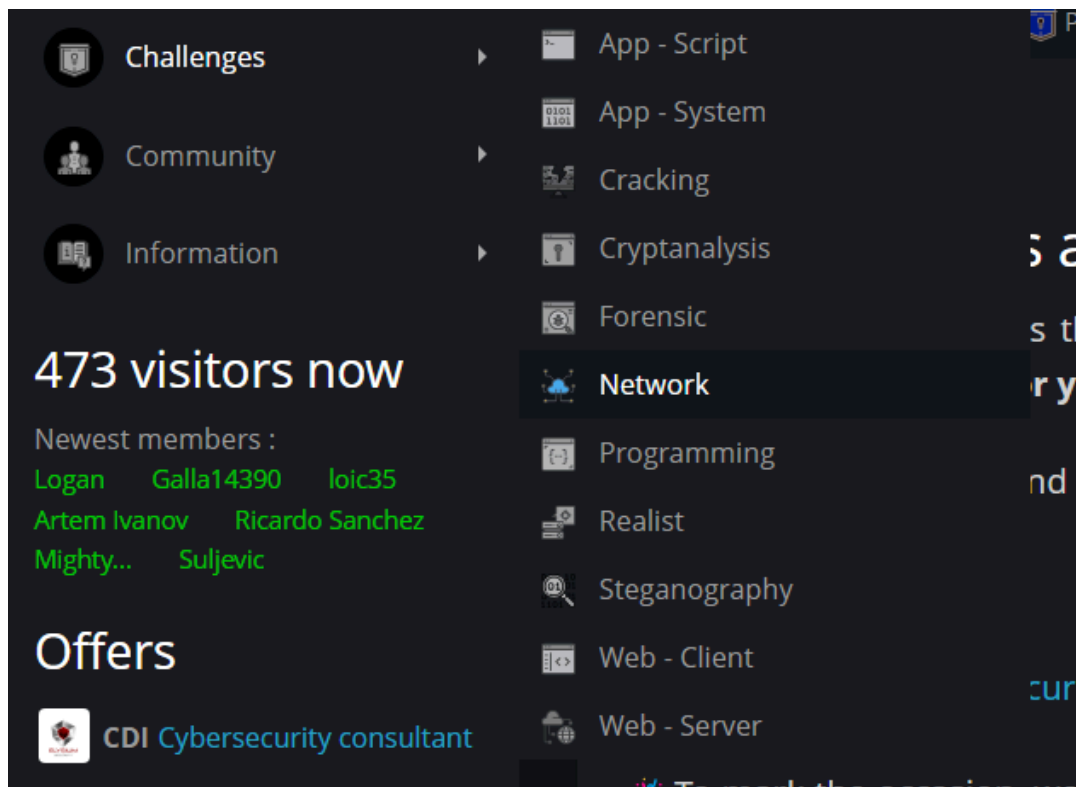
Root-me.org

Einen Account erstellt



Das Dashboard

Unter Challenges findet man verschiedene Kategorien



Unter Network findet man folgende Challenges

27 Challenges Filter									
Results	Name	Validations	Number of points	Difficulty	Author	Note	Solution	Date	
✗	FTP - authentication	30% 96012	5	1	g0uZ	😊	8	30 August 2010	
✗	TELNET - authentication	27% 85601	5	1	g0uZ	😊	10	30 August 2010	
✗	ETHERNET - frame	22% 68759	10	1	abu_youssef	😊	12	20 May 2013	
✗	Twitter authentication	22% 74136	15	1	g0uZ	😊	7	30 August 2010	
✗	Bluetooth - Unknown file	10% 29557	15	1	Neptune	😊	5	1 March 2019	
✗	CISCO - password	15% 48254	15	1	ThanatOs	😊	10	10 July 2013	
✗	DNS - zone transfert	8% 23791	15	1	g0uZ	😊	10	20 May 2013	

FTP:

FTP - authentication

5 Points

Packet capture analysis

Author

g0uZ, 30 August 2010

Level

Validations

96012 Challengers

Note

★★★★★ 9481 Votes

I like

I don't like

Statement

An authenticated file exchange achieved through FTP. Recover the password used by the user.

[Start the challenge](#)

1 related ressource(s)

- rfc959 (RFC)

Validation

Problem: Wenn man auf Start the challange drückt wird versucht eine neue Seite zu starten aber wird dann sofort wieder geschlossen

Try hack me

Ein Konto erstell und gleich kann man sich für 3 Sachen entscheiden

Welcome to TryHackMe

Choose your learning path

RED TEAMING

Learn the skills needed to become a Red Team Operator

- Use diverse techniques for initial access
- Enumerate and persist on targets
- Evade security solutions
- Exploit Active Directory

SOC LEVEL 1

Learn the skills to work as a Junior Security Analyst in a Security Operations Centre

- Detect and analyse traffic anomalies
- Monitor endpoints for threats
- Utilise SIEM tools to handle incidents
- Investigate forensic artefacts

JR PENETRATION TESTER

Learn the necessary skills to start a career as a penetration tester

- Pentesting methodologies and tactics
- Enumeration, exploitation and reporting
- Realistic hands-on hacking exercises
- Learn security tools used in the industry

Ich dem Fall wurde sich für JR Penetration Tester entschieden

We will use a command-line application called "GoBuster" to brute-force FakeBank's website to find hidden directories and pages. GoBuster will take a list of potential page or directory names and tries accessing a website with each of them; if the page exists, it tells you.

Step 1) Open a terminal

A terminal, also known as the command-line, allows us to interact with a computer without using a graphical user interface. On the machine, open the terminal using the Terminal icon:

► Stuck? See video

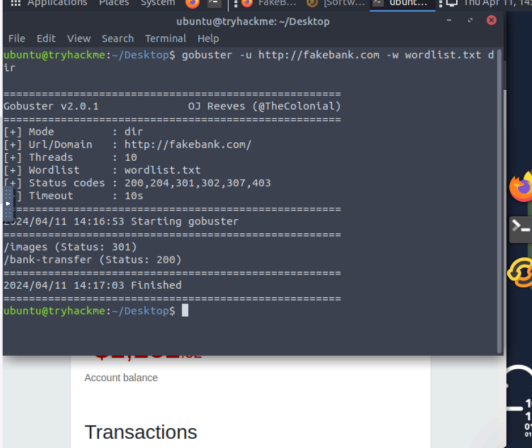
Step 2) Find hidden website pages

Most companies will have an admin portal page, giving their staff access to basic admin controls for day-to-day operations. For a bank, an employee might need to transfer money to and from client accounts. Often these pages are not made private, allowing attackers to find hidden pages that show, or give access to, admin controls or sensitive data.

Type the following command into the terminal to find potentially hidden pages on FakeBank's website using GoBuster (a command-line security application).

```
gobuster -u http://fakebank.com -w wordlist.txt dir
```

The command will run and show you an output similar to this:



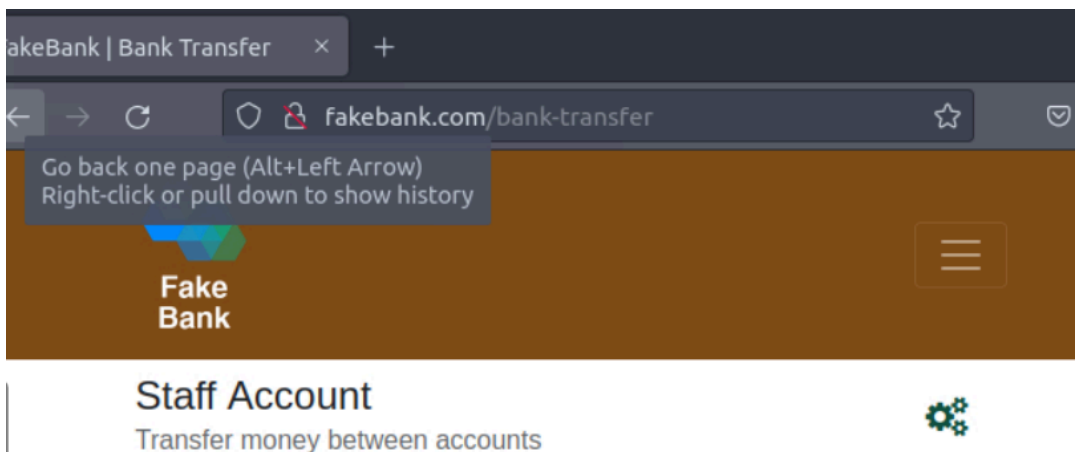
```

ubuntu@tryhackme: ~/Desktop
File Edit View Search Terminal Help
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.com -w wordlist.txt dir
=====
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====
[+] Mode       : dir
[+] Url/Domain  : http://fakebank.com/
[+] Threads    : 10
[+] Wordlist    : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout    : 10s
=====
2024/04/11 14:16:53 Starting gobuster
=====
/images (Status: 301)
/bank-transfer (Status: 200)
=====
2024/04/11 14:17:03 Finished
=====
ubuntu@tryhackme:~/Desktop$

```

Danach werden einem gleich Fragen gestellt und Aufgaben wo eine virtuelle Maschine für einen Bereit gestellt wird

Man findet eine Url die /bank-transfer ist



Room progress (40%)

Bank Account Number

Amount to send in USD

Amount

0:07 / 0:07

This page allows an attacker to steal money from any bank account, which is a critical risk for the bank. As an ethical hacker, you would (with permission) find vulnerabilities in their application and report them to the bank to fix before a hacker exploits them.

Transfer \$2000 from the bank account 2276, to your account (account number 8881).

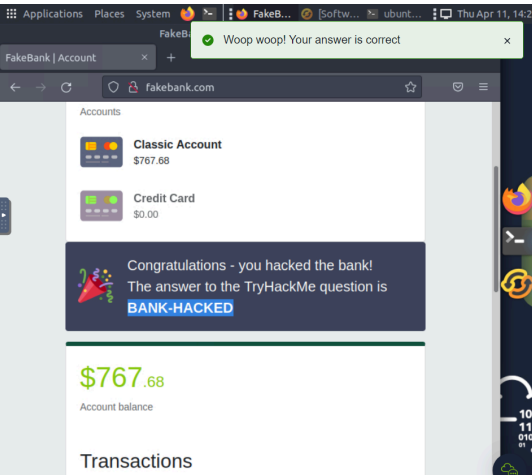
Answer the questions below

If your transfer was successful, you should now be able to see your new balance reflected on your account page. Go there now and confirm you got the money! (You may need to hit Refresh for the changes to appear)

Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need?

BANK-HACKED ✓ Correct Answer 🔍 Hint

If you were a penetration tester or security consultant, this is an exercise you'd perform for companies to test for vulnerabilities in their web applications; find hidden pages to investigate for



Man "Überweist" sich selber ein Menge von Geld und bekommt dann die Lösung