1, Leave only one open port for attacker

step 1, Scan the vulnerabilities on windows 2001

Use the command: netstat -ano

step 2, Find the open port and search the corresponding service on internet.

step 3, Choose the port 445 as the only remaining port to be attacked.

step 4, Through step 2, we already know corresponding services to some open

ports.

|  |  |
| --- | --- |
| Port | Service |
| 21 | FTP service |
| 80 | HTTP service |
| 135 | PRC DCOM service |
| 139 | Netbios/smb service |

Then stop and disabled the corresponding service to shut down those open ports.

step 5, Create a new IP security policy to filter the remaining open ports.

When port number exceeds 1025, It means the port is assigned to a random service.

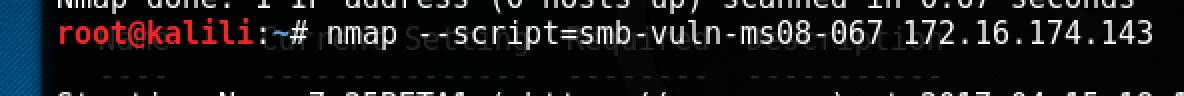
Build up a IP security to block any IP addresses to access through those open ports.

It is finished!

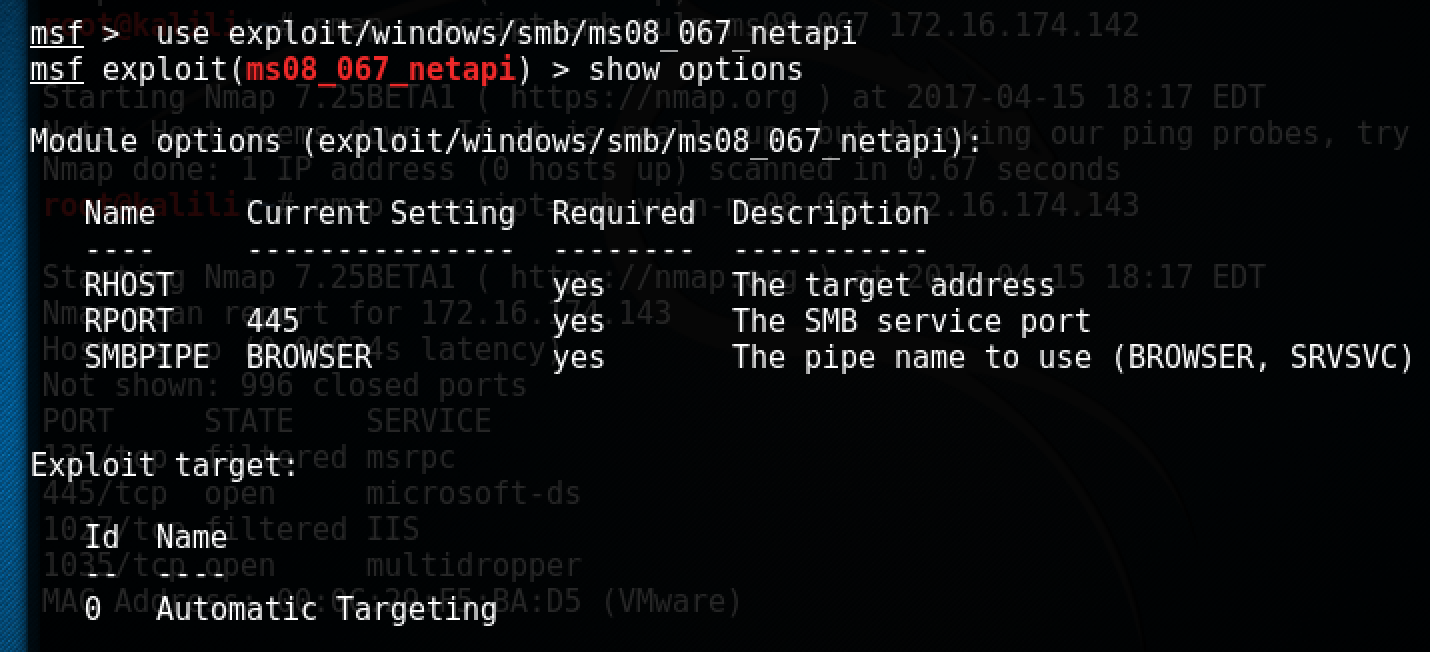
2, Write-up for question 9

1, Scan the vulnerabilities on windows 2003

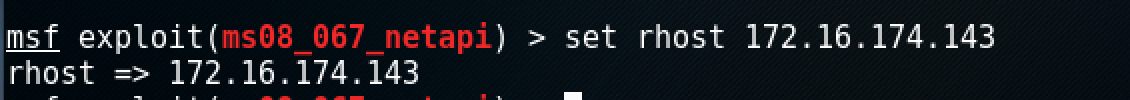
Use the command:



2, Choose the appropriate payload, such as the below one



3, Set options



4, Exploit the payload and get the shell of windows 2003

