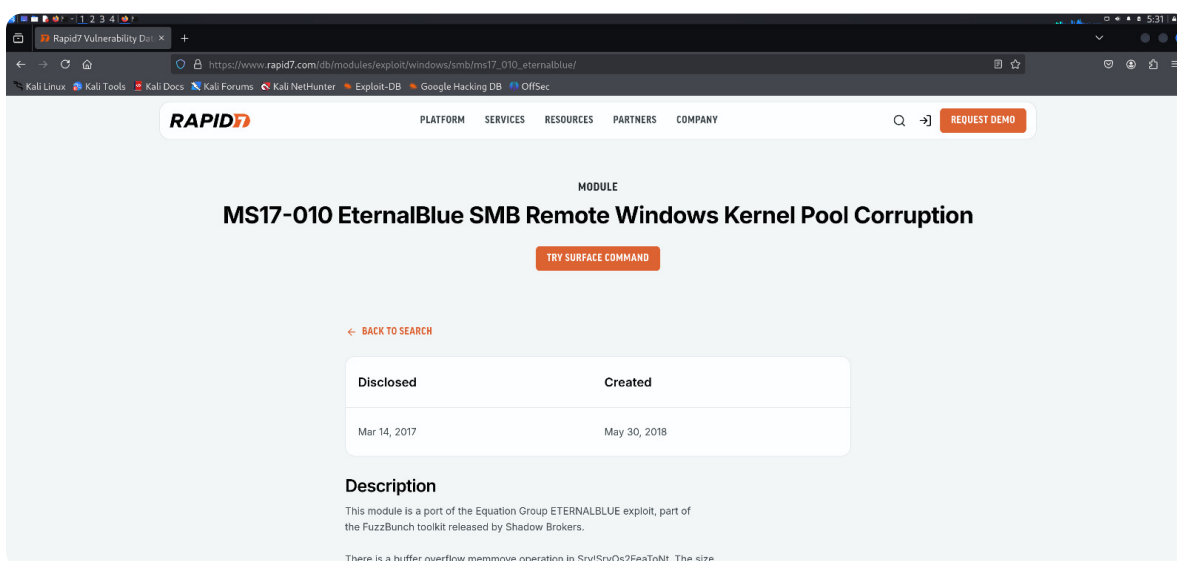


🔍 Enumeration & Discovery

After completing the Nmap scan, we identified that the target machine (192.168.79.140) was running Microsoft Windows 7 SP1 with SMB (port 445) exposed. This was our first clue that the machine could be vulnerable to well-known exploits like MS17-010 (EternalBlue).

To investigate further, we conducted manual research. Using Google, we searched terms such as **“windows 7 smb 445 vulnerability exploit”**. This led us to a Rapid7 blog post detailing the EternalBlue vulnerability affecting SMBv1.

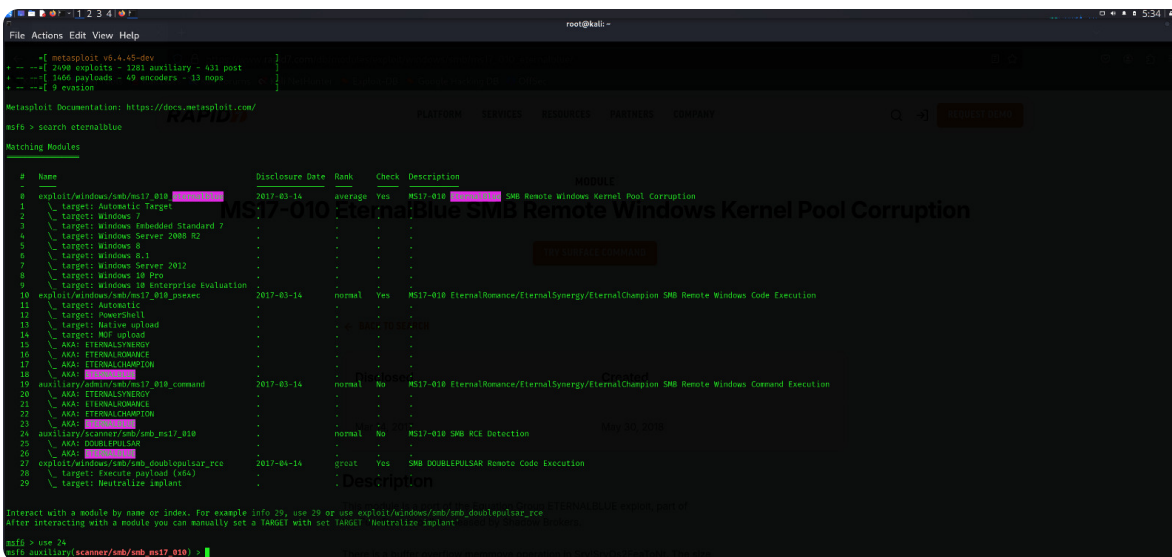
To confirm the target’s exposure, we used the Metasploit module `auxiliary/scanner/smb/smb_pipe` to enumerate named pipes. The target responded successfully, revealing accessible SMB services and confirming the OS version. This enumeration helped validate that the target was exploitable and ready for the next phase of the assessment.



The screenshot shows a web browser displaying the Rapid7 website. The URL in the address bar is https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/. The page features the Rapid7 logo and navigation links: PLATFORM, SERVICES, RESOURCES, PARTNERS, and COMPANY. A search bar with a magnifying glass icon and a "REQUEST DEMO" button are also visible. The main content area is titled "MODULE" and "MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption". Below the title is a "TRY SURFACE COMMAND" button. A link "← BACK TO SEARCH" is present. A table with two columns, "Disclosed" and "Created", shows the following data:

Disclosed	Created
Mar 14, 2017	May 30, 2018

Below the table is a "Description" section. The text reads: "This module is a part of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size



 Download PDF Report