ad atack

IP Address Ports Open
192.168.91.101 TCP:
80,135,139,445,5040,5672,8099,8243,8280,8672,9099,9443,9611,9711,9763,999

MS01 192.168.91.101

WSO2 API Manager running on port 9443 of the target system
Arbitrary File upload which leads to RCE for WSO2
https://github.com/hakivvi/CVE-2022-29464
python exploit.py https://ms01.oscp.exam:9443 shell.jsp
I successfully got the reverse shell

RemoteSystemMonitorService (Unquoted Service Path)

Service RemoteSystemMonitorService is vulnerable to Unquoted Service Path Vulnerability
generate with name inside remore.exe in TRIGONE directory
Restarted the system an take on nc rshell

Use mimikatz and found cred ms01/administrator and oscp\alice.walters
After do enabled RSP in target Set-ItemProperty ‘HKLM:-\SYSTEM\CurrentControlSet\Terminal Server \’ -Name “fDenyTSConnections” -Value 0
You can check Rdp port with nmap scan 3389 is open
Login rdp with admin creds

MS02 172.16.91.102

Enter in target macgine Alice.Walters rdp and login into ms02 system
aining the foothold,ound mysql is vulnerable to modifiable service files
Generatea payload with msfvenom for add Alice.Walters admin group
Replace service binary mysqld.exe with malicious exe
Restarted the system , alice will be in admin group

Using the mimikatz and found user john.howell ntlm hash
john.howell in Domain Admins group

DC01 172.16.91.100

Entering that computer

Enter-PSSession -ComputerName dc01 -Credential “OSCP/John.Howell”