Information Systems Security:
Windows command line interface

Windows command prompt is the environment that, sooner or later, all the IT experts will ha to work in. This exercise was developed to lead students to the basics of the Windows command prompt. The assumption is that the student already knows how to use the commands to list the folder contents, change the folder, etc. The replacement for the Windows command prompt is a PowerShell. Still, because of its complexity, we will cover only a few simple commands used in the Windows command prompt needed for the exercises we will be dealing with this semester. There are similarities between the Windows and Linux terminal commands. Next time we will cover the Linux command line interface, as this will be the foundation of most hacking exercises we will deal with.

Windows command prompt basics

Start Windows VM, log on and open the command prompt (Start -> Run -> type cmd.exe or WinKey+R -> type cmd.exe). You can use physical Windows also (if you do not have access to VM).

See the file contents:

One can display the file contents by using the command `type`, for example: `type filename`

Task: show the `win.ini` file contents in the folder `c:\windows`.
First, change the folder to c:\windows:

```
cd c:\windows
```

then use the `type` command to open the file:

```
type win.ini
```

Change the folder to a root of the drive c:

```
cd c:\
```

Which command would you use to show the contents no matter in which folder you are?
____

One can use the command `find` to find the specific string inside the file. One can also use the pipe (|) operator, which allows for stacking the commands and sending the output of one command as an input to the next one, like:

```
type filename.txt | find "something"
```

this command will search for "something" in the file named filename.txt
Important: the parameter used with the find command must be under quotes
Task: Using the `find` command, find the `win.ini` in the result of the command `dir c:\windows`.

Solution: ____

Task: If we want to search the result no matter the case (case insensitive), we must use a specific switch with the `find` command. Using the help with the find command, find which switch to use for a case-insensitive search. Hint: `find /?`.
Which flag will ignore the case with the `find` command?
____

Environment variables

Environment variables define various parameters the command line interface and other applications use. They are helpful when scripting is used. For instance, if one must reference the computer name from the script, and the script could be executed on any Windows computer, one can use the `%COMPUTERNAME%` variable, which will hold the current computer name. The point is that if one hard-codes the computer name in the script, it will only work on the computer with the hardcoded name. On the other hand, if one uses the variable, the name will be picked up dynamically at the execution time. The environment variables can be displayed with the `set` command.
IMPORTANT: Write down the commands you will use during this exercise directly into this document or a new one, as you will need those for the short exams!
Use the `set` command to show all environment variables defined on the computer.

What is the content of the `COMPUTERNAME` variable? (Use the pipe (|) and the find command to show ONLY the `COMPUTERNAME` variable.)?

____

We can achieve the same result by typing the variable name next to the `set` command. For example, `set username`. Which username is logged on?

____

What is the variable `PATH` used for?

____

What is the content of the `PATH` variable (HINT: type `path` command in the command line)?

____
____
____

`systemroot` variable shows the OS installation location. In which folder is the OS installed?

____

Using the percentage signs like this, one can use the contents of any variable in the command prompt. `%systemroot%` - this will replace the `systemroot` with the OS installation path.

What will happen if you type this command? `cd %systemroot%`

____

`Sc` **command**

`SC` command allows computer operators to see the services and their states and to change their configuration (if the user account has enough privileges).
What is the main difference between the windows program and the Windows service?

____

`sc query` command will show all the services on the OS. The service name and description are provided as a result of the command.

Try to find the `wscsvc` service. What is that service used for?

____

`sc` command has help that you can use, `sc  help`, that will help you do more advanced service management from the command line.

Check the `sc` help and answer the following questions:

Which command can be used to enumerate all the services and drivers?

____

How can one check the status of the event log service on a computer?

____

How can one start the service with the `sc` command?

____

How can one stop the service with the `sc` command?

____

FOR loop

FOR loop can help run multiple commands or the command until a specific condition is met. The `/L` parameter defines the counter as defined below:

```
for /L %i in (start, step, end) do [command]
```

`start` represents the initial value of the counter `%i`, the `step` represents the increment used to grow the `%i` variable, and the `end` represents the value when the for loop should stop at.

For instance, the following FOR lop will print the numbers from 1 to 10.

```
for /L %i in (1,1,10) do echo %i
```

This example will also type the command that is used in each loop. If one wants to remove the command and leave only the result of it, the @ should be used in front of the echo command like this. Make sure to try both commands before you continue with the exercise.

```
for /L %i in (1,1,10) do @echo %i
```

Task: Create the FOR flop that will echo the even numbers between and including 10 to 100 without showing the command used to echo the result.

____

Task: Create the infinite loop that will echo "Algebra" until you break it with the CTRL+C key combination.

____

DNS is one of the critical services of today's networks. It is almost impossible to surf the Internet without a DNS service. Imagine what happens when you type www.google.hr into the Internet browser – how did you end up on the right website? The answer is (in short) the DNS client service on your computer contacted the DNS servers, learned the corresponding IP address for the specified name, and "converted" the name of www.google.hr into an IP address. Based on that, the Internet browser is directed to www.gooogle.hr. Also, the DNS server can find the name (www.google.hr) based on the IP address (if the so-called reverse lookup zone on the DNS server is configured). The end user does not need to think about DNS service because everything works transparently without user interaction. Sometimes it is necessary to deal with the DNS resolving problems and test DNS operation and configuration.
The tool usually used for this in Windows is nslookup.
Task: Get to know how to use the `nslookup` command.
How can one identify the name registered with the 1.1.1.1 IP address with the `nslookup` command?

____

Task: Create the FOR loop that will use the `nslookup` command to find the results for the IP Address range given by the professor (it will be something like this: 192.168.0.1 – 192.168.0.255). We will use the IP address range in the classroom we are in.
Are there any results? Why yes (if there is), or why no (if there isn't)?

____

____

Username and group membership management

Some exercises will deal with computer hacking, so we must understand some basic commands one can use to manage users and group membership.
`Net` command is used to manage various network services.
Type the `net` command and press ENTER. All the net command sub-commands will be shown. We are interested in net user and loacalgroup commands in this exercise.
What will happen if you type the `net user` command?

____

What will happen if you type the `net localgroup` command?

____

Try to find (either by checking the help of the above commands or on the Internet) how to create the new user on Windows OS from the command line interface and add the user to the local administrators group. If you are an admin, the commands will create a new user and add it to the administrators group. If not, you will get a permission denied error message (System error 5). You will need this later in the semester when we will use BoF (Buffer Overflow) to hack Windows Server 2019.

`net user` command to create a new user is:

____

`net localgroup` command to add a newly created user in the administrators group is:

____

Homework:

For additional information, check the presentations (slides):
1_Windows_command_prompt_basics

To prepare for the next time, install the Kali Linux VM on any hypervisor you like (recommendation is either Hyper-V or VMware workstation Pro), and check the presentation:
2_Linux_Shell_basics.

Installation, or ready to use VMs can be downloaded here:
https://cdimage.kali.org/kali-weekly/

- kali-linux-2025-WXX-hyperv-amd64.7z -> Hyper-V ready VM
- kali-linux-2025-W07-vmware-amd64.7z -> VMware ready VM
- kali-linux-2025-W08-installer-amd64.iso -> 64-bit installation ISO image if you prefer to install it