Lab1
CS116
Phillip Roos 27 January 2025

https://github.com/tuftsdev/DefenseAgainstTheDarkArts/blob/gh-pages/labs/lab01-commandline.md

1. **How would you find the path (i.e., location) to the `gcc` command**?

   Use “whereis gcc”

2. **How would you download a file from the Internet?**

   You could use Wget <file from website>

3. **What is the full command to read the manual page of the command that formats and displays the on-line manual pages? (NOTE: there is no typo to this question)**

   I was unaware that this existed before, use “man man”

4. **What command can you use to find out your IP address and MAC address?**

   For windows, I normally use “ipconfig /all”. It lists your IPv4 address which is the internal IP to your computer and your MAC address under “physical address”. For Linux assuming you have net-tools installed, “ifconfig” does the trick

5. **What command can you use to show all the processes that are running on the system?**

   With linux you normally use “ps -e”. Alternatively, you could use either “ps” or “get-process” in windows powershell.

6. **What command can you use to get more details about running processes listening on ports?**

   For Linux, use netstat or ss comes to mind. netstat -tulnp will get you specific programs and shows the PID and whether its a UDP or TCP connection. However using sudo (because greater permissions are required) with ss or netstat might give you more information. Thus I recommend using either:

   Sudo netstat -tulnp or sudo ss -tulnp

   EXTRA: For windows power shell, Instinctively, I would use “Get-NetTCPConnection” in windows powershell as it lists all connections your computer is making with remote addresses and on what port. Upon doing more research and happening on some stackoverflow posts, to get more specific information on individual processes listening on what specified port, a more complex usage of Get-netTCPconnection should be used such as “ Get-NetTCPConnection | Where-Object { $_.State -eq "LISTEN" } | select

@{Name="Process";Expression={(Get-Process -Id $_.OwningProcess).ProcessName}}, localaddress, localport ”.

7. **What command with flag could you use to list every file, including hidden files, on the entire system, showing their owner, location, and access time? Please also note the flags that you used with command.**

   Straightforward in Linux: ls -laR /

   Extra: This is a lot more complicated to do in windows, I’ve used the “Get-ChildItem” command before. In windows, to see all files, including the hidden ones, you can start with the C:\ directory, you list the path using the -path flag top list it’s exact location and -recurse to list more than just the directory’s (and go into each directory and list each file). Although not required, you could also append “| Select-Object FullName” to make the command more beautiful and easier to read. “Get-ChildItem -Path C:\ -Recurse | Select-Object FullName”

8. **Assume you found a file named `warrent.pdf`. What command could you use to find out what type of file this was?**

   A little confused as to the exact nature of this question. I’m assuming that “file <filename>” is what you’re looking for as it displays file type.

9. **So you discovered that `warrent.pdf` is a binary executable. What command could you use to extract any readable information from the file without running it? Also, try this on a compressed file such a ZIP or JAR**

   To get the file contents, you could use “strings <filename>” and sometimes “nano <filename>”. If you try this on a zip file, you will get a lot of gibberish which most likely has to do with the compression files.

10. **What command can you use to find the IP address-to-MAC address mappings for systems on the local network?**

    This is easy to do with “arp -a”

11. **Consider the following IP address: 46.252.26.153. Where is the computer with that IP address located --in what country?**

    Appears to be in Germany

12. **For the previous question, what command did you use to determine the location of the computer?**

    I tried originally using just “curl” and “nslookup” but it didn’t appear to work with an offline IP. After doing more research, I ended up using:

    “curl ipinfo.io/46.252.26.153” which determined it to be in Germany. I also used https://infosniper.net/ to confirm this.

13. **What command can you use to securely delete a file?**

    You use “shred -u <filename>”

14. **What command can you use to see if you are a computer administrator or superuser?**

    In linux, the goal would be to see if it returns as “root”. You could use “sudo whoami” for this as an error is thrown for non-admins. A more sophisticated way to do this would be to type “id” and see what groups you belong to

    Extra: In windows this can be done with “net user <user>” where <user> is your windows login user.If there is an *adminstrator tag included, then you’re an administrator.

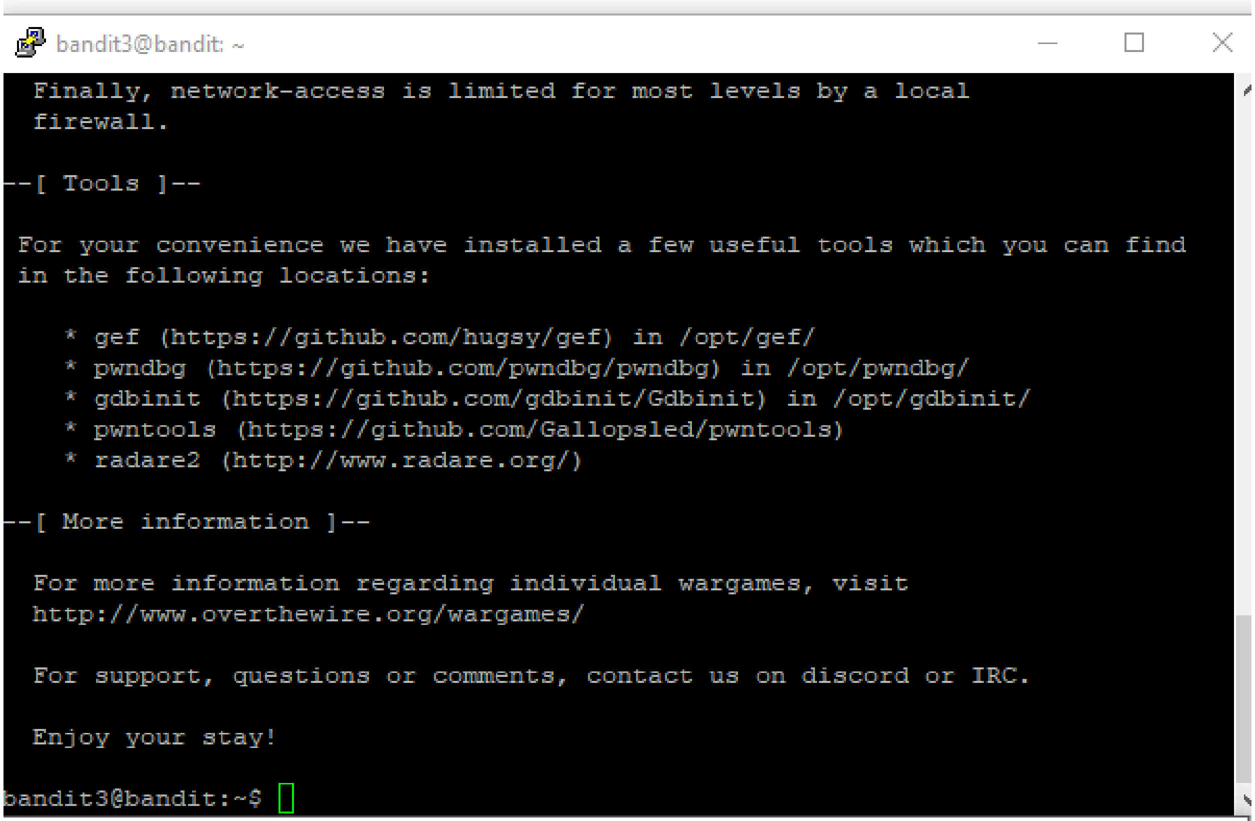
15. **What command can you use to see list of previous commands you have entered on command line?**

    A sophisticated person would use “history” in powershell. Personally I just use “the Up Arrow”. For windows or linux, it’s the same.

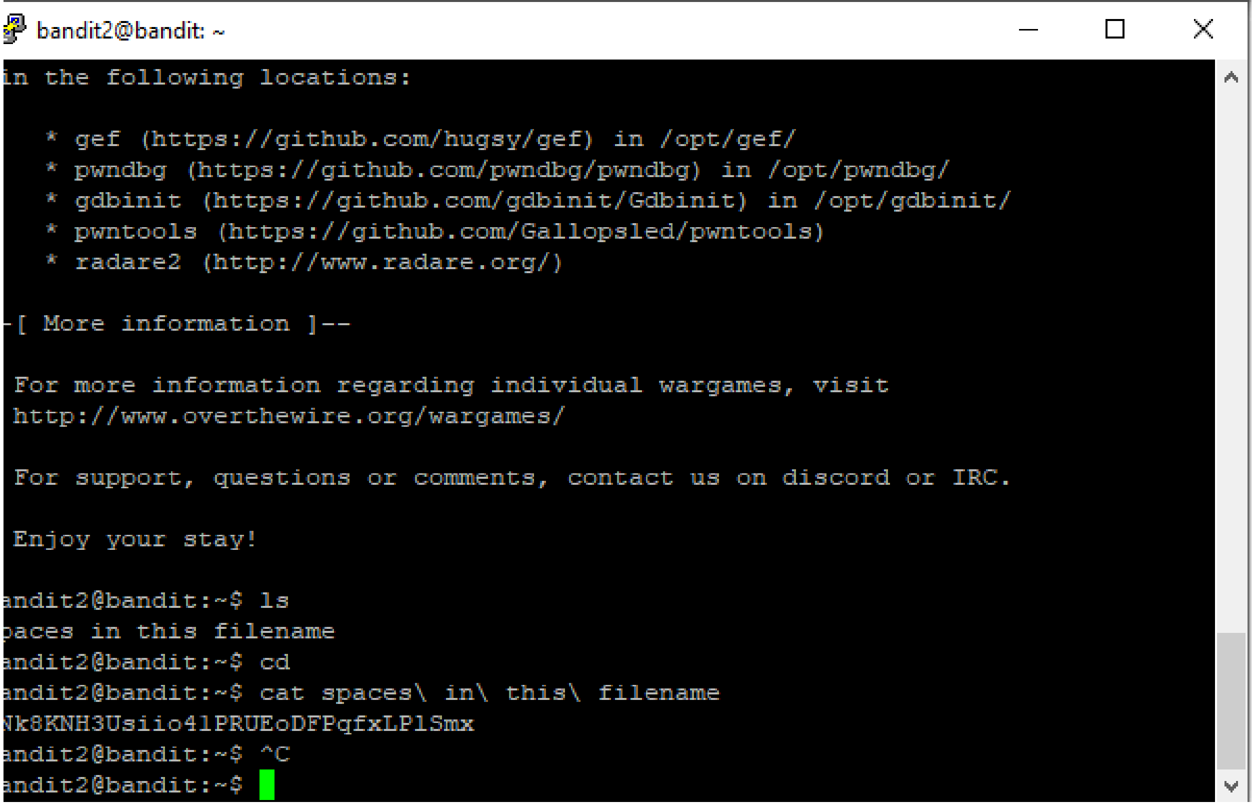
16. **What command can you use to see list of scheduled tasks running on your computer?**

    On linux you could do “crontab -l”. Was previously unaware of this command. On windows powershell this would be schtask /query.

Part 2:



```
  Finally, network-access is limited for most levels by a local
  firewall.

--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

bandit3@bandit:~$
```



```
in the following locations:

   * gef (https://github.com/hugsy/gef) in /opt/gef/
   * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
   * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
   * pwntools (https://github.com/Gallopsled/pwntools)
   * radare2 (http://www.radare.org/)

-[ More information ]--

 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us on discord or IRC.

 Enjoy your stay!

andit2@bandit:~$ ls
paces in this filename
andit2@bandit:~$ cd
andit2@bandit:~$ cat spaces\ in\ this\ filename
Nk8KNH3Usiio41PRUEoDFPqfxLP1Smx
andit2@bandit:~$ ^C
andit2@bandit:~$
```