SSH and How to do it?

1. SSH or "Secure Shell" is essentially a magic way to safely access unsafe networks. This is commonly used to remotely login to a computer and execute commands.
2. To use SSH to remote login:
    a. On Windows: Use an SSH client like PuTTY.
    b. On Mac or Linux: In terminal, type "*ssh {user}@{host}*". User refers to the account you want to access and host is the domain or IP address of the computer you are trying to access.

For more in-depth understanding of SSH, please follow this link:
https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work

1. Netcat is a tool that can help you read or write data over the internet and is called "The Swiss Army Knife of Information Security" by its fans.
2. It earned its nickname because one can use netcat to perform a lot of different tasks including file transfer, chatting, port scanning and can even serve as both a client and a server.
3. The basic syntax for netcat commands is "*nc [options] [destination] [port]*". Here,
    a. *Options* is an optional argument or "flag" that you can use to change the behavior of netcat. For example "nc -h" prints helpful information about nc.
    b. *Destination*, is the IP address of the computer you are trying to contact.
    c. *Port* is the endpoint and helps identify the type of communication happening

To understand how to use netcat, follow this link:

https://www.poftut.com/netcat-nc-command-tutorial-examples/