**Name-Ujjawal Mandhani**

**Batch-F6**

**Enroll No.-9918103237**

**ISL LAB – Week 2 A**

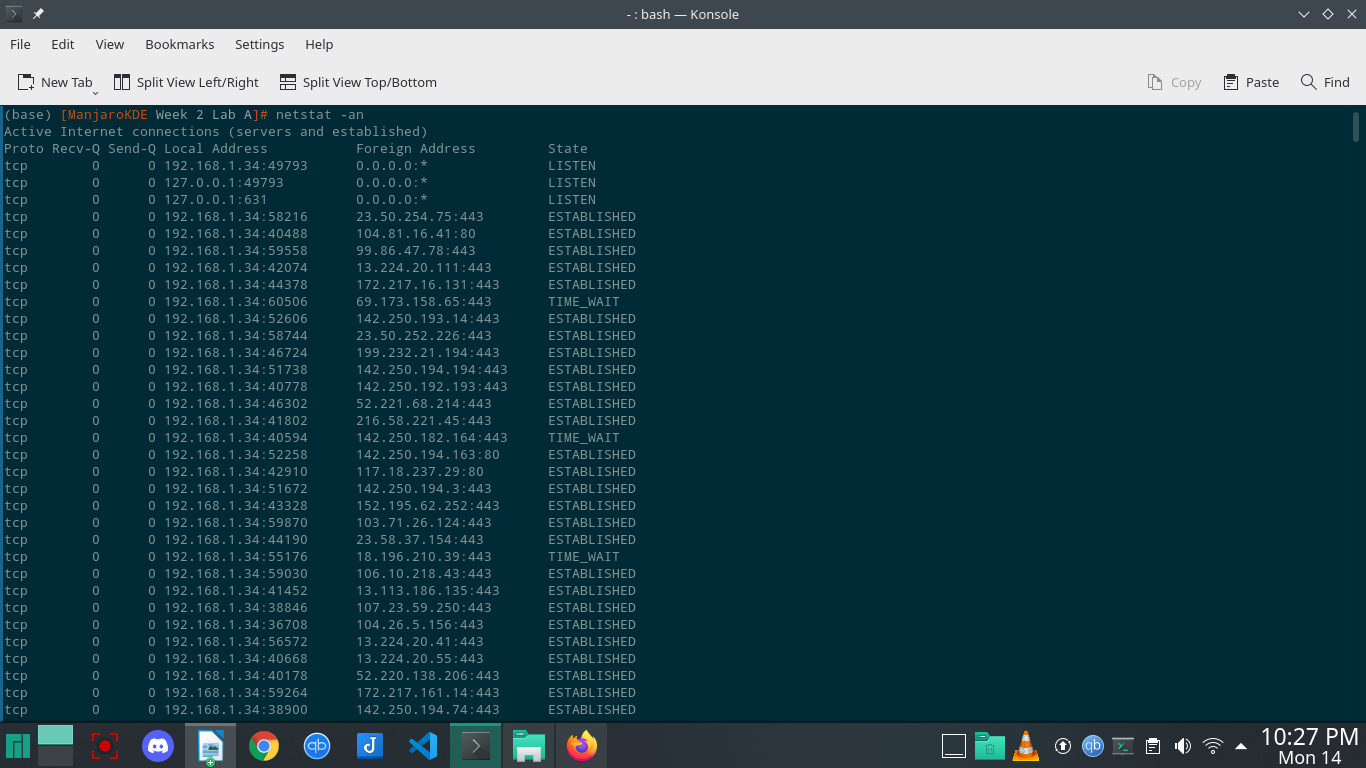
**Question 1**: **Use your web browser to investigate the technical difference between a virus, a worm and a Trojan horse. Try typing each of these terms into your favourite Internet search engine. Do you get better results if you type in each term separately or if you type them in all together? What search strings proved most helpful to you?**

**Virus -** Virus is a computer program or software that connects itself to another software or computer program to harm a computer system. When the computer program runs attached with a virus it performs some action such as deleting a file from the computer system. Viruses can’t be controlled remotely.

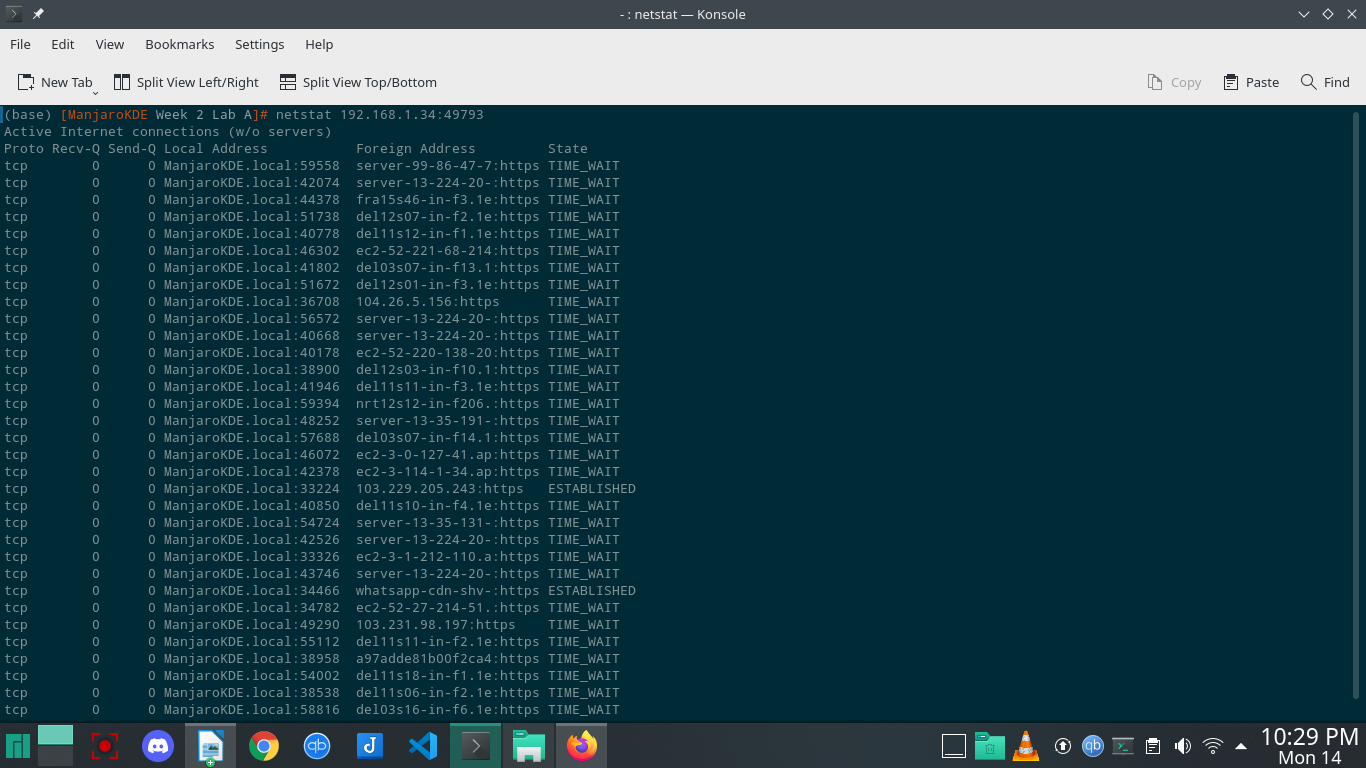
**Worms -** Worms is also a computer program like virus but it does not modify the program. It replicates itself more and more to slow down the computer system. Worms can be controlled by remote.

**Trojan Horse -** Trojan Horse does not replicate itself like viruses and worms. It is a hidden piece of code which steals the important information of the user. For example, Trojan horse software observes the e-mail ID and password while entering in a web browser for logging. Results were better when collectively searched.

**Question 2:Run “netstat –an” on your own computer. On a computer running Microsoft Windows, open acommand prompt. Often this can be done by going to the Start menu, then choosing Programs >Accessories > Command Prompt. The netstat command will actually work on many other operating systems, including Linux.**



**Question 3:Choose another line of the netstat output and do a similar investigation of what service runs there and what viruses, if any, have targeted that service.**



**Question 5:A group called the Internet Assigned Numbers Authority decides what services run on what ports. Do a web search for “well-known port numbers” and another for the “Internet Assigned Numbers Authority”.**

**Well known Ports** - Port numbers can run from 0 to 65353. Port numbers from 0 to 1023 are reserved for common TCP/IP applications and are called *well-known ports*. The use of well-known ports allows client applications to easily locate the corresponding server application processes on other hosts.

**Internet Assigned Numbers -** The Internet Assigned Numbers Authority (IANA) is a standards organization that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and Internet numbers.

**Question 6:Give some examples of what malware tries to accomplish.**

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.

**Question 7: Describe ways that white-hat hackers try to make computer systems more secure.**

One definition of White Hat hackers includes those individuals who perform security assessments within a contractual agreement. Although this definition works in most cases, there is no legal or ethical component associated with it. When compared to the definition of Black Hat, this omission becomes glaringly obvious. However, this is the definition that most people think of when they talk about White Hats and will work for our discussion.

Just like in the movies of the Wild West, White Hat hackers are considered the good guys. They work with companies to improve their client's security posture at either the system or the network level, or finding vulnerabilities and exploits that could be used by a malicious or unauthorized user. The hope is that once a vulnerability or exploit is discovered by a White Hat, the company will mitigate the risk.

**Question 8:Describe things you can do to secure your computer against attack.**

Steps we could keep the system secure are:

* + Keep an up-to-date anti-virus software running at all times.
  + Start using an alternative web browser to Internet Explorer such as Mozilla Firefox.
  + Use an alternative email program other than Outlook Express.
  + Never open suspicious looking emails or attachments.
  + Stop using peer to peer file sharing sites and downloading “cute” programs.
  + Set up a Firewall.
  + Backup your files every night.