**Project Name: Check if malware has infected the network/ Harden network**

**Technology: WireShark/ Cyber Security principals**

**Market:  Security**

**Name / Group: Gagneet Sahota**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tools: Wireshark, Parrot OS, Nmap, Malware Bytes**

**Basic Procedure:**

1. Take last version of malware bytes to scan on each PC
2. Use Process explorer on each PC-

<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>

1. Start Wireshark to monitor traffic with all computers on, to see if each computer is communicating with each other more than it needs to.
2. If no malware is detected proceed to hardening the network.
3. Confirm all Pc’s have windows updates to date.
4. Run nmap scan on network
5. Install mcafee, one subscription covers 5 PC’s.
6. Install disconnect on each computer that uses internet browsing.
7. Ensure passwords are 8 characters in length with use of atleast 2 special characters, Caps, and not dictionary words.

**Documentation:**

On Mac “Smart Search” an unwanted browser hijacker was installed with the CVE name of **(116c0469b1be5b44d66fa4f844c269a0.virobj)**

**Went into Library to delete all files pertaining to the virus**

* Under Users/\*\*USERNAME\*\*/(Hiddenfolder)Library/application Support deleted unwanted application of “Mac Auto Fixer” Potential of virus due to unknown identity
* Found application of Similar Photo Cleaner, removed
* Malicious folder of “Vlag” under “Launch Agents” with unknown identity
* Removed “.com.copypaste.helper.plst” – adware
* Removed “/var/root/.mitmproxy”
* A.akamaihd.net threat is found on the computer, result of a fake adobe flash update that installed more spyware or extensions
  + Looking into Profiles in settings found 3 user profiles from Smart Search, with the earliest found in October 6th 2019
  + Installed Disconnect to prevent future adware installs