ODSC THE STOLEN SZECHUAN SAUCE CASE SOLUTIONS:

1. OVERVIEW

- **What are the hostnames for the Desktop and DC?**

  CITADEL-DC01 and DESKTOP-SDN1RPT are the hostnames.
  While using "windows_registry_installation" to find out about the systems' information, you can look at the hostname column to find information about the hostnames.
  You may also find out the hostname under the "Constant Columns" on other registry keys when using simple()

- **How many users are there on the Desktop?**

  6 users. While using xanalysis with the Overview option we can check all users, hostname, timezone and installation information.

2. SUCCESSFUL LOGON ANALYSIS

- **Which are the events that give us logon information?**

  Within the events, we can find Security events, in particular, 4624 events give us information about successful logons and 4625 events give us information about failed attempts.

- **Is there any suspicious logon on the Domain Controller/Server?**

  Yes. We can see on the xanalysis() graph some activity that had not previously occurred. This activity corresponds to the IP address 194.61.24.102 and the Workstation Name of kali.

- **Which logon type is it and what does it mean?**

  The Logon Types are 3 and 10.

  - 3: Network (i.e. connection to shared folder on this computer from elsewhere on the network)

  - 10: RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)

- **What about the Desktop?**

We have suspicious activity with the IP address 10.42.85.10 with the user Administrator.

The Logon Types are 3 and 10.

- 3: Network (i.e. connection to shared folder on this computer from elsewhere on network)

- 10: RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)

3. CLOSER LOOK INTO DOMAIN CONTROLLER LOGONS

- **At what time did the suspicious logon ocurred on the Domain Controller/Server?**

  Looking at the information, we can see that the 19th of September 2020 there was a suspicious successful logon at 03:21 AM

4. FAILED LOGONS

- **How many failed logons occurred on the Domain Controller/Server?**

  There were 23 failed logons

- **At what time was the Brute Force used?**

  The Brute Force took place at approximately 3:00 AM on the 19th of September 2020

5. LOOKING INTO THE FSTL & AUTORUNS

- **Is there any suspicious activity?**

  The atacker had access to several files, shared them and, besides, we can see that there's been a download from Internet Explorer: coreupdater.exe that was moved to /Windows/System32 folder

- **Was there an Internet download?**

  There's been a download from Internet Explorer: coreupdater.exe

- **Is coreupdater.exe a malware?**

  The information in VirusTotal suggests that it is a malware!

6. GETTING MORE INFORMATION FROM SHELLBAGS

- **Which folders did the attacker visit?**

  - 'Secret' file on Fileshare

- There's been an access to the Downloads folder

7. ANALYZING NETWORK TRAFFIC

- **What is the port number that the attacker downloaded the malware from?**

  The victims downloaded from port 80 (HTTP) from 194.61.24.102 that the attack hosted using HTTP server.

  HTTP GET Method is a common method that attackers use to disguise as legitimate traffic

  Other possible ways are:

  - Phishing emails
  - Vulnerabilities
  - Bundleware
  - Exploit kits