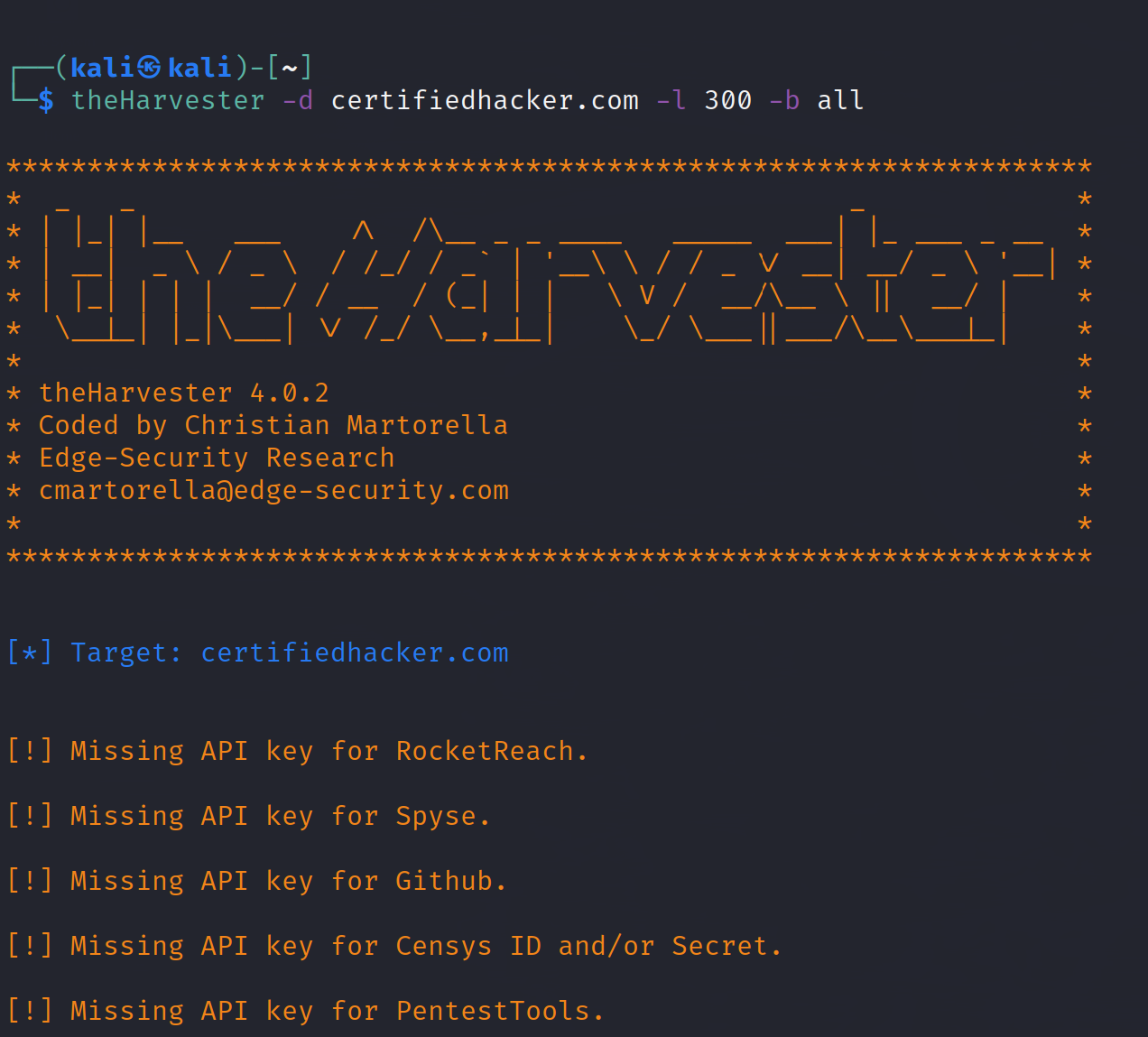
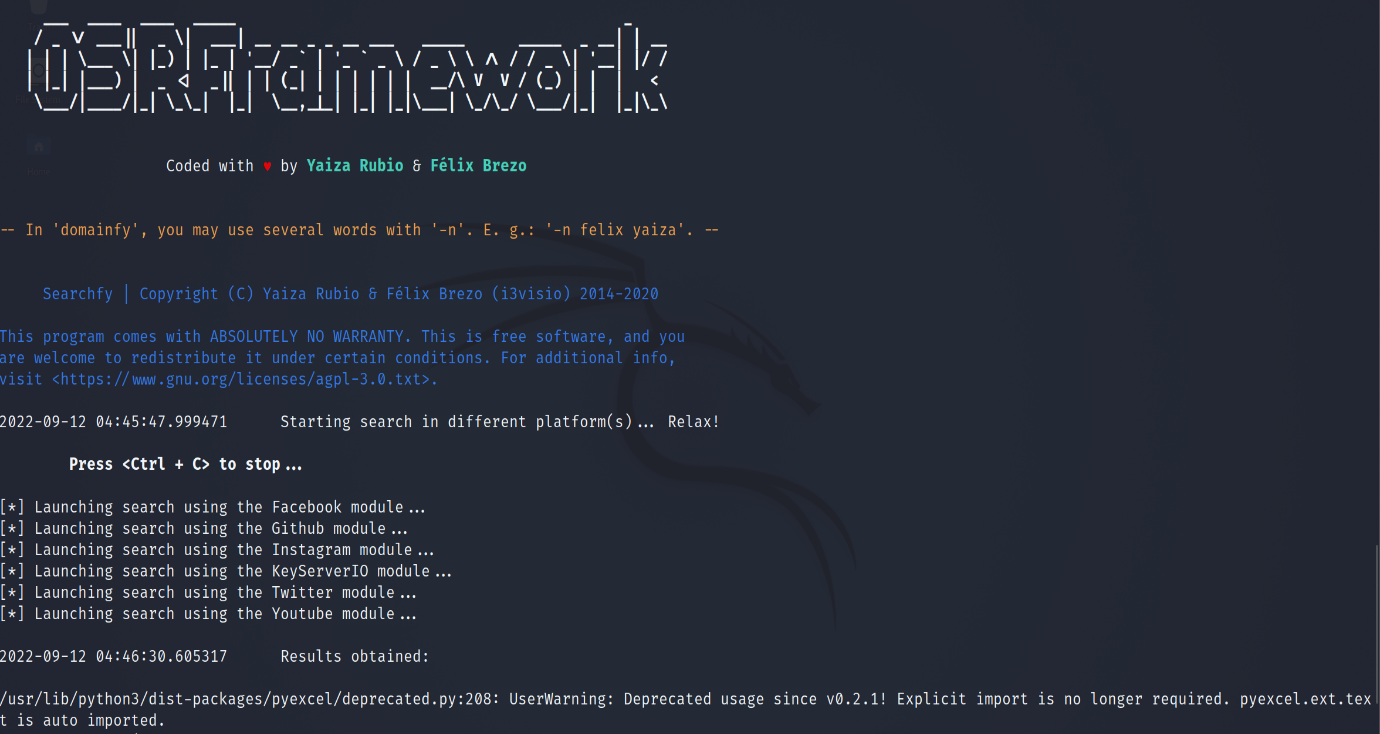
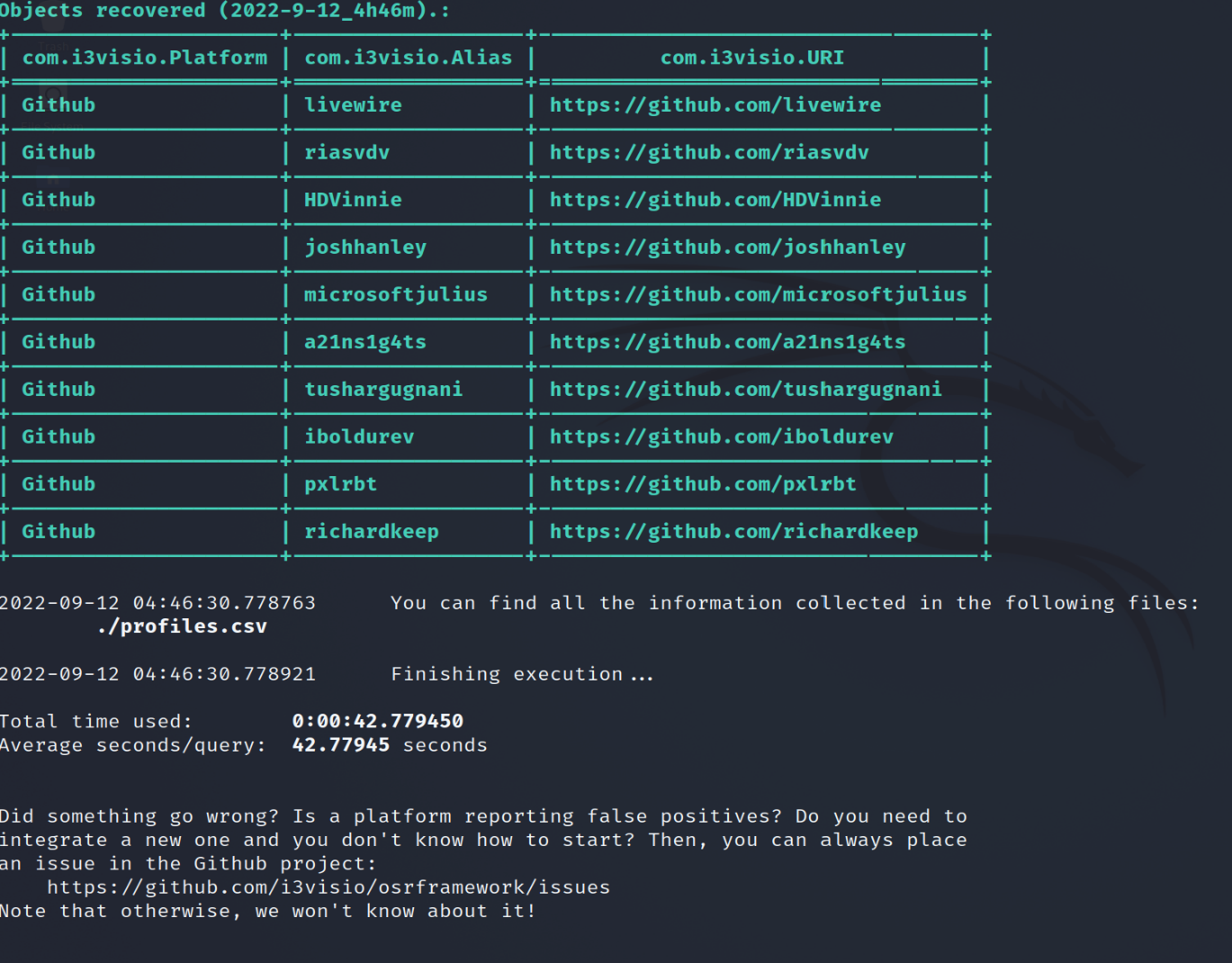
**1)Information gathering using the Harvester:**



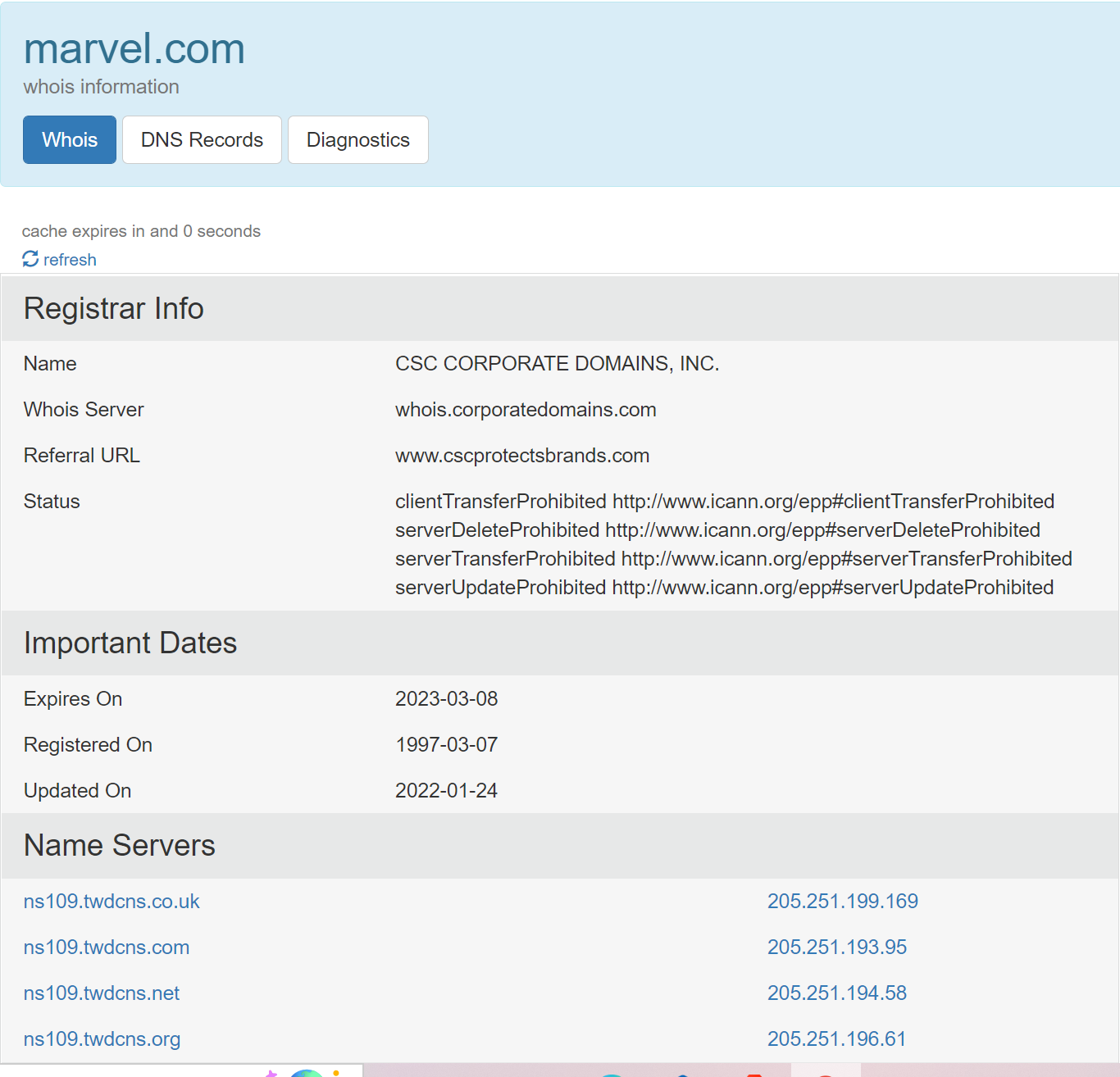


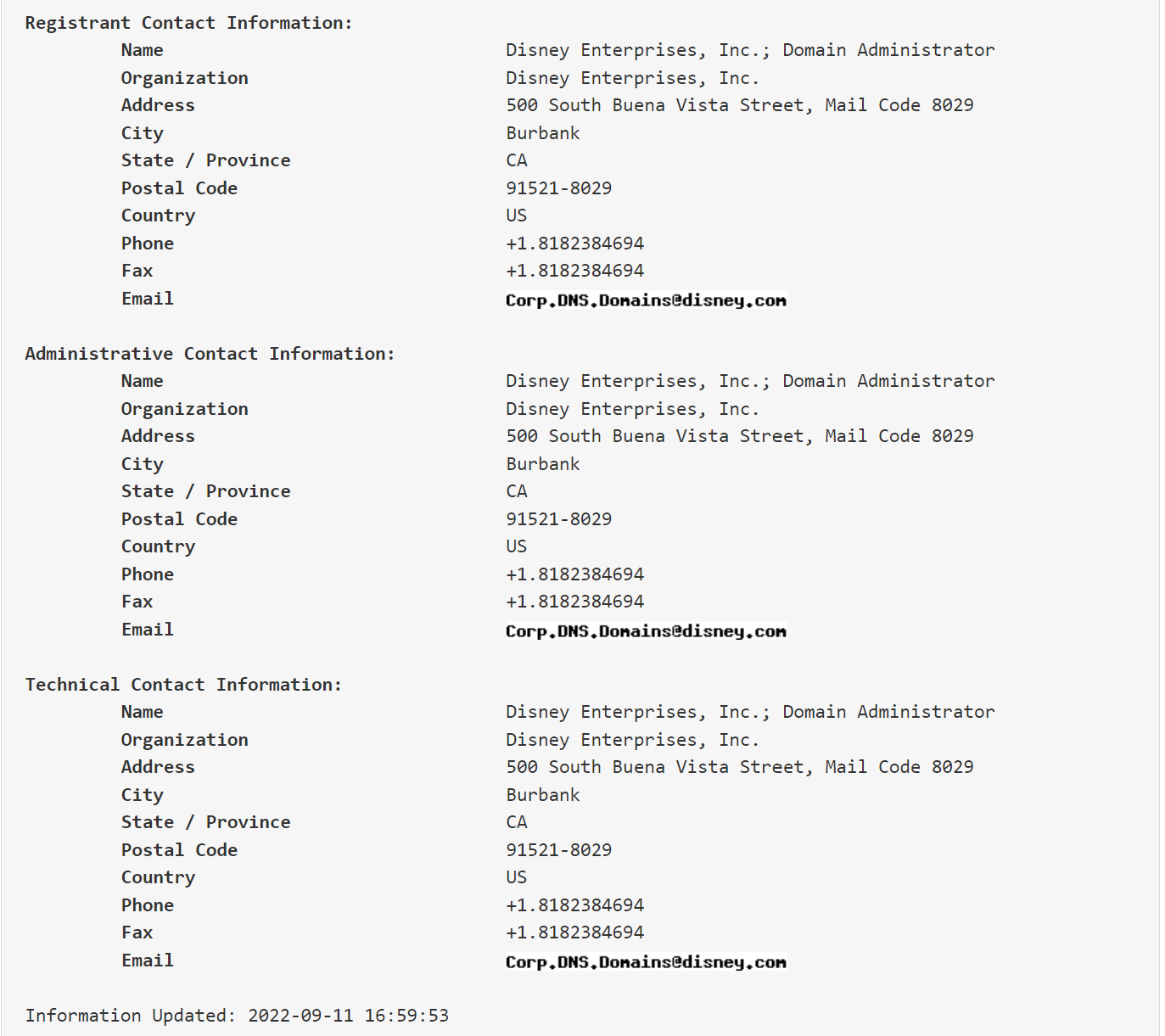
**2) Open Source Intelligence Gathering using OSR Framework:**





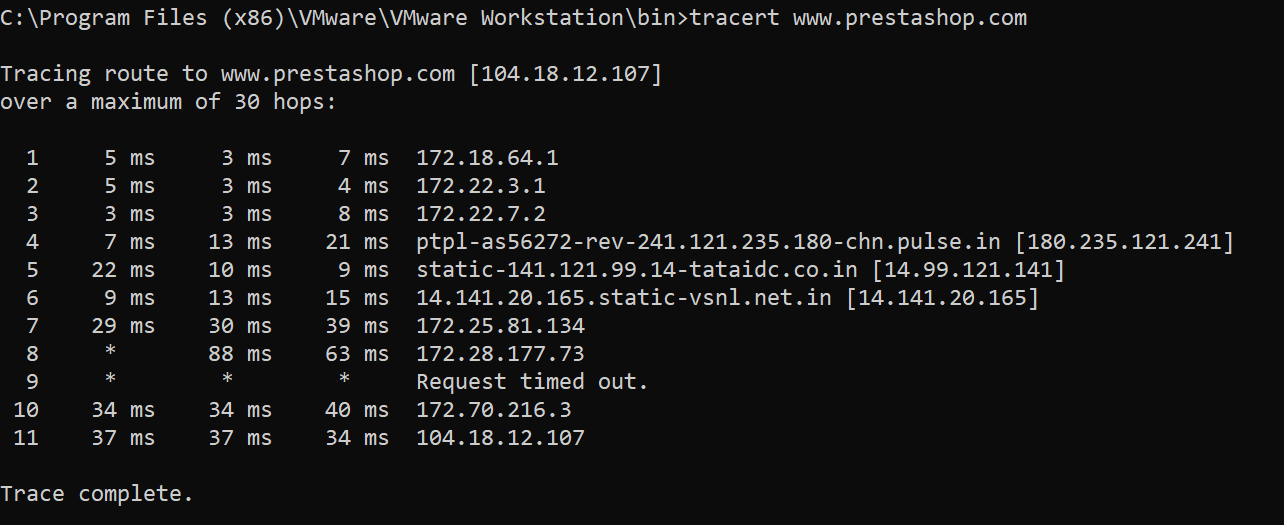
**3) Using who.is:**





**4) Using Trace Route, ping, if config, netstat command:**

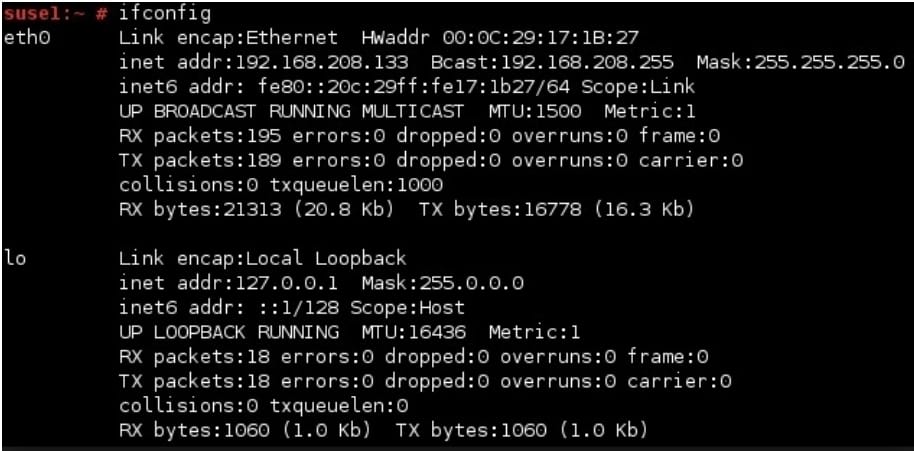
**Trace Route:**



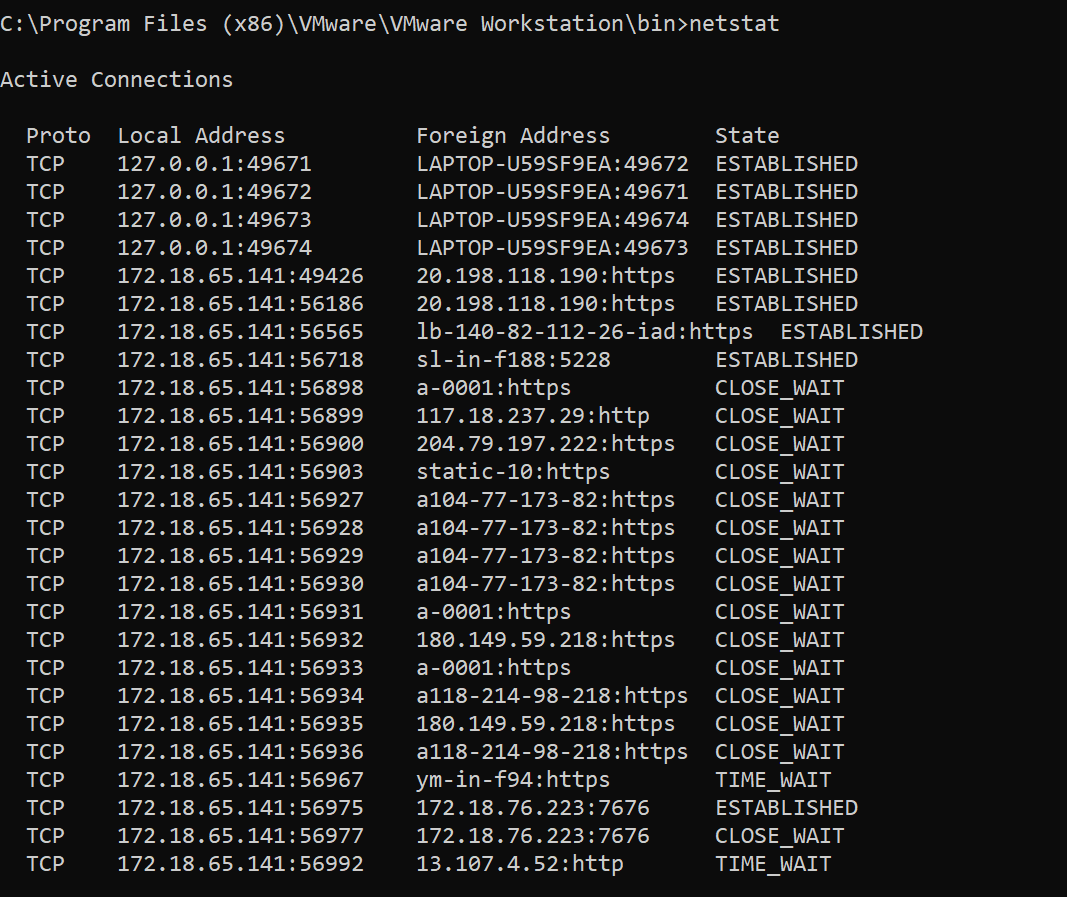
**Ping:**



**If config:**

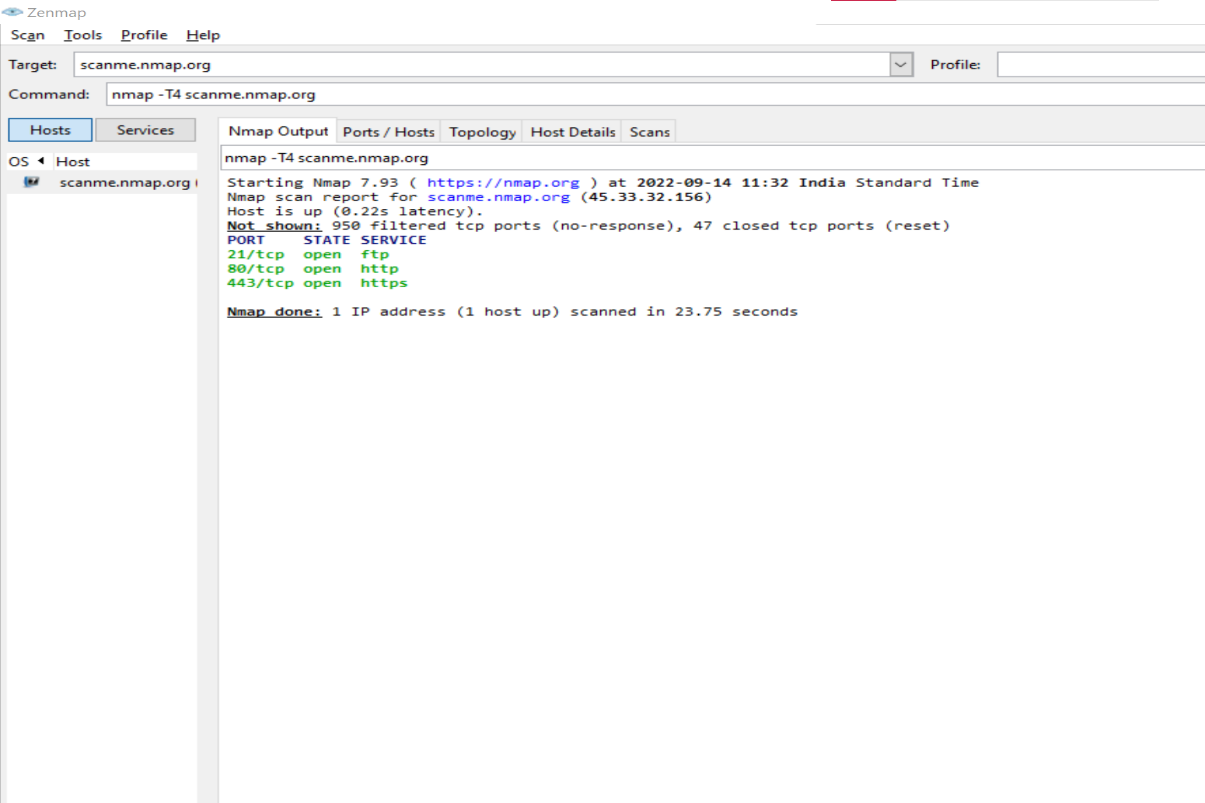


**Netstat:**

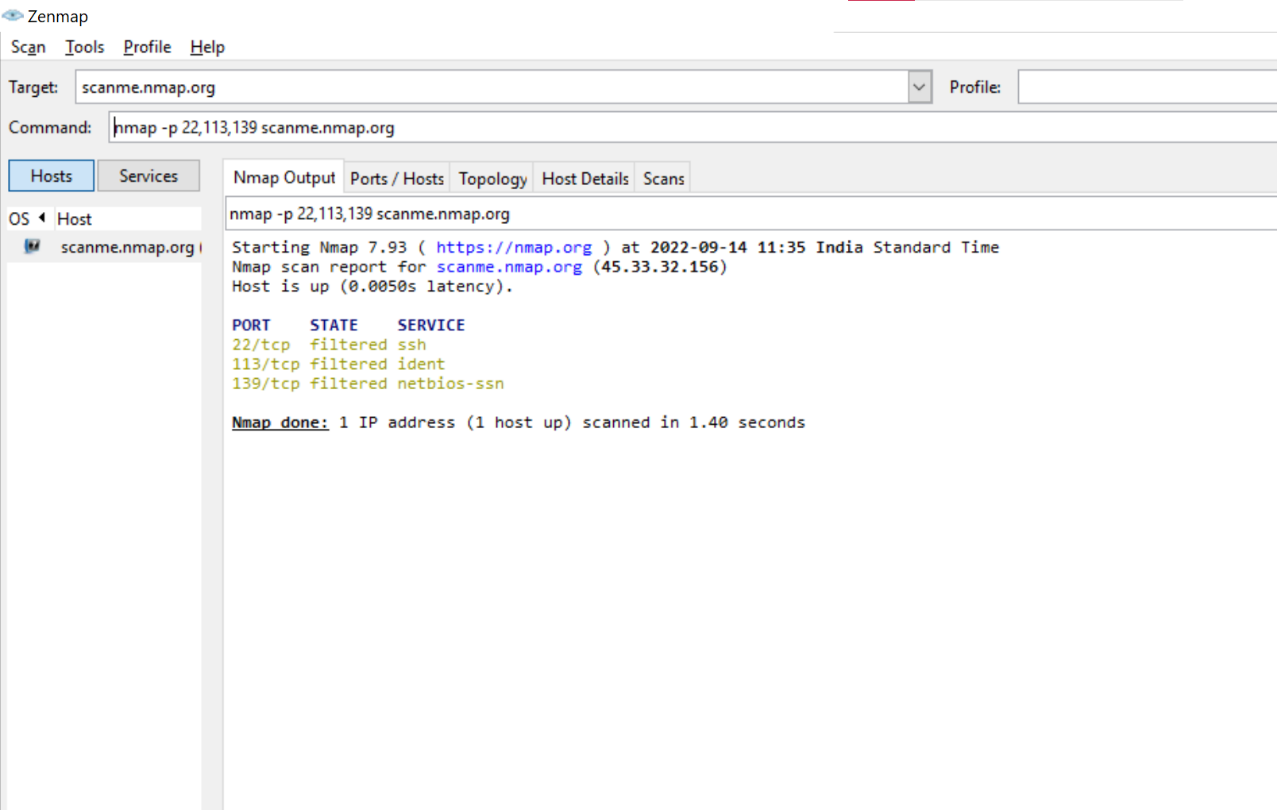
****

**5)** **Using Nmap Scanner to perform port scanning** :

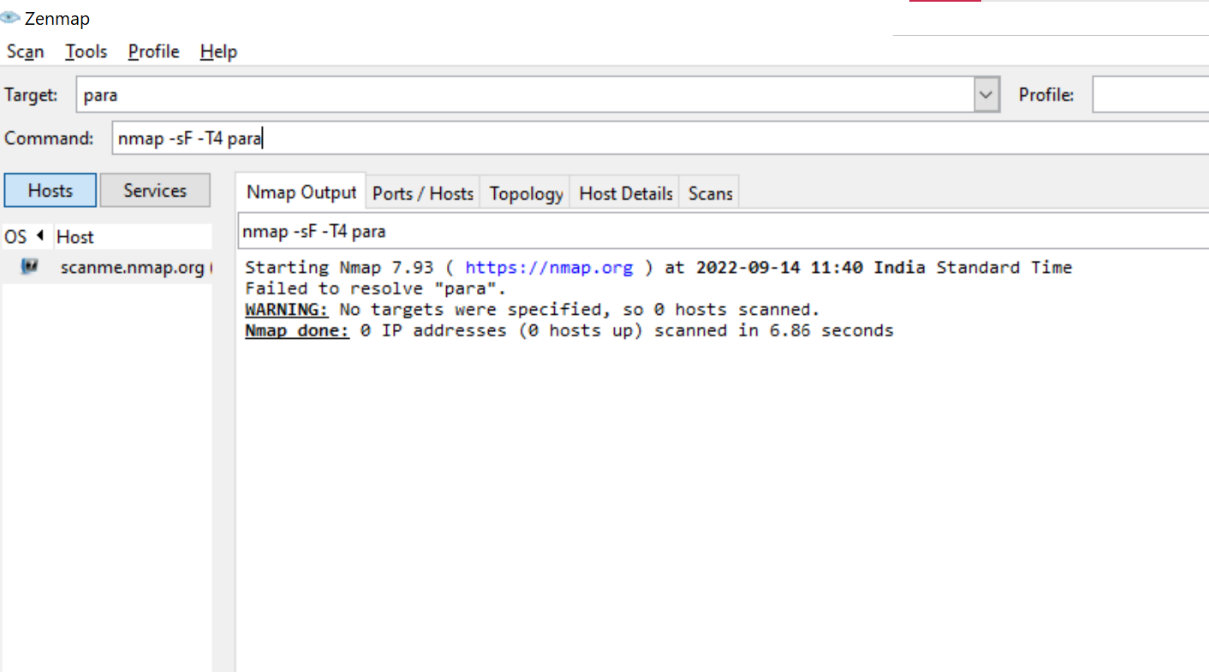
**Ack:**



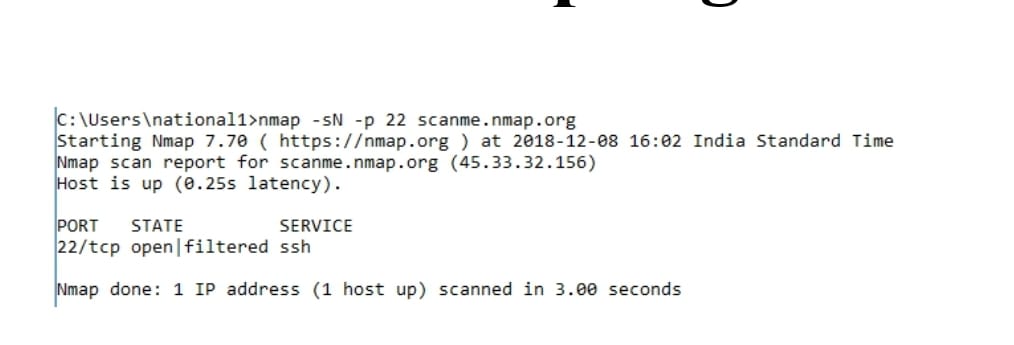
**SYN:**

****

**FIN Scan:**



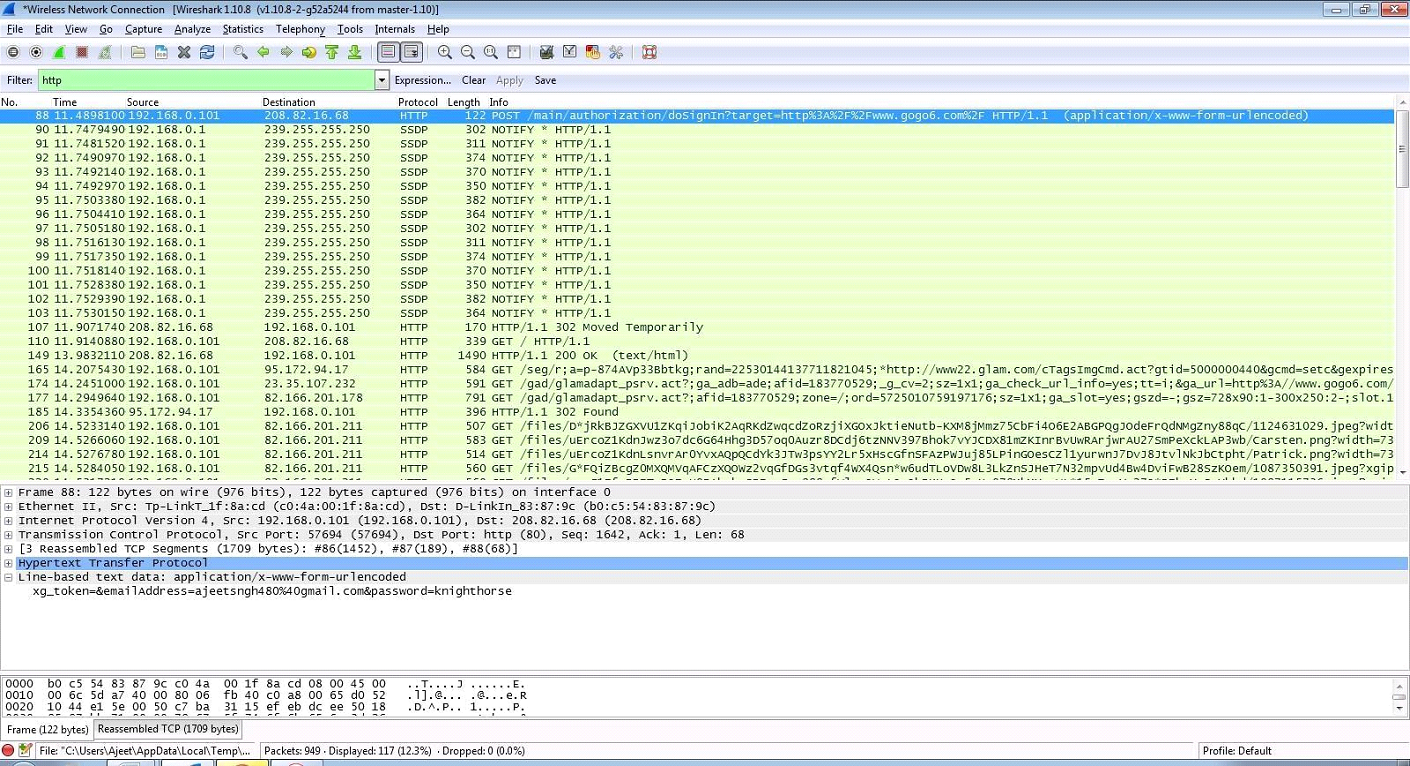
**NULL Scan:**



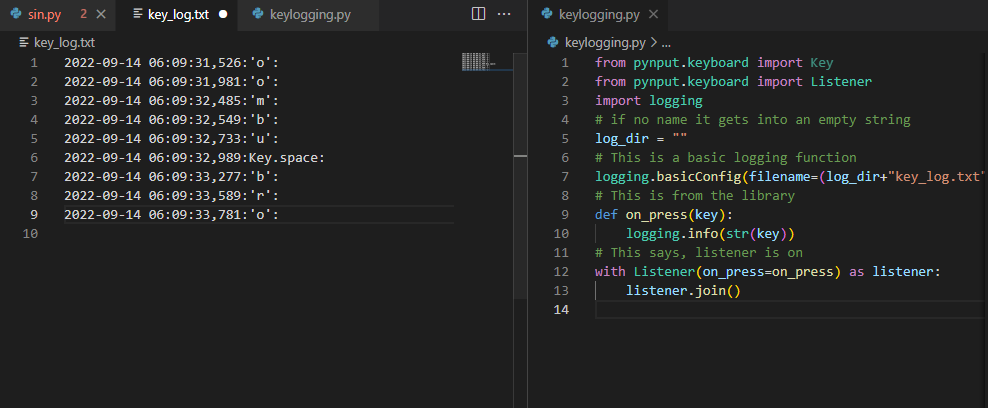
**X Mas Scan:**



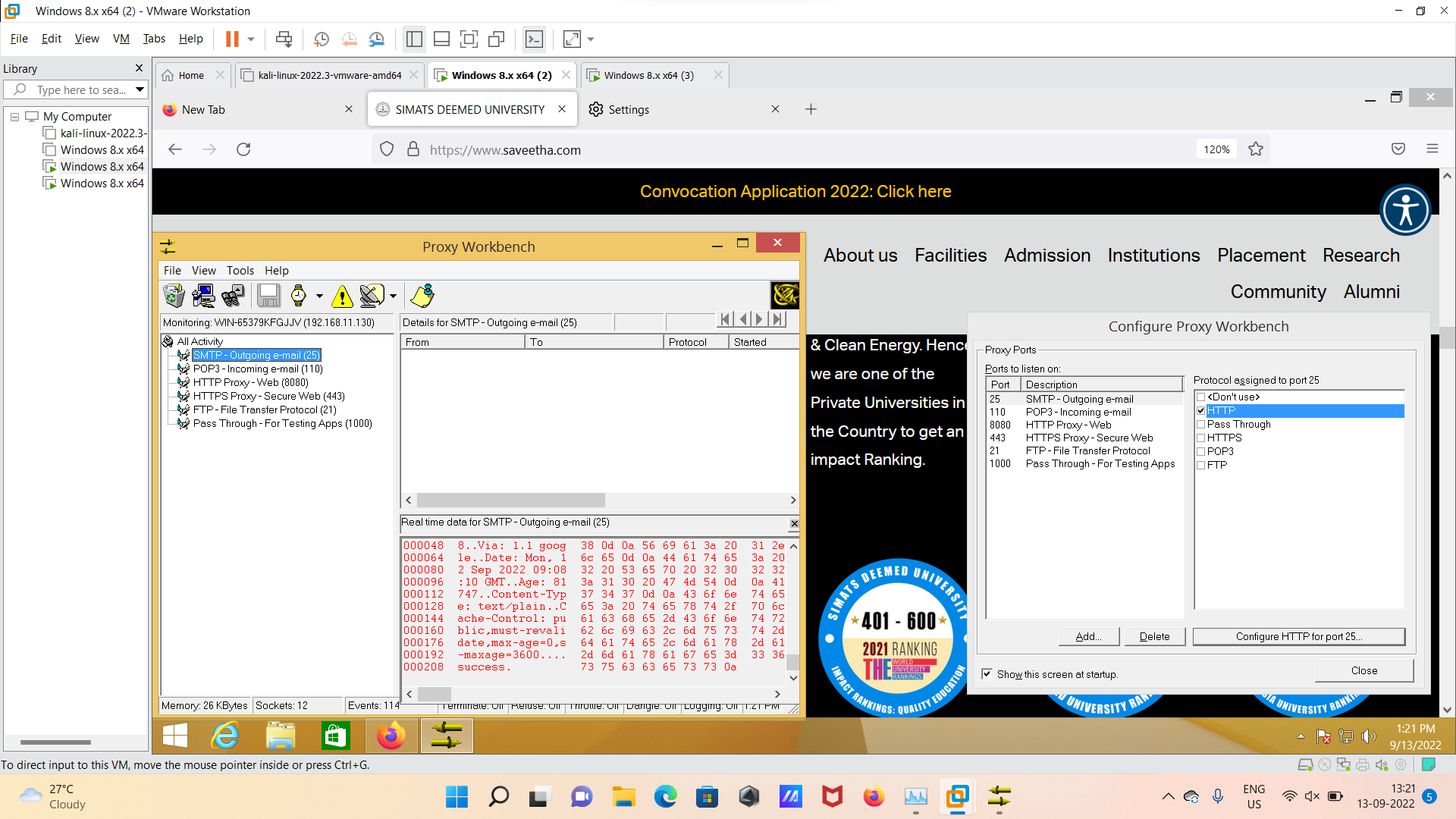
**6) Use WireShark sniffer to capture network traffic:**



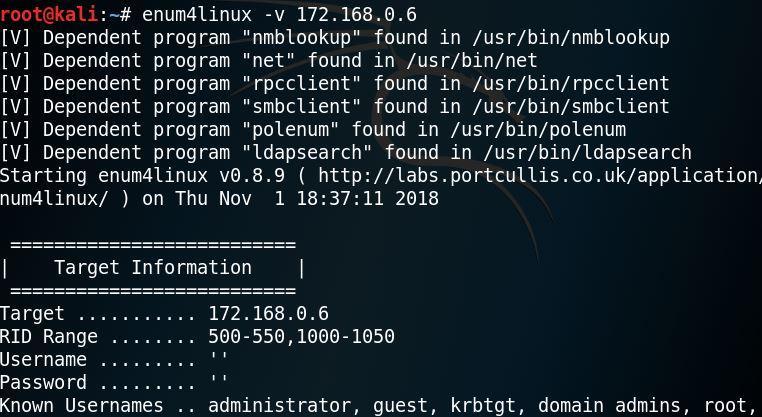
**7) Create a simple keylogger using python code:**



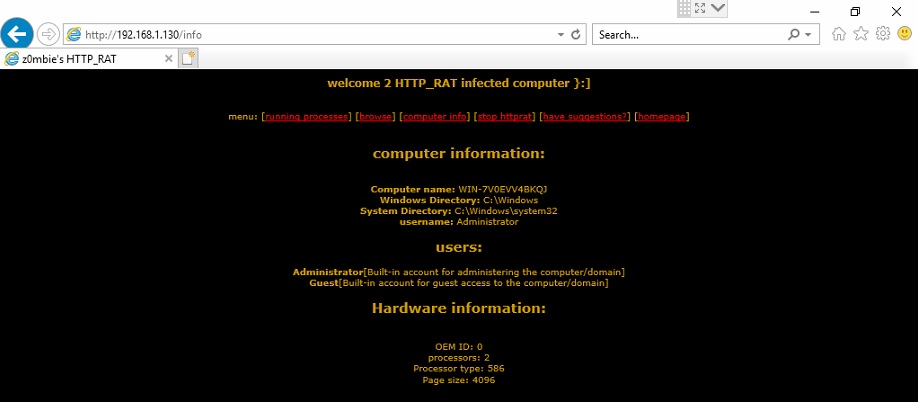
**8) Scanning Network-Daisy chaining using proxy workbench:**



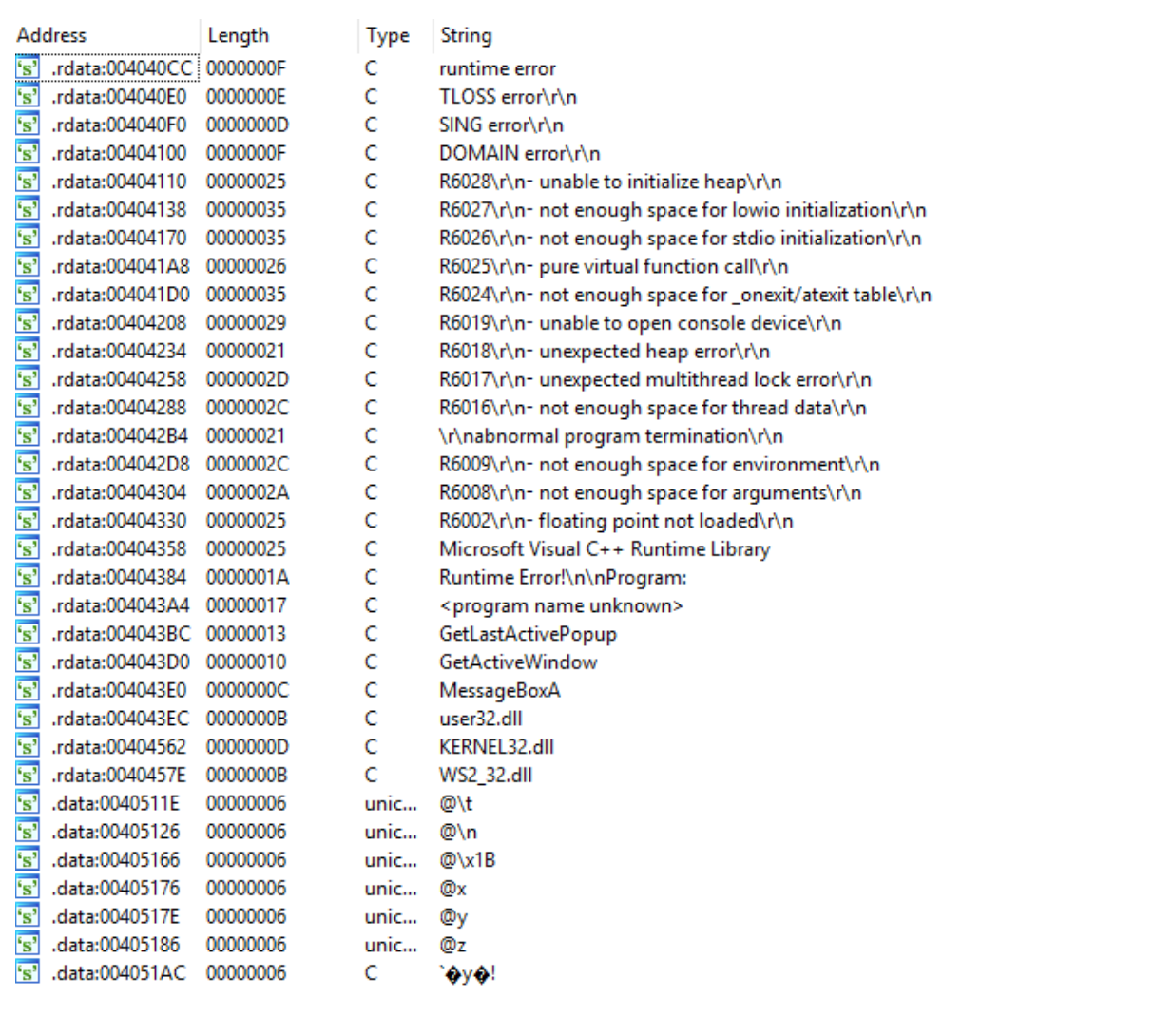
**9) ENUMERATION:**



**10) MALWARE THREATS:**



**11) Virus Analysis using OllyDbg:**



**12) Image Steganography using QuickStego:**

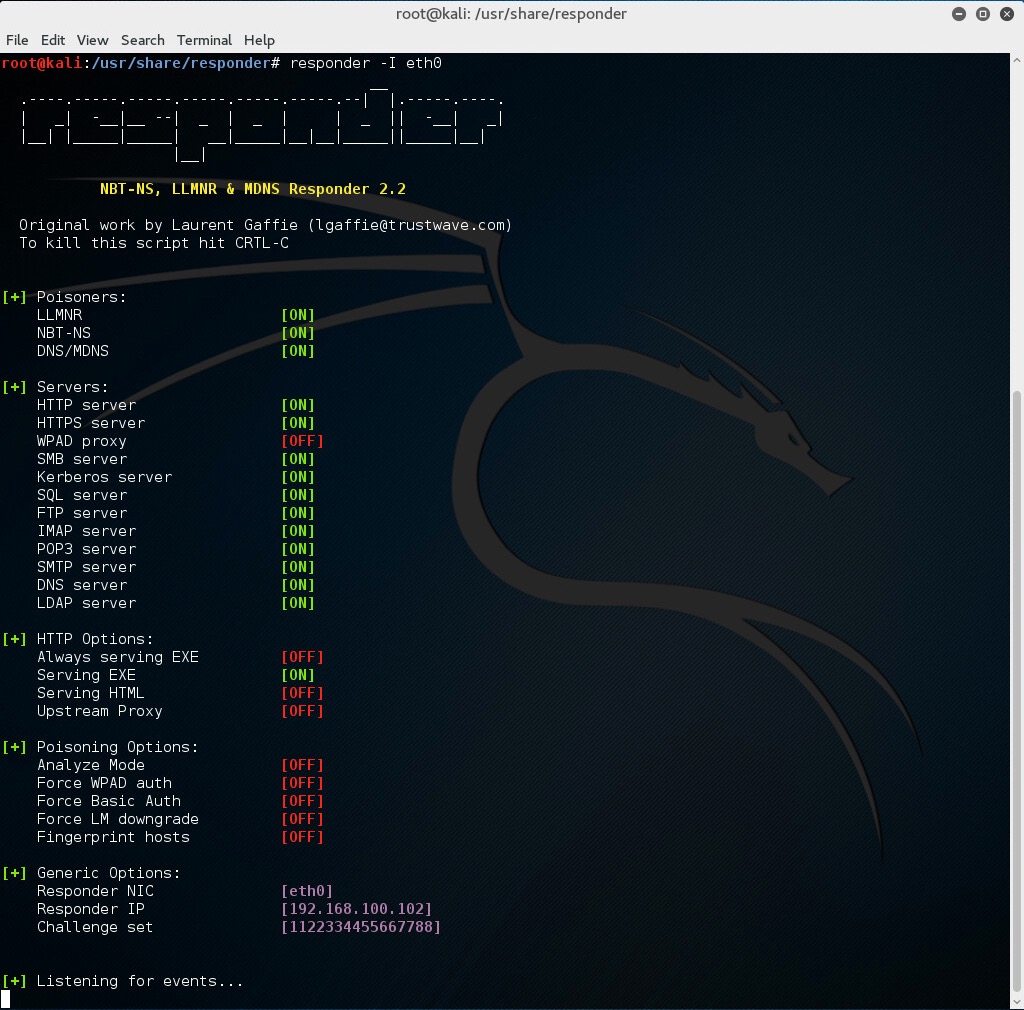
**Before image:**



**After image:**



**13) System Hacking Active online Attack using Responder:**



**14) Foot-printing a Target using Malte-go:**

