INT301: open source Technologies

Project Report

Name: korada Avinash

REG NO: 11915141

SECTION: KEO22

ROLL NO: 35

1.INTRODUCTION

1.1 OBJECTIVE OF THE PROJECT: BruteShark is a Network Forensic Analysis Tool (NFAT) that performs deep processing and inspection of network traffic (mainly PCAP files, but it also capable of directly live capturing from a network interface). It includes: password extracting, building a network map, reconstruct TCP sessions, extract hashes of encrypted passwords and even convert them to a Hashcat format in order to perform an offline Brute Force attack.

1.2 DESCRIPTION OF THE PROJECT

Extracting and encoding usernames and passwords (HTTP, FTP, Telnet, IMAP, SMTP…)

Extract authentication hashes and crack them using Hashcat (Kerberos, NTLM, CRAM-MD5, HTTP-Digest…)

Build visual network diagram (Network nodes, Open Ports, Domain Users)

Extract DNS queries

Reconstruct all TCP & UDP Sessions

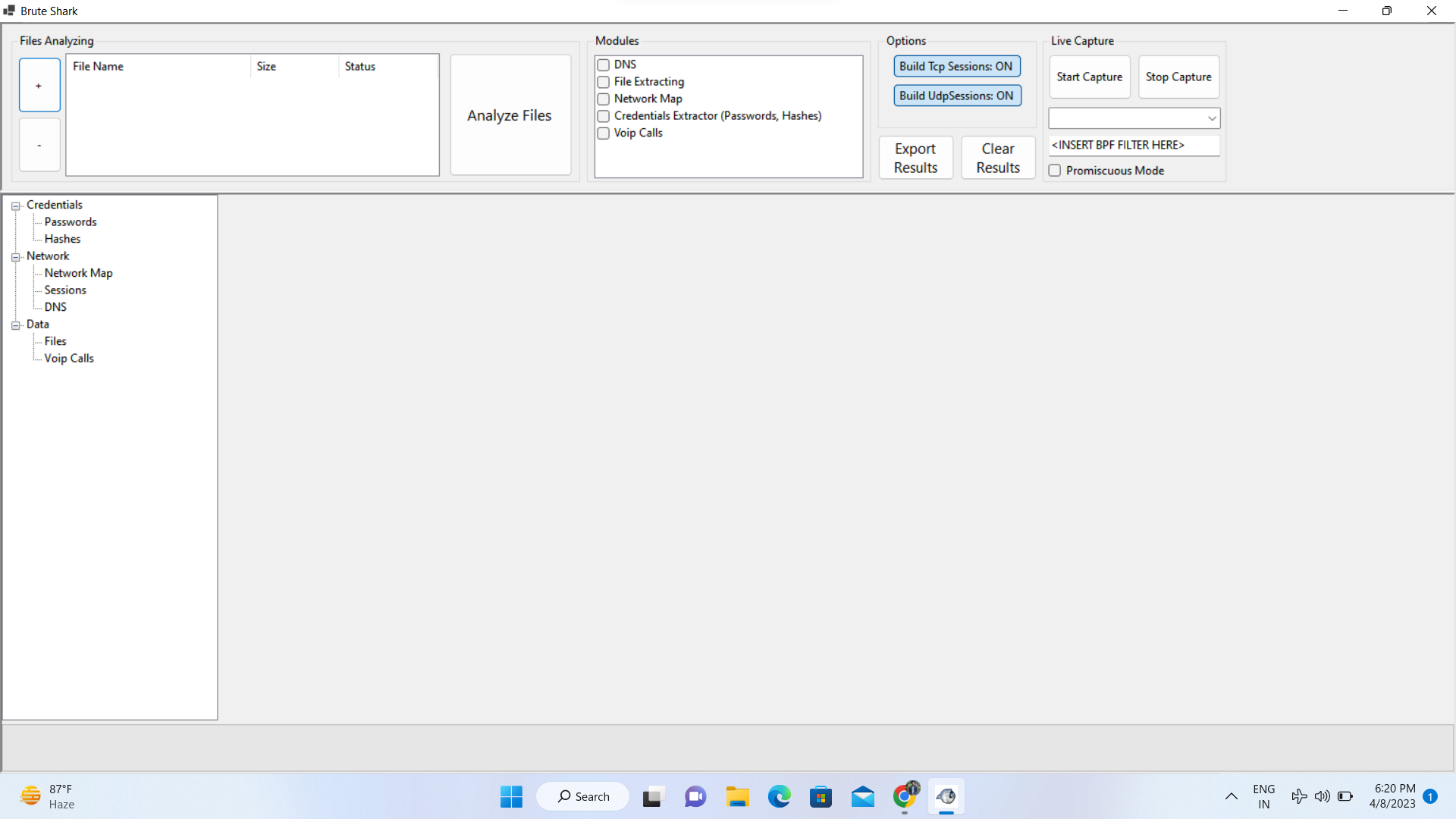
File Carving

Extract Voip calls (SIP, RTP)

Hypertext Transfer Protocol (HTTP) surely needs no introduction either. It typically runs on port 80/tcp and since it is a plain text protocol, it offers very little to no privacy to the communicating parties. Anybody who is in position to eavesdrop on the communication can capture everything over this channel, including passwords.

Even though there has been a tremendous effort done by all major browser vendors to discourage usage of HTTP as much as possible, we can still see HTTP being used on internal networks during penetration tests. Here’s an example of login credentials captured in a HTTP communication in a POST request

After the successful Installation of Brute shark tool this is how it will show the Main page of Brute shark tool:



It consists of modules like:

1.DNS

2.FILE EXTRACTING

3.NETWORK MAP

4.CREDENTIALS EXTRACTOR(passwords,hashes)

5.voip calls

This module is responsible for extracting and encoding usernames and passwords as well as authentication hashes. In fact this module is responsible for updating two display tables, passwords table and hashes table. While usernames and passwords are straight forward to use, hashes most often used in more complex attacks like pass-the-hash or by brute-forcing them to get the password. BruteShark is integrated with Hashcat so all the hashes extracted can be converted to a Hashcat input file.

CREDENTIALS:

\*Passwords

\*Hashes

NETWORK:

\*Network maps

\*Sessions

\*DNS

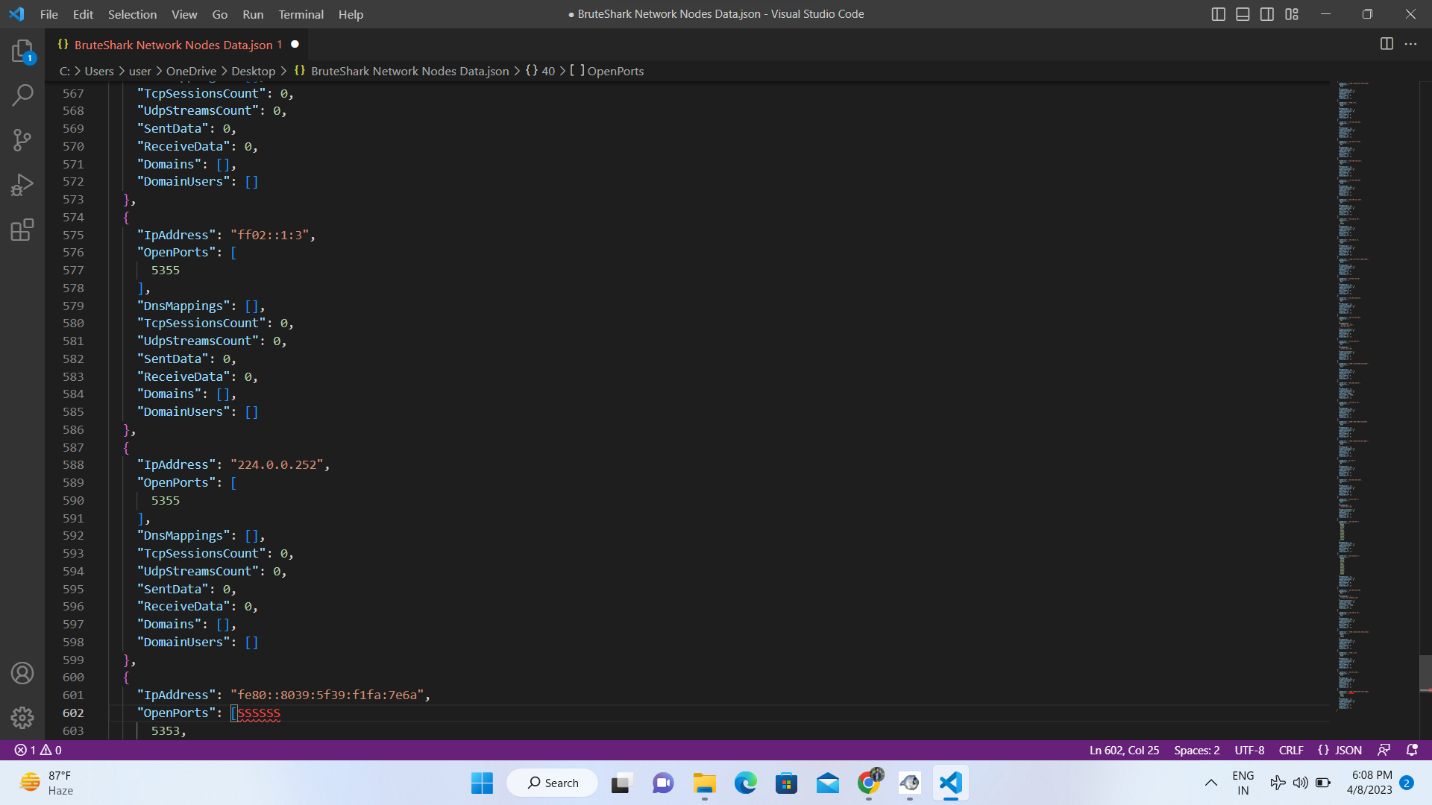
DATA:

\*Files

\*Voip calls

The below screenshort consists of:d

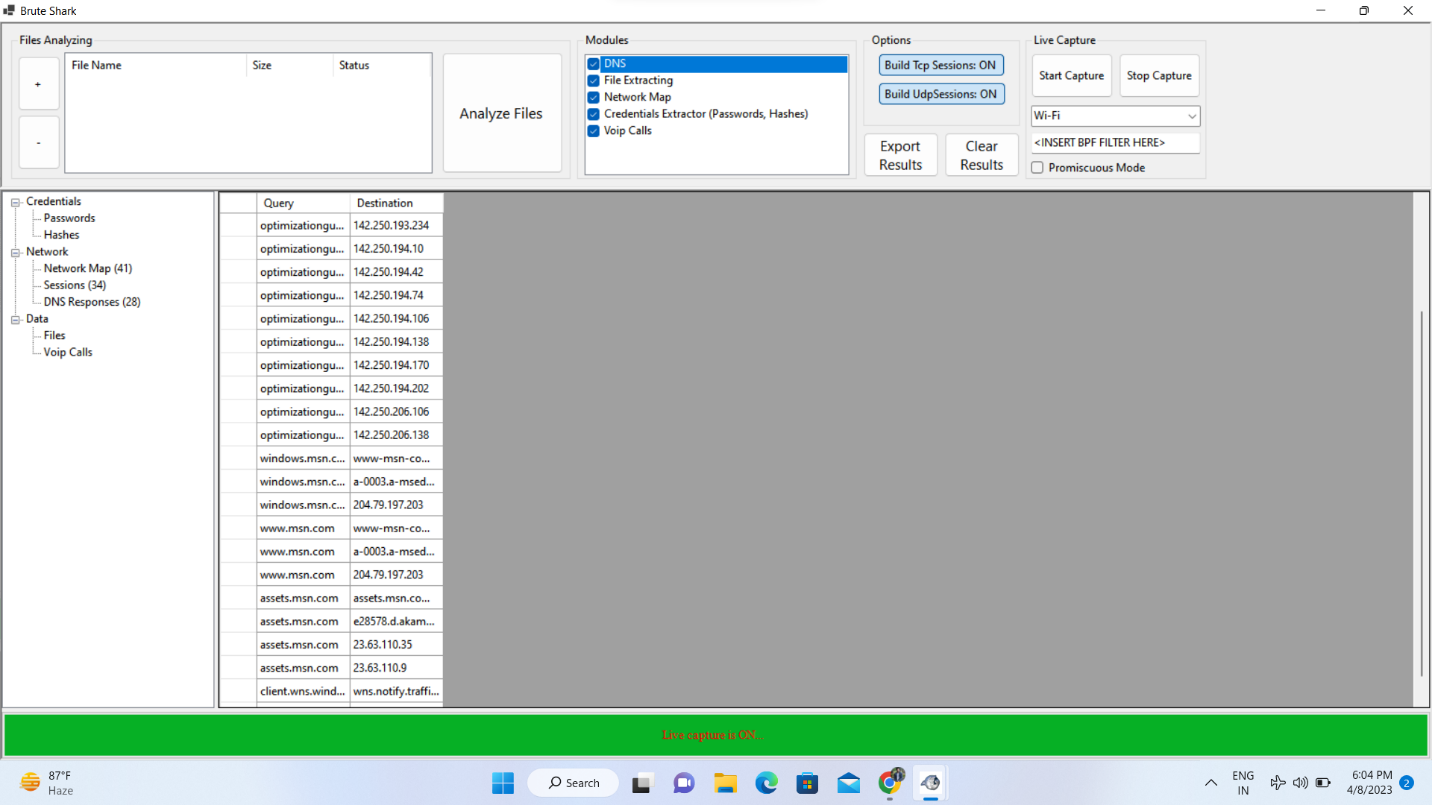
IP address,openports, DNS mappings etc



IP address:An Internet Protocol (IP) address is a unique numerical identifier for every device or network that connects to the internet. Typically assigned by an internet service provider (ISP), an IP address is an online device address used for communicating across the internet

OPEN PORT:An open port is a software-defined value that identifies a network endpoint. Any connection made on a TCP/IP network has a source and destination port that are used with the respective IP addresses to uniquely identify the sender and receiver of every message

DNS Mappings:DNS mapping can solve the problem by configuring a table that specifies the mapping between domain names, public IP addresses, public port numbers, and protocol types. In this manner, the mapping between domain names of servers on the private network and public network information is established.

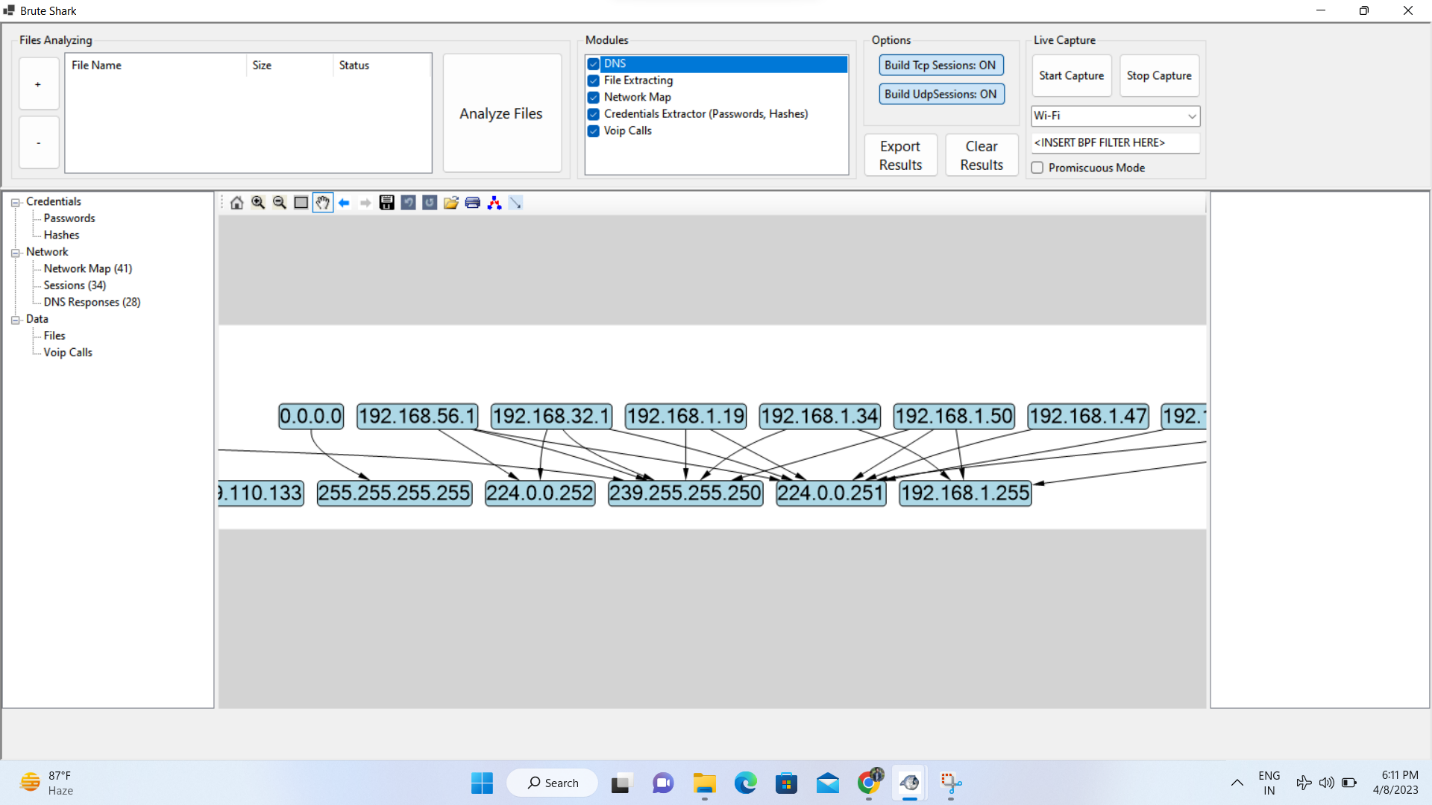


DNS:

The dns-brute.nse script attempts to enumerate DNS hostnames by brute force guessing of common subdomains. With the dns-brute.srv argument, dns-brute will also try to enumerate common DNS SRV records.

Wildcard records are listed as "\*A" and "\*AAAA" for IPv4 and IPv6 respectively.

BUILDING A NETWORK: Network building means working together within a group, between groups, between communities or between villages. Forming a group is one way of building a network.



Basic elements of a computer network include hardware, software, and protocols. The interrelationship of these basic elements constitutes the infrastructure of the network.

