دا فيل سريع كدا عملته يا دكتر بحيث أوضح لحضرتك البروجكت باختصاروالبروجكت كا كل موجود علي github و دا

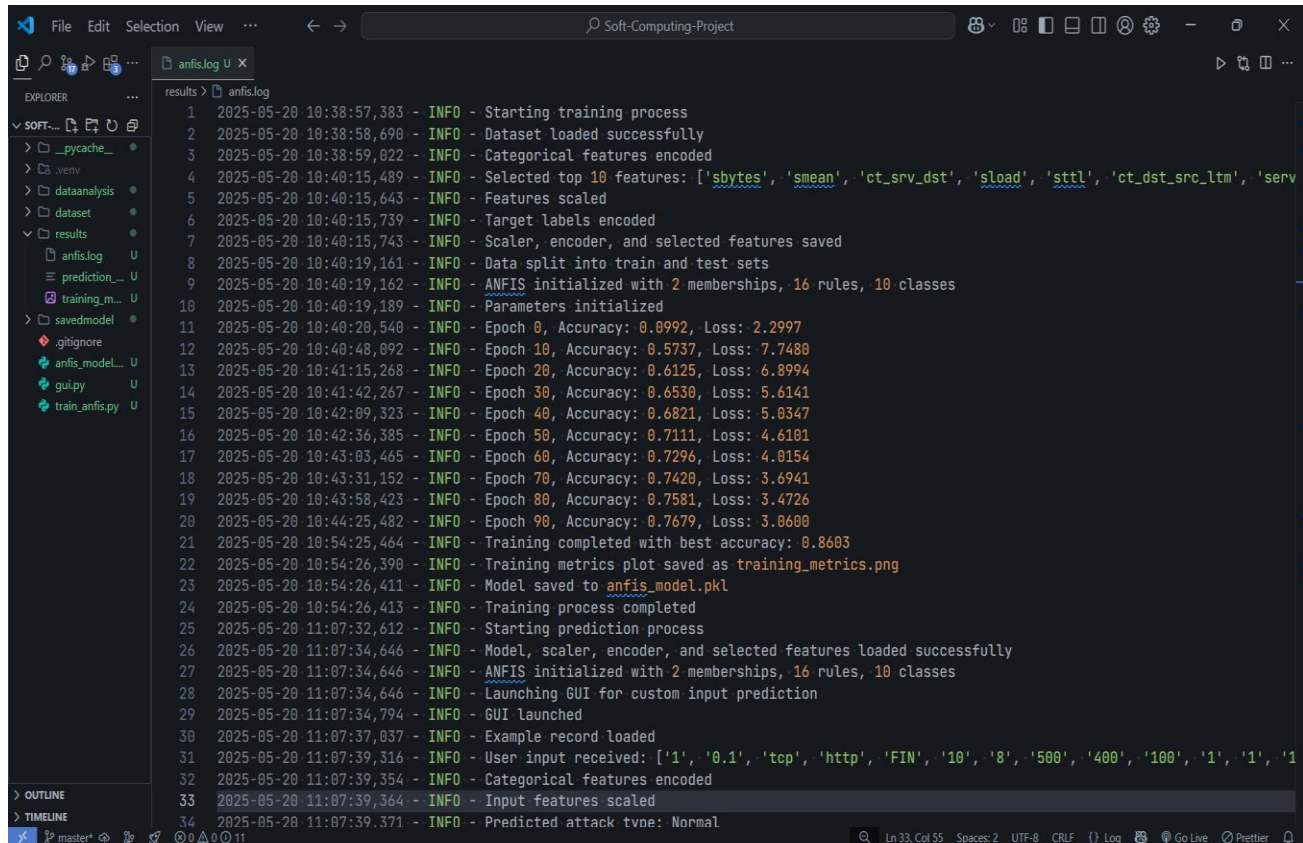لنك الريبو https://github.com/AhmedRedaG/Soft-Computing-Project

التيم: Black Entry

● احمد رضا فاروق
● اسامه الكيال
● عبدالرحمن الطهراني
● فداء القنيشي

فكرة البروجكت باختصار عبارة عن موديل بيقدرر يعمل كلاسيفيكيشن للترافك الحاصل علي النتورك عندي ويحدد اذا كان الترافيك الحاصل دا عبارة عن اتاك او لا وبيحدد مابين 8 أنواع من الاتاكس الي ممكن تحصل

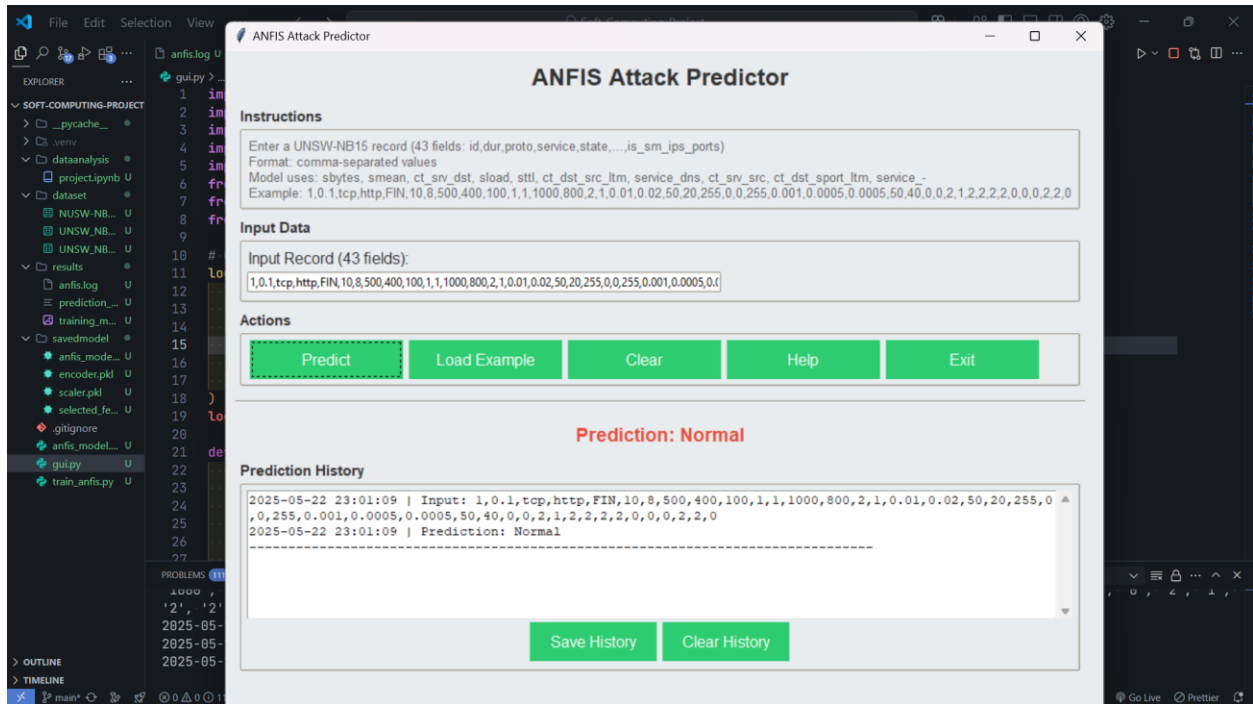والترين علي داتا حوالي 250 الف ريكورد و 45 اتربيوت

دي شوية صور كدا توضيحية سريعه

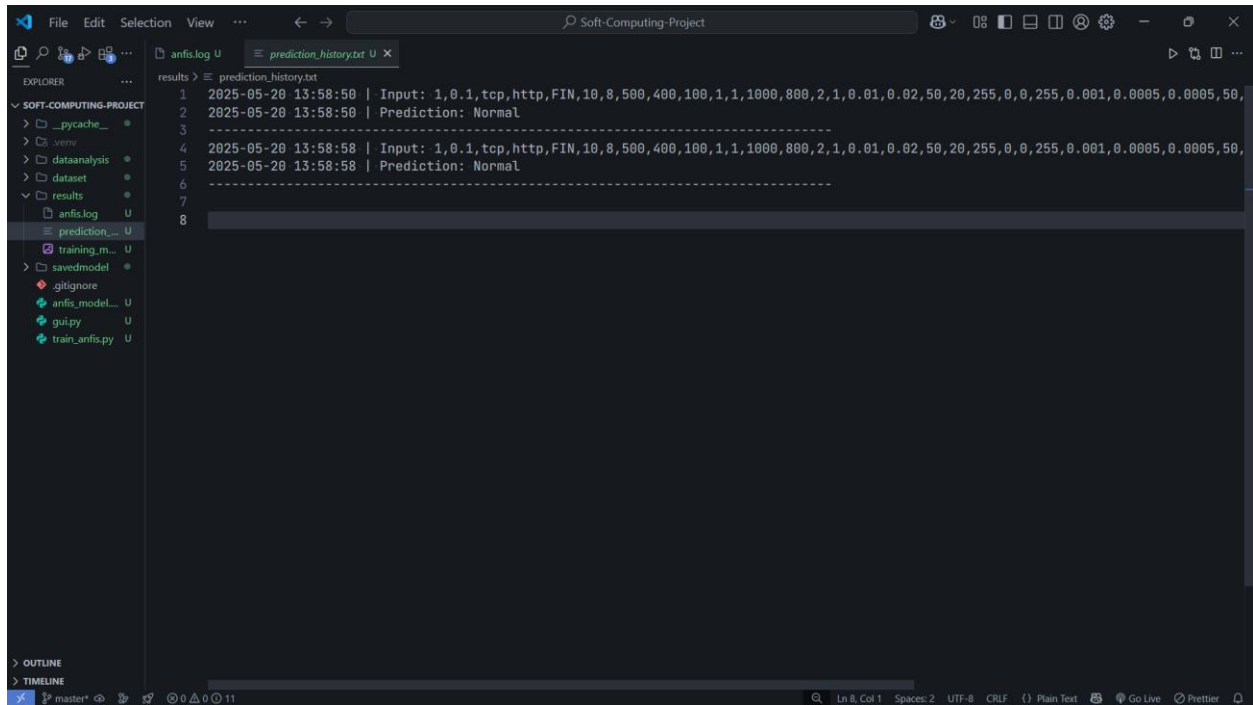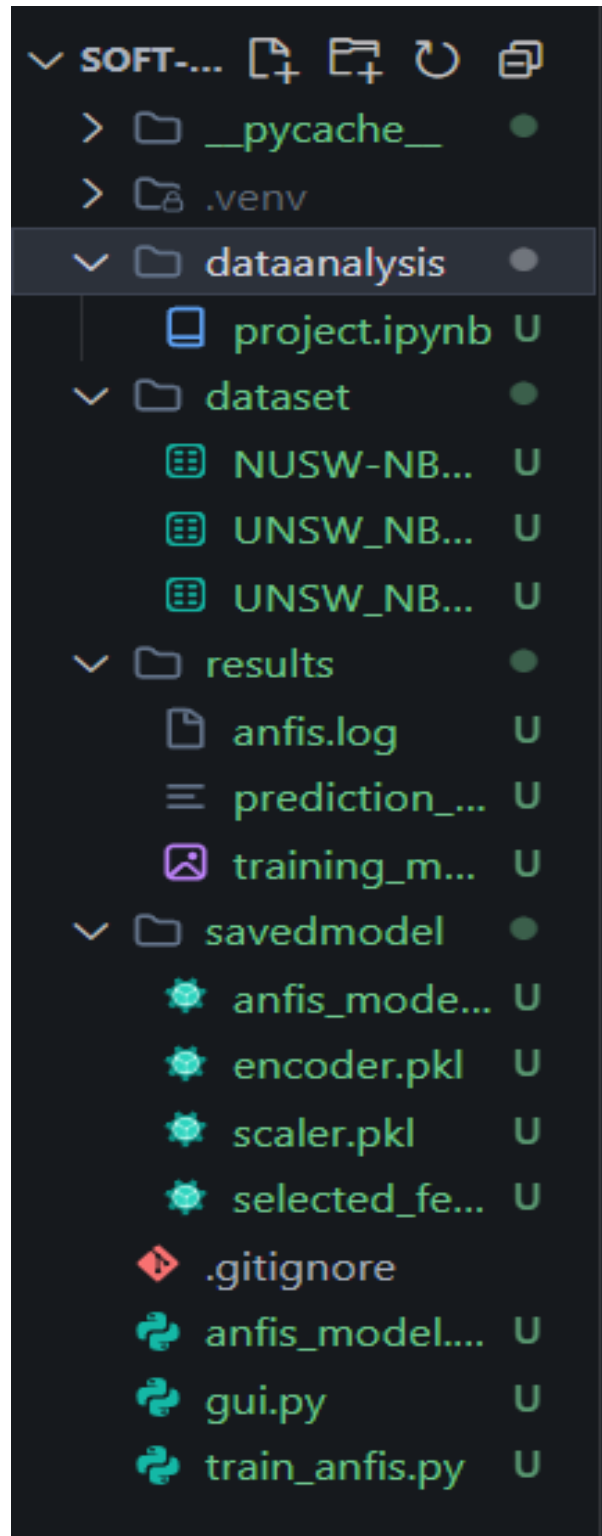دا ملف ال logging بجمع فيه أي log بيحصل وانا برن الموديل

دي ال gui البسيطه الي بتست بيها الترافيك

دا ال history للتستات الي جربتها قبل كدا

دا ال file structure الخاص بالبروجكت

دي شوية تفاصيل عن الداتا

Data

The raw network packets of the UNSW-NB 15 dataset was created by the IXIA PerfectStorm tool in the Cyber Range Lab of UNSW Canberra for generating a hybrid of real modern normal activities and synthetic contemporary attack behaviors. The tcpdump tool was utilized to capture 100 GB of the raw traffic (e.g., Pcap files). This dataset has nine types of attacks, namely, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms. The Argus, Bro-IDS tools are used and twelve algorithms are developed to generate totally 49 features with the class label. These features are described in the UNSW-NB15_features.csv file.

source: https://research.unsw.edu.au/projects/unsw-nb15-dataset

```
id,dur,proto,service,state,spkts,dpkts,sbytes,dbytes,rate,sttl,dttl,sload,dload,sloss,dloss,sinpkt,dinpkt,sjit,djit,swin,
1,0.000011,udp,-,INT,2,0,496,0,90909.0902,254,0,180363632,0,0,0,0.011,0,0,0,0,0,0,0,248,0,0,0,2,2,1,1,2,0,0,0,1,2
2,0.000008,udp,-,INT,2,0,1762,0,125000.0003,254,0,881000000,0,0,0,0.008,0,0,0,0,0,0,0,881,0,0,0,2,2,1,1,1,2,0,0,0,1
3,0.000005,udp,-,INT,2,0,1068,0,200000.0051,254,0,854400000,0,0,0,0.005,0,0,0,0,0,0,0,534,0,0,0,3,2,1,1,3,0,0,0,1
4,0.000006,udp,-,INT,2,0,900,0,166666.6608,254,0,600000000,0,0,0,0.006,0,0,0,0,0,0,0,450,0,0,3,2,2,2,1,3,0,0,0,2,
5,0.00001,udp,-,INT,2,0,2126,0,100000.0025,254,0,850400000,0,0,0,0.01,0,0,0,0,0,0,0,1063,0,0,0,3,2,2,2,1,3,0,0,0,2,
6,0.000003,udp,-,INT,2,0,784,0,333333.3215,254,0,1045333312,0,0,0,0.003,0,0,0,0,0,0,0,392,0,0,0,2,2,2,2,1,2,0,0,0,2
7,0.000006,udp,-,INT,2,0,1960,0,166666.6608,254,0,1306666624,0,0,0,0.006,0,0,0,0,0,0,0,980,0,0,0,2,2,2,2,1,2,0,0,0,
8,0.000028,udp,-,INT,2,0,1384,0,35714.28522,254,0,197714288,0,0,0,0.028,0,0,0,0,0,0,0,692,0,0,0,3,2,1,1,3,0,0,0,1
9,0,arp,-,INT,1,0,46,0,0,0,0,0,0,0,0,60000.688,0,0,0,0,0,0,0,0,46,0,0,0,2,2,2,2,2,2,0,0,0,2,2,1,Normal,0
10,0,arp,-,INT,1,0,46,0,0,0,0,0,0,0,0,60000.712,0,0,0,0,0,0,0,0,46,0,0,0,2,2,2,2,2,2,0,0,0,2,2,1,Normal,0
11,0,arp,-,INT,1,0,46,0,0,0,0,0,0,0,0,60000.688,0,0,0,0,0,0,0,0,46,0,0,0,2,2,2,2,2,2,0,0,0,2,2,1,Normal,0
12,0,arp,-,INT,1,0,46,0,0,0,0,0,0,0,0,60000.712,0,0,0,0,0,0,0,0,46,0,0,0,2,2,2,2,2,2,0,0,0,2,2,1,Normal,0
13,0.000004,udp,-,INT,2,0,1454,0,250000.0006,254,0,1454000000,0,0,0,0.004,0,0,0,0,0,0,0,727,0,0,0,3,2,1,1,3,0,0,0
14,0.000007,udp,-,INT,2,0,2062,0,142857.1409,254,0,1178285696,0,0,0,0.007,0,0,0,0,0,0,0,1031,0,0,0,3,2,1,1,3,0,0,0
15,0.000011,udp,-,INT,2,0,2040,0,90909.0902,254,0,741818176,0,0,0,0.011,0,0,0,0,0,0,0,1020,0,0,0,1,2,1,1,1,0,0,0,
16,0.000004,udp,-,INT,2,0,1052,0,250000.0006,254,0,1052000000,0,0,0,0.004,0,0,0,0,0,0,0,526,0,0,0,3,2,1,1,3,0,0,0
17,0.000003,udp,-,INT,2,0,314,0,333333.3215,254,0,418666656,0,0,0,0.003,0,0,0,0,0,0,0,157,0,0,0,2,2,1,1,2,0,0,0,1
18,0.00001,udp,-,INT,2,0,1774,0,100000.0025,254,0,709600000,0,0,0,0.01,0,0,0,0,0,0,0,887,0,0,0,2,2,1,1,2,0,0,0,1,
19,0.000002,udp,-,INT,2,0,1568,0,500000.0013,254,0,3136000000,0,0,0,0.002,0,0,0,0,0,0,0,784,0,0,0,3,2,1,1,2,0,0,0
20,0.000004,udp,-,INT,2,0,2054,0,250000.0006,254,0,2054000000,0,0,0,0.004,0,0,0,0,0,0,0,1027,0,0,0,3,2,1,1,2,0,0,
21,0.00001,udp,-,INT,2,0,2170,0,100000.0025,254,0,868000000,0,0,0,0.01,0,0,0,0,0,0,0,1085,0,0,0,2,2,1,1,2,0,0,0,1
22,0.000009,udp,-,INT,2,0,202,0,111111.1072,254,0,89777776,0,0,0,0.009,0,0,0,0,0,0,0,101,0,0,0,2,2,1,1,2,0,0,0,1,
23,0.00001,udp,-,INT,2,0,1334,0,100000.0025,254,0,533600000,0,0,0,0.01,0,0,0,0,0,0,0,667,0,0,0,3,2,1,1,3,0,0,0,1,
24,0.000005,udp,-,INT,2,0,2058,0,200000.0051,254,0,1646400000,0,0,0,0.005,0,0,0,0,0,0,0,1029,0,0,0,3,2,2,1,3,0,0,0,
25,0.000003,udp,-,INT,2,0,286,0,333333.3215,254,0,381333312,0,0,0,0.003,0,0,0,0,0,0,0,143,0,0,0,3,2,2,2,1,3,0,0,0,2
26,0.000007,udp,-,INT,2,0,1500,0,142857.1409,254,0,857142848,0,0,0,0.007,0,0,0,0,0,0,0,750,0,0,0,2,2,2,2,1,2,0,0,0,2
27,0.000006,udp,-,INT,2,0,902,0,166666.6608,254,0,601333312,0,0,0,0.006,0,0,0,0,0,0,0,451,0,0,0,2,2,2,2,1,2,0,0,0,2
28,0.000002,udp,-,INT,2,0,1626,0,500000.0013,254,0,3252000000,0,0,0,0.002,0,0,0,0,0,0,0,813,0,0,0,2,2,1,1,1,0,0,0,0
29,0.000007,udp,-,INT,2,0,364,0,142857.1409,254,0,208000000,0,0,0,0.007,0,0,0,0,0,0,0,182,0,0,0,3,2,1,1,1,0,0,0,2
30,1.436166,tcp,-,FIN,10,6,530,268,10.459041,254,252,2660,780829,1249,506714,2,1,151.243111,270.886813,10042,8699,468,508
```

	No.	Name	Type	Description
0	1	srcip	nominal	Source IP address
1	2	sport	integer	Source port number
2	3	dstip	nominal	Destination IP address
3	4	dsport	integer	Destination port number
4	5	proto	nominal	Transaction protocol
5	6	state	nominal	Indicates to the state and its dependent proto...
6	7	dur	Float	Record total duration
7	8	sbytes	Integer	Source to destination transaction bytes
8	9	dbytes	Integer	Destination to source transaction bytes
9	10	sttl	Integer	Source to destination time to live value
10	11	dttl	Integer	Destination to source time to live value
11	12	sloss	Integer	Source packets retransmitted or dropped
12	13	dloss	Integer	Destination packets retransmitted or dropped
13	14	service	nominal	http, ftp, smtp, ssh, dns, ftp-data ,irc and ...
14	15	Sload	Float	Source bits per second
15	16	Dload	Float	Destination bits per second
16	17	Spkts	integer	Source to destination packet count
17	18	Dpkts	integer	Destination to source packet count
18	19	swin	integer	Source TCP window advertisement value
19	20	dwin	integer	Destination TCP window advertisement value
20	21	stcpb	integer	Source TCP base sequence number
21	22	dtcpb	integer	Destination TCP base sequence number
22	23	smeansz	integer	Mean of the ?ow packet size transmitted by the...
23	24	dmeansz	integer	Mean of the ?ow packet size transmitted by the...
24	25	trans_depth	integer	Represents the pipelined depth into the connec...
25	26	res_bdy_len	integer	Actual uncompressed content size of the data t...
26	27	Sjit	Float	Source jitter (mSec)
27	28	Djit	Float	Destination jitter (mSec)
28	29	Stime	Timestamp	record start time
29	30	Ltime	Timestamp	record last time
30	31	Sintpkt	Float	Source interpacket arrival time (mSec)
31	32	Dintpkt	Float	Destination interpacket arrival time (mSec)
32	33	tcprtt	Float	TCP connection setup round-trip time, the sum ...
33	34	synack	Float	TCP connection setup time, the time between th...
34	35	ackdat	Float	TCP connection setup time, the time between th...
35	36	is_sm_ips_ports	Binary	If source (1) and destination (3)IP addresses ...
36	37	ct_state_ttl	Integer	No. for each state (6) according to specific r...
37	38	ct_flw_http_mthd	Integer	No. of flows that has methods such as Get and ...
38	39	is_ftp_login	Binary	If the ftp session is accessed by user and pas...
39	40	ct_ftp_cmd	integer	No of flows that has a command in ftp session.
40	41	ct_srv_src	integer	No. of connections that contain the same servi...
41	42	ct_srv_dst	integer	No. of connections that contain the same servi...
42	43	ct_dst_ltm	integer	No. of connections of the same destination add...
43	44	ct_src_ltm	integer	No. of connections of the same source address ...
44	45	ct_src_dport_ltm	integer	No of connections of the same source address (...
45	46	ct_dst_sport_ltm	integer	No of connections of the same destination addr...
46	47	ct_dst_src_ltm	integer	No of connections of the same source (1) and t...
47	48	attack_cat	nominal	The name of each attack category. In this data...
48	49	Label	binary	0 for normal and 1 for attack records

Distribution of attack categories

Service Counts by Attack Categories

Correlation Heatmap between Numeric Features