

Feb 1st 2024
Thủ Đức, TP. HCM



BÁO CÁO ĐỒ ÁN MÔN HỌC Hệ Thống Phát Hiện Xâm Nhập Mạng Trục Tuyến

SV1 – MSSV 1

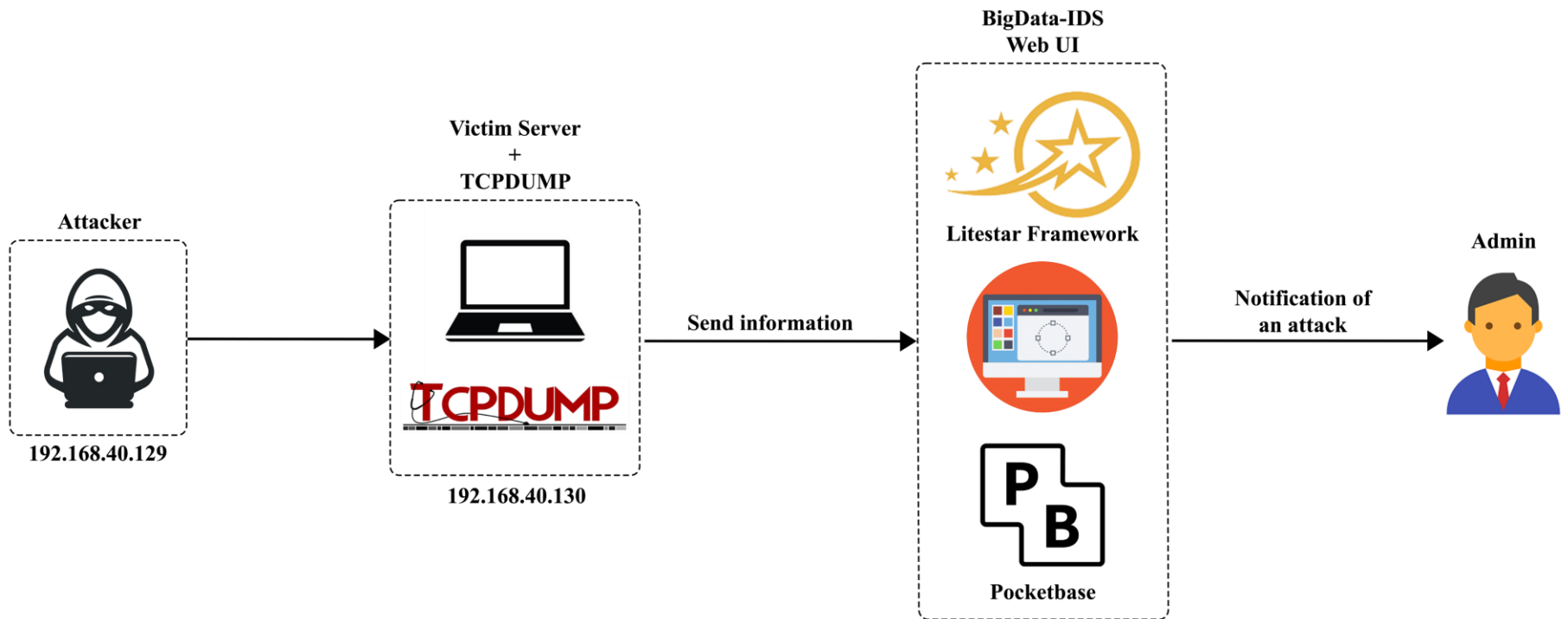
...

GVHD: ...

- **Nghiên cứu liên quan**
- **Mô hình đề xuất**
- **Thực nghiệm và đánh giá**
- **Kết luận và hướng phát triển**

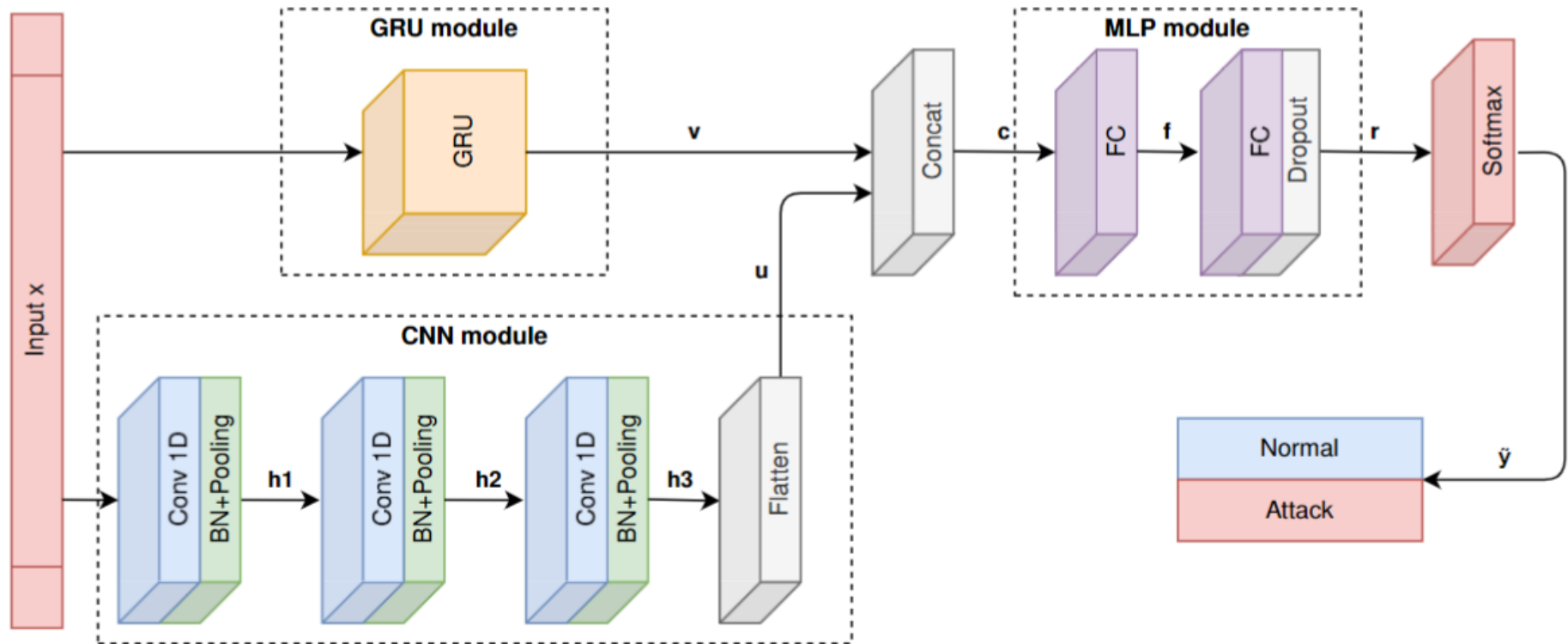
[1] Vy, N.C., Quyen, N.H., Duy, P.T., Pham, V.H. (2021). Federated Learning-Based Intrusion Detection in the Context of IIoT Networks: Poisoning Attack and Defense. In: Yang, M., Chen, C., Liu, Y. (eds) Network and System Security. NSS 2021. Lecture Notes in Computer Science(), vol 13041. Springer, Cham.

Tổng quan hệ thống:



Hình 1: Kiến trúc hệ thống phát hiện xâm nhập mạng BD-IDS

Mô hình học sâu cho IDS:



Hình 1: Kiến trúc mô hình IDS ứng dụng học sâu

Cài đặt thực nghiệm:

➤ Môi trường và ngôn ngữ cài đặt:

- Ngôn ngữ lập trình: Python
- Thư viện: PySpark, BigDL,...
- Cấu hình máy thực nghiệm: 32GB RAM, 300 GB Hard Drive, Intel Core i5-8300H 16-core CPU.

Dữ liệu thực nghiệm:

- Bộ dữ liệu: Kitsune Network Attack Dataset
- Bộ dữ liệu tự thu thập

Dataset	Attack Samples	Normal Samples
Kitsune	6.998	2.764.276
Tự thu thập	400.000	80.000

Bảng 1: Thống kê dữ liệu huấn luyện mô hình học sâu

Kết quả thực nghiệm:

➤ Hiệu năng của mô hình DL-based IDS :

Model	Accuracy	F1-score
CNNGRU	99.99%	99.99%

Cài đặt thu thập dữ liệu tấn công:

```
r3ckl3ss@ubuntu: ~/Desktop
r3ckl3ss@ubuntu:~/Desktop$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --
rand-source 192.168.40.130
[sudo] password for r3ckl3ss:
HPING 192.168.40.130 (ens33 192.168.40.130): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
192.168.40.130 hping statistic ---
1194446 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Thực nghiệm và đánh giá



Cài đặt thu thập dữ liệu tấn công:

The image shows a desktop environment with a file manager window titled 'BigData' and a terminal window titled 'cometofruition@cometofruition: ~/Desktop/BigData'.

File Manager (BigData):

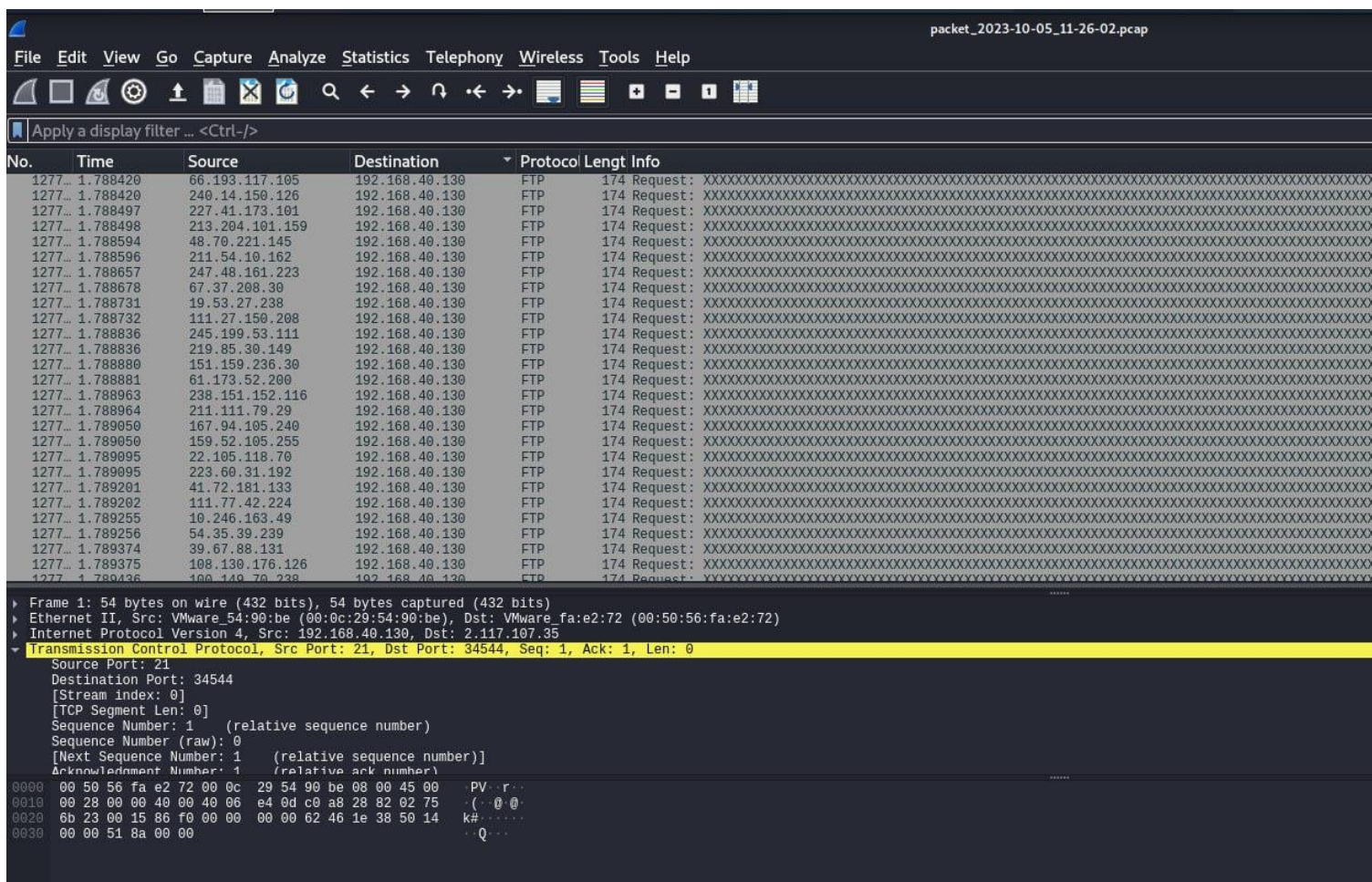
- Places: Computer, cometofruition, Desktop, Trash, Documents, Music, Pictures, Videos, Downloads.
- Devices: File System, Network, Browse Network.
- Files in Desktop/BigData:
 - capture_packet.sh
 - capture_pcap.py
 - packet_2023-10-05_11-25-27.pcap
 - packet_2023-10-05_11-26-02.pcap
 - packet_2023-10-05_11-28-20.pcap
 - packet_2023-10-07_02-00-53.pcap
 - packet_2023-10-07_02-03-30.pcap
 - packet_2023-10-07_02-03-35.pcap
 - packet_2023-10-07_02-03-40.pcap
 - packet_2023-10-07_02-03-46.pcap
 - packet_2023-10-07_02-03-51.pcap
 - packet_2023-10-07_02-03-56.pcap
 - packet_2023-10-07_02-04-01.pcap
 - packet_2023-10-07_02-04-06.pcap
 - packet_2023-10-07_02-04-11.pcap
- Summary: 15 files: 680.9 MiB (713,954,388 bytes), Free space: 17.3 GiB

Terminal Window:

```
File Actions Edit View Help
0 packets dropped by kernel
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
100 packets captured
1292 packets received by filter
0 packets dropped by kernel
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
100 packets captured
1291 packets received by filter
0 packets dropped by kernel
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
100 packets captured
1286 packets received by filter
0 packets dropped by kernel
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
100 packets captured
1270 packets received by filter
0 packets dropped by kernel
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
100 packets captured
1304 packets received by filter
0 packets dropped by kernel
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
100 packets captured
1310 packets received by filter
0 packets dropped by kernel
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
100 packets captured
1301 packets received by filter
0 packets dropped by kernel
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
100 packets captured
1277 packets received by filter
0 packets dropped by kernel
```



Cài đặt thu thập dữ liệu tấn công:



The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter is applied: "Apply a display filter ... <Ctrl-/>". The packet list table shows the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The table contains 27 rows of data, all of which are FTP requests from various source IP addresses to 192.168.40.130. The selected packet is the 27th row, which is a request from 192.168.40.130 to 192.168.40.130. The packet details pane shows the following information:

- Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
- Ethernet II, Src: VMware_54:90:be (00:0c:29:54:90:be), Dst: VMware_fa:e2:72 (00:50:56:fa:e2:72)
- Internet Protocol Version 4, Src: 192.168.40.130, Dst: 2.117.107.35
- Transmission Control Protocol, Src Port: 21, Dst Port: 34544, Seq: 1, Ack: 1, Len: 0
- Source Port: 21
- Destination Port: 34544
- [Stream Index: 0]
- [TCP Segment Len: 0]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 0
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)

The packet bytes pane shows the raw data of the selected packet, which is a zero-length TCP segment. The bytes are displayed in hexadecimal and ASCII format.

Kết luận:

- Xây dựng được mô hình phát hiện xâm nhập mạng có độ chính xác cao trên 99.97%.
- Xây dựng được giao diện người dùng hỗ trợ quản lý và sử dụng.

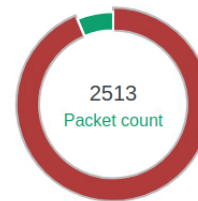
Hướng phát triển:

- Hạn chế của lượng dữ liệu tự thu thập cần gia tăng lượng dữ liệu.
- Hệ thống vẫn chưa có khả năng phân loại được chính xác loại xâm nhập.
- Hệ thống vẫn chưa đưa ra được lý do chính xác cho các dự đoán.

BD-IDS

Choose File No file chosen

Submit



● Attack ● Benign

Previous 1 2 3 4 5 Next

ID	PREDICTION	TIMESTAMP	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	LENGTH	TTL	OFFSET	DF	MF
32e1ef1c-20d1-4f97-909d-7774d3087beb	Attack	2023-10-13 19:39:35.230898	192.168.40.130	23	192.168.40.129	34730	40	64	0	1	0
0fcb7ce2-e677-4efb-a55e-b61f4453441a	Attack	2023-10-13 19:39:35.230941	192.168.40.129	39686	192.168.40.130	80	60	64	0	1	0
d0f610c2-3d92-47f0-94ba-477e7d55bda8	Attack	2023-10-13 19:39:35.230985	192.168.40.130	80	192.168.40.129	39686	60	64	0	1	0
55b35b91-20bf-4254-b38b-71d9f92bd6ed	Attack	2023-10-13 19:39:35.231009	192.168.40.129	39594	192.168.40.130	5900	60	64	0	1	0
adbaff22-f0a9-4be4-bec7-1f83fc253257	Attack	2023-10-13 19:39:35.231467	192.168.40.130	5900	192.168.40.129	39594	40	64	0	1	0
aebd0a08-f874-4ef9-928b-0797b5bf641a	Attack	2023-10-13 19:39:35.231490	192.168.40.129	38010	192.168.40.130	135	60	64	0	1	0

BD-IDS

Choose File input.pcap

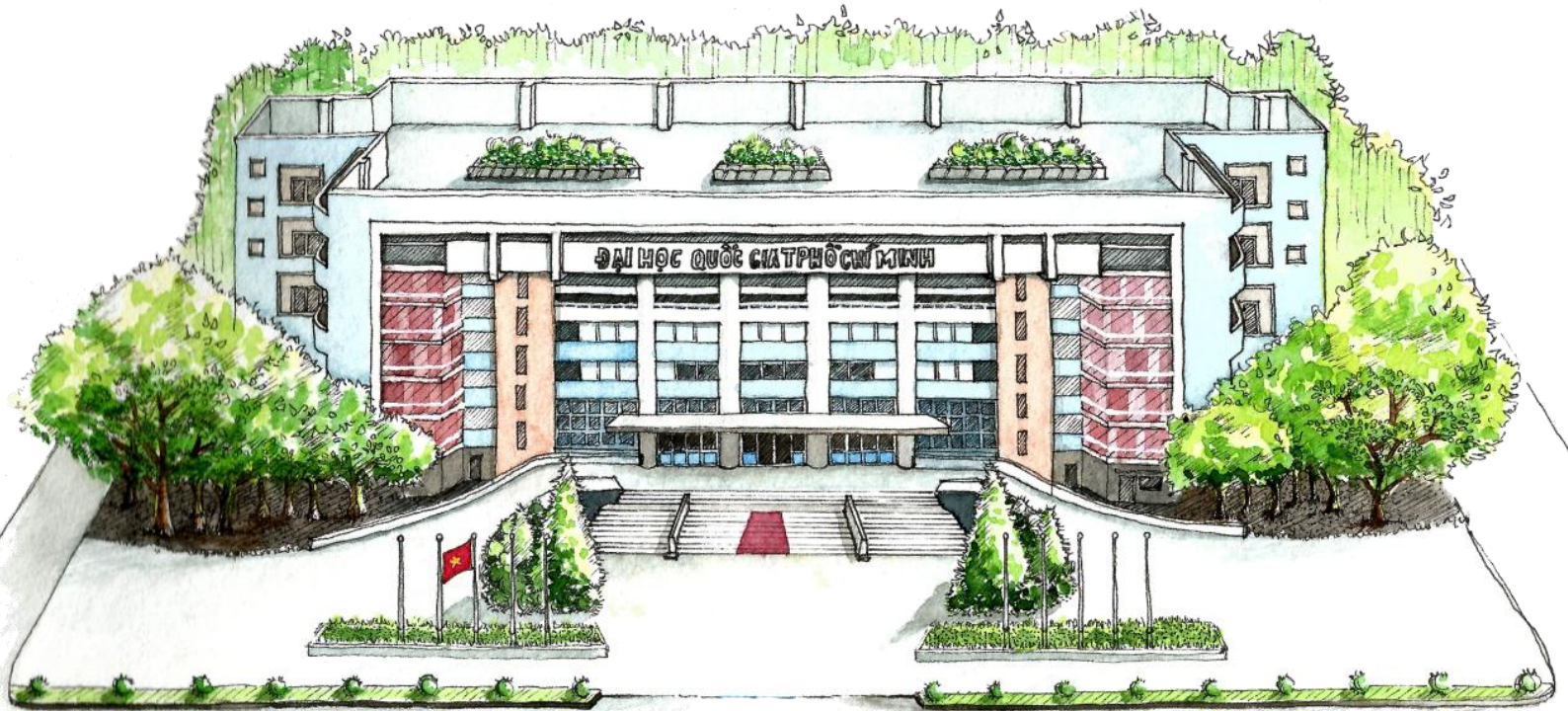
Submit



● Attack ● Benign

Previous 1 2 3 4 5 Next

ID	PREDICTION	TIMESTAMP	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	LENGTH	TTL	OFFSET	DF	MF
7660d8e5-b82b-4c3e-8009-e7e6a0484e46	Attack	2023-10-13 19:32:58.246658	27.213.11.100	37586	192.168.40.130	21	160	64	0	0	0
4c334e9d-475e-443c-ac40-18a6e004ff15	Attack	2023-10-13 19:32:58.246677	192.168.40.130	21	27.213.11.100	37586	40	64	0	1	0
bea815f7-e82f-4d7e-8407-c837381adaec	Attack	2023-10-13 19:32:58.246716	83.155.96.36	37587	192.168.40.130	21	160	64	0	0	0
7add2ed-276c-41d9-8630-3f3f7a8a4884	Attack	2023-10-13 19:32:58.246727	192.168.40.130	21	83.155.96.36	37587	40	64	0	1	0
bd5e1398-280a-424c-9952-812e94836c67	Attack	2023-10-13 19:32:58.246745	206.43.10.44	37588	192.168.40.130	21	160	64	0	0	0
ea7c5412-bd8d-4b42-b69f-40d1145afd86	Attack	2023-10-13 19:32:58.246752	192.168.40.130	21	206.43.10.44	37588	40	64	0	1	0



THANK YOU!