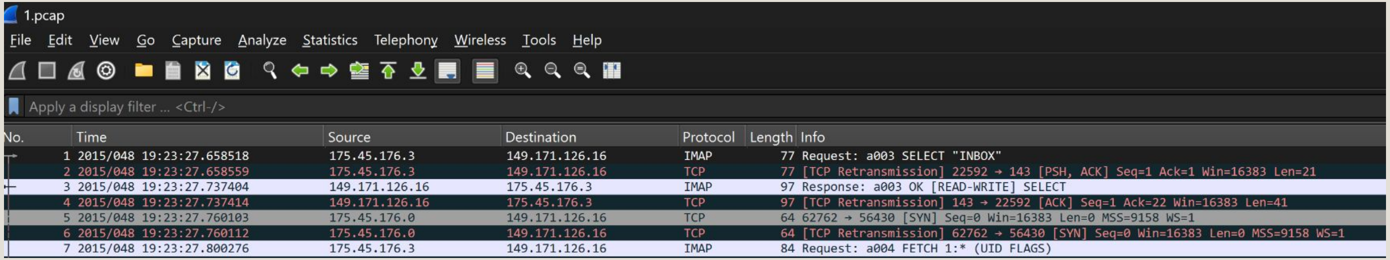
# Cyber Range Network Classification

By: Donovan, Roberto, Ashley, Will

# Chosen Dataset

- UNSW-NB15 Dataset
    - Raw network packets from Cyber Range Lab of UNSW Canberra
    - Nine malicious classes as well as benign
- We will be looking into the raw PCAP files for these attacks




| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 2015/048 19:23:27.658518 | 175.45.176.3 | 149.171.126.16 | IMAP | 77 | Request: a003 SELECT "INBOX" |
| 2 | 2015/048 19:23:27.658559 | 175.45.176.3 | 149.171.126.16 | TCP | 77 | [TCP Retransmission] 22592 → 143 [PSH, ACK] Seq=1 Ack=1 Win=16383 Len=21 |
| 3 | 2015/048 19:23:27.737404 | 149.171.126.16 | 175.45.176.3 | IMAP | 97 | Response: a003 OK [READ-WRITE] SELECT |
| 4 | 2015/048 19:23:27.737414 | 149.171.126.16 | 175.45.176.3 | TCP | 97 | [TCP Retransmission] 143 → 22592 [ACK] Seq=1 Ack=22 Win=16383 Len=41 |
| 5 | 2015/048 19:23:27.760103 | 175.45.176.0 | 149.171.126.16 | TCP | 64 | 62762 → 56430 [SYN] Seq=0 Win=16383 Len=0 MSS=9158 WS=1 |
| 6 | 2015/048 19:23:27.760112 | 175.45.176.0 | 149.171.126.16 | TCP | 64 | [TCP Retransmission] 62762 → 56430 [SYN] Seq=0 Win=16383 Len=0 MSS=9158 WS=1 |
| 7 | 2015/048 19:23:27.800276 | 175.45.176.3 | 149.171.126.16 | IMAP | 84 | Request: a004 FETCH 1:* (UID FLAGS) |

# Our Project Idea

- Use the 80 PCAP files to train a ML model that detects malicious or benign traffic
  - Fuzzers
  - Backdoors
  - DoS
  - Exploits
  - Reconnaissance
  - Shellcode
  - Worms
  - Analysis
  - Generic

# Extracting Information

- Utilized PCAP reader from Scapy
- Traverse .pcap files looking at features
- Each feature is unique based on protocol
- Created a csv file with unique mappings per packet identifying features

```
Internet Protocol Version 4, Src: 175.45.176.3, Dst: 149.171.126.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0xc47d (50301)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
```

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| srcip | sport | dstip | dsport | proto | state | dur | sbytes | dbytes | sttl | dttl | sloss | dloss | service | Sload | Dload | Spkts | Dpkts | swin | dwin | stcpb |
| 10.40.85.1 | 0 | 224.0.0.5 | 0 | 89 | 0 | 290.0253 | 2400 | 0 | 1 | 0 | 0 | 0 | - | 66.20111 | 0 | 30 | 0 | 0 | 0 | |
| 10.40.182. | 0 | 224.0.0.5 | 0 | 89 | 0 | 290.0253 | 2400 | 0 | 1 | 0 | 0 | 0 | - | 66.20112 | 0 | 30 | 0 | 0 | 0 | |
| 192.168.24 | 0 | 192.168.24 | 0 | ICMP | 0 | 280.0005 | 7440 | 0 | 64 | 0 | 0 | 0 | - | 212.5711 | 0 | 20 | 0 | 0 | 0 | |
| 0 | 0 | 0 | 0 | NONIP | 0 | 256.1389 | 4542 | 0 | 0 | 0 | 0 | 0 | - | 141.8605 | 0 | 84 | 0 | 0 | 0 | |
| 175.45.176 | 13284 | 149.171.12 | 80 | TCP | A | 2.39039 | 1586 | 364 | 255 | 253 | 0 | 0 | http | 5307.921 | 1218.211 | 14 | 6 | 16383 | 16383 | 3.9E |
| 59.166.0.5 | 3593 | 149.171.12 | 53 | UDP | 0 | 0.001209 | 164 | 196 | 32 | 30 | 0 | 0 | dns | 1085176 | 1296918 | 2 | 2 | 0 | 0 | |
| 59.166.0.3 | 49664 | 149.171.12 | 53 | UDP | 0 | 0.001169 | 178 | 210 | 32 | 30 | 0 | 0 | dns | 1218170 | 1437167 | 2 | 2 | 0 | 0 | |
| 59.166.0.5 | 6645 | 149.171.12 | 80 | TCP | A | 29.26807 | 1180 | 984 | 32 | 30 | 0 | 0 | http | 322.5358 | 268.9621 | 8 | 10 | 5792 | 5792 | 1.91E |
| 59.166.0.3 | 42587 | 149.171.12 | 25 | TCP | A | 34.07718 | 38190 | 4052 | 32 | 30 | 0 | 0 | smtp | 8965.531 | 951.2525 | 52 | 42 | 5792 | 5792 | 4.06E |

# Data Cleaning And Labeling

- Cleaned the uncleaned csv of all PCAPs
- Added in features that require multiple packet analysis
- Used certain features to gather more information for the cleaned csv
- Used ground truth labels for malware vs. benign to label our data
    - Malicious types out of the 9
    - Benign

```
srcip,sport,dstip,dsport,proto,state,dur,sbytes,dbytes,sttl,dttl,sloss,dloss,service,Sload,Dload,Spkts,Dpkts,swin,dwin,stcpb,dtcpb,smeansz,dmeansz,trans_depth,res_b
10.40.85.1,0,224.0.0.5,0,89,0,0,80,0,1,0,0,0,0,0,0,1,0,0,0,0,0,80.0,0,0,44,0,0,1421927376.907079,1421927376.907079,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0
10.40.182.1,0,224.0.0.5,0,89,0,0,80,0,1,0,0,0,0,0,0,1,0,0,0,0,0,80.0,0,0,44,0,0,1421927376.907101,1421927376.907101,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0
192.168.241.243,0,192.168.241.243,0,ICMP,0,0,372,0,64,0,0,0,0,0,0,1,0,0,0,0,0,372.0,0,0,0,0,0,1421927381.000961,1421927381.000961,0,0,0,0,0,1,3,0,0,0,0,0,0,0,0,0,
```

# Random Forest

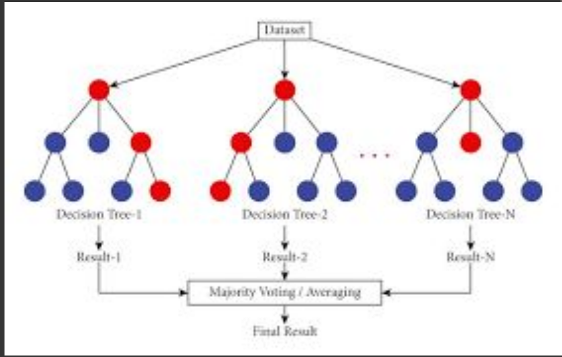
A machine learning algorithm that combines many individual decision trees to make more accurate and stable predictions

Pros:

- Handles large feature sets
- Robust to noise
- Easy to train

Why We Chose It:

- Excellent baseline
- Can classify multiclass problems



# Random Forest Results

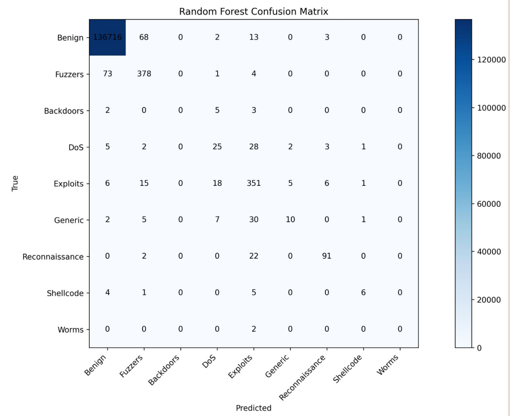
- Correctly counted all attacks for each category
- Consistently obtained a 99.74% accuracy
- Confusion matrix has a strong diagonal showing it should have a good accuracy
- Data imbalance
  - Benign has much higher accuracy
  - Malicious categories have low accuracy
- Will continue to work on and update code

```
Attack category counts after normalization:
 attack_cat
Benign            684009
Fuzzers             2282
Exploits            2009
Reconnaissance       573
DoS                  328
Generic              274
Shellcode             80
Backdoors             49
Worms                 12
Name: count, dtype: int64
Accuracy: 0.9974841216902062
```

```
Classification Report:
                precision    recall  f1-score   support

        Benign       1.00      1.00      1.00    136802
       Fuzzers       0.80      0.83      0.82       456
     Backdoors       0.00      0.00      0.00        10
           DoS       0.43      0.38      0.40        66
      Exploits       0.77      0.87      0.82       402
       Generic       0.59      0.18      0.28        55
Reconnaissance       0.88      0.79      0.83       115
     Shellcode       0.67      0.38      0.48        16
         Worms       0.00      0.00      0.00         2

      accuracy                           1.00    137924
     macro avg       0.57      0.49      0.51    137924
  weighted avg       1.00      1.00      1.00    137924
```



# XGBoost

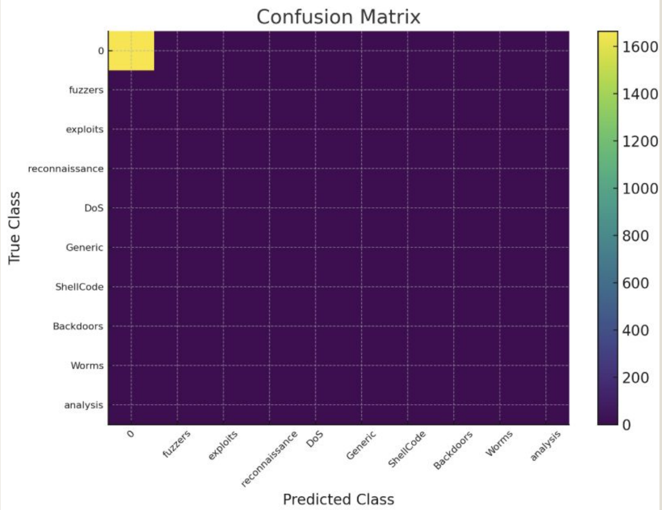
An optimized and efficient machine learning algorithm that builds predictions by combining many simple decision trees in a sequential process

- Pros:
    - Simple to train
    - Higher accuracy than Random Forest
    - Considered one of best current models

- Why We Chose It:
    - Very effective with extremely large datasets
    - Learns well with Little instruction

# XGBoost Results

- Overall accuracy came out to nearly 100% on overall data
- Confusion matrix shows extreme bias towards benign due to focus on minimized error
- Best results for fuzzers and reconnaissance
- Next Steps:
    - Hyperparameter tuning, SMOTE

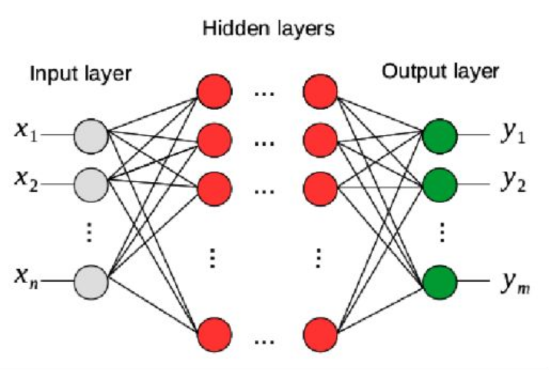



| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Fuzzers | 0.95 | 0.99 | 0.97 | 571 |
| Backdoors | 0.00 | 0.00 | 0.00 | 12 |
| Benign | 1.00 | 1.00 | 1.00 | 171002 |
| DoS | 0.32 | 0.28 | 0.30 | 82 |
| Exploits | 0.77 | 0.88 | 0.83 | 502 |
| Generic | 0.67 | 0.20 | 0.31 | 69 |
| Reconnaissance | 0.92 | 0.80 | 0.85 | 143 |
| Shellcode | 0.60 | 0.45 | 0.51 | 20 |
| Worms | 0.00 | 0.00 | 0.00 | 3 |
| accuracy | | | 1.00 | 172404 |
| macro avg | 0.58 | 0.51 | 0.53 | 172404 |
| weighted avg | 1.00 | 1.00 | 1.00 | 172404 |

# Deep Feedforward Neural Network

Neural network where data flows in only one direction, from the input layer through multiple hidden layers to the output layer, without any loops or feedback.

- Pros:
  - Learns complex patterns
  - Handles many classes well
  - Performs well with large datasets
  - Automatically learns feature interactions
  - Higher accuracy than shallow networks
- Why We Chose It:
  - Can learn more complex patterns in network traffic
    - Benign vs 9 types of malware



# Deep FeedForward Neural Network Results

- The overall accuracy of the Deep Feedforward Neural Network is 99.56%
  - Its highest precision attack category is currently benign
  - Analysis, backdoor, and worms all have a 0% accuracy because they did not show up in the validation split
- The Confusion Matrix has a pretty strong diagonal showing that it should have an overall decent accuracy
- We will continue to work on the model before using the testing split

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Benign | 0.9978 | 0.9993 | 0.9985 | 136802 |
| Fuzzers | 0.6623 | 0.4386 | 0.5277 | 456 |
| Analysis | 0.0000 | 0.0000 | 0.0000 | 0 |
| Backdoors | 0.0000 | 0.0000 | 0.0000 | 10 |
| DoS | 0.4118 | 0.3182 | 0.3590 | 66 |
| Exploits | 0.7171 | 0.8259 | 0.7676 | 402 |
| Generic | 0.2500 | 0.0727 | 0.1127 | 55 |
| Recon | 0.6667 | 0.4348 | 0.5263 | 115 |
| Shellcode | 0.4000 | 0.3750 | 0.3871 | 16 |
| Worms | 0.0000 | 0.0000 | 0.0000 | 2 |
| accuracy | | | 0.9956 | 137924 |
| macro avg | 0.4106 | 0.3464 | 0.3679 | 137924 |
| weighted avg | 0.9949 | 0.9956 | 0.9951 | 137924 |

```
====== CONFUSION MATRIX ======
[[136703     66      0      0     22      1      9      1      0]
 [   232    200      0      1     11      2     10      0      0]
 [     0      1      0      5      4      0      0      0      0]
 [     4      2      0     21     34      4      1      0      0]
 [    15     23      0     18    332      5      3      6      0]
 [     4      5      0      6     33      4      1      2      0]
 [    39      5      0      0     21      0     50      0      0]
 [     5      0      0      0      4      0      1      6      0]
 [     0      0      0      0      2      0      0      0      0]]
```

# Our ML Selection

- Continue to work on and update our code for each ML model
- Based on classification reports from each model
  - Select the best option for our project
- Our prediction:
  - XGBoost
    - Based on researching and comparing all three models

# Thank you!
# Questions?