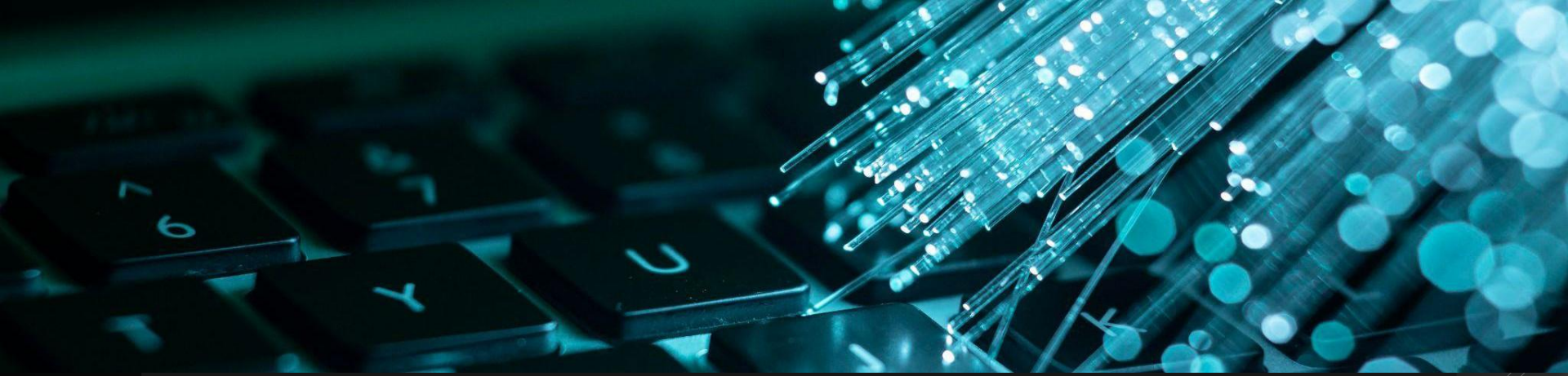


Técnicas de Perceção de Redes DNS Tunneling

João Viegas - 98372
Tiago Marques - 98459

Janeiro 2023 | 2nd Presentation

The Problem

DNS Tunneling presents a serious threat to business and security as a whole:

1. Is a very flexible attack, can be used for C&C, exfiltration and others

2. Is hard to be detected because of the DNS protocol nature

Our focus

- We will monitor the network traffic patterns of known good users to understand how they behave.
- Using that behaviour we will try to establish a profile.
- Based on that profile we will try to distinguish the normal traffic from anomalous traffic

Used Datasets

Not malicious Source

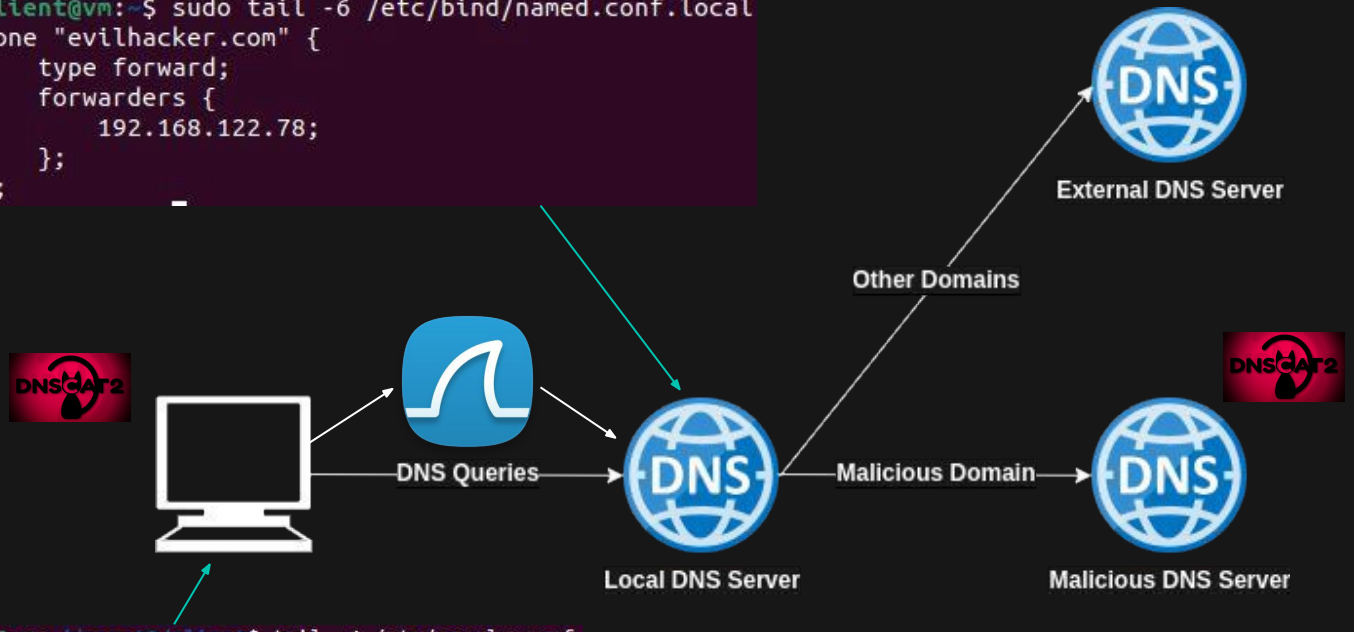
The non-malicious datasets should be obtained from an IEEE dataset w/10 days of DNS traffic put it has some heird communications.

Malicious Source

Our malicious dataset will be generated in-house through the use of virtualization (VMs), DNScat2 (DNS Tunneling Software) and bind9(DNS software).

Test Scenario

```
client@vm:~$ sudo tail -6 /etc/bind/named.conf.local
zone "evilhacker.com" {
    type forward;
    forwarders {
        192.168.122.78;
    };
};
```




```
client@vm:~/dnscat2/client$ tail -4 /etc/resolv.conf
nameserver 192.168.122.58
nameserver 127.0.0.53
options edns0 trust-ad
search .
```

General approach of our attack

1 º - Attacker establishes a DNS connection with a client.

2 º - Attacker opens a shell session through DNS

3 º - Commands like pwd, ls, cat, echo are made to search, read and modify files in the client.

4 º - A selected file is exfiltrated.

Our Types of Attacks

Our attackers used DNS tunneling to send commands via DNS.

- Attack 1 uses DNS tunneling with 3 seconds delay.
- Attack 2 uses DNS tunneling with 3 seconds steady delay.
- Attack 3 uses DNS tunneling with 5 seconds delay.
- Attack 4 uses DNS tunneling with 5 seconds steady delay.

Delay -> Maximum delay between packets

Steady -> The system consistently waits for the specified delay before transmitting the next message

Data Processing

- Collect raw packet data with a sampling period of 5 and 10 seconds.
- Filter data to allow only DNS or Secure DNS packets.
- Detect anomalous user behaviour

- Observation Windows :
  - Size of and 10 minutes
  - Sliding 1 every minute

Extracted Metrics

- To extract these metrics a custom application was written using python and pyshark library

- Metrics:
  - Number of DNS Query packets
  - Number of upload bytes
  - Number of DNS Reply Packets
  - Number of upload bytes
  - Sum time between a DNS Reply and the last DNS Query packet
  - Sum time between two sequential DNS Query packets
  - Sum time between two sequential DNS packets
  - Min time between two sequential DNS packets
  - Max time between two sequential DNS packets

Extracted Features

- To extract these metrics a custom application was written using python and numpy library

- Number of DNS Query / DNS Reply packets:
  - Mean, Median, Standard Deviation, Variance

- Ratio Upload Bytes/DNS Query and Download Bytes/DNS Reply:
  - Mean, Median, Standard Deviation, Variance

Extracted Features

- Sum of time between DNS response time / DNS Queries / DNS Packets:
  - Mean, Median, Standard Deviation, Variance
- Min/Max Time between DNS Packets:
  - Mean, Median, Standard Deviation, Variance
- Periodicity:
  - Time between DNS Queries
  - Min time between DNS packets
  - Max time between DNS packets
- Covariance:
  - DNS Query and Upload bytes
  - Min and Max time between DNS packets

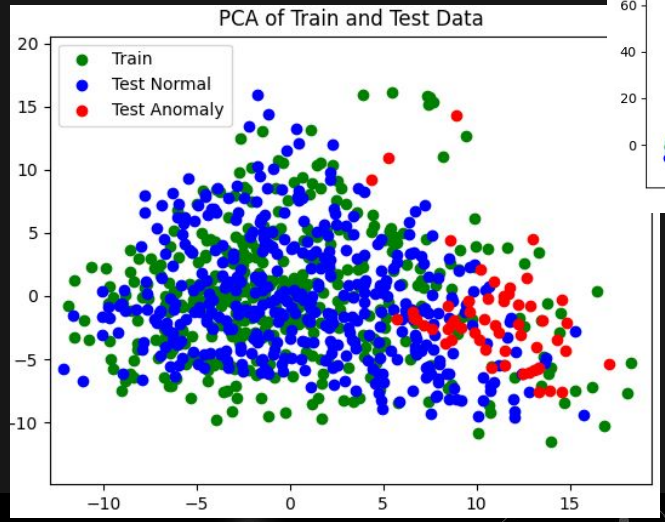
Features Processing

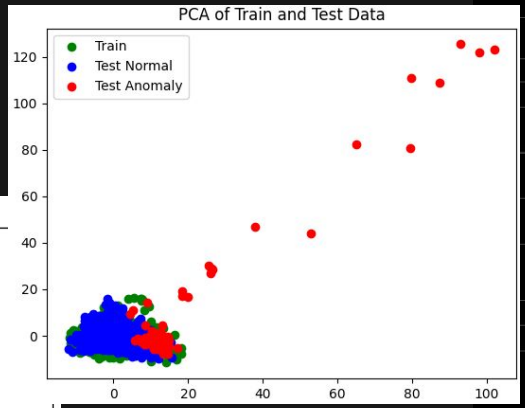
- Features are split into 2 dataset
  - Training, containing 50% of all normal features
  - Testing, containing the other 50% of all normal features and all anomaly features
- The data is scaled using a standard scaler
  - Fitted on the training data
  - It is recommended for support vector machines
- PCA is performed to reduce the number of features

DNS Attack 1

Through DNS this attacker sends responses with injected sh commands with steady non active for 3 seconds.

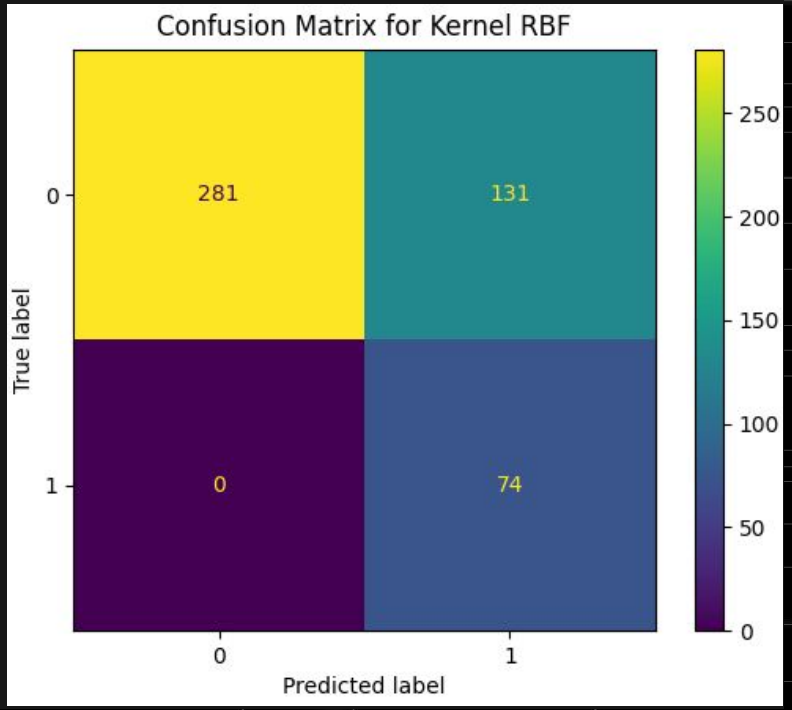
- Window size : 10 minutes
- Sliding window every : 1 minute
- Sampling period : 5 seconds





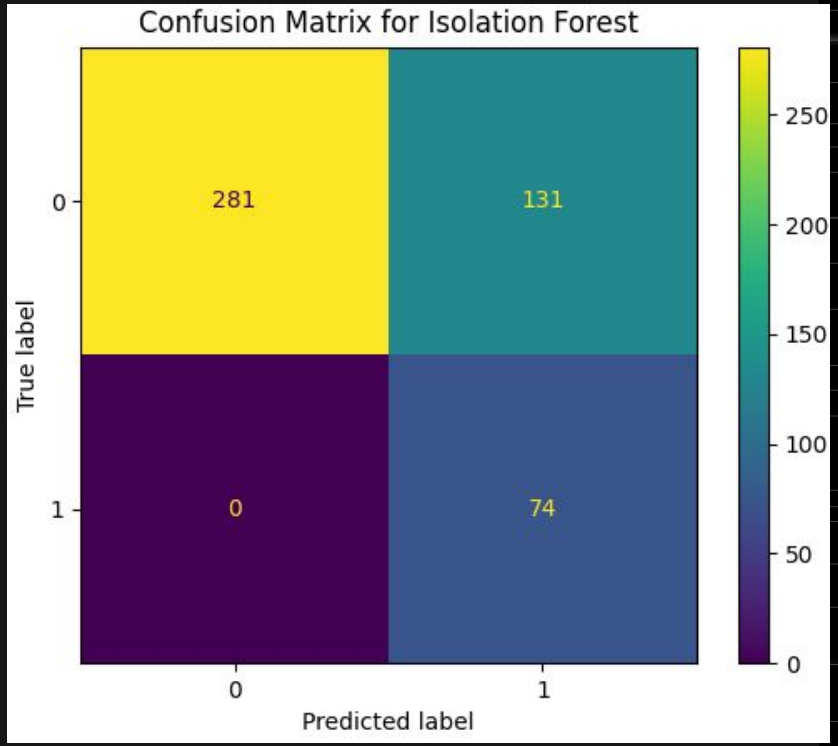
DNS Attack 1 - RBF results

- Accuracy: 73.04%
- Precision: 36.09%
- Recall: 100%
- F-1: 53.04%



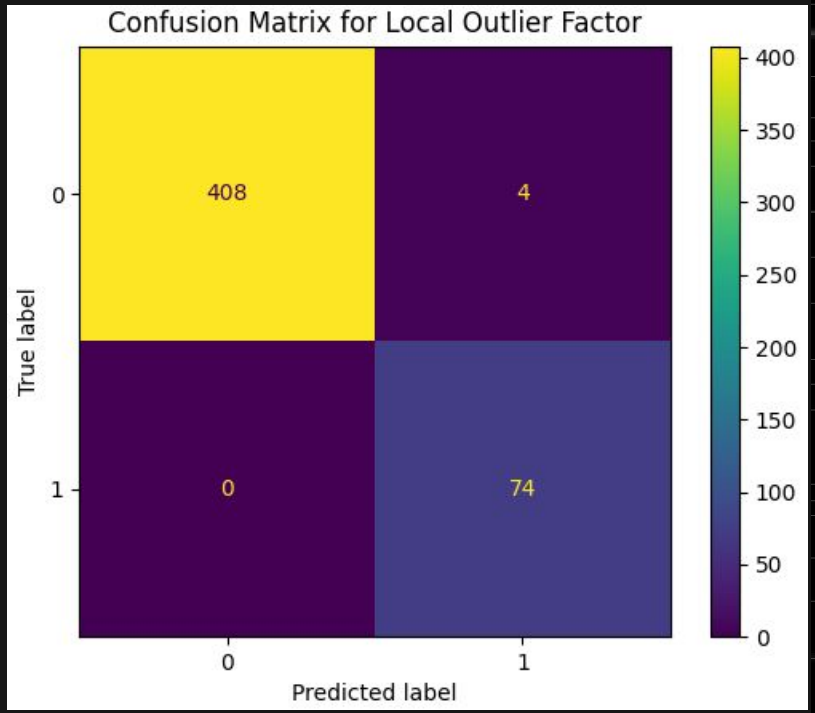
DNS Attack 1 - Isolation Forest results

- Accuracy: 73.04%
- Precision: 36.09%
- Recall: 100%
- F-1: 53.04%

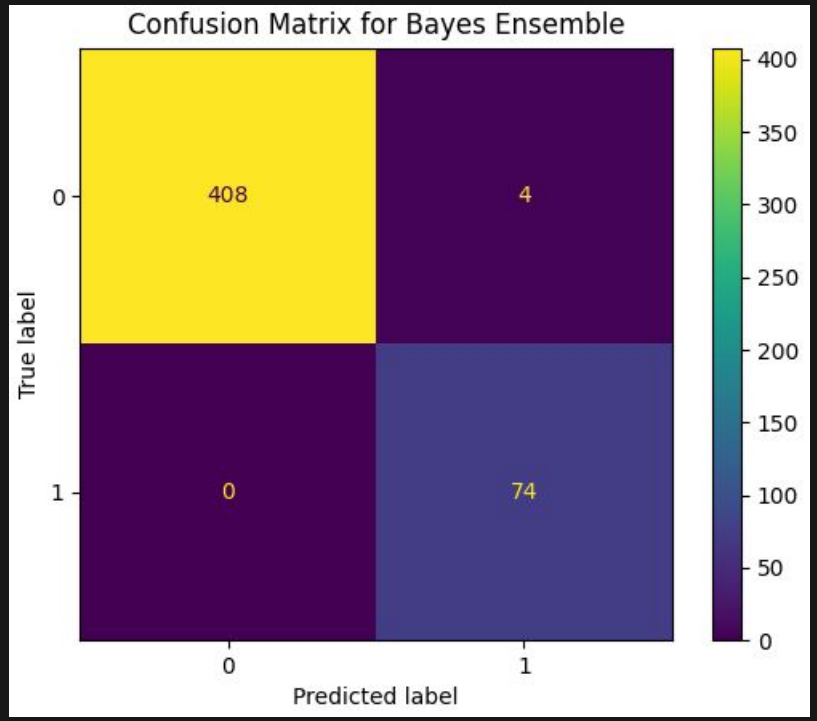


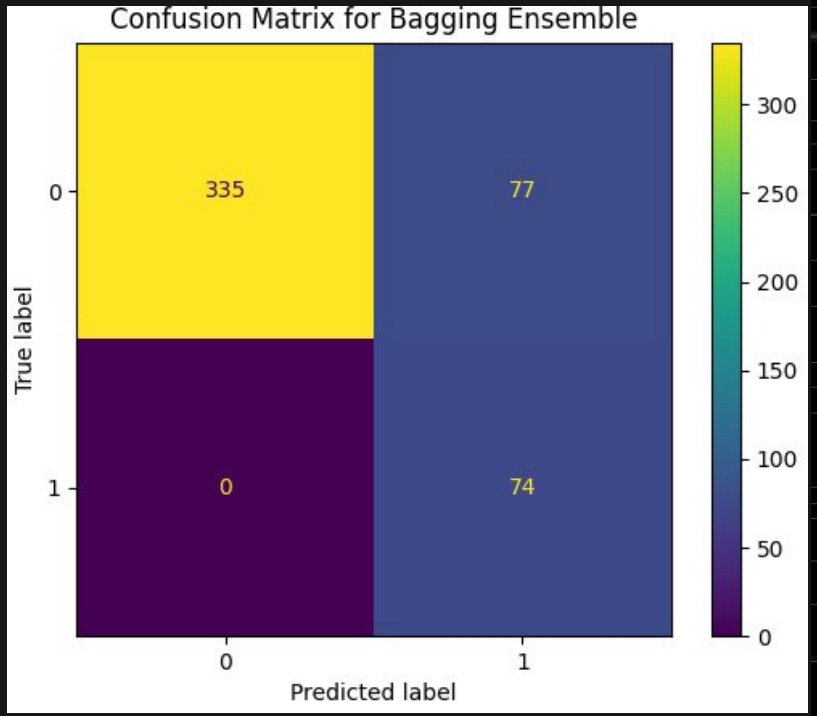
DNS Attack 1 - LocalOutlierFactor results

- Accuracy: 99.17%
- Precision: 94.87%
- Recall: 100%
- F-1: 97.36%



DNS Attack 1 - Ensemble

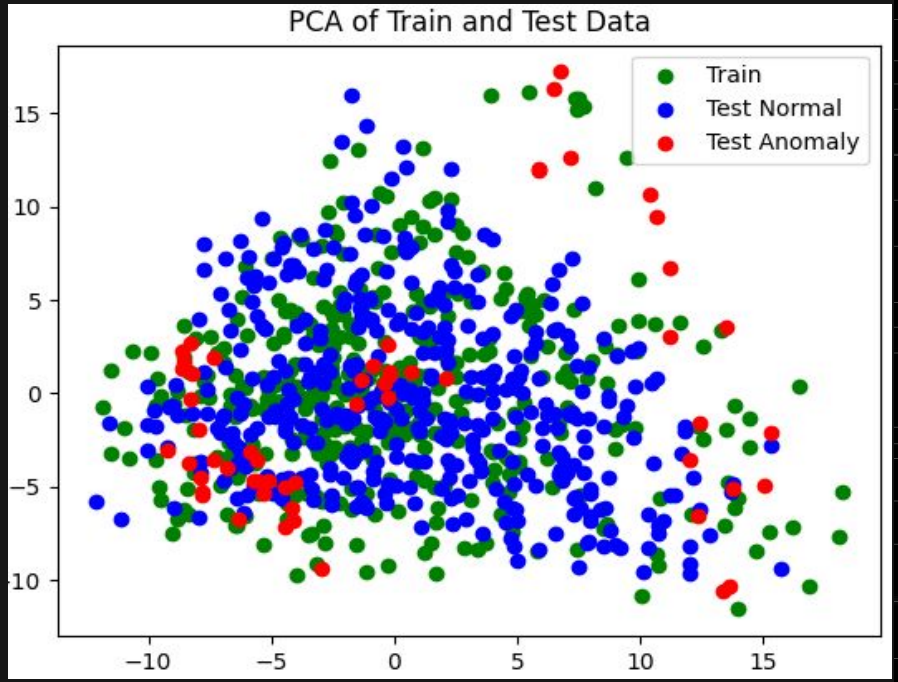




DNS Attack 2

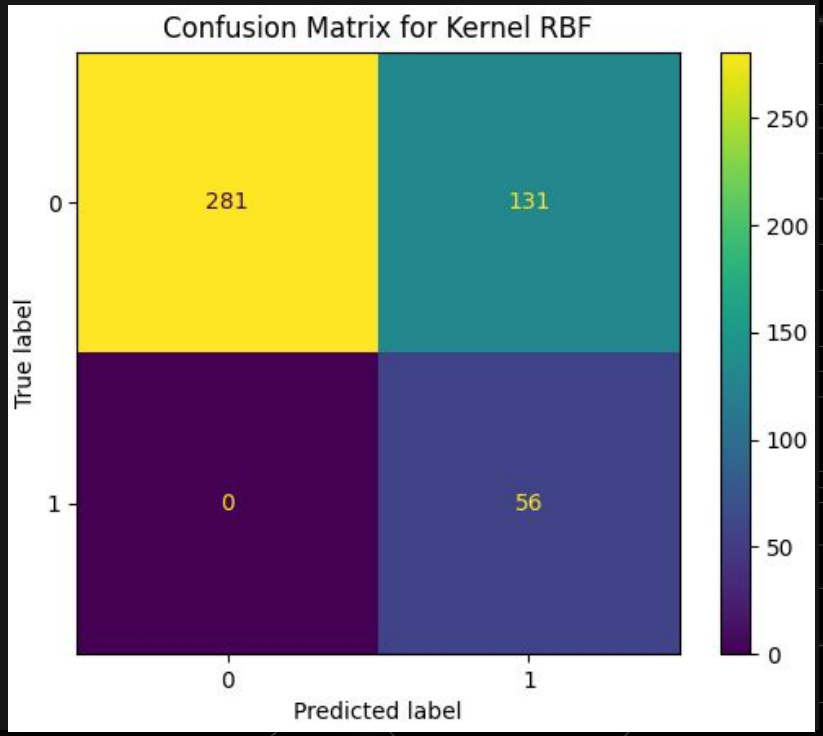
Through DNS this attacker sends responses with injected sh commands with steady active for 3 seconds.

- Window size : 10 minutes
- Sliding window every : 1 minute
- Sampling period : 5 seconds



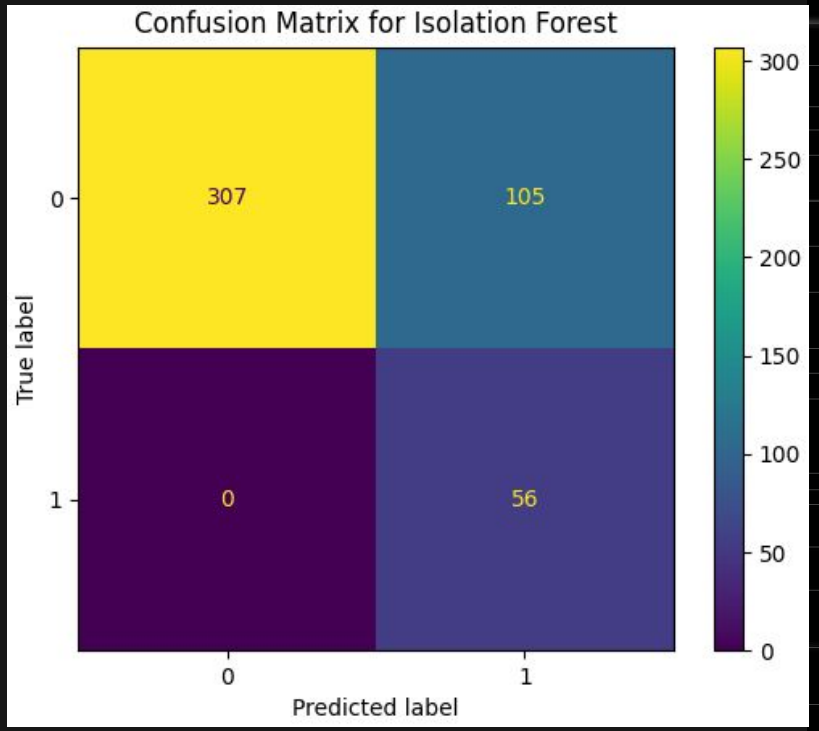
DNS Attack 2 - RBF results

- Accuracy: 72.00%
- Precision: 29.94%
- Recall: 100%
- F-1: 46.09%



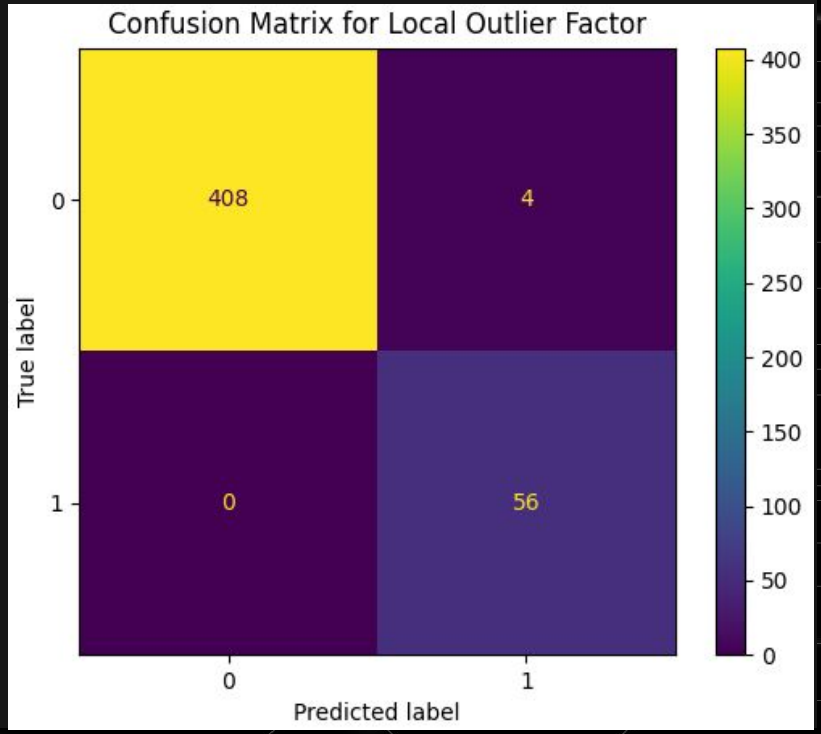
DNS Attack 2 - Isolation Forest results

- Accuracy: 77.56%
- Precision: 34.78%
- Recall: 100%
- F-1: 51.61%

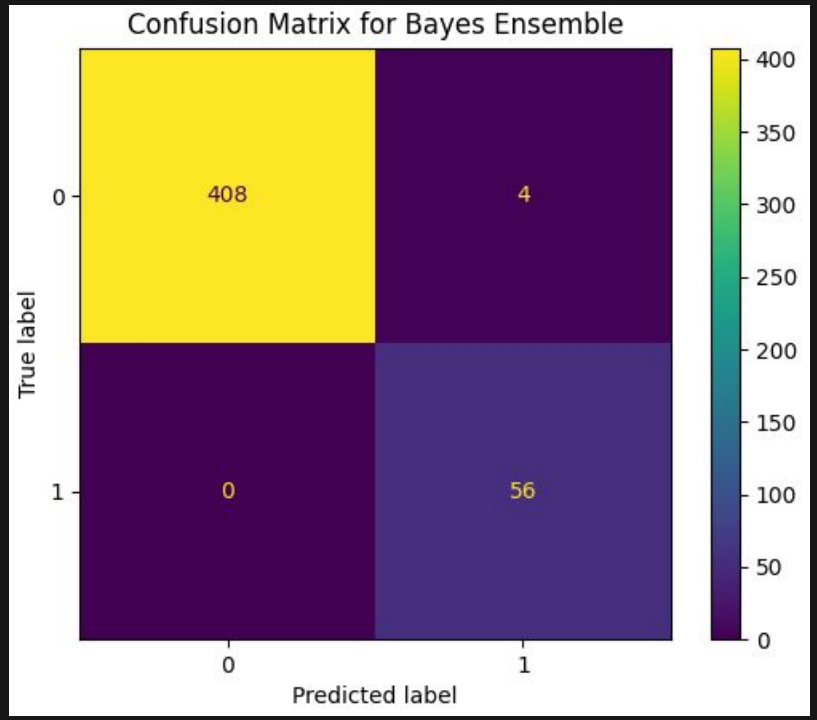


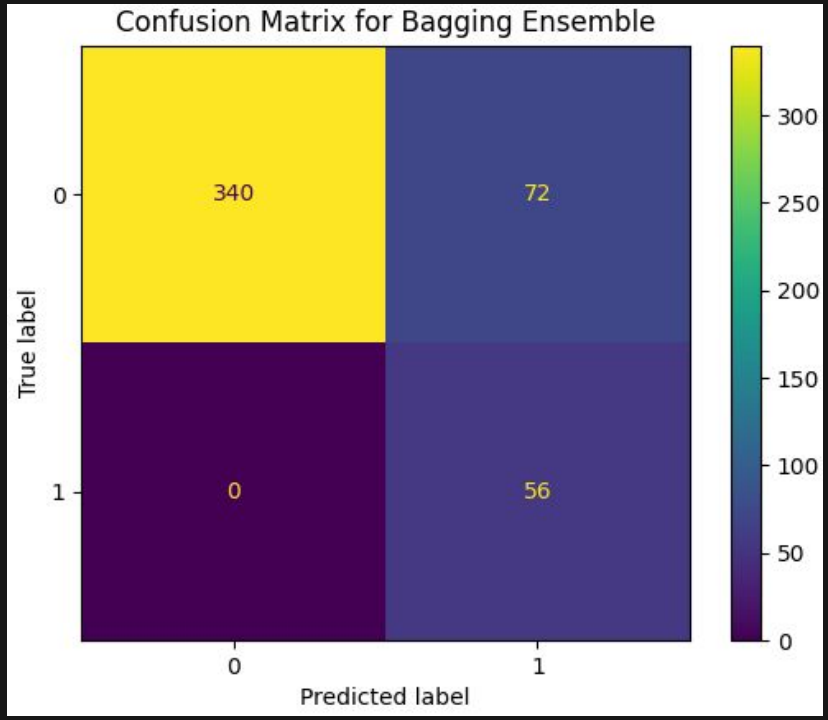
DNS Attack 2 - LocalOutlierFactor results

- Accuracy: 99.14%
- Precision: 93.33%
- Recall: 100%
- F-1: 96.55%



DNS Attack 2 - Ensemble

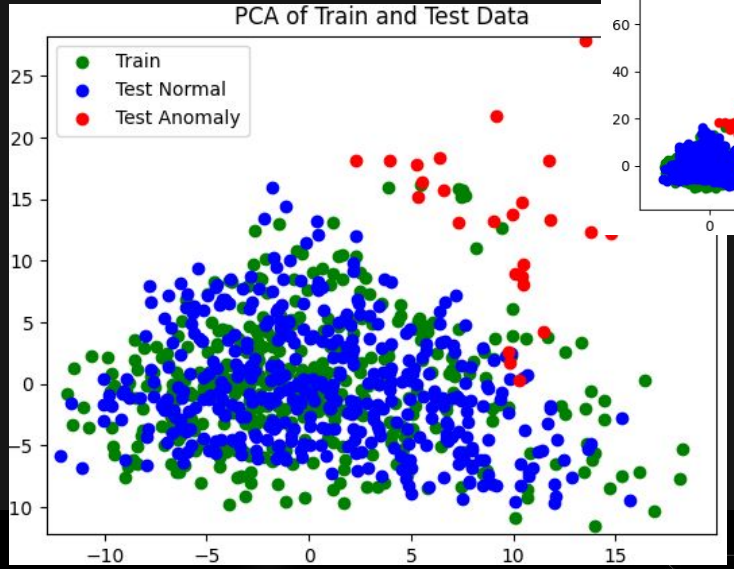


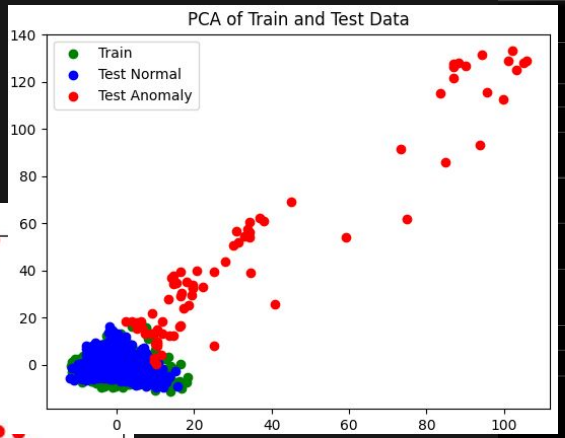


DNS Attack 3

Through DNS this attacker sends responses with injected sh commands with steady non active for 5 seconds.

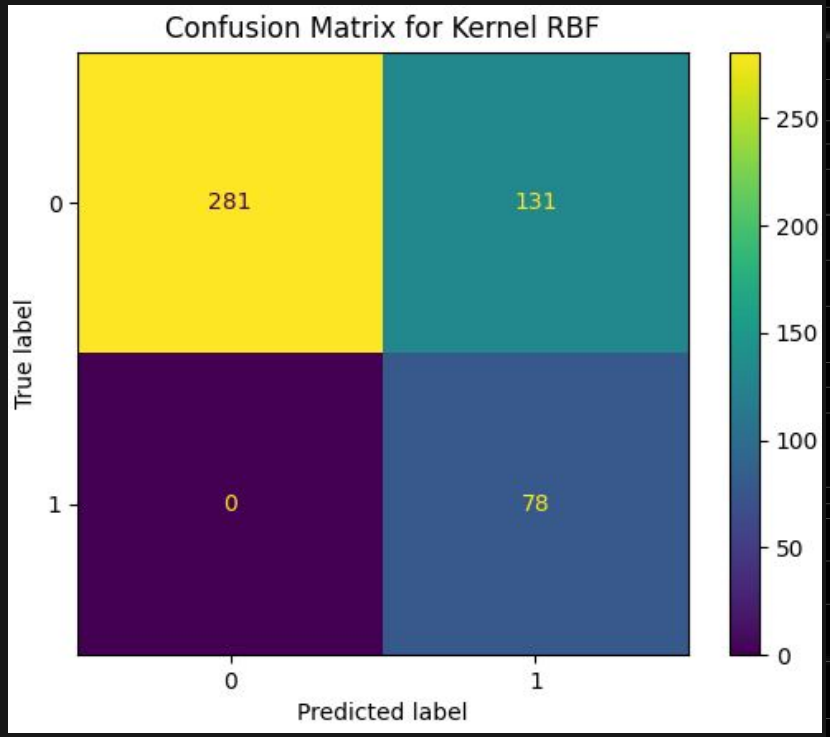
- Window size : 10 minutes
- Sliding window every : 1 minute
- Sampling period : 10 seconds





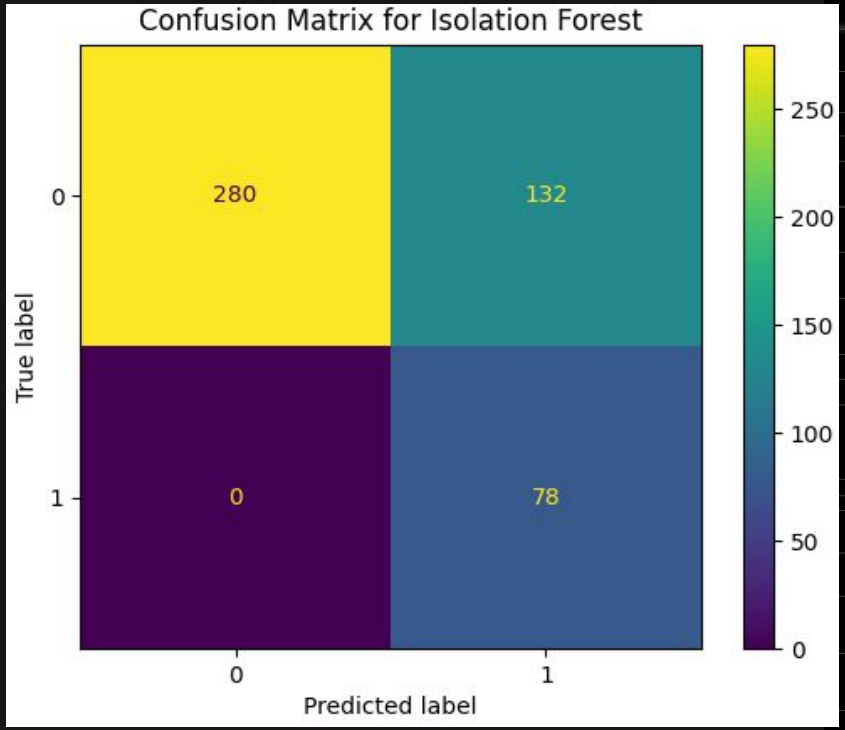
DNS Attack 3 - RBF results

- Accuracy: 73.26%
- Precision: 37.32%
- Recall: 100%
- F-1: 54.35%



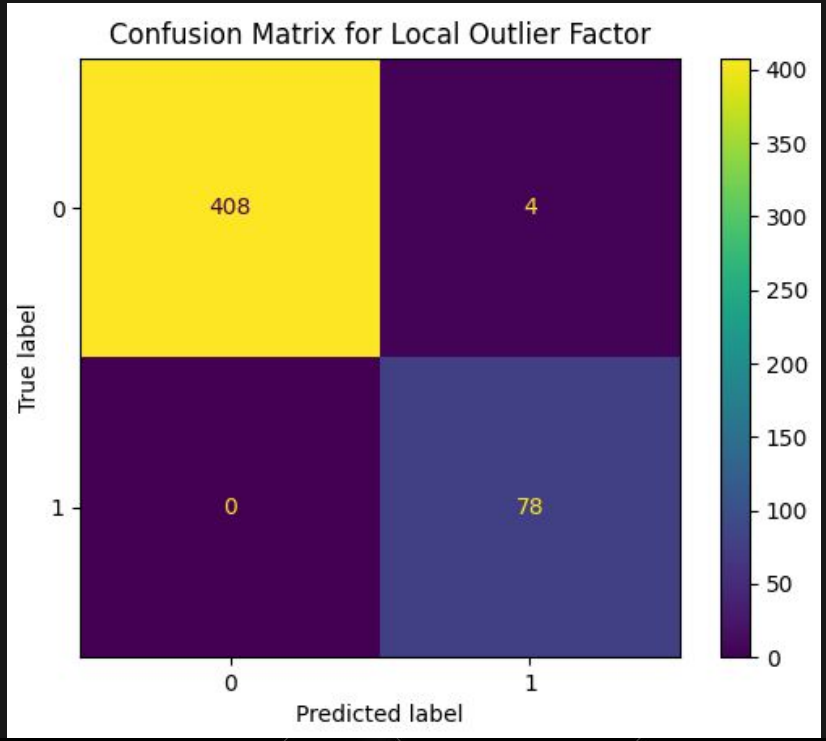
DNS Attack 3 - Isolation Forest results

- Accuracy: 73.06%
- Precision: 37.14%
- Recall: 100%
- F-1: 54.16%

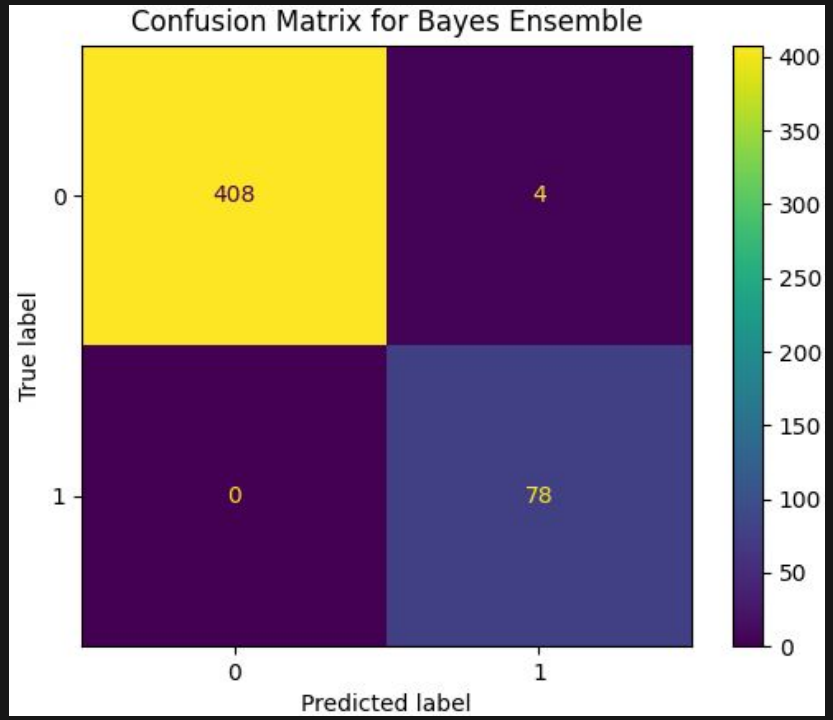


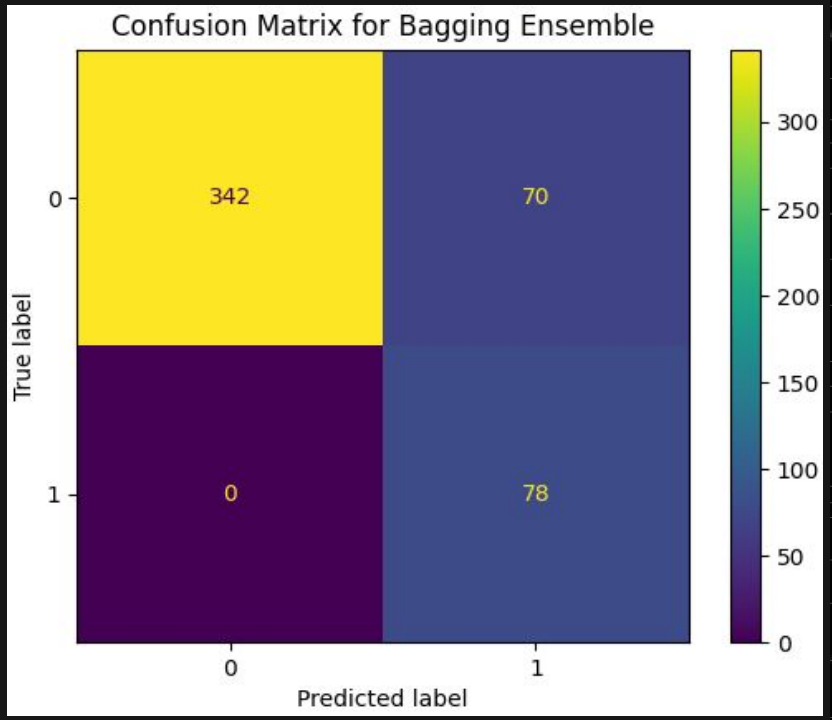
DNS Attack 3 - LocalOutlierFactor results

- Accuracy: 99,18%
- Precision: 95.12%
- Recall: 100%
- F-1: 97.50%



DNS Attack 3 - Ensemble

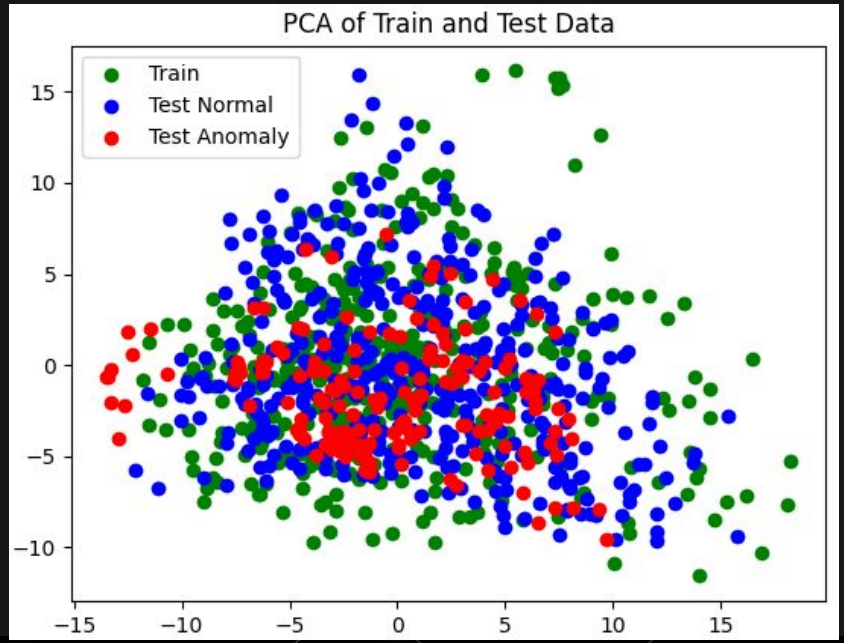




DNS Attack 4

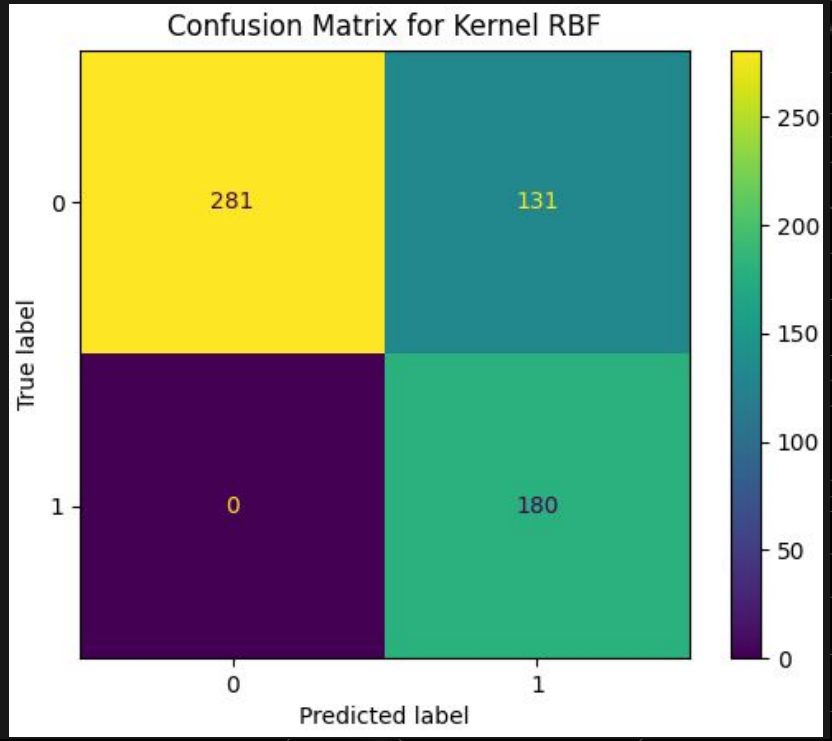
Through DNS this attacker sends responses with injected sh commands with steady non active for 5 seconds.

- Window size : 10 minutes
- Sliding window every : 1 minute
- Sampling period : 10 seconds



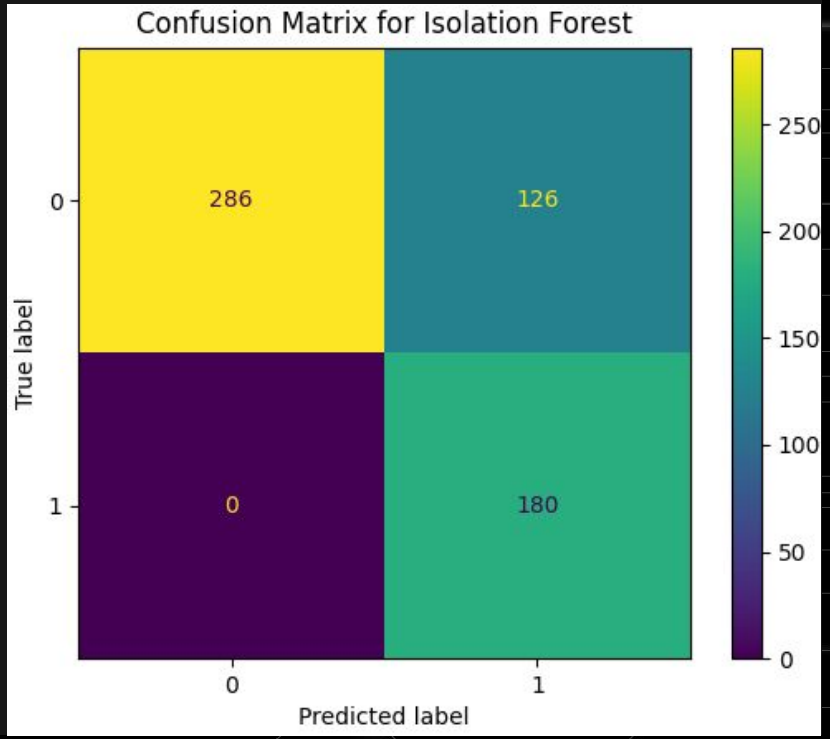
DNS Attack 4 - RBF results

- Accuracy: 77.87%
- Precision: 57.87%
- Recall: 100%
- F-1: 73.31%



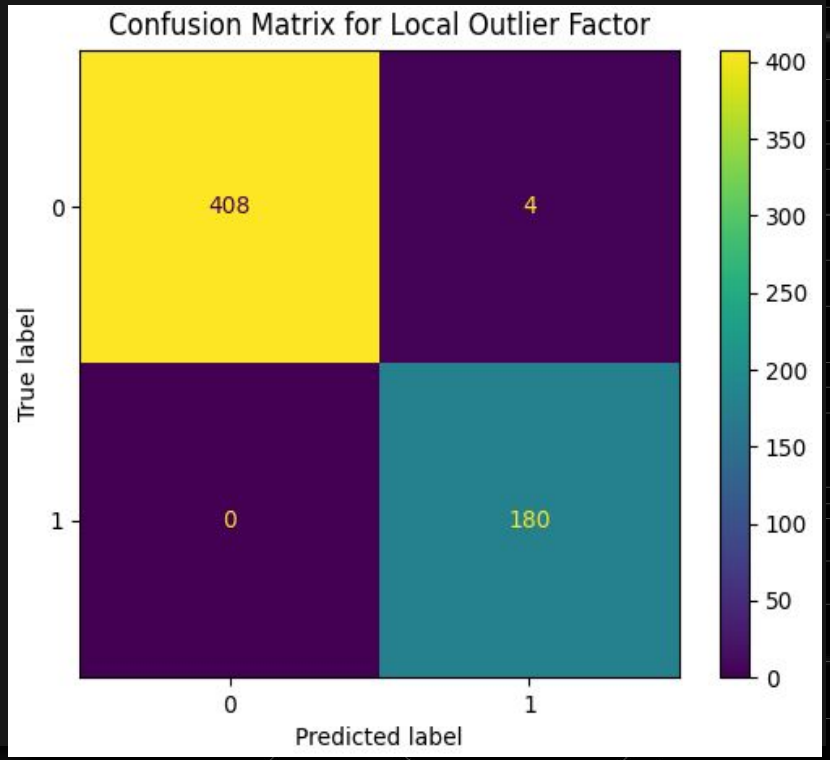
DNS Attack 4 - Isolation Forest results

- Accuracy: 78.71%
- Precision: 58.82%
- Recall: 100%
- F-1: 74.07%

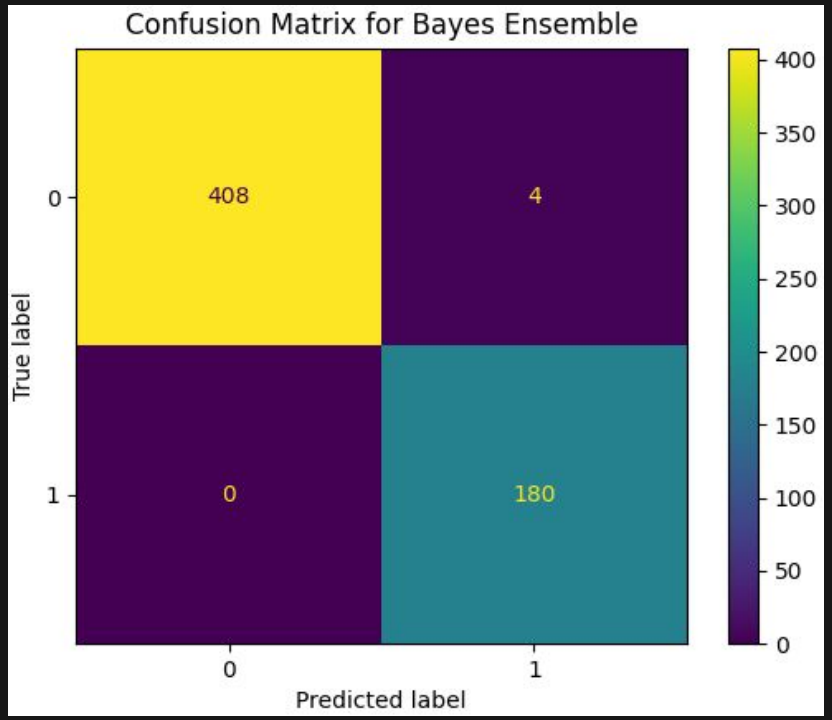


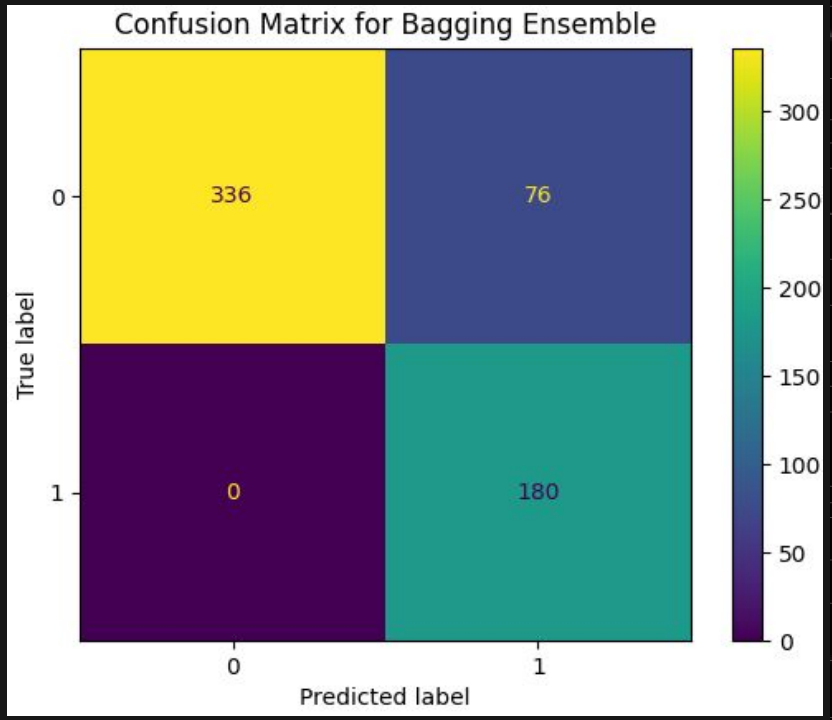
DNS Attack 4 - LocalOutlierFactor results

- Accuracy: 99.32%
- Precision: 97.82%
- Recall: 100%
- F-1: 98.90%



DNS Attack 4 - Ensemble





Any
questions?

References

https://ieee-dataport.org/documents/ti-2016-dns-dataset
https://scikit-learn.org/stable/modules/classes.html
https://github.com/KimiNewt/pyshark
https://numpy.org/doc/stable/reference/index.html#reference

https://github.com/Tiagura/TPR_Project -> project code