TÉCNICAS DE PERCEPÇÃO DE REDES

Project Problem Presentation

Nuno Ferreira 121758
Patricia Cardoso 103243

APPLICATION LAYER DDOS ATTACK

It is designed to target the “top” layer in the OSI model where HTTP requests occur.

Overwhelms specific features of a website or app to disable them, preventing the application from delivering content to users.

They often target specific functions, such as login that require more processing power than static pages.

Challenge of L7 Attack for Traditional Solutions

01

Mimic legitimate traffic, making detection difficult

Layer 7 attacks, are designed to replicate normal user behavior

02

Low Traffic Volume

Unlike volumetric attacks that generate high traffic, Layer 7 attacks can be executed with a small number of requests

03

Limited Detection Capabilities

Many firewalls, IPS focus on network layer threats and are not equipped to analyze the content and context of application layer traffic

REAL WORLD SCENARIO - DATA ACQUISITION

Centralized Log Collection Using Syslog

Using a centralized logging server like Syslog allows real time collection and management of logs from multiple sources in one location

TEST SCENARIO - DATA ACQUISITION

- Apache2 Web Server Logs

```
185.16.38.232 - - [07/Nov/2024:12:21:12 +0000] "GET /cgi-bin/luci/;stok=/locale HTTP/1.1" 404 436 "-" "-"
185.191.126.248 - - [07/Nov/2024:12:24:13 +0000] "GET / HTTP/1.1" 200 1925 "-" "-"
172.18.0.3 - - [07/Nov/2024:12:34:18 +0000] "GET / HTTP/1.1" 200 1012 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 17_6_1 like Mac OS X
) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.6 Mobile/15E148 Safari/604.1"
172.18.0.3 - - [07/Nov/2024:12:34:20 +0000] "GET /favicon.ico HTTP/1.1" 404 445 "https://webapp.nunonetwork.com/" "Mozilla/5.0 (iP
hone; CPU iPhone OS 17_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.6 Mobile/15E148 Safari/604.1"
179.43.191.98 - - [07/Nov/2024:12:39:09 +0000] "GET / HTTP/1.1" 200 1925 "-" "-"
154.216.16.110 - - [07/Nov/2024:12:53:07 +0000] "GET /phpmyadmin/index.php HTTP/1.1" 404 455 "-" "Mozilla/5.0 (X11; Linux i686) Ap
pleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/65.0.3325.181 Chrome/65.0.3325.181 Safari/537.36"
5.8.11.202 - - [07/Nov/2024:12:58:58 +0000] "\x16\x03\x02\x01o\x01" 400 483 "-" "-"
141.98.11.175 - - [07/Nov/2024:13:01:17 +0000] "POST /cgi-bin/hotspotlogin.cgi HTTP/1.1" 404 436 "-" "Mozilla/5.0 (Windows NT 10.0
; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36"
```

DATA PROCESSING (FEATURE EXTRACTION)

- **sourceAddress:** Identifies the user's IP within a time window.
- **requestTimes**: Counts user requests in a time window.
- **diffReqTimes**: Number of unique requests by the same user.
- **timesOfCode200**: Number of successful requests (HTTP 200 status)
- **totalLength**: Total bytes requested.
- **sessionDuration**: Time from the first to last request.Normal users spend more time per session (detect rapid requests) .
- **sequenceOfUrlLevel**: URL depth for each request.
- **sequenceOfRequestFrequency**: Request frequency across sub-windows.
- **sequenceOfRequestInterval**: Time between consecutive requests.

Time Windows

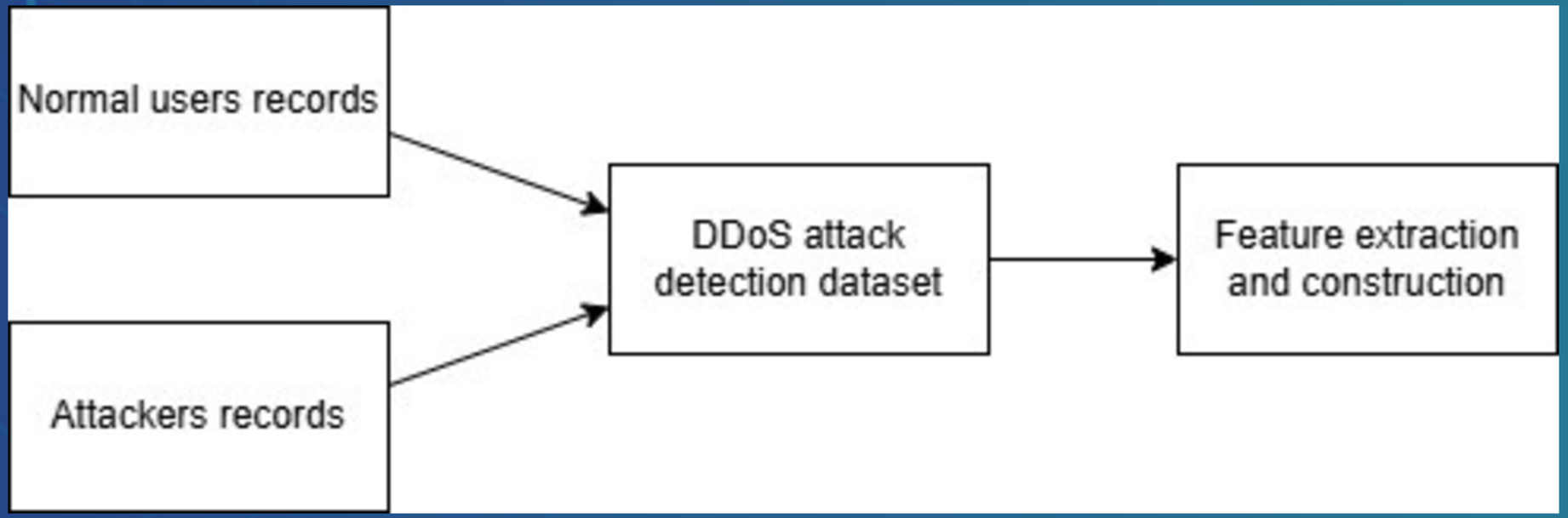
Set 20 minutes as a time window and 1 minute as a sub-time window

DATA PROCESSING (FEATURE CONSTRUCTION)

More complex features to distinguish better from malicious traffic

- **avgBytePerRequest**: Average bytes per request, helping to identify bandwidth usage.
- **status200Percent**: Percentage of successful requests, useful for evaluating how many requests returned with a 200 status code.
- **maxFrequency**: Maximum number of requests within a sub-window, useful for detecting suspicious activity spikes.
- **urlLevelRate**: Rate of variation in URL level, which reflects changes in navigation patterns.

DATASET CREATION AND FEATURE EXTRACTION



FUTURE WORK

Behavioral Model Development:

- Creation of individual behavioral models tailored for each user, specifically two models.

Exploration of New Attack Types:

- Explore the Slow Post Attack