

# GUARDING THE GATEWAY:

## UNDERSTANDING NETWORK ATTACK

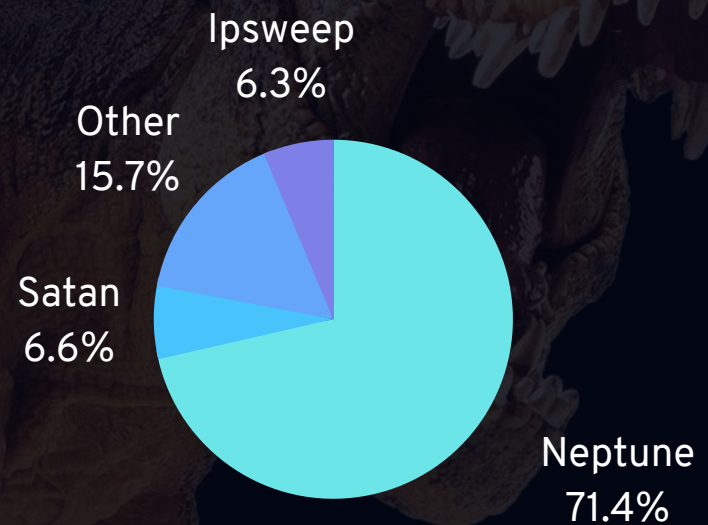


### TYPE OF NETWORK ATTACK

- 1 Neptune
- 2 Satan
- 3 Ipsweep
- 4 Portsweep

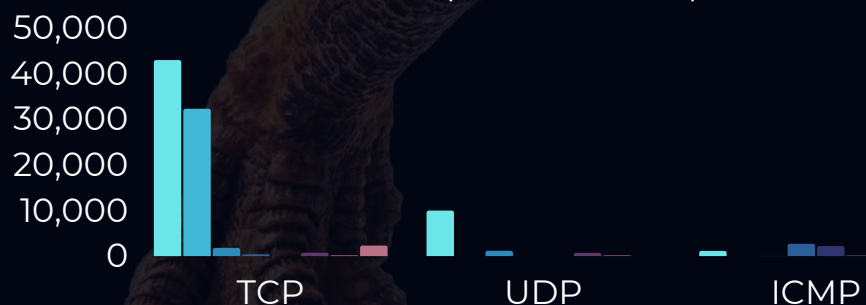
- 5 Smurf
- 6 Denial of Service Attack
- 7 Nmap

### MOST COMMON NETWORK ATTACKS



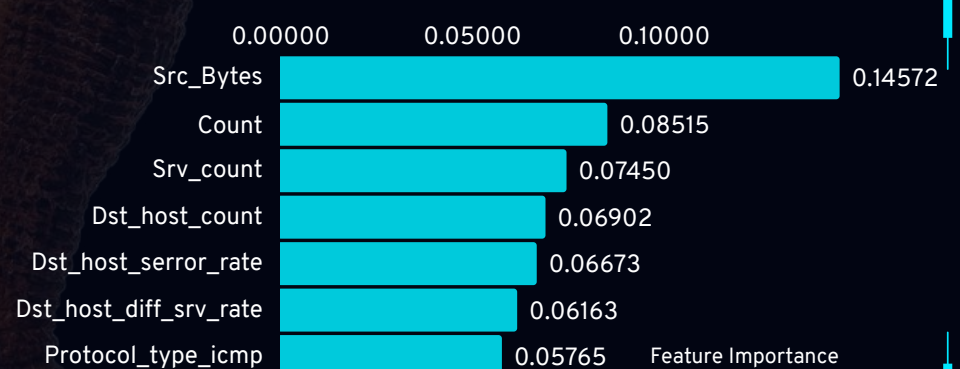
### COUNT OF NETWORK ATTACK BASED ON PROTOCOL TYPE

■ Normal ■ Neptune ■ Satan ■ Ipsweep  
■ Smurf ■ Denial of Service Attack  
■ Nmap ■ Portsweep



**TCP AND UDP ARE THE PROTOCOL TYPES THAT ARE MOST VULNERABLE TO NETWORK ATTACKS WITHOUT A DETECTION SYSTEM.**  
**TCP IS MOST PRONE TO BE ATTACKED BY NEPTUNE TYPE NETWORK ATTACK**

### MOST IMPORTANT FEATURE TO DETECT TYPE OF NETWORK ATTACK



**SRC BYTES - CONNECTION COUNT - SRV COUNT ARE THE FEATURES THAT HAVE THE MOST INFLUENCE ON DETECTING THE TYPE OF NETWORK ATTACK WITH RANDOM FOREST CLASSIFIER ALGORITHM.**

**WE NEED A DETECTION SYSTEM AND RANDOM FOREST CLASSIFIER WITH SMOTE OVERSAMPLING MODEL IS ONE OF THE BEST MODEL TO DETECT TYPE OF NETWORK ATTACK BY CONSIDERING RECALL AND PRECISION VALUE TO AVOID FALSE ALARM**

### THE BEST MODEL HAS

**96% ACCURACY, 96% RECALL, 97% PRECISION, AND 96% F-1 SCORE**