Feature Table for UM-NIDS Dataset

Feature List and Descriptions

This table lists the features included in the NIDS dataset along with their descriptions:

Feature Name	**Description**
id	Unique identifier for the network flow.
expiration_id	Flow expiration ID to indicate the termination of a flow.
src_ip	The source IP address of the flow.
src_mac	The source MAC address of the flow.
src_oui	Organizationally Unique Identifier (OUI) for the source MAC address.
src_port	The source port of the flow.
dst_ip	The destination IP address of the flow.
dst_mac	The destination MAC address of the flow.
dst_oui	Organizationally Unique Identifier (OUI) for the destination MAC address.
dst_port	The destination port of the flow.
protocol	The protocol used in the network flow (e.g., TCP, UDP).
ip_version	The IP protocol version (IPv4 or IPv6).
vlan_id	VLAN identifier for the flow if applicable.
tunnel_id	Identifier for tunnel traffic (such as GRE or VPN traffic).
bidirectional_first_seen_ms	The first time the flow was seen, in milliseconds.
bidirectional_last_seen_ms	The last time the flow was seen, in milliseconds.
bidirectional_duration_ms	Duration of the flow, calculated in milliseconds.
bidirectional_packets	The total number of packets in both directions in the flow.
bidirectional_bytes	The total number of bytes transferred in both directions.
src2dst_first_seen_ms	The first time the source-to-destination flow was seen, in milliseconds.
src2dst_last_seen_ms	The last time the source-to-destination flow was seen, in milliseconds.
src2dst_duration_ms	Duration of the source-to-destination flow, in milliseconds.
src2dst_packets	The total number of packets in the source-to-destination direction.
src2dst_bytes	The total number of bytes transferred from source to destination.
dst2src_first_seen_ms	The first time the destination-to-source flow was seen, in milliseconds.
dst2src_last_seen_ms	The last time the destination-to-source flow was seen, in milliseconds.
dst2src_duration_ms	Duration of the destination-to-source flow, in milliseconds.
dst2src_packets	The total number of packets in the destination-to-source direction.
dst2src_bytes	The total number of bytes transferred from destination to source.
bidirectional_min_ps	Minimum packet size in the bidirectional flow.
bidirectional_mean_ps	Mean packet size in the bidirectional flow.
bidirectional_stddev_ps	Standard deviation of the packet size in the bidirectional flow.

bidirectional_max_ps	Maximum packet size in the bidirectional flow.
src2dst_min_ps	Minimum packet size in the source-to-destination direction.
src2dst_mean_ps	Mean packet size in the source-to-destination direction.
src2dst_stddev_ps	Standard deviation of the packet size in the source-to-destination direction.
src2dst_max_ps	Maximum packet size in the source-to-destination direction.
dst2src_min_ps	Minimum packet size in the destination-to-source direction.
dst2src_mean_ps	Mean packet size in the destination-to-source direction.
dst2src_stddev_ps	Standard deviation of the packet size in the destination-to-source direction.
dst2src_max_ps	Maximum packet size in the destination-to-source direction.
bidirectional_min_piat_ms	Minimum packet inter-arrival time in the bidirectional flow, in milliseconds.
bidirectional_mean_piat_ms	Mean packet inter-arrival time in the bidirectional flow, in milliseconds.
bidirectional_stddev_piat_ms	Standard deviation of the packet inter-arrival time in the bidirectional flow.
bidirectional_max_piat_ms	Maximum packet inter-arrival time in the bidirectional flow.
src2dst_min_piat_ms	Minimum packet inter-arrival time in the source-to-destination direction.
src2dst_mean_piat_ms	Mean packet inter-arrival time in the source-to-destination direction.
src2dst_stddev_piat_ms	Standard deviation of packet inter-arrival time in the source-to-destination direction.
src2dst_max_piat_ms	Maximum packet inter-arrival time in the source-to-destination direction.
dst2src_min_piat_ms	Minimum packet inter-arrival time in the destination-to-source direction.
dst2src_mean piat_ms	Mean packet inter-arrival time in the destination-to-source direction.
dst2src_stddev_piat_ms	Standard deviation of packet inter-arrival time in the destination-to-source direction.
dst2src_max_piat_ms	Maximum packet inter-arrival time in the destination-to-source direction.
bidirectional_syn_packets	Number of SYN packets in the bidirectional flow.
bidirectional_cwr_packets	Number of Congestion Window Reduced (CWR) packets in the bidirectional flow.
bidirectional_ece_packets	Number of Explicit Congestion Notification-Echo (ECE) packets in the bidirectional flow.
bidirectional_urg_packets	Number of URG packets in the bidirectional flow.
bidirectional_ack_packets	Number of ACK packets in the bidirectional flow.
bidirectional_psh_packets	Number of PSH packets in the bidirectional flow.
bidirectional_rst_packets	Number of RST packets in the bidirectional flow.
bidirectional_fin_packets	Number of FIN packets in the bidirectional flow.
src2dst_syn_packets	Number of SYN packets in the source-to-destination direction.
src2dst_cwr_packets	Number of CWR packets in the source-to-destination direction.
src2dst_ece_packets	Number of ECE packets in the source-to-destination direction.
src2dst_urg_packets	Number of URG packets in the source-to-destination direction.
src2dst_ack_packets	Number of ACK packets in the source-to-destination direction.
src2dst_psh_packets	Number of PSH packets in the source-to-destination direction.
src2dst_rst_packets	Number of RST packets in the source-to-destination direction.

src2dst_fin_packets	Number of FIN packets in the source-to-destination direction.
dst2src_syn_packets	Number of SYN packets in the destination-to-source direction.
dst2src_cwr_packets	Number of CWR packets in the destination-to-source direction.
dst2src_ece_packets	Number of ECE packets in the destination-to-source direction.
dst2src_urg_packets	Number of URG packets in the destination-to-source direction.
dst2src_ack_packets	Number of ACK packets in the destination-to-source direction.
dst2src_psh_packets	Number of PSH packets in the destination-to-source direction.
dst2src_rst_packets	Number of RST packets in the destination-to-source direction.
dst2src_fin_packets	Number of FIN packets in the destination-to-source direction.
application_name	Name of the application being used.
application_category_name	Category of the application.
application_is_guessed	Flag indicating if the application is guessed.
application_confidence	Confidence score in the application detection.
requested_server_name	The name of the requested server in the network flow.
client_fingerprint	Client's fingerprint, used for identification.
server_fingerprint	Server's fingerprint, used for identification.
user_agent	User agent string from the HTTP header.
content_type	Content type from the HTTP request.
udps.payload_data	Payload data of the packet.
udps.delta_time	Time difference between packets.
udps.packet_direction	Direction of the packet (source to destination or vice versa).
udps.ip_size	Total size of the IP packet.
udps.transport_size	Size of the transport-layer segment.
udps.payload_size	Size of the payload.
udps.syn	Indicates if the SYN flag is set in the TCP header.
udps.cwr	Indicates if the CWR flag is set in the TCP header.
udps.ece	Indicates if the ECE flag is set in the TCP header.
udps.urg	Indicates if the URG flag is set in the TCP header.
udps.ack	Indicates if the ACK flag is set in the TCP header.
udps.psh	Indicates if the PSH flag is set in the TCP header.
udps.rst	Indicates if the RST flag is set in the TCP header.
udps.fin	Indicates if the FIN flag is set in the TCP header.
udps.srcdst_packet_size_variation	Variation in packet size between source and destination pair within the specified time window.
udps.srcdst_udp_packet_count	Rolling window sum of UDP packets sent by the specific source to destination
udps.udp_packet_count	Total UDP packet count recevied by destination within the rolling time window
udps.srcdst_tcp_packet_count	Rolling window sum of TCP packets sent by the specific source to destination
udps.tcp_packet_count	Total TCP packet count recevied by destination within the rolling time window
udps.srcdst_ack_packet_count	Rolling window sum of ACK packets sent by the specific source to destination
udps.ack_packet_count	Total ACK packet count recevied by destination within the rolling time window
udps.srcdst_fin_packet_count	Rolling window sum of FIN packets sent by the specific source to destination
udps.fin_packet_count	Total FIN packet count recevied by destination within the rolling time window

udps.srcdst_rst_packet_count	Rolling window sum of RST packets sent by the specific source to destination
udps.rst_packet_count	Total RST packet count recevied by destination within the rolling time window
udps.srcdst_psh_packet_count	Rolling window sum of PSH packets sent by the specific source to destination
udps.psh_packet_count	Total PSH packet count recevied by destination within the rolling time window
udps.srcdst_syn_packet_count	Rolling window sum of SYN packets sent by the specific source to destination
udps.syn_packet_count	Total SYN packet count recevied by destination within the rolling time window
udps.srcdst_unique_ports_count	Number of unique ports probed by specific source to the destination
udps.srcdst_icmp_packet_count	Rolling window sum of ICMP packets sent by the specific source to destination
udps.icmp_packet_count	Total ICMP packet recevied by destination within the rolling time window
udps.srcdst_http_ports_count	Total HTTP ports accessed by the specific source-to- specific destination within the rolling time window
udps.http_ports_count	Total HTTP port requests recevied by destination within the rolling time window
udps.srcdst_bidirectional_duration_avg	Average bidirectional duration between specific source and destination pair within defined time window.
udps.bidirectional_duration_avg	Average bidirectional duration in the flow.
udps.srcdst_dns_port_count	Number of time DNS port is accessed by specific count in the source destination pair in time window
udps.dns_port_count	Total times DNS port accessed at the destination within the rolling time window
udps.srcdst_dns_port_src_count	Total DNS port count from the source in the source-to-destination direction.
udps.dns_port_src_count	Total DNS port count from the source in the flow.
udps.srcdst_vul_ports_count	Total vulnerable ports count in the source-to-destination pair in rolling time window
udps.src2dst_packet_count	Rolling window sum of packet counts in the specific source-to-destination direction.
udps.bidirectional_packet_count	Total bidirectional packet count recevied by destination within the rolling time window
udps.srcdst_src2dst_packet_count	Total source-to-destination packet count in the source-destination pair.
udps.srcdst_bidirectional_packet_count	Total bidirectional packet count in the source-to-destination pair.
file	The name of the file being processed.
label	The label associated with the flow, used for classification or training purposes.