Anomaly Fields

	Anomaly ID	Anomaly Description	Anomaly Tag	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
1	P-TCP-001	SYN and FIN flags SET (1)	TCP SYN FIN ERROR	P-TCP-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_when_fin_and_syn_flag_set	Total no. of All Frames				
2	P-TCP-002	SYN Frame with Payload	TCP SYN FRAME ERROR	P-TCP-002	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_when_syn_with_payload	Total no. of All Frames				
3	P-TCP-003	All TCP Flags are RESET (0)	TCP ALL FLAGS ERROR	P-TCP-003	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_when_all_flag_not_set	Total no. of All Frames				
4	P-TCP-004	Large amount wa	TCP LARGE WA	P-TCP-004	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Count of RST	Count of PSH_RS	Count of PSH_UR	Count of URG	Total no. of All Fra	

		rning flags	RNING FLAGS ERROR									flags	T flags	G flags	flags	mes		
5	P-TCP-005	TCP HandShake Anomaly	TCP HANDSHAKE ALERT	P-TCP-005	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Count of Handshake Anomaly	Total no. of All Frames				
6	P-TCP-006	TCP Congestion detected	TCP CONGESTION ALERT	P-TCP-006	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_ip_dsfield_ecn_is_3	Total no. of All Frames				
7	P-TCP-007	TCP header for Congestion indication	TCP CONGESTION ALERT 2	P-TCP-007	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_cwr_set_syn_reset	count_ecn_set_syn_reset	Total no. of All Frames			
8	P-TCP-008	TCP Retransmission frames >	TCP RETRANSMISSION WA	P-TCP-008	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of All Frames	Total no. of Retransmit Fra	Retransmit Threshold			

		30 %	RNING										mes				
9	P-TCP-009	TCP Duplicate ACK > 30 %	TCP DUPLICATE ACK WARNING	P-TCP-009	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of All Frames	Total no. of Dup ACK Frames	Dup ACK Threshold	ACK flag		
10	P-TCP-010	TTL min max difference	TCP TTL MIN MAX ERROR	P-TCP-010	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	TTL MIN	TTL MAX	Total no. of TTL difference	Total no. of All Frames		
11	P-TCP-011	TCP Checksum Error	TCP CHECKSUM ERROR	P-TCP-011	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of All Frames	Total no. of frames with checksum error	TCP_Checksum_Error_Threshold			
12	P-TCP-012	TCP Land Attack	TCP LAND ATTACK	P-TCP-012	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Count of Land Attack Frames					
13	P-TCP-013	TCP	TCP	P-TC	Start	End	SRC	SRC	SRC	DST	DST IP	Port	Count	Port				

		Port Scan	PORTSCAN	P-013	Time-Stamp	Time-Stamp	MAC	IP	Port	MAC		scan timed uration	of port scanned	scan Threshold				
14	P-TCP-014	TCP SYN-ACK-ACK Proxy	TCP SYN-ACK-ACK	P-TCP-014	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	No of session detected	Session Threshold	Timeout(Minute)			
15	P-TCP-015	Source IP-Based Session Limit	SOURCE-IP LIMIT	P-TCP-015	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	No of IP sessions	Session Threshold	Timeout(Minute)						
16	P-TCP-016	Destination IP-Based Session Limit	DEST-IP LIMIT	P-TCP-016	Start Time-Stamp	End Time-Stamp	DST MAC	DST IP	DST Port	No of IP sessions	Session Threshold	Timeout(Minute)						
17	P-TCP-017	TCP Jumbo Frame	TCP JUMBO FRAME AL	P-TCP-017	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of All Frames	Count of Jambo Frame	JumboFrame Threshold			

			ERT														
18	P-TCP-018	Invalid TCP Header Length	TCP INVALID HEADER LENGTH	P-TCP-018	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_invalid_tcp_hdr_len	Total no. of All Frames				
19	P-TCP-019	TCP Invalid Port	TCP INVALID PORT ALERT	P-TCP-019	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Count_of_Invalid_Port_Packets					
20	P-TCP-020	TCP Packet Lost	TCP PACKET LOST WARNING	P-TCP-020	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of All Frames	Count_of_Packet_Lost	Packet Lost Threshold			
21	P-TCP-021	TCP Suspect Conversations	TCP SUSPECTED CONVERSATION ALERT	P-TCP-021	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of All Frames	Count_of_Suspected_Frames	Conversation Stage			

22	P-TCP-022	TCP Uncorrelated Request Response	TCP UNCORRELATED REQUEST RESPONSE	P-TCP-022	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of All Frames	Count_of_Uncorrelated_req_res	Conversation Stage			
23	P-TCP-023	TCP Network Loop	TCP NETWORK LOOP	P-TCP-023	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	ip.id	Total no. of frames with same ip.id	Network Loop Threshold	Total no. of All Frames		
24	P-TCP-024	TCP Sequenct No Attack	TCP SEQUENCE NO ATTACK	P-TCP-023	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of All Frames	Count_of_TCP_OutOfOrder_Packets	TCP_OutOfOrder_Threshold			
25	P-ICMP-001	Excessive Port unreachable	ICMP EXC PORT UNREAC	P-ICMP-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	Count ICMP Header Type=	Total no. of All Frames								

		frames	HABLEALERT						0x03									
26	P-ICMP-002	Multiple Echo requests/replies in sequencial patter n tranmitted on network	ICMPECHOSEQPATTERNALERT	P-ICMP-002	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	Count ICMP Header Type= 0x08	Total no. of All Frames							
27	P-ICMP-003	Excessive use of ICMP messages to cripple network de	ICMPEXCMSGALERT(DoS)	P-ICMP-003	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	Count ICMP Header Type= 0x00	Count ICMP Header Type= 0x08	Total no. of All Frames					

		vices															
28	P-ICMP-004	ICMP/PingSWEEP	ICMPPINGSWEEPWARNING	P-ICMP-004	Start Time-Stamp	End Time-Stamp	MAC-1 from Pair	MAC-2 from Pair	IP-1 from Pair	IP-2 from Pair	Count ICMP Header Type=0x00	Count ICMP Header Type=0x08	Total no. of All Frames				
29	P-ICMP-005	Ping Flood	ICMPPINGFLOODWARNING	P-ICMP-005	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	Count ICMP Header Type=0x00	Count ICMP Header Type=0x08	Total no. of All Frames						
30	P-ICMP-006	ICMP tunneling	ICMPTUNNELINGWARNING	P-ICMP-006	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	ICMP Header Type	ICMP Header Code			
31	P-ICMP-007	Forged ICMP redirects	ICMPFORGEDALERT	P-ICMP-007	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC-1	DST IP-1	DST Port-1	DST MAC-n	DST IP-n	DST Port-n		
32	P-ICMP-008	Ping of Death Attack	PINGOFDEATH	P-ICMP-008	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	udp_src_port	udp_dst_port	tcp_src_port	tcp_dst_port	Count of Frames with	Total no. of All Frames	

														len >65507				
33	P-ICMP-009	ICMP Fragments	ICMP FRAGMENTERROR	P-ICMP-009	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	udp_src_port	udp_dst_port	tcp_src_port	tcp_dst_port	Count of Large Payload Frames and MF set	Total no. of All Frames		
34	P-ICMP-010	Large ICMP Packets	LARGE ICMP	P-ICMP-010	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	udp_src_port	udp_dst_port	tcp_src_port	tcp_dst_port	Count of Frames with len > 1024	Total no. of All Frames		
35	P-ICMP-011	Time Exceeded	TIME EXCEEDED	P-ICMP-011	Start Time-Stamp	End Time-Stamp	SRC IP	UDP SRC PORT	TCP SRC PORT	Count distinct MAC	Total no. of All Frames							
36	P-ICMP-012	Parameter Error	ICMP PARAERROR	P-ICMP-012	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	udp_src_port	udp_dst_port	tcp_src_port	tcp_dst_port	Count of Error Frames	Comma Seperated Values limit	Total no. of All Frames	

																10 (Parameterize)		
37	P-ICMP-013	ICMP Invalid Port	ICMP INVALID PORT	P-ICMP-013	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	udp_src_port	udp_dst_port	tcp_src_port	tcp_dst_port	Count of Invalid (Zero or Null) Ports			
38	P-ICMP-014	ICMP Checksum Error	ICMP CHECKSUM ERROR	P-ICMP-014	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	udp_src_port	udp_dst_port	tcp_src_port	tcp_dst_port	Total no. of frames with checksum error	ICMP_Checksum_Error_Threshold	Total no. of All Frames	
39	P-UDP-001	UDP Flood	UDP FLOOD	P-UDP-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	Total no. of All Frames	Total no. of UDP Frames	Total Sum of Bytes of UDP Packets					
40	P-UDP-002	UDP Amplificati	UDP AMP ATT	P-UDP-002	Start Time-	End Time-	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Count of udp	Total no. of All				

		on Attack	ACK		Stamp	Stamp							frames with Src IP == Dst IP	Frames				
41	P-UDP-003	UDP Ping Pong Attack	UDP PING-PONG ATTACK	P-UDP-003	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	SRC PORT	DST PORT	Count of records where source port is either 19 or 7	Count of records where dest port is either 19 or 7	Total no. of All Frames			
42	P-UDP-004	UDP Invalid Port	UDP INVALID PORT	P-UDP-004	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	DST MAC	DST IP	Count of Invalid (Zero or Null) SRC Port	Count of Invalid (Zero or Null) DST Port	Total no. of All Frames					

43	P-UDP-005	UDP Checksum Error	UDP CHECKSUM ERROR	P-UDP-005	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	Total no. of frames with checksum error	UDP_Checksum_Error_Threshold	Total no. of All Frames			
44	P-IP-001	Unknown Protocol	Unknown Protocol	P-IP-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	ip.protocol value					
45	P-IP-002	IP Checksum Error	IP Checksum Error	P-IP-002	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	ip.checksum.status	ip.checksum	ip.checksum_calculated			
46	P-IP-003	Invalid IP Length	Invalid IP Length	P-IP-003	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	ip.len					
47	P-IP-004	Invalid IP Header Length	Invalid IP Header Length	P-IP-004	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	ip.hdr_len					
48	P-IP-005	Network Loop	Network Loop	P-IP-005	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	ip.id	Total no. of frames	Network Loop Thr	Total no. of All Fra		

														with same ip.id	eshold	mes		
49	P-IP-006	IPv6 Packet Warning	IPv6 PACKET	P-IP-006	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC_OUI_RESOLVED	DST MAC	DST_OUI_RESOLVED	IP_Version							
50	P-HTTP-001	Unsecure Protocol	Unsecure Communication	P-HTTP-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_HTTP_packets	Total no. of All Frames				
51	P-FTP-001	Unsecure Protocol	Unsecure Communication	P-FTP-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_FTP_packets	Total no. of All Frames				
52	P-SMB1-001	Unsecure Protocol	Unsecure Communication	P-SMB-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_SMB1_packets	Total no. of All Frames				
53	P-TELNET-001	Unsecure Protocol	Unsecure Communication	P-TELNET-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_TELNET_packets	Total no. of All Frames				

54	P-MODBUS-001	Invalid Modbus Length		P-MODBUS-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_MODBUS_invalid_len	Total no. of All Frames				
55	P-MODBUS-002	Excessive Read Operation		P-MODBUS-002	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_read_op	Total no. of All Frames	Excessive Read Threshold ('%')			
56	P-MODBUS-003	Excessive Write Operation		P-MODBUS-003	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_write_op	Total no. of All Frames	Excessive Write Threshold ('%')			
57	P-MODBUS-004	Excessive Diagnostic Operation		P-MODBUS-004	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_diagnostic_op	Total no. of All Frames	Excessive Diagnostic Threshold ('%')			

58	P-MODBUS-005	Excessive Exception Code Operation		P-MODBUS-005	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	count_of_exception	Total no. of All Frames	Excessive Exception Threshold ('%')			
59	P-MODBUS-006	Vendor Scanning Alert		P-MODBUS-006	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	total_vendor_info_req_frame	Total no. of All Frames	Scanning Threshold							
60	P-FR-001	Invalid Frame Length	Invalid Frame Length	P-FR-001	Start Time-Stamp	End Time-Stamp	SRC MAC	SRC IP	SRC Port	DST MAC	DST IP	DST Port	frame.len					
61	P-ARP-001	Suspected ARP Attack	Suspected ARP Attack	P-ARP-001	Start Time-Stamp	End Time-Stamp	SRC MAC	Total Frames										
62	P-ERROR	Undefined Anomaly detected (For any unkno	Undefined Anomaly detected	P-ERROR	Anomaly ID(1st column of undefined anom													

		wn fra me rec eiv ed by DS tea m)			aly/ fra me)														