

Attack leaf variables

- uap = Use_alternative_port (leaf)
- tp = Tunnel_payload_inside_allowed_protocol (tunnel)
- extract = Extract_tunneled_data_inside_host
- alter_tcp = Alter_TCP_header
- ensure_hdrs = Ensure_valid_headers
- normalize = Normalize_TCP_fields
- send_from_inside = Send_traffic_from_inside
- clean_fmt = Clean_payload_formatting
- discover_port = Discover_block_port
- exploit_misconfig = Exploit_misconfiguration
- exhaust_mbuf = Exhaust_Mbuf_pool
- degrade_perf = Degrade_inspection_performance
- maintain_flood = Maintain_flooding
- send_blocked = Send_blocked_traffic

Defense variables

- D_DPI = DeepPacketInspection active
- D_InputPatch = InputValidationPatch / defensive parsing active
- D_Rate = RateLimit active
- D_Egress = EgressFilter active
- D_SmartNIC = SmartNIC_Offload active
- D_HIDS = Host-based detection active

Counter-attack (attacker neutraliser) variables

- c_enc = EncodePayload (neutralizes D_DPI)
- c_misconf = BypassFirewallConfig (neutralizes D_Rate and D_Egress)
- c_zero = ZeroDayExploit (neutralizes D_InputPatch)
- c_smart = Bypass_SmartNIC_Firmware (neutralizes D_SmartNIC)

$$f(R) = f(A) \vee f(B) \vee f(C)$$

- A = Bypass_inspection_logic
- B = Exploit_data_parsing_flaw
- C = Disable_firewall_engine

$$f(A) =$$

$$\begin{aligned} & (\text{uap} \wedge \text{Block}(\text{D_DPI}, \text{c_enc})) \\ & \vee (\text{tp} \wedge \text{Block}(\text{D_DPI}, \text{c_enc}) \wedge \text{Block}(\text{D_HIDS}, \text{false})) \\ & \vee ((\text{alter_tcp} \wedge \text{ensure_hdrs} \wedge \text{normalize}) \wedge \text{Block}(\text{D_DPI}, \text{c_enc})) \\ & \vee (\text{send_from_inside} \wedge \text{Block}(\text{D_SmartNIC}, \text{c_smart}) \wedge \text{Block}(\text{D_DPI}, \text{c_enc})) \end{aligned}$$

f(B) =
 (clean_fmt \wedge Block(D_InputPatch,c_zero))
 \vee (normalize \wedge Block(D_InputPatch,c_zero))
 \vee ((discover_port \vee exploit_misconfig) \wedge Block(D_InputPatch,c_zero))

f(C) =
 (exhaust_mbuf \wedge Block(D_Rate,c_misconf) \wedge Block(D_Egress,c_misconf))
 \vee (degrade_perf \wedge Block(D_Rate,c_misconf))
 \vee (maintain_flood \wedge Block(D_Rate,c_misconf))
 \vee (send_blocked \wedge Block(D_Egress,c_misconf))

f(R) =
 [(uap \wedge B(D_DPI,c_enc))
 \vee (tp \wedge B(D_DPI,c_enc) \wedge \neg D_HIDS)
 \vee ((alter_tcp \wedge ensure_hdrs \wedge normalize) \wedge B(D_DPI,c_enc))
 \vee (send_from_inside \wedge B(D_SmartNIC,c_smart) \wedge B(D_DPI,c_enc))
]
 \vee
 [(clean_fmt \wedge B(D_InputPatch,c_zero))
 \vee (normalize \wedge B(D_InputPatch,c_zero))
 \vee ((discover_port \vee exploit_misconfig) \wedge B(D_InputPatch,c_zero))
]
 \vee
 [(exhaust_mbuf \wedge B(D_Rate,c_misconf) \wedge B(D_Egress,c_misconf))
 \vee (degrade_perf \wedge B(D_Rate,c_misconf))
 \vee (maintain_flood \wedge B(D_Rate,c_misconf))
 \vee (send_blocked \wedge B(D_Egress,c_misconf))
]