

## 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

$$f(A) =$$

```
( uap ∧ Block(D_DPI,c_enc) )  
∨ ( tp ∧ Block(D_DPI,c_enc) ∧ Block(D_HIDS, false) )  
∨ ( (alter_tcp ∧ ensure_hdrs ∧ normalize) ∧ Block(D_DPI,c_enc) )  
∨ ( send_from_inside ∧ Block(D_SmartNIC,c_smart) ∧ Block(D_DPI,c_enc) )
```

$f(B) =$   
 $(\text{clean\_fmt} \wedge \text{Block}(D_{\text{InputPatch}}, c_{\text{zero}}))$   
 $\vee (\text{normalize} \wedge \text{Block}(D_{\text{InputPatch}}, c_{\text{zero}}))$   
 $\vee ((\text{discover\_port} \vee \text{exploit\_misconfig}) \wedge \text{Block}(D_{\text{InputPatch}}, c_{\text{zero}}))$

$f(C) =$   
 $(\text{exhaust\_mbuf} \wedge \text{Block}(D_{\text{Rate}}, c_{\text{misconf}}) \wedge \text{Block}(D_{\text{Egress}}, c_{\text{misconf}}))$   
 $\vee (\text{degrade\_perf} \wedge \text{Block}(D_{\text{Rate}}, c_{\text{misconf}}))$   
 $\vee (\text{maintain\_flood} \wedge \text{Block}(D_{\text{Rate}}, c_{\text{misconf}}))$   
 $\vee (\text{send\_blocked} \wedge \text{Block}(D_{\text{Egress}}, c_{\text{misconf}}))$

$f(R) =$   
 $[(\text{uap} \wedge B(D_{\text{DPI}}, c_{\text{enc}}))$   
 $\vee (\text{tp} \wedge B(D_{\text{DPI}}, c_{\text{enc}}) \wedge \neg D_{\text{HIDS}})$   
 $\vee ((\text{alter\_tcp} \wedge \text{ensure\_hdrs} \wedge \text{normalize}) \wedge B(D_{\text{DPI}}, c_{\text{enc}}))$   
 $\vee (\text{send\_from\_inside} \wedge B(D_{\text{SmartNIC}}, c_{\text{smart}}) \wedge B(D_{\text{DPI}}, c_{\text{enc}}))$   
 $]$   
 $\vee$   
 $[(\text{clean\_fmt} \wedge B(D_{\text{InputPatch}}, c_{\text{zero}}))$   
 $\vee (\text{normalize} \wedge B(D_{\text{InputPatch}}, c_{\text{zero}}))$   
 $\vee ((\text{discover\_port} \vee \text{exploit\_misconfig}) \wedge B(D_{\text{InputPatch}}, c_{\text{zero}}))$   
 $]$   
 $\vee$   
 $[(\text{exhaust\_mbuf} \wedge B(D_{\text{Rate}}, c_{\text{misconf}}) \wedge B(D_{\text{Egress}}, c_{\text{misconf}}))$   
 $\vee (\text{degrade\_perf} \wedge B(D_{\text{Rate}}, c_{\text{misconf}}))$   
 $\vee (\text{maintain\_flood} \wedge B(D_{\text{Rate}}, c_{\text{misconf}}))$   
 $\vee (\text{send\_blocked} \wedge B(D_{\text{Egress}}, c_{\text{misconf}}))$   
 $]$