SBC Threat Protection

UDP Threats

- UDP Short Header
- UDP Flood
- UDP spoofed boradcast echo (Fraggle Attack)
- UDP attack on diag ports (Pepsi Attack)

RTP Threats

- RTP rogue packets (after-call)
- RTP flooding during call
- RTP flooding attacks
- RTP spoofing

SIP Threats

- SDP malformed contents (Protos Test)
- SIP malformed packet
- SIP request message flood attack
- SIP response message flood attack
- SIP Invite spoof
- SIP Register spoof
- SIP Registerfloodattack
- SIP request spoof
- SIP response spoof
- SIP end-callattack

IP Threat

- Unknown Protocol
- ARP Flood (Poink Attack)
- IP Stream Option
- IP Spoofing
- IP Source Route Option, Strict
- IP Source Route Option, Loose
- IP Short Header
- IP Malformed Packet
- IP bad Option
- IP address Session Limit
- Fragments – too many
- Fragments, Large – Offset
- Fragments – Storm
- Fragments – Same Offset
- Fragments – Reassembly w/different offsets (tear drop)
- Fragments – Reassembly w/different offsets and padding (new tear attack)
- Fragments – Reassembly w/different offsets and oversize (Bonk/Boink attack)
- Fragments – Reassembly off by one IP header (Nestea attack)
- Fragments – flood initial fragment only (Rose Attack)
- Fragments – Deny

ICMP Threat

- ICMP Source quench
- ICMP mask request
- ICMP large packet(>1472)
- ICMP oversized packet(>65536) – ping of death/ssping attack)
- ICMP info request
- ICMP incompatible fragment (jolt attack)
- ICMP flood
- ICMP broadcast with spoofed source (Smurf/Pong attack)
- ICMP error packets flood (Trash attack)
- ICMP spoofed unreachable (Click attack)

- ICMP spoofed unreachable flood (smack/bloop/puke attack)

TCP Threat

- TCP Packets without flag
- TCP packets, oversized
- TCP FIN bit with no ACK bit
- TCP packet with URG/OOB flag (nuke attack)
- TCP SYN fragments – reassembly with overlap (syndrop attack)
- SYN fragment
- SYN attack w/ip spoofing (land attack)
- SYN attack (syn flood)
- SYN and FIN bits set
- Scan attack– TCP port