

ARP

- Cache poisoning
- Excessive dpdu length
- Hardware address spoofing
- Incorrect specified lengths
- for address fields
- Invalid operation
- Translation cache size

Ethernet

- Broadcast destination address tolerance
- Jumbo frame tolerance
- Multicast destination address tolerance
- Protocol address spoofing
- Runt frame tolerance
- Truncated dpdu
- Unicast destination address tolerance

ICMPv4

- Malformed pdus of defined pdu types
- Pdus of appropriate pdu type but with invalid field content
- Pdus of contextually inappropriate pdu type
- Ping of death
- Processing of npdus that reference undefined or supposedly nonimplemented protocol types
- Rejection of ip multicasts and broadcasts
- Rejection of npdus with invalid source ip addresses
- Undefined pdu types

IPv4

- Bad checksum flood to exhaust stateful firewalls
- Illogical or inconsistent npdu flag values
- Invalid npdu header ip version
- Npdu fragment mis reassembly
- Npdu options
- Receipt of npdus with various ttl field values
- Truncated fixed header
- Truncated header options

TCPv4

- Land and latierra attacks
- Malformed or undefined tpdu options
- Spoofed tcp flags
- Truncated tpdu truncated fixed header
- Truncated tpdu truncated header options
- Truncated tpdu truncated priority data
- Unrestricted interpretation of select tpdu options

UDPv4

- Rejection of tpdu addressed to reserved destination ports
- Tpdu length signedness
- Truncated tpdu header with negative length field
- Truncated tpdu header with non-negative length field
- Valid tpdu shorter than ip npdu payload

IPv6

- Fragmentation null reference
- Fragmentation overlap
- Incomplete fragmentation
- Multicast ping
- Multicast udp ping
- Multiple nesting
- Router advertisement dos
- Truncated fixed header
- Truncated option

SSL/TLS

- AES CCM (Test count: 229)
- AES GCM Nonce (Test count: 3)
- ALPN Negotiation (Test count: 18)
- Atypical Padding (Test count: 11)
- Bleichenbacher Timing (Test count: 0)
- Bleichenbacher Workaround (Test count: 609)
- Certificate Malformed (Test count: 0)
- Certificate Request (Test count: 3)
- Certificate Verify (Test count: 4)
- Certificate Verify Malformed (Test count: 266)
- Certificate Verify Malformed Sig (Test count: 7)
- Chacha20 (Test count: 152)
- Client Compatibility (Test count: 140)
- Client Hello Max Size (Test count: 2)
- Client Hello MD5 (Test count: 3)
- Connection Abort (Test count: 13)
- Conversation (Test count: 1)
- CVE-2016-2107 (Test count: 2)
- CVE-2016-6309 (Test count: 3)
- CVE-2016-7054 (Test count: 129)
- DHE Key Share Random (Test count: 9)
- DHE No Shared Secret Padding (Test count: 9)
- DHE RSA Key Exchange (Test count: 1)
- DHE RSA Key Exchange Signatures (Test count: 26)
- DHE RSA Key Exchange With Bad Messages (Test count: 8)
- Downgrade Protection (Test count: 4)

SSL/TLS

- Early Application Data (Test count: 4)
- ECDHE Padded Shared Secret (Test count: 21)
- ECDHE RSA Key Exchange (Test count: 2)
- ECDHE RSA Key Exchange With Bad Messages (Test count: 7)
- ECDHE RSA Key Share Random (Test count: 21)
- ECDSA In Certificate Ver EDSSA In Certificate Verify (Test count: 0)
- ECDSA In Certificate Verify (Test count: 0)
- ECDSA Sig Flexibility (Test count: 7)
- Empty Extensions (Test count: 2)
- Encrypt Then MAC (Test count: 2)
- Encrypt Then MAC Renegotiation (Test count: 2)
- Export Ciphers Rejected (Test count: 153)
- Extended Master Secret Extension (Test count: 17)
- Extended Master Secret Extension With Client Cert (Test count: 0)
- Extensions (Test count: 291)
- Fallback SCSV (Test count: 24)
- FFDHE Expected Params (Test count: 2)
- FFDHE Negotiation (Test count: 40)
- Fuzzed Ciphertext (Test count: 337)
- Fuzzed Finished (Test count: 9)
- Fuzzed MAC (Test count: 31)
- Fuzzed Padding (Test count: 12)
- Fuzzed Plaintext (Test count: 53)
- Heartbeat (Test count: 568)
- Hello Request By Client (Test count: 2)
- Interleaved Application Data And Fragmented Handshakes In Renegotiation (Test count: 4)
- Interleaved Application Data In Renegotiation (Test count: 4)
- Invalid Cipher Suites (Test count: 26)
- Invalid Client Hello (Test count: 7929)
- Invalid Compression Methods (Test count: 3)
- Invalid Content Type (Test count: 4)
- Invalid RSA Key Exchange Messages (Test count: 6)
- Invalid Server Name Extension (Test count: 15)
- Invalid Server Name Extension Resumption (Test count: 5)
- Invalid Session ID (Test count: 2)
- Invalid Version (Test count: 2)
- Large Hello (Test count: 3403)
- Legacy Renegotiation (Test count: 9)
- Lengths (Test count: 1001)
- Lucky13 (Test count: 0)
- Message Duplication (Test count: 9)
- Message Skipping (Test count: 10)
- No Heartbeat (Test count: 6)
- OCSP Stapling (Test count: 3)
- OpenSSL 3712 (Test count: 2)

SSL/TLS

- Record Layer Fragmentation (Test count: 23)
- Record Size Limit (Test count: 38)
- Renegotiation Changed ClientHello (Test count: 13)
- Renegotiation Disabled (Test count: 5)
- Renegotiation Disabled Client Certificate (Test count: 3)
- Resumption With Wrong Ciphers (Test count: 5)
- RSA PSS Sigs on Certificate Verify (Test count: 0)
- RSA Sigs on Certificate Verify (Test count: 0)
- ServerHello Random (Test count: 9)
- SessionID Resumption (Test count: 3)
- Sig Algs (Test count: 17)
- Sig Algs Renegotiation Resumption (Test count: 11)
- Signature Algorithms (Test count: 275)
- SSL Death Alert (Test count: 2)
- SSLv2 Connection (Test count: 3)
- SSLv2 Force Cipher (Test count: 21)
- SSLv2 Force Cipher 3DES (Test count: 3)
- SSLv2 Force Cipher Non 3DES (Test count: 18)
- SSLv2 Force Export Cipher (Test count: 6)
- SSLv2 Hello Protocol (Test count: 6)
- SSLv3 Padding (Test count: 5)
- TLSv12 Rejected Without TLSv12 (Test count: 53)
- TLSv13 Ortt Garbage (Test count: 10)
- TLSv13 CCS (Test count: 10)
- TLSv13 Certificate Request (Test count: 3)
- TLSv13 Certificate Verify (Test count: 0)
- TLSv13 Connection Abort (Test count: 14)
- TLSv13 Conversation (Test count: 1)
- TLSv13 Count Tickets (Test count: 2)
- TLSv13 CRFG Curves (Test count: 17)
- TLSv13 DHE Shared Secret Padding (Test count: 7)
- TLSv13 ECDHE Curves (Test count: 32)
- TLSv13 ECDHE In Certificate Verify (Test count: 0)
- TLSv13 ECDSA Support (Test count: 5)
- TLSv13 EDDSA In Certificate Verify (Test count: 0)
- TLSv13 Empty Alert (Test count: 9)
- TLSv13 FFDHE Groups (Test count: 61)
- TLSv13 FFDHE Sanity (Test count: 6)
- TLSv13 Finished (Test count: 713)
- TLSv13 Finished Plaintext (Test count: 2)
- TLSv13 HRR (Test count: 2)
- TLSv13 Invalid Ciphers (Test count: 606)
- TLSv13 Keyshare Omitted (Test count: 4)
- TLSv13 Keyupdate (Test count: 266)
- TLSv13 Key Update From Server (Test count: 2)
- TLSv13 Large Number of Extensions (Test count: 81)
- TLSv13 Legacy Version (Test count: 9)
- TLSv13 Lengths (Test count: 1001)
- TLSv13 Multiple CCS Messages (Test count: 6)

SSL/TLS

- TLSv13 No Ciphers (Test count: 2)
- TLSv13 Non Support (Test count: 52)
- TLSv13 Obsolete Curves (Test count: 170)
- TLSv13 PKCS Signature (Test count: 7)
- TLSv13 Post Handshake Auth (Test count: 5)
- TLSv13 PSK DHE Ke (Test count: 3)
- TLSv13 PSK Ke (Test count: 1)
- TLSv13 Record Layer Limits (Test count: 145)
- TLSv13 Record Padding (Test count: 3)
- TLSv13 RSA PSS Signatures (Test count: 7)
- TLSv13 RSA Signatures (Test count: 7)
- TLSv13 ServerHello Random (Test count: 7)
- TLSv13 Session Resumption (Test count: 2)
- TLSv13 Shuffled Extensions (Test count: 18)
- TLSv13 Signature Algorithms (Test count: 281)
- TLSv13 Symetric Ciphers (Test count: 1158)
- TLSv13 Unrecognised Groups (Test count: 31)
- TLSv13 Version Negotiation (Test count: 268)
- TLSv13 Zero Content Type (Test count: 7)
- TLSv13 Zero Length Data (Test count: 10)
- Truncating of Client Hello (Test count: 29)
- Truncating of Finished (Test count: 3)
- Truncating of kRSA Client Key Exchange (Test count: 3)
- Unsupported Curve Fallback (Test count: 8)
- X25519 (Test count: 8)
- Zero Length Data (Test count: 1)

Canbus Attacks

- Cherokee - Kill brakes
- Cherokee - Kill engine
- Cherokee - Turn steering
- Diagnostic - State
- Ecu - Hard reset
- Ford - Escape diagnostic packets
- Ford - Escape door ajarSpooF
- Ford - Escape kill engine
- Honda - Car lock and unlock
- Ignis - Zeta fuel seatbelt spooF
- Jeep - Wrangler evicsend
- Kill - Bus
- Malibu - Overheat
- Mazda2 - Ic fuzzer
- Mazda - Ic mover
- Pdo - Input output controller
- Peugeot207 - Ic fuzzer
- Peugeot207 - Ic mover
- Peugeot207 - Ic reboot
- Prius - Park killEngine
- Reset - Mileage
- Rx8 - R
- Spam - Bus
- Tesla - Disable esp abs
- Tesla - Open trunk
- Uds - Sec access

Web Application Penetration Testing/Fuzzing

- GraphQL
- Complete metasploit implementation