Man in the Middle (MITM) Attack - BETTERCAP:

[1] alert ip any any -> any any (msg:"MITM attack detected - ARP Spoofing"; ether proto 0x0806; content:"\x00\x01"; offset:6; depth:2; sid:1000001;)

[2] alert ip any any -> any any (msg:"MITM attack detected - Duplicate IP"; detection_filter: track by_src, count 5, seconds 10; sid:1000002;)

[3] alert ip any any -> any any (msg:"MITM attack detected - Abnormal packet flow"; flowbits:set,mitm_detected; threshold:type both, track by_src, count 50, seconds 30; sid:1000003;)

[4] alert ip any any -> any any (msg:"MITM attack detected - ARP Reply flood"; content:"\x00\x02"; offset:6; depth:2; detection_filter: track by_src, count 100, seconds 10; sid:1000004;)

[5] alert tcp any any -> any any (msg:"MITM attack detected - SSL Strip Attempt"; content:"HTTP/1.1 301"; http_header; sid:1000005;)

[6] alert ip any any -> any any (msg:"MITM attack detected - Abnormal DNS responses"; content:"\xC0\x0C"; offset:2; depth:2; sid:1000006;)

[7] alert ip any any -> any any (msg:"MITM attack detected - Spoofed DNS reply"; content:"\x00\x01\x00\x01\x00\x00"; offset:2; depth:6; sid:1000007;)

[8] alert ip any any -> any any (msg:"MITM attack detected - Suspicious DHCP Traffic"; content:"\x35\x01\x05"; offset:240; depth:3; sid:1000008;)

[9] alert tcp any any -> any any (msg:"MITM attack detected - SSL Certificate Anomaly"; tls.cert_subject; content:"CN=FakeCA"; sid:1000009;)

[10] alert ip any any -> any any (msg:"MITM attack detected - Excessive HTTP redirects"; detection_filter: track by_src, count 50, seconds 10; sid:1000010;)

Additional MITM attack detection rules:

[11] alert ip any any -> any any (msg:"MITM attack detected - Fake SMTP EHLO"; content:"EHLO attacker"; sid:1000026;)

[12] alert ip any any -> any any (msg:"MITM attack detected - TLS session resumption anomaly"; tls.store; detection_filter: track by_src, count 50, seconds 30; sid:1000027;)

[13] alert tcp any any -> any any (msg:"MITM attack detected - DNS Cache Poisoning Attempt"; content:"\x00\x01\x00\x01\x00\x00"; offset:2; depth:6; sid:1000028;)

[14] alert ip any any -> any any (msg:"MITM attack detected - Fake POP3 Server Response"; content:"+OK FakeServer"; sid:1000029;)

[15] alert ip any any -> any any (msg:"MITM attack detected - Fake IMAP Server Response"; content:"* OK FakeIMAPServer"; sid:1000030;)

[16] alert tcp any any -> any any (msg:"MITM attack detected - SSL Cipher downgrade"; content:"TLS_RSA_WITH_NULL_MD5"; sid:1000031;)

[17] alert ip any any -> any any (msg:"MITM attack detected - HTTP Header Injection"; content:"Injected-Header:"; http_header; sid:1000032;)

[18] alert ip any any -> any any (msg:"MITM attack detected - Malformed HTTP Headers"; content:"Host: 127.0.0.1"; http_header; sid:1000033;)

[19] alert ip any any -> any any (msg:"MITM attack detected - Fake SSH Banner"; content:"SSH-2.0-FAKE"; sid:1000034;)

[20] alert ip any any -> any any (msg:"MITM attack detected - Fake FTP Server Response"; content:"220 Welcome to FakeFTP"; sid:1000035;)

[21] alert ip any any -> any any (msg:"MITM attack detected - Malformed DHCP Offer"; content:"\x02\x01\x06\x00"; offset:0; depth:4; sid:1000036;)

[22] alert ip any any -> any any (msg:"MITM attack detected - Excessive TCP Reset Packets"; detection_filter: track by_src, count 100, seconds 30; sid:1000037;)

[23] alert ip any any -> any any (msg:"MITM attack detected - DNS Request with Fake IP"; content:"\x7F\x00\x00\x01"; offset:12; depth:4; sid:1000038;)

[24] alert ip any any -> any any (msg:"MITM attack detected - Multiple SSL Certificates in One Session"; detection_filter: track by_src, count 3, seconds 10; sid:1000039;)

[25] alert tcp any any -> any any (msg:"MITM attack detected - Abnormal TLS Handshake"; tls.version; content:"\x03\x03"; sid:1000040;)

[26] alert ip any any -> any any (msg:"MITM attack detected - Fake NTP Server Response"; content:"Stratum 1, Fake Time Server"; sid:1000041;)

[27] alert tcp any any -> any any (msg:"MITM attack detected - HTTPS Certificate Signed by Untrusted CA"; tls.cert_issuer; content:"CN=UntrustedCA"; sid:1000042;)

[28] alert ip any any -> any any (msg:"MITM attack detected - Fake SIP Server Response"; content:"SIP/2.0 200 OK"; sid:1000043;)

[29] alert ip any any -> any any (msg:"MITM attack detected - Unauthorized TLS Renegotiation"; tls.renegotiation_attempted; sid:1000044;)

[30] alert ip any any -> any any (msg:"MITM attack detected - Unexpected ICMP Redirects"; icmp_type:5; sid:1000045;)