WIRESHARK

30+ Wireshark Filters for Threat Detection

No	Threat Type	How It Works	Display Filter	Detection Method
1	HTTP GET Flooding	High volume of HTTP GET requests to overload server	http.request.method == "GET"	Check for abnormal number of requests from same source IP; investigate suspicious patterns in user-agent strings
2	Suspicious HTTP User-Agent	Irregular User-Agent strings used to mask identity	http.user_agent	Examine HTTP headers for unusual or malformed User-Agent strings; correlate requests with known malicious IP addresses
3	Malicious HTTP User-Agent	Specific malicious user-agent strings used by attackers	http.user_agent contains "malicious_string"	Check for known malicious user-agent strings; correlate with other suspicious activities
4	SQL Injection via HTTP	Malicious SQL commands inserted into application queries via HTTP	http.request.uri contains "SELECT" or http.request.uri contains "UNION"	Inspect HTTP GET and POST requests for SQL keywords in unexpected places; analyze request parameters for special characters
5	Cross-Site Scripting (XSS)	Malicious scripts injected into web pages viewed by other users	http.request.uri contains "<script>"	Examine HTTP request URIs and POST data for script tags or encoded JavaScript
6	HTTP Directory Traversal	Attempts to access restricted directories via manipulated URLs	http.request.uri contains ".."	Analyze HTTP request URIs for directory traversal patterns like "../"; look for encoded versions
7	Suspicious HTTP POST Requests	HTTP POST requests used for data exfiltration or malicious uploads	http.request.method == "POST"	Review HTTP headers for POST requests with large payloads or to unknown IP addresses; inspect content for encoded data

8	DNS Tunneling	DNS queries manipulated to transmit data, bypassing firewalls	dns	Inspect DNS query field for abnormal payload sizes or repeated requests; analyze DNS response time for unusual delays
9	DNS Tunneling (Advanced)	Long DNS query names used for data exfiltration	dns.qry.name.len > 50	Look for unusually long DNS query names; analyze frequency and patterns of queries
10	DNS Amplification	Small request triggers large DNS responses, overwhelming target	dns.qry.name	Check DNS response section for large-sized responses and unexpected source addresses; look at TTL field for unusually low values
11	DNS Poisoning	DNS responses altered to redirect users to malicious websites	dns.flags.rcode != 0	Analyze DNS response headers for mismatched IP addresses or altered TTL values; check response time field for unexpected delays
12	SMB Brute Force	Multiple login attempts via SMB protocol to guess valid credentials	smb.cmd == (=0x73)	Check SMB headers for failed login attempts; monitor SMB command response times
13	SMB Brute Force (Specific)	Failed SMB login attempts	smb.cmd == 0x73 and smb.nt.status == 0xc000006d	Monitor for repeated failed SMB authentication attempts from the same source
14	SMB Null Session Exploitation	Attempts to access SMB shares without authentication	smb.setup.action == 1 && smb.setup.native_os == ""	Monitor SMB setup requests for null session attempts; check for empty native OS fields in SMB negotiation
15	SYN Flood Attack	Flood target server with SYN packets without completing TCP handshake	tcp.flags.syn == 1 && tcp.flags.ack == 0	Review TCP headers for high volume of SYN packets without corresponding ACKs; look for delayed ACKs or connection resets

16	ICMP Flooding (Ping of Death)	Numerous ICMP requests to overload device	icmp	Review ICMP headers for high frequency of Echo Request packets from single source; inspect for ICMP packets larger than standard 64 bytes
17	ICMP Tunneling	Data exfiltration or covert channel using ICMP packets	icmp.type == 8 and ip.payload_len > 64	Detect ICMP echo requests with unusually large payloads
18	ARP Spoofing	Falsified ARP messages link wrong MAC addresses with IP addresses	arp.duplicate-address-frame	Inspect ARP header for mismatches between IP and MAC addresses; check for ARP requests with identical source IPs but different MAC addresses
19	ARP Spoofing (Duplicate Address)	Conflicting ARP messages to manipulate network traffic	arp.duplicate-address-detected	Identify instances of duplicate IP addresses in ARP traffic
20	FTP Plaintext Authentication	FTP transmits login credentials in plaintext	ftp.request.command == "USER"	Review FTP request headers for visible usernames and passwords; inspect packet payloads for plaintext data in FTP stream
21	FTP Command Injection	Attacker attempts to inject malicious commands into FTP sessions	ftp.request.command contains ";"	Look for FTP commands containing semicolons or other potential command separators
22	SSL/TLS Heartbleed Vulnerability	Exploit in OpenSSL library allowing memory content theft	ssl.heartbeat.payload_length > 16384	Check SSL/TLS heartbeat messages for abnormally large payload lengths; analyze response data for potential memory leaks
23	SSL Downgrade Attack	Force use of weaker SSL/TLS encryption protocols	ssl.record.version < 0x0303	Check SSL/TLS handshake headers for negotiation with older protocol versions; inspect certificate chains for self-signed or expired certificates

24	Suspicious TLS Certificate	Invalid or self-signed TLS certificates used to compromise encrypted communications	ssl.handshake.type == 11	Review SSL handshake header for certificates signed by unknown authorities; verify encryption protocol for downgrade attempts
25	DHCP Starvation	Attacker floods network with DHCP requests to exhaust IP pool	dhcp.option.dhcp == 1	Monitor for high volume of DHCP Discover messages from multiple MAC addresses; check for rapid succession of requests from single source
26	Rogue DHCP Server	Unauthorized DHCP server assigns IP addresses to redirect traffic	dhcp	Review DHCP Offer packets and compare server IP address to authorized DHCP servers; check for abnormal lease durations or renewals
27	SNMP Community String Bruteforce	Attempts to guess SNMP community strings for unauthorized access	snmp.community	Monitor for multiple SNMP requests with different community strings from same source; check for high rate of SNMP authentication failures
28	RDP Bruteforce	Repeated login attempts to RDP services	tcp.port == 3389	Analyze TCP traffic on RDP port for multiple failed connection attempts; look for patterns in timing and source of connection requests
29	SSH Bruteforce	Multiple SSH login attempts to guess valid credentials	tcp.port == 22	Monitor SSH traffic for repeated failed authentication attempts; analyze timing and source of connection requests
30	VOIP Call Hijacking	Unauthorized interception or manipulation of VOIP calls	sip	Examine SIP traffic for unexpected INVITE or BYE messages; look for discrepancies in call IDs or sudden changes in RTP endpoints