Network Attacks and Their Signatures in Wireshark: A Guide

This guide provides a quick and concise overview of common network attacks, their characteristics, and how they might manifest in a Wireshark packet analysis. Network attacks are pervasive threats in the digital landscape, targeting individuals, businesses, and even governments. These attacks exploit network vulnerabilities to compromise system integrity, breach data confidentiality, and impair availability of services. The ability to identify and understand these attacks is critical in today's cybersecurity landscape.

Wireshark, as a leading network protocol analyzer, can be an invaluable tool in recognizing the hallmarks of these network threats. By examining network packet data, one can spot anomalies or patterns indicative of a potential network attack. Although Wireshark isn't inherently a security tool and cannot mitigate these threats, it plays an essential role in security analysis and forensics.

This guide empowers you to understand, detect, and ultimately contribute to the mitigation strategies for these threats in your network environment.

Attack Name	**Attack Features**	**Attack Signatures**
DDoS Attacks (Distributed Denial of Service)	• This involves overwhelming a network or system with a flood of internet traffic. It is one of the most common forms of network attack. • These attacks are designed to overwhelm a system's resources, making it unable to respond to any other requests. A DDoS attack is a DoS attack that comes from multiple devices at once.	• Look for unusually high amounts of traffic. High volumes of traffic from a single IP address, or set of IP addresses, could indicate a DDoS attack/ • Filter the traffic by protocol (e.g., ICMP, TCP, or UDP) to identify the type of attack. For example, a large number of ICMP packets could be a sign of a Ping of Death or Smurf attack, while a high amount of TCP SYN packets could indicate a SYN flood attack. • Check the packet details. Unusually large packet sizes could indicate a form of DDoS attack, like a Ping of Death or fragmentation attack.
MITM Attacks (Man-in-the-Middle)	• Here, the attacker intercepts and potentially alters communication between two parties without their knowledge. • In these attacks, the attacker intercepts communication between two parties without their knowledge, potentially altering the communication.	• Look for duplicate packets: In many types of MITM attacks (like ARP spoofing), you'll see duplicate packets with different MAC addresses. This is a clear sign of a MITM attack. • Analyze ARP packets: ARP spoofing is a common way to perform MITM attacks. If you see ARP replies from a machine that did not request it, this could be a sign of ARP spoofing. • Check for SSL/TLS inconsistencies: If you're analyzing HTTPS traffic and you see a different certificate being presented or any TLS handshake anomalies, that could indicate a MITM attack.
Phishing and Spear Phishing Attacks	• This is an attack that involves tricking the email recipient into disclosing confidential information such as passwords and credit card numbers.	• Filter traffic by HTTP or HTTPS to check for communication with known malicious websites (Xie, 2020). Look for GET requests to suspicious domains.

	• These attacks involve sending fraudulent emails or other messages that seem like they come from a trusted source, with the goal of getting the recipient to reveal sensitive information.	• Check for any DNS requests to suspected phishing domains. Phishing attacks often involve domains that resemble legitimate ones but with slight spelling differences. • Check the details of any SSL/TLS traffic. Phishing sites often use self-signed certificates or certificates that don't match the domain name.
Drive-by download attacks	• This type of attack occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without their consent	• Filter traffic by HTTP or HTTPS to check for communication with suspicious or known malicious websites • Look for a large number of packets sent to or received from a specific IP address or set of IP addresses. • Check for file downloads, especially executable files (.exe, .dll, .jar, etc.) or files commonly associated with exploits (.swf for Flash, .pdf for Adobe Reader, etc.).
Password attacks	• These involve trying to gain unauthorized access to a system by guessing or cracking users' passwords. This could be done by brute force (trying many different options until one works) or by using a list of commonly used passwords. • Here, the attacker attempts to obtain or bypass users' passwords using various techniques such as brute force, dictionary attacks, or keyloggers.	• Look for multiple unsuccessful login attempts from the same IP address within a short period of time. These could indicate a brute force or dictionary attack (Peltier, 2016). • Filter traffic by protocol (e.g., HTTP, HTTPS, FTP, SSH, Telnet) to inspect login activities. • Watch out for unencrypted protocols (e.g., HTTP, Telnet, FTP) transmitting credentials in plaintext.
SQL Injection	• This involves inserting malicious SQL code into a database query. If successful, this could allow the attacker to view, manipulate, or delete data. • This is a code injection technique that attackers use to attack data-driven applications by inserting malicious SQL statements into entry fields for execution.	• Look for packets with contents like ' OR '1'='1, ; DROP TABLE, or other suspicious SQL queries (Clarke, 2014). (Use Wireshark's "Find Packet" feature to search for these strings.) • Filter for HTTP or HTTPS traffic and look for GET and POST requests that contain these suspicious SQL queries.
Cross-site Scripting (XSS)	• This is a type of injection attack in which malicious scripts are injected	• Look for suspicious packets: In an XSS attack, the attacker injects malicious scripts into web pages viewed by other users. You would be looking for HTTP

	into trusted websites. Unlike other web attacks, XSS targets the user rather than the application itself.	GET or POST requests that contain these scripts. This would typically be in the form of Javascript code included in the URL or body of the HTTP request. • This could be things like "<script>", "alert(", "onload", "onerror", "<img", "src=x" in URLs or form data. These are not necessarily attacks, but could potentially be part of an XSS attack. • The specifics will depend on the nature of the XSS attack. It could be a simple alert popup, or a more complex attack that steals session cookies or defaces the website.
Malware attacks	• These attacks involve malicious software such as viruses, worms, trojans, ransomware, spyware, adware, and botnets. • Viruses: Self-replicating programs that attach themselves to clean file and spread throughout a computer system, infecting files with malicious code. • Trojans: Malware that disguises itself as a normal file or program to trick users into downloading and installing more malware. • Ransomware: A type of malware that encrypts the victim's files and demands a ransom to restore access. • Spyware: Software that enables attackers to obtain covert information about another's computer activities by transmitting data covertly from their hard drive. • Adware: Automatically delivers advertisements to a user's computer system. • Botnets: Networks of private computers infected with malicious	• Malware often communicates with a command-and-control (C2) server, which may involve connections to unusual IP addresses or ports, large or continuous data transfers, or communications at unusual times. If you have a list of known bad Ips (from threat intelligence feeds, for example), you can filter or search for these Ips using the Wireshark filter or search feature.

	software and controlled as a group without the owners' knowledge. • In this attack, malicious software infiltrates a computer or network and can cause damage or allow unauthorized access.	
ARP Spoofing	• In this type of attack, an attacker sends fake ARP messages to an Ethernet LAN. This links the attacker’s MAC address with the IP address of a legitimate computer or server on the network. • Where an attacker sends fake ARP messages onto a Local Area Network in order to link their MAC address with the IP address of a legitimate computer or server on the network.	• Look for suspicious ARP packets: In a normal network, you will see two types of ARP packets - ARP Request and ARP Reply. An ARP Spoofing attack can be identified by observing multiple ARP Reply packets being sent without a corresponding ARP Request. • Check for duplicate MAC addresses: If you see different IP addresses associated with the same MAC address (unless it's a multi-homed device or there's some form of network address translation), this could be a sign of an ARP Spoofing attack. In Wireshark, you can use the "Endpoints" list (Statistics -> Endpoints) to quickly identify duplicate MAC addresses.
DNS Spoofing/DNS Cache Poisoning	• This involves corrupting the domain name system, redirecting internet traffic away from its intended destination. • In this type of attack, an attacker introduces corrupt Domain Name System (DNS) cache information to divert traffic to their own IP.	• Look for suspicious DNS responses: DNS Spoofing often involves sending multiple DNS responses to a request, in the hope that the DNS server will accept the malicious response. Look for multiple responses to a single request, especially if they provide different IP addresses. • Check the time between request and response: In a DNS Spoofing attack, the attacker needs to respond to a DNS request before the legitimate DNS server. Therefore, an unusually quick DNS response could be a sign of DNS Spoofing.
Eavesdropping Attack (Passive Attack)	• This involves the attacker intercepting information transmitted over the network. • Also known as sniffing or snooping, the attacker passively intercepts data traveling through the network to gather information and personal details.	• Look for unencrypted sensitive data: An eavesdropper can easily intercept unencrypted traffic, so check if sensitive data like usernames, passwords, or personal details are being sent in plain text. Use Wireshark's "Follow TCP Stream" feature to easily view the contents of TCP sessions. • Check the use of insecure protocols: Protocols like HTTP, FTP, Telnet, and others send data in clear text, making them vulnerable to eavesdropping. Using Wireshark, you can filter for these protocols to identify their usage in your network. • Analyze the network for insecure practices: For instance, you could look for evidence of misconfigured network devices that are broadcasting sensitive information.

IP Spoofing	• In this type of attack, an attacker sends IP packets from a false (or “spoofed”) source address in order to hide their identity, impersonate another computing system, or both.	• Unusual increase in traffic from a particular IP address. • A large number of SYN packets which might indicate a SYN flood attack, a type of DoS attack often associated with IP spoofing.
Zero-Day	• This attack occurs when a vulnerability in software or hardware is exploited by an attacker before the developer or manufacturer has released a patch. • This type of attack occurs the same day a network vulnerability becomes known, before a patch or solution is implemented. The attacker exploits the security breach before the vendor or those responsible can fix it.	• Unusually high volume of traffic, frequent connections to an unknown IP address, or unexpected types of packets.

Jane Pierre
Cybersecurity & Networking Fellow
Innovation Fellowship
The Knowledge House
May 2023