Identifying Web attacks trhough logs Glossary

1. **3 Way Handshake** – Process that TCP uses to establish a connection between two hosts
2. **ACK –** Acknowledge TCP flag
3. **Attacker –** A person or group of people that attack a network, application or system
4. **Internet** - A huge network composed of many interconnected smaller networks
5. **Browser –** A computer program used to access Web Applications
6. **Client-Server Model** – Model that consists of a client requesting information from a server
7. **DVWA –** Damn Vulnerable Web Application
8. **Decode** – Reversing the encoding process
9. **Encode** – Process to change how a message looks without changing its content
10. **HTML (Hypertext markup language) –** Default Language to build Web Pages and Web Applications
11. **HTTP (Hypertext Transfer Protocol)** – Protocol used to send web data through networks like the internet.
12. **HTTP Methods –** The action of the user agent (GET, POST,…)
13. **HTTP Status Code –** 3 number codes generated by a Web Server to describe its action
14. **HTTP Referer** – The page the client was at when the request was executed
15. **IDS (Intrusion Detection System) –** A device or application that monitors a network or systems to identify policy violations or malicious activity based on signatures or traffic anomalies
16. **IETF –** Internet Engineering Task Force
17. **IP (Internet Protocol) –** Set of rules used to address and route traffic by assigning a computer a unique identifying address so data knows where to go – there are two versions: version 4 and version 6
18. **IPS (Intrusion Prevention System) –** A machine that reads packets and identifies and blocks attacks based on signatures or rules.
19. **LFI –** Local File Inclusion
20. **Log –** A full written record of a journey, a period of time, or an event

21. **Multi-Layer Architecture –** Architecture that consists of many separate layers that all have independent functions. Communication is allowed between adjacent layers
22. **NOC –** Network Operations Center
23. **OSI Model (Open System Interconnection Model) –** Model that standardizes the communication functions of network layers based on ISO (International Organization for Standardization).
24. **OWASP –** Open Web Application Security Project – owasp.org
25. **OWASPBWA –** OWASP Broken Web Application Project
26. **PHP (Hypertext Preprocessor) –** Programming language commonly used to build Web Applications
27. **Risk –** "the possibility of something bad happening" – Cambridge Dictionary.
28. **RFC (Request for comments) –** Document format from IETF that describes a technology
29. **RFC1413** – Identification Protocol - https://tools.ietf.org/html/rfc1413
30. **RFI –** Remote File Inclusion
31. **SOC –** Security Operations Center
32. **SQL –** Structured Query Language
33. **SYN –** Synchronize TCP flag
34. **Syslog (System Logging Protocol) –** Protocol that provides a method for send event data to a logging server.
35. **Syslog Server –** A dedicated server to store logs
36. **TCP –** Transport Control Protocol
37. **TCP/IP Model –** A network model based on OSI that describes networks layers
38. **User Agent –** A unique string that contains technical information about the device and web client that sent the request
39. **URI –** Universal Resource Identifier
40. **URL –** Uniform Resource Locator
41. **Vulnerability -** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat. (*https://csrc.nist.gov/glossary/term/vulnerability*)
42. **XSS –** Cross-Site Script
43. **WAF (Web Application Firewall) –** A specific type of firewall. Specialized in detecting and blocking Web Application Attacks.
44. **WEB Application –** Applications that run on Web Servers
45. **Web Server –** Usually a dedicated Server that runs web applications
46. **WWW (World Wide Web)** A specific portion of the Internet known as the Web