ASSIST

CYBERSECURITY GLOSSARY

100 Essential Cybersecurity Terms

Erasmus+ KA210-ADU Project
2023-1-TR01-KA210-ADU-000165733

Erasmus+

THREATS - Malicious Software

1. **Virus** - Malicious software that infects computers and replicates itself to damage files.
2. **Worm** - Self-replicating malware that spreads automatically through networks.
3. **Trojan Horse** - Malware disguised as legitimate software that performs harmful actions.
4. **Ransomware** - Malware that encrypts files and demands payment for decryption.
5. **Spyware** - Software that secretly collects user information and activities.
6. **Adware** - Software that displays unwanted advertisements and slows browsers.
7. **Rootkit** - Malware that hides deep in the system to gain complete control.
8. **Keylogger** - Software that records keystrokes to steal passwords and data.
9. **Botnet** - Network of infected computers controlled remotely by hackers.
10. **Malware** - General term for malicious software including viruses, worms, trojans.
11. **Zero-Day** - Newly discovered security vulnerability with no available patch.
12. **Exploit** - Code or technique that takes advantage of security vulnerabilities.
13. **Backdoor** - Hidden access point allowing unauthorized entry to a system.
14. **RAT** - Remote Access Trojan. Allows complete remote control of a computer.
15. **Cryptojacking** - Unauthorized use of someone's computer for cryptocurrency mining.
16. **Scareware** - Fake security warnings designed to frighten users into paying.
17. **Logic Bomb** - Malicious code that activates when specific conditions are met.
18. **Fileless Malware** - Malware operating in memory without leaving files on disk.
19. **Dropper** - Program designed to download and install other malware.

20 **Wiper** - Malware that permanently destroys data beyond recovery.

ATTACKS - Cyber Attack Techniques

21 **Phishing** - Fraudulent attempts to steal information via fake emails or websites.

22 **Smishing** - Phishing attack conducted through SMS text messages.

23 **Vishing** - Voice phishing attack conducted through phone calls.

24 **Spear Phishing** - Targeted phishing attack aimed at specific individuals or organizations.

25 **Whaling** - Phishing attack specifically targeting high-level executives.

26 **DDoS** - Distributed Denial of Service. Attack from multiple sources to overwhelm systems.

27 **DoS** - Denial of Service. Attack that makes a system unavailable.

28 **Man-in-the-Middle** - Attack that secretly intercepts communication between two parties.

29 **SQL Injection** - Attack that inserts malicious SQL code into database queries.

30 **XSS** - Cross-Site Scripting. Injecting malicious scripts into websites.

31 **Brute Force** - Attack trying all possible password combinations systematically.

32 **Dictionary Attack** - Attack using a list of common passwords to guess credentials.

33 **Credential Stuffing** - Using stolen credentials to attempt access on other sites.

34 **Session Hijacking** - Taking over an active session to gain unauthorized access.

35 **DNS Spoofing** - Manipulating DNS records to redirect users to fake websites.

36 **ARP Spoofing** - Manipulating ARP tables to intercept network traffic.

37 **Pharming** - Redirecting users to fraudulent websites through DNS manipulation.

38 **Social Engineering** - Manipulating people psychologically to reveal information.

39 **Baiting** - Luring victims with promises of free items or rewards.

40 **Pretexting** - Creating a fake scenario to gain trust and extract information.

PROTECTION - Security Measures

41 **Antivirus** - Security software that detects and removes malicious programs.

42 **Firewall** - Security system that monitors and controls network traffic.

43 **2FA** - Two-Factor Authentication. Additional security verification layer.

44 **MFA** - Multi-Factor Authentication. Multiple verification methods.

45 **Encryption** - Converting data into unreadable code for protection.

46 **SSL/TLS** - Protocols that encrypt internet traffic for secure connections.

47 **HTTPS** - Secure HTTP protocol with encrypted web connections.

48 **VPN** - Virtual Private Network. Encrypts and anonymizes internet traffic.

49 **Backup** - Creating copies of data for protection against loss.

50 **Update** - Keeping software current to fix security vulnerabilities.

51 **Password Manager** - Application that securely stores and manages passwords.

52 **Sandbox** - Isolated environment for safely testing suspicious files.

53 **IDS** - Intrusion Detection System. Monitors for suspicious activities.

54 **IPS** - Intrusion Prevention System. Detects and blocks attacks.

55 **WAF** - Web Application Firewall. Protects web applications.

56 **Endpoint Security** - Protection for computers and devices on a network.

57 **Zero Trust** - Security approach: never trust, always verify.

58 **Patch** - Software update that fixes bugs and security flaws.

59 **Whitelist** - Allowing only approved applications or addresses.

60 **Blacklist** - Blocking known malicious sites or software.

TOOLS - Technology & Infrastructure

61 **IP Address** - Unique numerical identifier for devices on the internet.

62 **MAC Address** - Unique physical address of a network interface card.

63 **DNS** - Domain Name System. Translates domain names to IP addresses.

64 **Router** - Device that directs network traffic between networks.

65 **Proxy** - Intermediary server that forwards internet requests.

66 **Port** - Virtual connection point for network communications.

67 **Protocol** - Rules for communication between devices. HTTP, FTP, TCP.

68 **Cookie** - Small data files stored by websites in your browser.

69 **Cache** - Temporary storage of data for faster access.

70 **Token** - Digital key used for authentication purposes.

71 **Hash** - Fixed-length value generated from data. Digital fingerprint.

72 **API** - Application Programming Interface. Allows software communication.

73 **Cloud** - Remote server services accessed over the internet.

74 **Metadata** - Data that provides information about other data.

75 **Bandwidth** - Data transfer capacity of a network connection.

76 **Latency** - Delay time in data transmission.

77 **Ping** - Command to test network connectivity.

78 **Traceroute** - Tool showing the path data packets travel.

79 **Tor** - Network enabling anonymous internet browsing.

80 **Dark Web** - Hidden part of internet accessible with special software.

CONCEPTS - Fundamental Knowledge

81 **Cybersecurity** - Practice of protecting digital systems and data from threats.

82 **Data Breach** - Unauthorized access to sensitive or confidential data.

83 **Identity Theft** - Stealing someone's personal information for fraudulent use.

84 **Spam** - Unwanted bulk emails or messages.

85 **CAPTCHA** - Test to distinguish humans from automated bots.

86 **Privacy** - Protection of personal information from unauthorized access.

87 **Anonymous** - Having an unknown or hidden identity online.

88 **Open Source** - Software with publicly available source code.

89 **Penetration Test** - Authorized simulated attack to test security. Pentest.

90 **Vulnerability** - Weakness in a system that can be exploited.

91 **Risk** - Assessment of potential threats and their impact.

92 **Compliance** - Adherence to security standards and regulations.

93 **GDPR** - General Data Protection Regulation. EU data protection law.

94 **Cyber Attack** - Deliberate attempt to damage or disrupt digital systems.

95 **Hacker** - Person who breaks into computer systems. Ethical or malicious.

96 **White Hat** - Ethical hacker who tests security with permission.

97 **Black Hat** - Malicious hacker who breaks into systems illegally.

98 **Bug Bounty** - Program rewarding people who find security vulnerabilities.

99 **Digital Footprint** - Traces and data left behind from internet activities.

100 **Cyber Hygiene** - Best practices for maintaining digital security.