

Top 50 Cybersecurity Acronyms You Should Know

- 1. DoS (Denial of Service):** Service interruption from bugs or vulnerabilities.
- 2. DDoS (Distributed Denial of Service):**
A flood of traffic meant to overload resources and cause them to crash.
- 3. CVE (Common Vulnerabilities and Exposures):**
A database of known vulnerabilities found in various open-market software.
- 4. DNS (Domain Name Service):** is one of the Internet's backbone protocols for translating domain names to IP addresses.
- 5. FQDN (Fully Qualified Domain Name):**
This is a friendly domain name for web services linked to an IP address.
- 6. SSH (Secure Shell):** An encrypted remote-control protocol for controlling servers and other network equipment.
- 7. RCE (Remote Code Execution):** An exploit allowing for execution of malicious code.
- 8. XSS (Cross-Site Scripting):** A web vulnerability allowing for the injection of malicious scripts.
- 9. IDS (Intrusion Detection System):** Background procedures monitoring an environment for anomalies in network traffic.
- 10. IPS (Intrusion Prevention System):**
A system that proactively blocks and contains anomalies in network traffic.
- 11. JWT (JSON Web Token):** Tokens are sent to a web application for authentication and authorization.
- 12. MitM (Man in the Middle):** Interception of a web data transfer to eavesdrop on traffic.
- 13. MFA (Multifactor Authentication):** An added layer of authentication requirements to improve the protection of accounts.
- 14. EPP (Endpoint Protection Platform):**
Infrastructure used to protect vulnerable endpoints such as smartphones or laptops.
- 15. VPN (Virtual Private Network):** A tunneling service that adds data encryption between a user endpoint and the internal network.
- 16. AV (Antivirus):** Software running on a server or user device that prevents malicious code from executing on the local machine.
- 17. SOC (Security Operation Center):** An enterprise team with a group of security analysts reviewing and investigating potential cyber-events.
- 18. ZTNA (Zero-Trust Network Access):** is a methodology for improving security by always validating resource requests for authorized access.
- 19. C2 (Command and Control):** Malware used to remotely control a device and send data back to a central attacker-controlled server.
- 20. IR (Incident Response):** A process to contain, eradicate, and investigate a cyber-incident.
- 21. TI (Threat Intelligence):** The collection of information from various darknet locations and cleanest sources to better understand zero-day threats and the cybersecurity landscape.
- 22. INFOSEC (Information Security):** A general term for information security.
- 23. IPSec (IP Security):** A set of rules created to define how security and encryption perform over an IP network.
- 24. NIST (National Institute of Standards and Technology):** A US institute that creates best practices and methodologies for better data security.
- 25. OPSEC (Operational Security):** A general term used to refer to strategies for operational security.

Top 50 Cybersecurity Acronyms You Should Know

- 26. CISO (Chief Information Security Officer):** Enterprise employee overseeing cybersecurity and data protection.
- 27. Pen-Test (Penetration Testing):** Finding corporate software and hardware vulnerabilities.
- 28. SAST (Static Application Security Testing):** Whitebox detection of finding vulnerabilities, usually done as developers create their code.
- 29. DAST (Dynamic Application Security Testing):** Blackbox testing deployed applications using scripts and methods like attackers.
- 30. RFI (Remote File Inclusion):** An exploit to add a malicious file for execution against a remote site.
- 31. LFI (Local File Inclusion):** An exploit in web applications to access sensitive files remotely.
- 32. VLAN (Virtual Local Area Network):** Virtual networks running on physical switches that could be misconfigured to allow unauthorized access.
- 33. OD (Zero-Day):** A vulnerability or exploit unseen in the wild and often used to bypass security scanners.
- 34. CI (Command Injection):** Exploits such as SQL injection or LDAP injection are used to inject malicious commands into a server or application.
- 35. LDAP (Lightweight Directory Access Protocol):** A protocol to authenticate users to a directory of resources shared in a heterogeneous environment.
- 36. NAT (Network Address Translation):** is a translation tool for turning private, unrouteable IP addresses into public addresses.
- 37. CTF (Capture the Flag):** A game played by hackers to improve their skills and compete with other experienced hackers.
- 38. ACL (Access Control List):** A list of rules to disallow or allow specific protocols or ports often used on a router.
- 39. RAT (Remote Access Trojan):** Malware installed on a targeted system allows an attacker to control or exfiltrate data.
- 40. APT (Advanced Persistent Threat):** Malware or exploits that can often bypass common security controls with backdoors to avoid complete eradication.
- 41. RDP (Remote Desktop Protocol):** A Microsoft Windows protocol that remotely controls a Windows-based server or desktop.
- 42. HTTPS (Hypertext Transfer Protocol Secure):** is a secure way to transfer data between two devices using the HTTP protocol.
- 43. CSP (Content Security Policy):** Server headers limit executable code from loading on pages such as JavaScript or CSS.
- 44. DLP (Data Loss Prevention):** Methodologies and best practices for preventing data loss from cyber-risks and vulnerabilities.
- 45. DRAAS (Disaster Recovery as a Service):** Cloud-based services used to protect data from loss after downtime and application failure.
- 46. SANS (SysAdmin, Audit, Network, and Security):** An institution for training cybersecurity professionals and guiding best practices and policies.
- 47. SSID (Service Set Identifier):** An identification value broadcasted by Wi-Fi routers to offer user connections.
- 48. PUP (Potentially Unwanted Program):** Unwanted software is usually downloaded to a local device but causes malicious behavior, such as adware or spyware.
- 49. DMARC (Domain-Based Message Authentication, Reporting, and Conformance):** A set of rules and methods to validate email senders and stop spam.
- 50. SPF (Sender Policy Framework):** is an email authentication protocol that helps prevent email spoofing, a common tactic in phishing and spam. SPF allows receiving mail servers to verify if incoming emails are sent from a domain authorized by that domain's administrator.