Network Security Tools & Technologies 💻🛡️

Network Security | Tools | Cybersecurity | Technologies

- Port Scanning & Enumeration
  - Nmap: Port scanning, OS detection, NSE scripting.
    - Comprehensive port scanner, OS fingerprinting, and vulnerability detection through NSE scripts.
  - Netcat: Network utility for banner grabbing and tunneling.
    - Versatile networking tool for reading/writing data across network connections; useful for banner grabbing and establishing secure tunnels.
  - Masscan: Ultra-fast port scanner.
    - Extremely fast port scanner ideal for large-scale scans, covering a wide range of ports quickly.
- Packet Sniffing & Analysis
  - Wireshark: GUI-based protocol analyzer.
    - Powerful and widely used network protocol analyzer with a graphical user interface, enabling detailed packet inspection.
  - tcpdump: CLI-based packet sniffer.
    - Command-line based packet capture tool that offers powerful filtering and capturing capabilities.
  - Tshark: Terminal version of Wireshark.
    - Command-line version of Wireshark, providing similar functionality but through the terminal.
- Vulnerability Scanning
  - Nessus: Commercial vulnerability scanner.
    - Comprehensive commercial vulnerability scanner offering a wide range of vulnerability checks and reporting features.
  - OpenVAS: Open-source alternative.
    - Open-source vulnerability scanner similar to Nessus, offering many of the same features but without the commercial cost.
  - Nikto: Web server vulnerability scanner.
    - Specialized scanner for detecting vulnerabilities in web servers, focusing on outdated software and insecure configurations.
- Exploitation & Penetration Testing
  - Metasploit: Framework for payloads and post-exploitation.
    - Penetration testing framework providing a vast library of exploits and tools for assessing system vulnerabilities and gaining unauthorized access.
  - Hydra: Brute-force login cracker.
    - Tool used for attempting to guess passwords through brute-force attacks against various services.
  - SQLmap: Automated SQL injection tool.
    - Automated tool for detecting and exploiting SQL injection vulnerabilities in web applications.
  - Responder: LLMNR/NBT-NS poisoning tool.
    - Tool that exploits weaknesses in the LLMNR and NBT-NS protocols to capture network credentials.
- Password Cracking
  - John the Ripper: Offline password cracker.
    - Popular offline password cracker capable of testing various password hashes.
  - Hashcat: GPU-accelerated password recovery.
    - High-performance password recovery tool that leverages the power of GPUs for significantly faster cracking speeds.
- Web Application Security
  - Burp Suite: Web app pentest suite.
    - Comprehensive suite of tools for penetration testing web applications, including proxy, scanner, and repeater functions.
  - OWASP ZAP: Open-source web scanner.
    - Open-source web application security scanner, useful for detecting a wide range of vulnerabilities.
  - Dirb/Dirbuster: Directory brute-force tools.
    - Tools used to automatically attempt to guess directory paths on a web server, potentially uncovering hidden files or directories.
- Network Monitoring & IDS/IPS
  - Snort: Signature-based IDS.
    - Network intrusion detection system that relies on predefined signatures to identify malicious network traffic.
  - Suricata: Multi-threaded IDS/IPS engine.
    - High-performance intrusion detection and prevention system capable of handling large volumes of network traffic.
  - Zeek (Bro): Network behavior analysis tool.
    - Network security monitor that analyzes network traffic patterns to identify suspicious activities.
- Forensics & Incident Response
  - Volatility: Memory forensics.
    - Framework for analyzing computer memory images to recover data and evidence related to security incidents.
  - Autopsy: GUI-based digital forensics tool.
    - Graphical user interface-based digital forensics platform aiding in the analysis and investigation of digital evidence.
- Wireless Security
  - Aircrack-ng: Wi-Fi monitoring and cracking.
    - Suite of tools for monitoring and cracking Wi-Fi networks, useful for penetration testing and security assessments.
  - Kismet: Wireless network detector/sniffer.
    - Wireless network detector that passively monitors wireless traffic and identifies nearby networks and their characteristics.
- Proxying & Tunneling
  - Proxychains: Forces applications through a proxy.
    - Tool that routes network connections through multiple proxies, enhancing anonymity and security.
  - Socat: Data relay for tunneling and pivoting.
    - Versatile tool for creating data relays, often used to establish secure tunnels and facilitate pivoting within networks.
- Anonymity & VPNs
  - Tor: Anonymous browsing and routing.
    - Network that enables anonymous communication by routing internet traffic through multiple relays, masking the user's IP address.
  - I2P: Anonymous P2P network.
    - Anonymous peer-to-peer network that provides anonymous communication and data sharing.
  - OpenVPN: Secure VPN tunneling protocol.
    - Open-source VPN protocol used to create secure encrypted connections between devices, commonly used for secure remote access.
- Log Management & SIEM
  - Syslog: Logging protocol for systems/devices.
    - Standard protocol for transmitting log messages from various systems and devices to a central logging server.
  - Graylog: Centralized log management.
    - Open-source log management system for collecting, processing, and analyzing log data from various sources.
  - ELK Stack: Logstash + Elasticsearch + Kibana.
    - Popular open-source log management and analysis suite consisting of Logstash (log processing), Elasticsearch (search and storage), and Kibana (visualization).
  - Splunk: Commercial SIEM and analytics tool.
    - Commercial security information and event management (SIEM) platform offering advanced log analysis and security monitoring capabilities.
  - Wazuh: Open-source SIEM, FIM, threat detection.
    - Open-source SIEM, file integrity monitoring (FIM), and threat detection platform.
  - Security Onion: Complete NSM platform.
    - Comprehensive network security monitoring (NSM) platform that integrates several open-source tools for security analysis.
  - AlienVault OSSIM: Open-source SIEM solution.
    - Open-source SIEM solution providing log management, vulnerability assessment, and security information management functionalities.