Cyber Security Tools

Sure, here is a list of some widely-used cybersecurity tools categorized by their primary functions:

**Network Security**

1. **Wireshark**
   * A network protocol analyzer used for network troubleshooting, analysis, and protocol development.
2. **Nmap**
   * A network scanning tool that is used for network discovery and security auditing.
3. **Snort**
   * An open-source network intrusion detection system (NIDS) capable of performing real-time traffic analysis and packet logging.
4. **Zeek (formerly Bro)**
   * A network analysis framework that focuses on network security monitoring.
5. **Nagios**
   * An open-source monitoring tool for network infrastructure.

**Endpoint Security**

1. **OSSEC**
   * An open-source host-based intrusion detection system (HIDS) that performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response.
2. **Tripwire**
   * A tool that monitors and alerts on specific file changes on a range of systems and devices.
3. **ClamAV**
   * An open-source antivirus engine for detecting trojans, viruses, malware, and other malicious threats.

**Penetration Testing**

1. **Metasploit**
   * A penetration testing framework that helps security professionals find, exploit, and validate vulnerabilities.
2. **Kali Linux**
   * A Debian-based Linux distribution designed for digital forensics and penetration testing, pre-installed with numerous penetration testing tools.
3. **Burp Suite**
   * An integrated platform for performing security testing of web applications.
4. **John the Ripper**
   * A fast password cracker available for many operating systems.
5. **Aircrack-ng**
   * A suite of tools for assessing Wi-Fi network security.

**Vulnerability Management**

1. **OpenVAS**
   * An open-source framework of several services and tools offering vulnerability scanning and vulnerability management.
2. **Nessus**
   * A proprietary vulnerability scanner developed by Tenable, Inc.
3. **QualysGuard**
   * A cloud-based suite of tools for asset discovery, security assessment, and vulnerability management.

**Security Information and Event Management (SIEM)**

1. **Splunk**
   * A platform for searching, monitoring, and analyzing machine-generated data via a web-style interface.
2. **ELK Stack (Elasticsearch, Logstash, Kibana)**
   * A collection of three open-source products for search, logging, and visualization of data.
3. **QRadar**
   * IBM's SIEM tool for log management and security analytics.
4. **AlienVault OSSIM**
   * An open-source SIEM tool that provides event collection, normalization, and correlation.

**Web Security**

1. **OWASP ZAP (Zed Attack Proxy)**
   * An open-source web application security scanner.
2. **Netsparker**
   * A web application security scanner that identifies vulnerabilities such as SQL Injection and Cross-site Scripting (XSS).
3. **Acunetix**
   * An automated web application security testing tool.

**Encryption**

1. **GnuPG**
   * A complete and free implementation of the OpenPGP standard for encrypting and signing data and communications.
2. **VeraCrypt**
   * An open-source disk encryption software.
3. **BitLocker**
   * A full volume encryption feature included with Microsoft Windows.

**Incident Response**

1. **TheHive**
   * A scalable, open-source Security Incident Response Platform (SIRP).
2. **Cortex**
   * An open-source tool that allows analysts to analyze collected digital artifacts.
3. **Cuckoo Sandbox**
   * An open-source automated malware analysis system.

**Forensics**

1. **Autopsy**
   * An open-source digital forensics platform and graphical interface to The Sleuth Kit.
2. **FTK Imager**
   * A forensic imaging tool for disk image creation and analysis.
3. **Volatility**
   * An open-source memory forensics framework for incident response and malware analysis.

**Firewall and IDS/IPS**

1. **pfSense**
   * An open-source firewall and router software distribution.
2. **Suricata**
   * An open-source network threat detection engine capable of real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline packet capture (PCAP) processing.
3. **iptables**
   * A user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel firewall.

**Email Security**

1. **SpamAssassin**
   * An open-source platform for email filtering that uses a variety of spam detection techniques.
2. **PhishTank**
   * A collaborative clearing house for data and information about phishing on the Internet.
3. **DMARC Analyzer**
   * A tool for implementing and monitoring DMARC (Domain-based Message Authentication, Reporting, and Conformance) policies.

**Endpoint Detection and Response (EDR)**

1. **CrowdStrike Falcon**
   * A cloud-delivered endpoint protection platform combining next-gen antivirus, endpoint detection and response (EDR), and a 24/7 managed hunting service.
2. **Carbon Black**
   * Provides endpoint security to prevent, detect, and respond to attacks.
3. **Cylance**
   * An AI-driven EDR solution that predicts and prevents known and unknown threats.

**Identity and Access Management**

1. **Okta**
   * An identity and access management service that provides single sign-on (SSO) and multi-factor authentication (MFA).
2. **Auth0**
   * A flexible, drop-in solution to add authentication and authorization services to applications.
3. **Keycloak**
   * An open-source identity and access management solution.

**Miscellaneous**

1. **Docker Bench for Security**
   * A script that checks for dozens of common best practices around deploying Docker containers in production.
2. **Lynis**
   * An open-source security auditing tool for Unix-based systems.
3. **Sysdig**
   * A powerful system-level exploration and troubleshooting tool for Linux.
4. **Nikto**
   * An open-source web server scanner which performs comprehensive tests against web servers for multiple items.
5. **Maltego**
   * An interactive data mining tool that renders directed graphs for link analysis.
6. **Shodan**
   * A search engine for Internet-connected devices and provides insights into what kind of devices are connected to the Internet, where they are located, and who is using them.