CYBER SECURITY TOOLS:

I) Network security monitoring tools:

1. Nagios: A free tool that monitors hosts, systems, and networks, and sends real-time alerts. It can track network resources such as HTTP, NNTP, ICMP, POP3, and SMTP.
2. Splunk: A cybersecurity software that monitors network security in real-time, and searches for threat data. It has a user interface for generating alerts, summaries, dashboards, and infographics.
3. Wireshark: An open-source penetration testing tool that monitors network activities and analyzes protocols.
4. Snort: A network intrusion detection system (IDS) that monitors network traffic in real-time. It examines every packet for potentially harmful payloads.
5. ManageEngine OpManager: A network monitoring tool that monitors devices such as routers, switches, firewalls, load balancers, and more.
6. Metasploit: A penetration testing tool that can test the security of computer systems, networks, and applications.
7. PRTG Network Monitor: A network monitoring tool that helps ensure that computer systems are working properly.

II) Encryption tools:

1. Micro Focus ZENworks FDE: A full disk encryption (FDE) solution that can be used to manage and enforce endpoint full-disk encryption.
2. Twofish: A free, fast symmetric encryption algorithm that uses a 128-bit key.
3. AxCrypt: A tool for simplified business file sharing.
4. NordLocker: A tool for cloud-based business file sharing.
5. Trend Micro Endpoint Encryption: A tool for managed business file sharing.

III) Web Vulnerability tools:

1. Burp Scanner: This tool can find vulnerabilities that other scanners might miss, such as asynchronous SQL injection and blind SSRF.
2. Rezonate: This tool scans web applications to identify potential flaws in authentication and permissions. It also provides a risk score for the web application's security.
3. Bright Security: This tool can scan web apps and APIs to help with regulatory compliance and DevSecOps. It provides actionable reports of vulnerabilities in real time.
4. RapidFire VulScan: This tool is designed for Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs). It offers a solution for vulnerability scanning and remediation.
5. Amazon Inspector: This tool scans applications deployed on Amazon and provides a list of potential vulnerabilities. It can perform assessments on both a network and a host level.

IV) Network Defense wireless tools:

1. Access control: A crucial part of security, access control prevents unauthorized access to systems and data. A strong password system is one way to boost access control measures.
2. Wireshark: A penetration testing tool that analyzes network and wireless traffic, including wireless over-the-air traffic.
3. Metasploit: A security software that contains tools for executing penetrating testing services.
4. Snort: A network intrusion detection system (IDS) that monitors network traffic in real-time and examines every packet for potentially harmful payloads.
5. Nessus: A vulnerability scanner that prevents hackers from attempting to access networks and scans for vulnerabilities that could allow remote hacking of sensitive data.

6. Aircrack-ng: A wireless security testing tool that identifies vulnerabilities in wireless networks and tests the security of wireless communication.
7. IDS system: An intrusion detection system that monitors activities on a computer system or network and analyzes them to recognize intrusions.

V) Packet sniffing tools, also known as **network analyzers, protocol analyzers, or packet analyzers**, monitor network traffic by examining data packets. They can provide information about the source and destination of packets, as well as the network protocols and packet length.

Examples of packet sniffing tools:

1. Wireshark: Captures packets and displays them in a list, with each packet labeled with a color to indicate the type of traffic.
2. NetworkMiner: An open-source Windows tool that can also capture packets on Linux, Mac OS X, and FreeBSD. It can perform passive network monitoring to track sessions, hostnames, and more.
3. Kismet: A wireless sniffer tool included with Kali Linux, it can detect networks, sniff packets, and perform intrusion detection for 802.11 wireless LANs.
4. Capsa: Monitors packets in real-time, displays data graphically, and logs data for future reference.
5. NetFlow Analyzer: An affordable packet sniffer that analyzes aggregated traffic data and provides insights.
6. Ettercap: An open-source packet sniffer that can modify data and run man-in-the-middle attacks.
7. Fiddler: A graphical packet sniffing tool that acts as a proxy between an application and remote services.
8. dSniff: A collection of tools that can parse application protocols and extract data.
9. EtherApe: A free and open-source tool that displays captured packets visually, rather than in text format.

VI) Firewall: There are several types of firewalls, including:

1. Packet filtering firewall: A firewall that uses security rules to filter incoming data packets and allow or block traffic.
2. Stateful inspection firewall: A firewall that monitors the state of active network connections to look for potential risks.
3. Cloud firewall: A virtual firewall that monitors and filters traffic for containers and VMs running in a cloud environment.
4. Hardware firewall: A firewall that uses hardware, such as a router, and software to block attackers on multiple computers.
5. Software firewall: A firewall that can be installed on individual computers and is often used by home users.
6. Internal firewall: A firewall that focuses on security threats within a network, such as traffic between devices.
7. Web application firewall (WAF): A cloud-based security solution that protects web applications from cyber threats like cross-site scripting (XSS) and SQL injection.
8. Circuit-level gateway: A firewall that quickly approves or denies traffic by verifying the transmission control protocol (TCP) handshake.
9. Application-level gateway firewall: A firewall that protects a specific Application Layer Protocol and works on the Application layer of the OSI model.

VII) Managed Detection and Response (MDR) services: use a combination of technology and human expertise to detect and respond to cyberattacks. Examples of MDR services include:

1. Threat detection: MDR services can continuously search for threats 24/7 to prevent malware and threats from hiding in systems.
2. Incident response: MDR services can provide 24/7 threat monitoring, risk analysis, and automated response orchestration to mitigate threats quickly.
3. Threat hunting: MDR services can proactively search for undetected intrusions within an organization's environment.
4. Endpoint Detection & Response (EDR): EDR solutions can monitor endpoints for threats, generate alerts, and respond to potential attacks.
5. CrowdStrike: CrowdStrike's platform is built for the cloud and can monitor cloud workloads, endpoints, and identities.
6. Alert Logic: Alert Logic's MDR service can provide threat detection, vulnerability assessment, and security recommendations for web applications and services hosted on cloud infrastructure.
7. Automated alerting: MDR services can automatically detect incidents and deploy security experts to review and classify the alert.

VIII) Public key infrastructure (PKI): is a security infrastructure that uses public and private keys to authenticate resources and establish identities on networks. Some examples of PKI services include:

1. SSL certificates: A common example of PKI implementation
2. S/MIME certificates: A common example of PKI implementation
3. Code signer certificates: A common example of PKI implementation
4. Digital signature certificates (DSC): A common example of PKI implementation
5. Authentication for IoT devices: A common example of PKI implementation
6. Microsoft Cloud PKI: A cloud-based service that automates certificate lifecycle management for Intune-managed devices
7. Dogtag Certificate System: An open-source certificate authority (CA) that supports many common PKI use cases

PKI is used in many industries, including BFSI, retail, government and defence, healthcare, telecom and IT, and manufacturing.

IX) Penetration testing tools: are used to simulate cyber-attacks on systems and networks to identify vulnerabilities and weaknesses. Security professionals and ethical hackers use these tools to: understand how cyber-attacks work, test the effectiveness of security measures, uncover new defects, and test the security of communication channels and integrations.

Some popular penetration testing tools include:

1. Metasploit: An open-source tool that helps identify flaws, set up a defence, and verify and manage security assessments.
2. Wireshark: A network protocol and packet analyser that inspects network and wireless traffic.
3. Nmap: An open-source tool that helps identify open ports and vulnerabilities in a network.
4. Burp Suite: A set of tools for penetration testing web applications that can be enhanced with add-ons.
5. Nessus: A tool that can identify and fix vulnerabilities in web applications and operating systems.
6. Sqlmap: An open-source tool that helps detect SQL injection vulnerabilities.
7. John the Ripper: A popular password-cracking tool that uses automated hash discovery and dictionary-based attacks.
8. Kali Linux: A Linux distribution with many pre-installed tools for uncovering vulnerabilities and weaknesses.