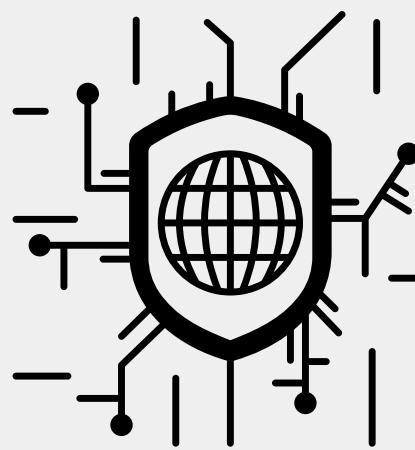




SECURITY TOOLS EXPLORATION

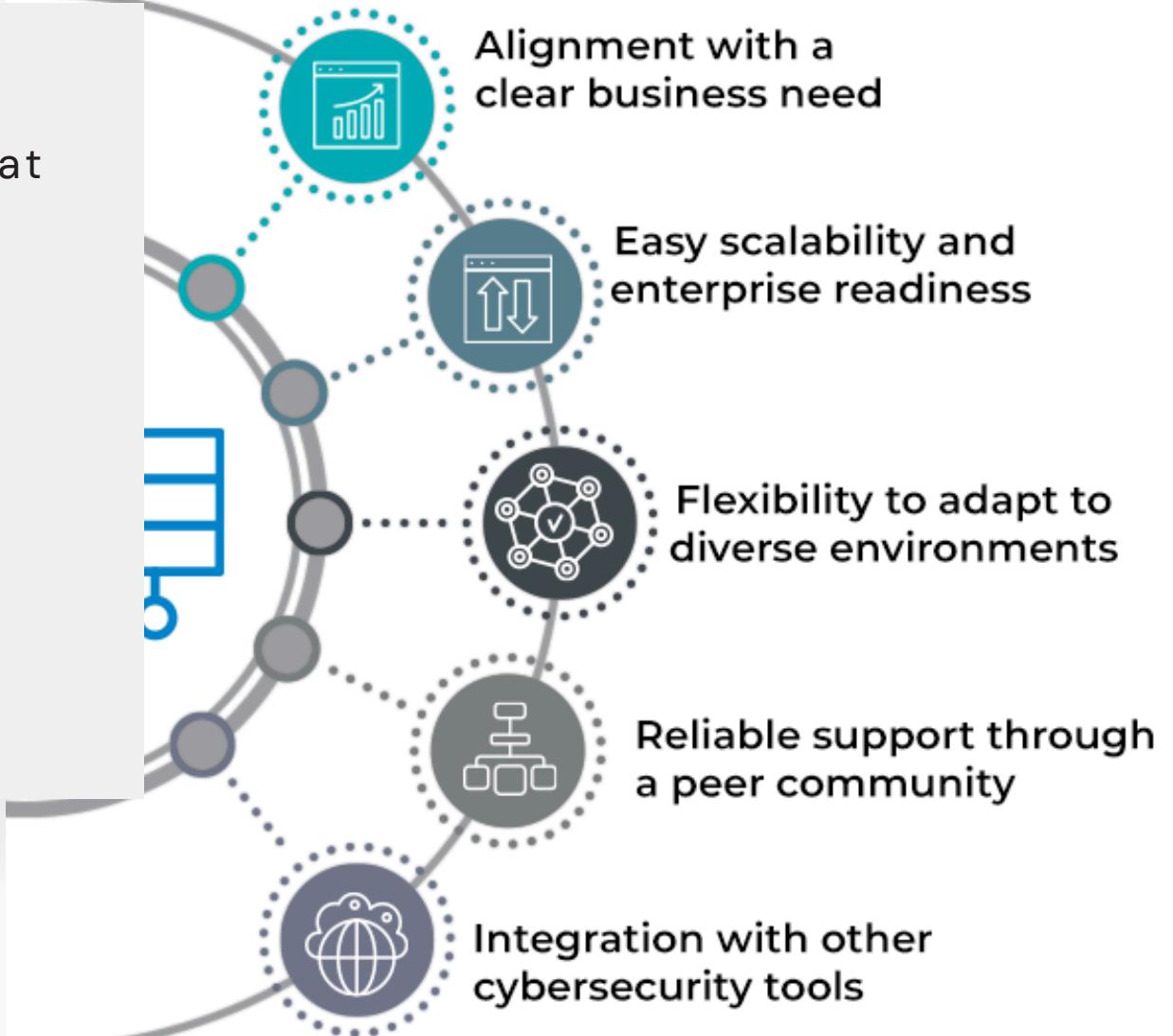
**PRESENTED BY- BSSE1405,BSSE1422,
BSSE1441,BSSE1443,
BSSE1445,BSSE1449**

ABOUT THE TOPIC



A security tool can be defined as a software or application that is used to identify and address vulnerabilities and threats in software development. These tools automate security testing and analysis, allowing flaws to be detected and fixed as soon as they are introduced, reducing the cost and effort required for remediation. They play a crucial role in ensuring the development of secure software by continuously inspecting the code for security issues throughout the software development life cycle.

MUST-HAVE FEATURES OF CYBERSECURITY TOOLS



WEBSITE SECURITY AND MONITORING TOOL: SITELOCK

SiteLock offers comprehensive website security to guard your site against malicious cyber threats, including web applications and your site code.

The service offers a range of security features, including daily website scans to identify threats, real-time notifications, and automated malware removal.

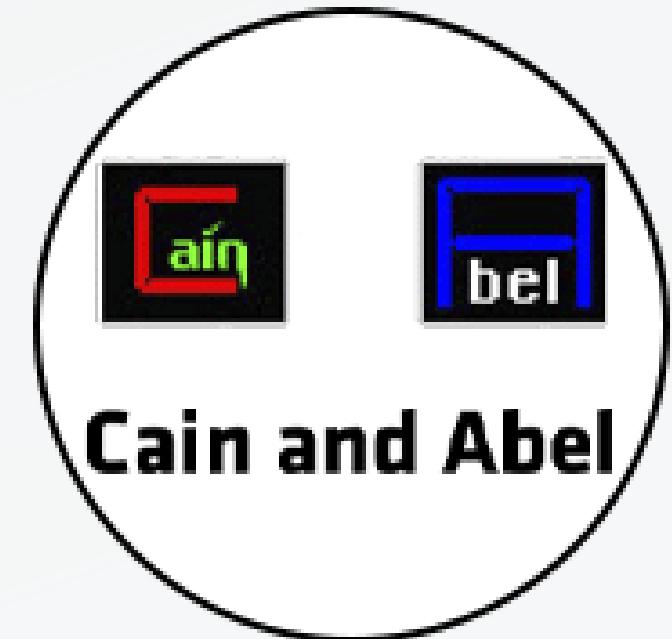
It includes tools like a web application firewall to intercept and block harmful traffic before it reaches the website, along with vulnerability and content management system (CMS)

Additionally, the service provides benefits such as a content delivery network (CDN) to boost site speed, potentially improving search engine optimization (SEO), and a firewall PCI report to aid eCommerce sites



PASSWORD RECOVERY TOOL: CAIN AND ABEL

Cain and Abel are one the oldest and best Cyber Security tools that help in identifying the weaknesses in Windows and password recovery. It allows Cyber Security experts to find vulnerabilities in the password security of various systems that run on Windows.



The tool can record VoIP communications, enabling users to monitor and analyze them for security purposes. This functionality aids in detecting any potential threats or breaches within voice-over-IP systems.

It has the capability to analyze routing protocols to assess the integrity of routed data packets. By scrutinizing these protocols, the tool can identify potential vulnerabilities or compromises in the network infrastructure.

The tool is adept at revealing sensitive information such as password boxes and cached passwords. Moreover, it can employ force attacks to crack encrypted passwords and decode scrambled passwords, enhancing its utility in password security assessment and management.

VULNERABILITY SCANNERS: ACUNETIX

Acunetix is a leading web vulnerability scanner used by cybersecurity professionals and organizations to identify and address security vulnerabilities in web applications and websites. It is designed to detect various types of security issues, such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities.

- 01**
- 02**
- 03**
- 04**
- 05**
- 06**

- Deep Scan Technology
- Vulnerability Assessment
- Intelligent Crawling
- Compliance Reporting
- Network Security Scans
- AcuSensor Technology



Acunetix

GOPHISH

Many of the costliest data breaches and ransomware attacks in recent years can be traced back to simple phishing campaigns because many company workers fall for them. One of the best protections is to secretly test your staff to see who is gullible, and for that you can use the free program Gophish. Gophish is open source and provides a full-featured toolkit for security administrators to build their own phishing campaigns with relative ease.



Gophish enables users to simulate various types of phishing attacks effectively. By replicating real-world scenarios

Its design aims to facilitate the setup and execution of phishing engagements and security awareness training.

The toolkit offers a user-friendly interface, allowing users to quickly and easily set up and execute phishing campaigns. Its intuitive design simplifies the process of simulating real-world phishing attacks, making it accessible to a wide range of users, including those without extensive technical expertise.

AIRCRACK-NG

This tool consists of numerous methods that help in analyzing the vulnerabilities of Wi-Fi security. Experts use Aircrack-ng to gather data packets connected through a network and to export these data packets to understandable text files that can go through various security assessments.

Tool's Services:

- 1.Wi-Fi Network Scanning
- 2.Packet Capture
- 3.Packet Injection
- 4.WEP/WPA/WPA2 Cracking
- 5.Dictionary and Brute-Force Attacks
- 6.Security Auditing



NETWORK INTRUSION DETECTION SOFTWARES

SNORT



Snort is referred to as a packet sniffer that monitors network traffic, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies.

- 01** **REAL-TIME TRAFFIC ANALYSIS**
- 02** **PACKET LOGGING**
- 03** **INTRUSION DETECTION**
- 04** **INTRUSION PREVENTION (OPTIONAL)**

Encryption Software

AxCrypt

For advanced encryption presented in a straightforward way, AxCrypt has served customers around the world for 20-plus years.

With plans tailored both for private users and organizations, AxCrypt provides file security with 128-bit or 256-bit encryption as well as cloud storage awareness and key sharing features that will help companies comply with data.



Features

- File Encryption
- Integration with File Systems
- Password Management
- File Shredding
- Multi-platform Support
- Collaboration and Sharing
- Free and Premium Versions

Penetration Testing Software

Metasploit

Tool's Services:

Metasploit offers a range of services and modules tailored to different stages of the penetration testing process:

- Module Exploitation
- Payload Development
- Post-Exploitation Framework
- Auxiliary Modules
- Integration and Automation



Firewall Softwares

PfSense



The firewall/router software pfSense can be installed on either a physical computer or virtual machine to protect networks. PfSense is based on the FreeBSD OS and has become one of the most popular open-source firewall/router projects available.

- **Stateful Firewall:** Pfsense inspects incoming and outgoing traffic, allowing only authorized connections based on pre-defined rules. This helps block malicious traffic and unauthorized access attempts.
- **VPN (Virtual Private Network):** Pfsense allows secure remote access to your network using various VPN protocols, encrypting data in transit and protecting sensitive information.
- **Multi-WAN (Wide Area Network):** Pfsense can manage multiple internet connections, providing redundancy and improving overall network reliability.

Additional Security Features:

- IDS/IPS (Intrusion Detection/Prevention System)
- Packet Filtering
- Web Filtering
- User Authentication
- Being open-source allows for continuous community development and improvement, with security vulnerabilities being identified and patched promptly.

PERSONAL CYBERSECURITY SOFTWARE

LIFELOCK

LifeLock offers comprehensive protection against identity theft by monitoring against easy-to-miss identity threats (like payday loans or crimes committed in your name) as well as identity restoration services and \$1 million coverage for lawyers and other experts if identity theft does occur while you are a member.

LifeLock Features

- Identity and social security number alerts
- Phone takeover monitoring
- Alerts on crimes committed in your name
- Credit reports and scores
- Home title monitoring
- Social media monitoring





THANK YOU!