

**Experiment No.: 05**

**Title: Exploring the tools in cyber security.**

**Batch: *A-4*** **Roll No.:** ***16010422211*** **Experiment No: 05**

**Aim:** Exploring the tools in cyber security.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Resources needed:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Theory:**

What are the different types of cyber security tools.

What kind of cyber security tools can be used for email forensics and intruder detection?

What are the steeps to be followed while using the cyber security tools?

*1)*Different types of cyber security tools include*;*

### ***Network security monitoring tools***

*Monitoring tools for network security are used to identify external network threats by detecting and preventing attacks that originate from the organization’s intranet.*

### ***Security compliance tools***

*Security compliance tools scan your network, tools, and processes to evaluate them against the requirements of regulatory frameworks. It detects non compliant activities and security failures and notifies system administrators to take corrective actions.*

### ***Network defence wireless-tools***

*Network defence wireless tools can significantly improve security as they protect data while maintaining the network’s usability and integrity. Network access is controlled by using both hardware and software technologies.*

### ***Encryption tools***

*Encryption tools decode or encode streams of data that are at rest or in transit, making them safe and unreadable by unauthorized individuals.*

### ***Firewalls***

*Firewalls prevent unauthorized users from accessing the company intranet and can be implemented as hardware, software or a hybrid of the two.*

### ***Packet sniffers***

*Packet sniffers let you discover apps that gather data for security analysis or create anomalous traffic and identify network demand spikes and dips while debugging application traffic.*

### ***Antivirus software***

*Antivirus software helps you monitor, block and remove viruses as well as other malware from your computer and other IT systems. It guards devices and networks against viruses, rootkits, spyware, keyloggers, botnets, browser hijackers, ransomware, adware, and Trojan horses.*

### ***Managed detection and response services***

*Managed detection and response services (MDR) are third-party services that aid organizations in monitoring, addressing, and removing threats.*

### ***Public key infrastructure services***

*PKI services enable you to distribute and identify public encryption keys. It permits computers and individuals to communicate data over the web securely while also verifying the sender’s identity.*

2) Cyber Security tools used for email forensics & intruder detection:

***Email Security Gateways****: These tools scan incoming emails for malicious content, filter spam, and protect against phishing attempts.*

***Email Forensics Tools****: Tools like email header analyzers help trace the origin of emails, aiding in the investigation of email-based attacks.*

***Network Packet Analyzers****: Capture and analyze network traffic, helping in detecting intrusions and unusual patterns.*

***Log Analysis Tools****: Analyze system and network logs to identify suspicious activities or security breaches.*

*3) Steps to follow while using cyber security tools:*

***Assessment:*** *Identify the specific security needs and vulnerabilities of your system or network.*

***Selection:*** *Choose appropriate cybersecurity tools based on your assessment, considering factors like compatibility, effectiveness, and ease of use.*

***Configuration:*** *Properly configure the selected tools according to best practices and security guidelines.*

***Monitoring:*** *Continuously monitor the tools to detect and respond to security threats promptly.*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**



**Results: (Queries printout with output)**

**Select any one cyber security tool and explore the same in terms of its UI, version, working steps, applications, and case study example.**

***Suricata****, a cybersecurity tool, is an open-source intrusion detection and prevention system (IDS/IPS) developed by the Open Information Security Foundation (OISF). It is designed to monitor network traffic and detect malicious activity*.

1. ***UI and Version***:

*Suricata primarily operates via command-line interface (CLI) and configuration files. While it doesn't have a traditional GUI, there are various third-party tools and integrations available that provide graphical representations of Suricata's data. As for the version, the software is actively developed, and newer versions continue to be released with improvements and features.*

1. ***Working Steps***:

*Traffic Capture: Suricata captures and analyzes network traffic in real-time.*

*Signature-based Detection: Suricata uses predefined rules (signatures) to identify known threats in network packets.*

*Anomaly-based Detection: It can also detect abnormal patterns of traffic that might indicate unknown or zero-day attacks.*

*Logging and Alerting: Suricata logs detected events and can generate alerts based on configured rules.*

*Multi-Threading: Suricata is multi-threaded, enabling it to handle high traffic loads efficiently.*

1. ***Applications***:

*Network Intrusion Detection: Suricata monitors network traffic for signs of intrusion attempts, malware, and other malicious activities.*

*Intrusion Prevention: It can actively block or prevent malicious traffic based on the detected threats, functioning as an intrusion prevention system.*

*Threat Hunting: Security analysts use Suricata to investigate past network traffic to identify patterns indicative of security threats.*

*Network Forensics: Suricata's detailed logging capabilities assist in network forensics investigations after a security incident.*

1. ***Case Study Example:***

*Use Case: Detecting a Web Application Attack*

*Background: A web server of a company is suspected to be under attack. The IT team is concerned about potential SQL injection attempts targeting their web applications*.

*Steps Taken*:

*Suricata Configuration: The IT team configures Suricata to monitor traffic to and from the web server.*

*Signature Rules: They deploy specific Suricata rules designed to detect SQL injection attempts and other web application attacks.*

*Real-time Monitoring: Suricata starts monitoring the traffic in real-time, analyzing HTTP requests and responses.*

*Alert Triggering: Suricata triggers an alert when it detects SQL injection patterns in the incoming HTTP requests.*

*Response: The IT team investigates the alerts, identifies the attack vectors, and implements additional security measures, such as patching vulnerable code and updating firewall rules to block the malicious IP addresses*.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Outcomes:** *Explored Suricata, a cybersecurity tool, in terms of its ui and version working steps, applications.*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion:** *Explored different tools in cyber security***.**

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**References:**

**Books:**

1. Nina Godbole, Sunit Belapure Cyber Security Understanding Cyber Crimes,Computer Forensics and Legal Prespectives” Wiley- India 1st Edition,

2 N S Nappinai Technology Laws Decodded LexisNexis 1 st Edition, 2017

<https://sprinto.com/blog/best-cybersecurity-tools/>

https://www.knowledgehut.com/blog/security/cyber-security-tools