**Assignment No :- 7**

**Aim :-**Demonstrate Nessus vulnerability scanner tool.

**Introduction:-**

****

Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.

Originally launched as an open source tool in 1998, its enterprise edition became a commercial product in 2005. Nessus now encompasses several products that automate point-in-time vulnerability assessments of a network's attack surface, with the goal of enabling enterprise IT teams to stay ahead of cyber attackers by proactively identifying and fixing vulnerabilities as the tool discovers them, rather than after attackers exploit them.

Nessus identifies software flaws, missing patches, malware, denial-of-service vulnerabilities, default passwords and misconfiguration errors, among other potential flaws. When Nessus discovers vulnerabilities, it issues an alert that IT teams can then investigate and determine what if any further action is required.

**Steps to install and run the NESSUS:**

**Step 1: Obtain Nessus:**

* Go to the official Tenable website (https://www.tenable.com/products/nessus) and register for an account.
* Download the appropriate version of Nessus for your operating system (Windows, Linux, or macOS)..



**Step 2: Install Nessus:**

* Follow the installation instructions provided for your specific operating system.
* During the installation process, you may be prompted to set up an administrator account and configure other settings.

**Step 3: Activate Nessus:**

* After installation, open a web browser and access the Nessus web interface by navigating to https://localhost:8834. Log in with the credentials you set during installation.
* Follow the on-screen instructions to activate Nessus. This usually involves entering the activation code obtained during the registration process.

**Step 4: Configure a Scan:**

* Once activated, log in to the Nessus web interface.
* Click on the "Scans" tab and then "New Scan" to create a new scanning configuration

**Step 5: Customize Scan Settings:**

* Configure scan settings based on your requirements. This may include selecting the type of scan (e.g., Basic Network Scan, Web Application Test, etc.) and adjusting advanced settings.

**Step 7: Review Results:**

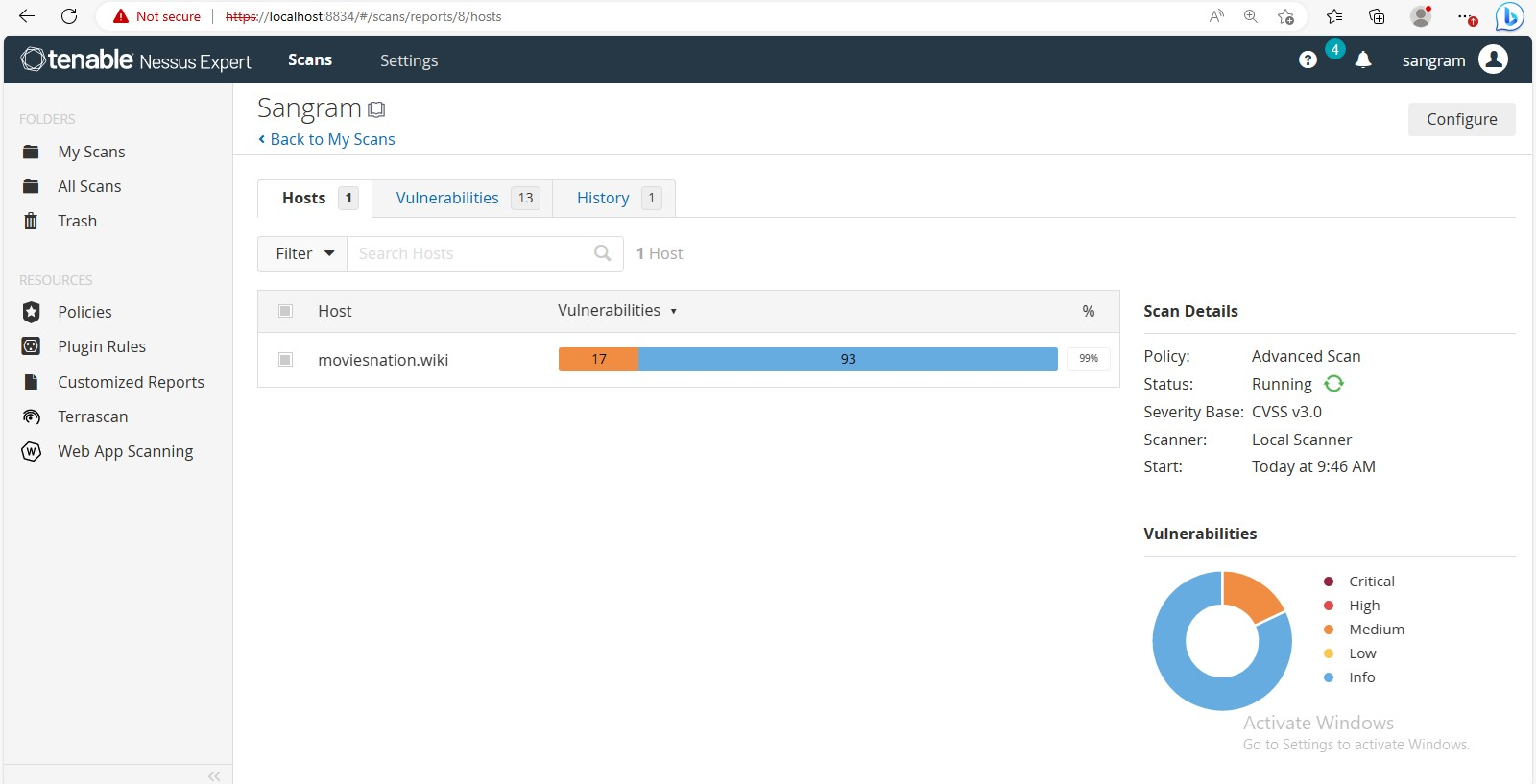
* Once the scan is complete, access the scan results to view detailed information about identified vulnerabilities.Nessus provides severity ratings, descriptions.

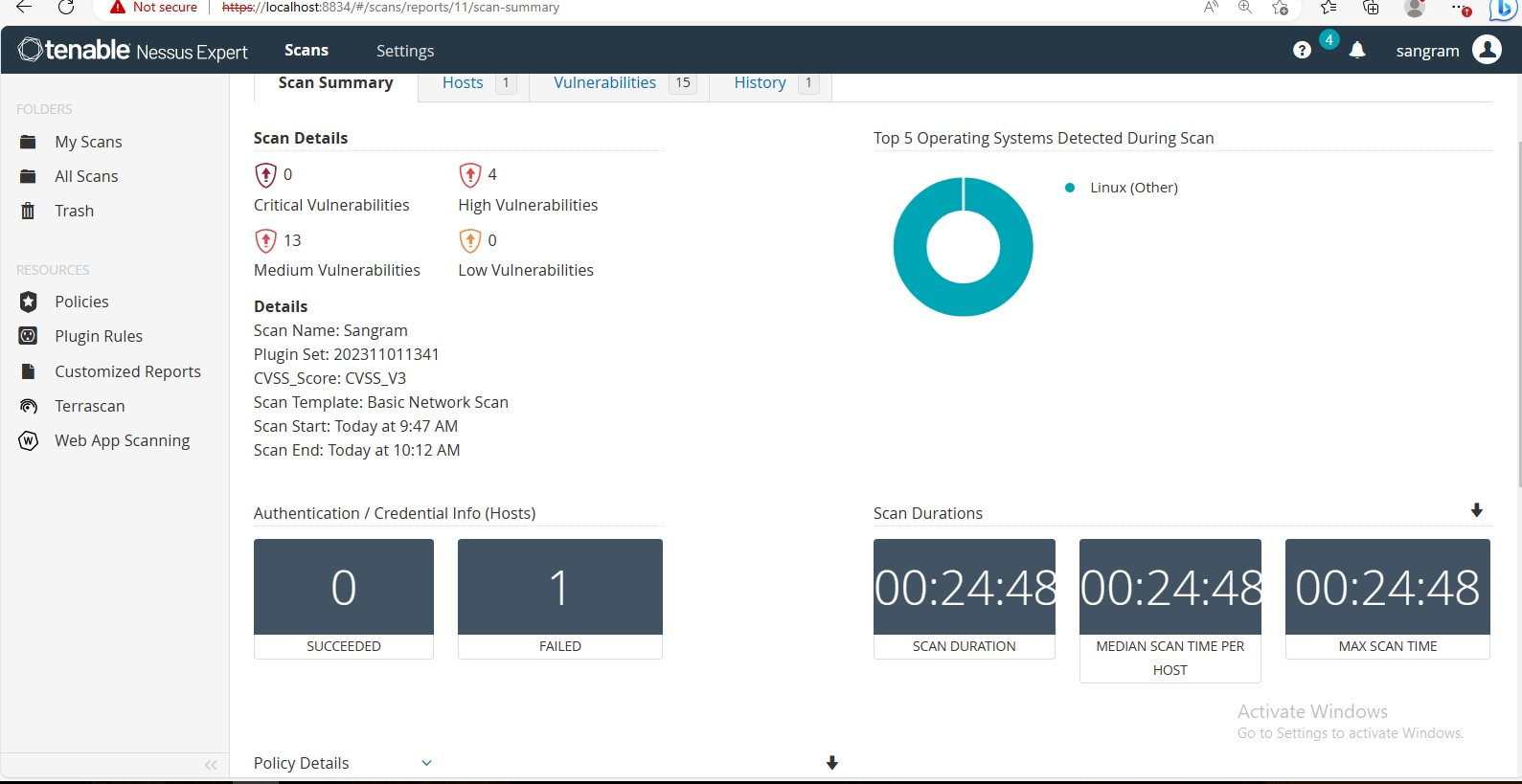
**vulnerability Scanning Websites:-**

**1)Third party movie website(Moviesnation):-**

**www.moviesnation.wiki**

So the website contain some medium level risks which is very dangerous of our system.The Scan Show that Vulnerabilities present in the websites The Nessus Scan all the Vulnerabilities

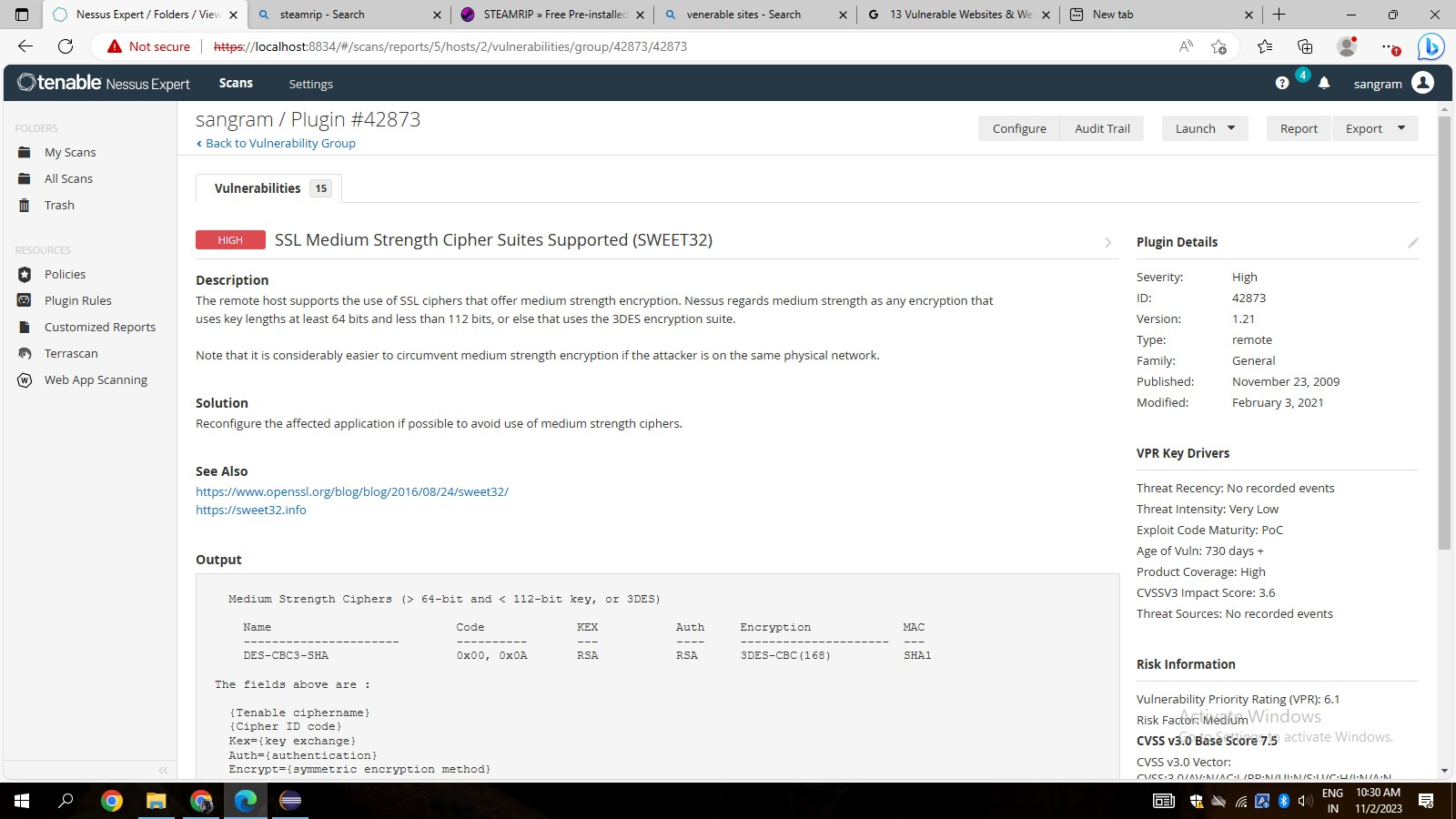




**2)Third party betting apps:-**

[**www.sweet32.info**](http://www.sweet32.info)

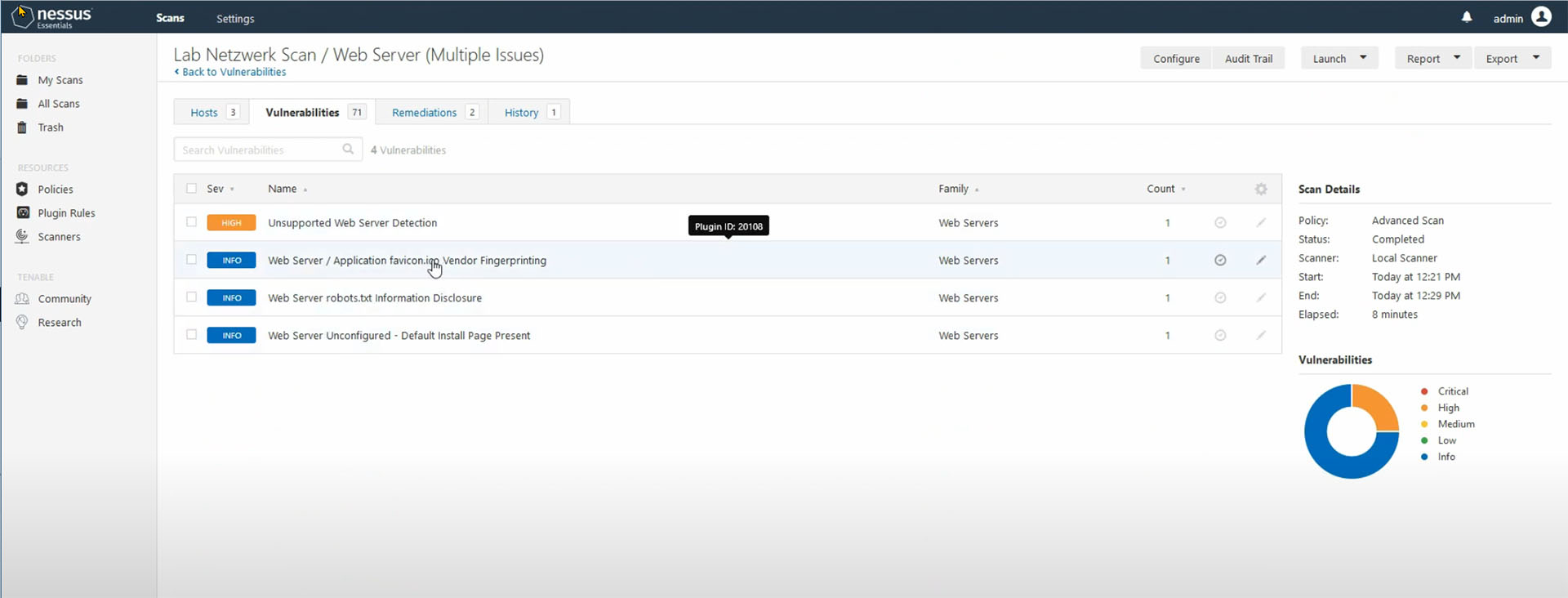
To address these vulnerabilities, it's recommended to take appropriate security measures and implement necessary fixes to ensure the website's safety and integrity. This may involve applying patches, updating software, or implementing additional security measures as suggested by the Nessus scan. Regular security scans and proactive measures can help maintain a secure online presence.



**3)CTFlearn WebSite Scan:-**

[**www.ctflearn.com**](http://www.ctflearn.com)

Capture the Flag (CTF) in computer security is an exercise in which participants attempt to find text strings, called "flags", which are secretly hidden in purposefully-vulnerable programs or websites.



**Features of Nessus :-**

**Comprehensive Vulnerability Scanning:**

Nessus conducts thorough scans to identify vulnerabilities, misconfigurations, and potential security threats across a variety of systems and applications.

**Plugin Architecture:**

Nessus uses a plugin-based architecture that allows for continuous updates to its vulnerability database. This ensures that the tool stays up-to-date with the latest security threats and vulnerabilities.

**Extensive Vulnerability Database:**

The tool maintains a vast and constantly updated database of known vulnerabilities, supporting a wide range of operating systems, applications, and network devices.

**Policy Compliance Auditing:**

Nessus can assess systems against predefined security policies and compliance standards, helping organizations adhere to regulatory requirements and industry best practices.

**Scalability:**

Nessus is scalable and can be used to scan both small and large environments, making it suitable for organizations of varying sizes.

**Multiple Scan Types:**

It supports various scan types, including host discovery scans, port scans, credentialed scans, web application scans, and more. This versatility allows users to tailor scans to their specific needs.

**Credential-based Scanning:**

Nessus supports credentialed scans, enabling it to access and assess the security posture of the target systems with the appropriate credentials. This provides a more accurate and comprehensive assessment.

**Advantages of Nessus :-**

1. **Regular Updates and Plugin Support:**
   * The tool's plugin architecture allows for frequent updates, ensuring that the vulnerability database stays current with the latest security threats and vulnerabilities.
2. **Accurate Credentialed Scanning:**
   * Nessus supports credentialed scans, allowing it to access target systems with proper credentials for a more accurate and thorough assessment of security vulnerabilities.
3. **Policy Compliance Auditing:**
   * Organizations can use Nessus to audit systems against predefined security policies and compliance standards, helping ensure adherence to regulatory requirements and industry best practices.
4. **Customizable Scan Policies:**
   * Users can tailor scan policies to meet specific needs, adjusting settings such as scan intensity, target selection, and compliance standards for a more flexible and targeted approach to vulnerability scanning.
5. **Detailed and Customizable Reporting:**
   * Nessus generates detailed reports that provide insights into identified vulnerabilities, their severity levels, and recommended remediation steps. Reports are customizable to suit various reporting needs, including compliance audits and risk assessments.

**Disadvantages of Nessus:-**

1. **Cost for Certain Features:**
   * While Nessus offers a free version, some advanced features and capabilities are only available in the paid versions. Organizations may need to invest in the Professional or Manager versions for more comprehensive functionality.
2. **Learning Curve:**
   * For beginners, Nessus can have a steep learning curve. Configuring and interpreting scan results may require some time and effort to become proficient, particularly for users who are new to vulnerability management tools.
3. **False Positives and Negatives:**
   * Like any vulnerability scanner, Nessus is not infallible. It may produce false positives (indicating vulnerabilities that aren't actually present) or false negatives (missing actual vulnerabilities), depending on network conditions, configurations, or the complexity of the target environment.
4. **Resource Intensive Scans:**
   * Intensive scans on large networks can be resource-intensive, consuming significant system resources and potentially impacting network performance. Care must be taken to schedule scans during periods of lower network activity.
5. **Dependency on Network Conditions:**
   * Results may vary based on the stability and conditions of the network being scanned. Unstable or congested networks may impact the accuracy and efficiency of the scanning process.

**Applications :-**

* **Security Audits:**
  + Organizations can use Nessus to conduct regular security audits of their IT infrastructure. This involves scanning networks, servers, and applications to identify vulnerabilities and assess the overall security posture.
* **Penetration Testing:**
  + Security professionals and ethical hackers use Nessus as part of penetration testing activities to simulate cyber-attacks and identify potential vulnerabilities that malicious actors could exploit.
* **Patch Management:**
  + Nessus helps organizations prioritize and remediate vulnerabilities by providing detailed reports on outdated software versions and missing patches. This assists in maintaining an up-to-date and secure environment.
* **Compliance Checks:**
  + Nessus is employed to ensure that systems comply with industry standards and regulatory requirements. It helps organizations assess and report on their adherence to specific security policies and guidelines.
* **Incident Response:**
  + During and after a security incident, Nessus can be used to conduct rapid vulnerability assessments to identify any new weaknesses that may have been exploited during the incident. This aids in the timely resolution of security issues.

**Conclusion :-**

In conclusion, Nessus stands as a cornerstone in the realm of cybersecurity, offering a robust and versatile solution for vulnerability management, security assessments, and compliance checks. Its extensive feature set, including comprehensive vulnerability scanning, policy compliance auditing, and detailed reporting, makes it a go-to tool for organizations seeking to fortify their defenses against evolving cyber threats.However, users must be mindful of potential challenges, such as a learning curve for beginners, false positives/negatives, and the need for responsible use to comply with legal and ethical standards. Additionally, organizations may need to consider the cost implications for accessing certain advanced features.