Raahul M

21BAI1537

**23/08/2023 - 25%**

**Task 1:**

**Top 10 Notorious Hackers in the World**

## **Kevin Mitnick**

Widely regarded as a pioneering figure in the world of hacking, Kevin Mitnick gained notoriety through audacious exploits, infiltrating prestigious organizations such as NORAD and DEC. Mitnick's journey transitioned from black hat to white hat, advocating for cybersecurity. His remarkable achievements inspired the creation of the renowned film "War Games" and played a pivotal role in raising widespread awareness about digital vulnerabilities.

## Anonymous

Operating as a loosely organized collective, Anonymous embodies hacktivist actions against injustices. Their gray hat stance blurs the white-black hat line while they target entities like the Church of Scientology. Anonymous's achievements involve impactful Distributed Denial of Service (DDoS) attacks and dedicated advocacy for social justice. Their hierarchical absence underscores their commitment to exposing societal issues.

## Adrian Lamo

Initially a gray hat, Adrian Lamo transitioned to black hat activities driven by curiosity and recognition. Lamo's intrusion into The New York Times' systems and involvement in high-profile hacks thrust him into moral ambiguity. His achievements encompass exposing security flaws and catalyzing ethical debates on responsible hacking.

## Albert Gonzalez

Starting in gray hat territory, Albert Gonzalez delved into black hat activities, orchestrating egregious credit card data breaches. Gonzalez's accomplishments include illicitly acquiring and selling millions of card accounts. Despite later cooperation, his malicious actions overshadow any white hat involvement.

## Matthew Bevan and Richard Pryce

Operating as deft gray hats, Bevan and Pryce exposed military vulnerabilities, inadvertently sparking international tensions. Their achievements lay in revealing weaknesses within military systems, provoking vital discussions on cybersecurity's role in global conflicts.

## Jeanson James Ancheta

Operating unequivocally in black hat territory, Ancheta harnessed botnets to compromise countless systems for profit. His achievements underscore the severe consequences of botnet exploitation, resulting in significant legal precedent.

## Michael Calce

Unabashedly a black hat, Calce's "Mafiaboy" hack unleashed destructive DDoS attacks. His achievements spotlighted economic loss and disruption due to cyber assaults, galvanizing discourse on cybersecurity legislation.

## Kevin Poulsen

Initially embracing black hat hacking, Poulsen transformed into a white hat advocate for cybersecurity and journalism. His accomplishments encompass shedding light on vulnerabilities, participating in projects like SecureDrop, and raising awareness about ethical hacking.

## Jonathan James

Operating audaciously as a black hat, Jonathan James breached government systems at a young age. His achievements highlighted the need for robust cybersecurity measures to safeguard sensitive government data.

## ASTRA

Operating in the black hat domain, ASTRA conducted cyber espionage and profited from illicit technology sales. Their identity obscurity and successful theft of cutting-edge technology highlighted the significant economic and security implications of cybercrime.

Outcome: Basic Terminologies in CyberSec

24/08/2023

Task 2 - Vulnerabilities of Popular Port Numbers

### 

Port 20 and (mainly) port 21 are File Transfer Protocol (FTP) ports that let users send and receive files from servers.

FTP is known for being outdated and insecure. As such, attackers frequently exploit it through:

* Brute-forcing passwords
* Anonymous authentication (it’s possible to log into the FTP port with “anonymous” as the username and password)
* Cross-site scripting
* Directory traversal attacks

### **Port 22 (SSH)**

Port 22 is for Secure Shell (SSH). It’s a TCP port for ensuring secure access to servers. Hackers can exploit port 22 by using leaked SSH keys or brute-forcing credentials.

### **Port 23 (Telnet)**

Port 23 is a TCP protocol that connects users to remote computers. For the most part, Telnet has been superseded by SSH, but it’s still used by some websites. Since it’s outdated and insecure, it’s vulnerable to many attacks, including credential brute-forcing, spoofing and credential sniffing.

### **Port 25 (SMTP)**

Port 25 is a Simple Mail Transfer Protocol (SMTP) port for receiving and sending emails. Without proper configuration and protection, this TCP port is vulnerable to spoofing and spamming.

### **Port 53 (DNS)**

Port 53 is for Domain Name System (DNS). It’s a UDP and TCP port for queries and transfers, respectively. This port is particularly vulnerable to DDoS attacks.

Port 69 (TFTP):

Unauthorized Access: Since TFTP lacks authentication, an open TFTP port might allow unauthorized users to upload or retrieve files, potentially leading to unlawful data access.

Port 80 (HTTP):

Cross-Site Scripting (XSS): Vulnerabilities in online applications can allow attackers to inject malicious scripts into web pages, potentially stealing user data or conducting activities on behalf of users.

Port 110 (POP3):

Credential Exposure: Unencrypted POP3 transmission can disclose login credentials, allowing attackers to obtain unauthorized access to users' email accounts.

Port 123 (NTP):

Amplification Attacks: Open NTP servers can be misused in DDoS amplification attacks, where attackers send small requests to the server, which subsequently delivers bigger responses to the target, overwhelming their network.

Port 143 (IMAP):

Data Leakage: Vulnerabilities in IMAP servers can lead to unauthorized access to users' emails, potentially leading in data leakage.

Port 443 (HTTPS):

Man-in-the-Middle Attacks: While HTTPS is secured, attackers can still attempt to perform SSL/TLS attacks, intercepting encrypted traffic and potentially stealing sensitive data.

25/08/2023

Task 3 - Owasp top 10 cwe’s

A01:2021-Broken Access Control:

CWE - 1345:

Description:

Weaknesses in this category are related to the A01 category "Broken Access Control" in the OWASP Top Ten 2021.

Business Impact:

Consider a scenario where users can bypass rightful restrictions and gain unauthorized access to confidential data or perform illicit actions. This situation undermines the fundamental principles of security and can give rise to a cascade of problems. These problems range from sensitive information leakage, eroding trust, to denial of service attacks that halt business operations, and even the potential for execution of malicious code.

Inconsistent or nonexistent access control checks invite chaos into the realm of digital security. Negligence in ensuring proper authorization allows unauthorized personnel to infiltrate secure areas, exposing sensitive data and jeopardizing critical systems. The implications reverberate throughout the organization, resulting in regulatory non-compliance penalties, financial losses due to fraudulent activities, operational disruptions that impair productivity, and, most insidiously, irreversible damage to the carefully built reputation.

To counter this menacing threat, robust access control mechanisms are of utmost importance. A meticulously designed system enforces privileges based on roles, responsibilities, and the principle of least privilege. This guarantees that users can only access resources that align with their authorized scope. Businesses must diligently maintain and regularly audit these access controls, for the repercussions of their failure extend far beyond the digital realm.

A02:2021-Cryptographic Failures:

**CWE CATEGORY: OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures**

Description:

Weaknesses in this category are related to the A02 category "Cryptographic Failures" in the OWASP Top Ten 2021.

Business summary:

The vulnerability in question can result in compromised user accounts, erosion of customer trust, non-compliance with regulations, and financial losses due to potential legal action and operational disruptions. The implementation of robust cryptographic techniques is of utmost importance in order to prevent unauthorized access, ensure compliance with regulations, safeguard customer data, and protect the reputation of the organization. Failure to address these issues can lead to negative public perception, legal challenges, and long-term security vulnerabilities. Hence, organizations must prioritize the adoption of strong cryptographic measures to mitigate these risks and ensure the overall security of their systems and sensitive information.

A03:2021-Injection:

**CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

**Description:**

**The product constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.**

**Business impact:**

**Exploiting this vulnerability can result in data breaches, leading to the exposure of confidential customer information and initiating legal consequences. Unauthorized transactions and manipulated financial records can result in financial losses. Moreover, the organization's reputation may be adversely affected, resulting in customer attrition and a decline in brand value. Compliance violations, operational disruptions, legal liabilities, and resource allocation for security measures are additional unfavorable outcomes. It is imperative to address SQL Injection vulnerabilities in order to prevent data breaches, financial losses, reputational damage, and legal consequences.**

A04:2021-Insecure Design:

CWE - 1348

Description:

Weaknesses in this category are related to the A04 "Insecure Design" category in the OWASP Top Ten 2021.

Business impact:

A05:2021-Security Misconfiguration:

CWE - 1349

Description:

Weaknesses in this category are related to the A05 category "Security Misconfiguration" in the OWASP Top Ten 2021.

Business impact:

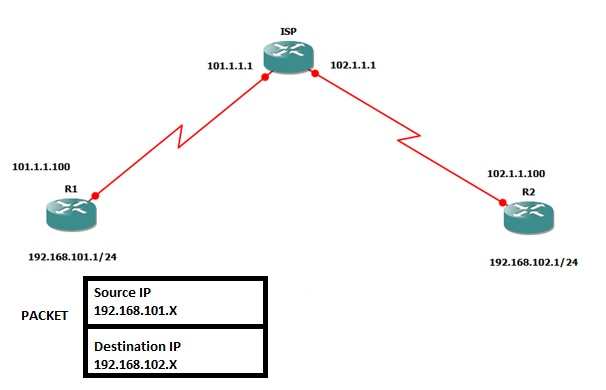
Security misconfigurations (Category ID: 1349) have the potential to result in severe business consequences. These can include breaches of data, financial losses, failure to comply with regulatory requirements, disruptions in services, and a loss of trust from customers. In addition, misconfigurations may lead to the theft of intellectual property, inefficiencies in operations, legal action, and long-term damage to an organization's reputation. It is imperative to address these security misconfigurations in order to prevent unauthorized access, maintain compliance, and protect sensitive information, thereby preserving customer trust and ensuring the viability of the business.

28/08/2023

Topic covered: Additional potential vulnerabilities in WebApps

Task 4: 10 Common Vulnerabilities on WebApps other tha OWASP

## **Encapsulation**

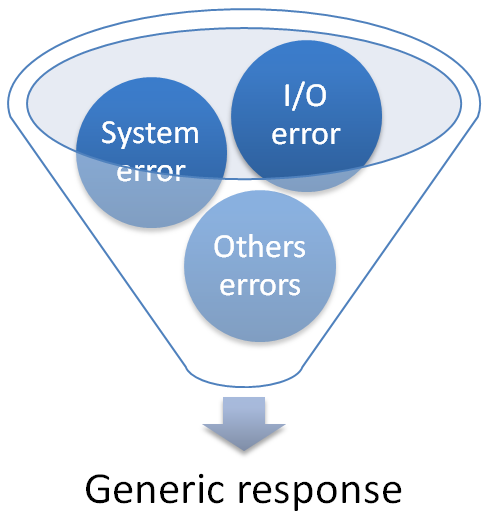


Unlike some of the other vulnerabilities that leverage web browser access to applications, encapsulation vulnerability exploits focus on weaknesses in the way a developer coded the application. The programming term encapsulation refers to bundling data and actions that can be taken on that data into a single unit. Encapsulation protects data by hiding details about how the code works which creates a better user interface. Users don’t need to know how the application brings them data; they just need access to it.

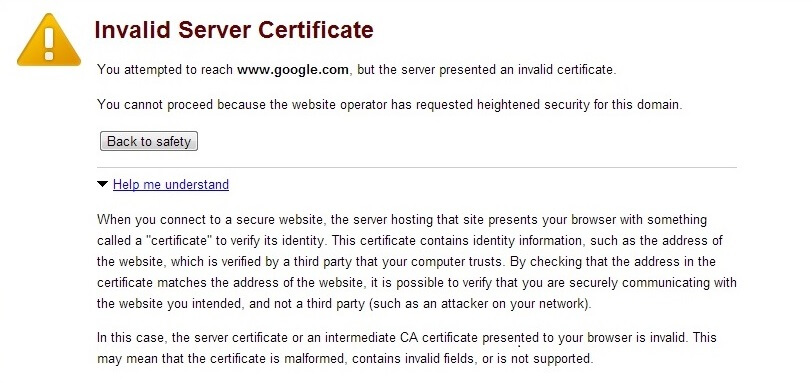
## **Error handling**

Several different attack methods rely on how an application responds to abnormal inputs or conditions. One example of an error message is the “404 not found” message when you try to access a website. For most enterprise applications and systems, error messages provide valuable information about how to fix a problem.

However, for web applications, too much information returned through an error message can give malicious actors that same information. Often, attackers send the web application a query that they know will return an error message. They usually do this during the reconnaissance phase, where they try to get as much information as possible so they can find exploitable vulnerabilities.



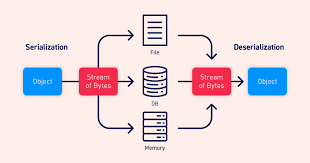
## **Improper certificate validation**



SSL certificates bind a domain name, server name, or hostname to a company and location. For example, GoodSecureCo installs the SSL certificate data files on its US web servers. Every time a browser asks for data from the US web server, the SSL certificate checks to make sure that the user’s browser connects with an approved owner. The two securely connect if the answer is yes.

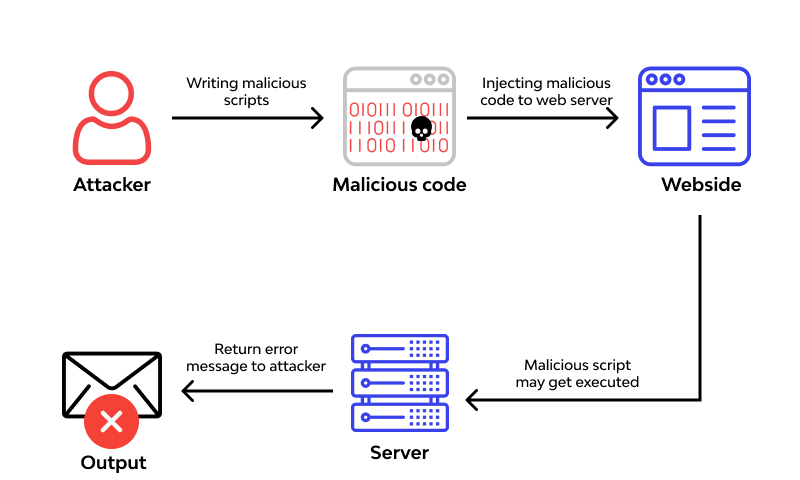
When software refuses to validate or incorrectly validates the certificate, it has an improper certificate validation vulnerability. Most often, attackers create a false trusted entity that tricks the server or application into thinking the certificate is valid so it accepts the data transfer as legitimate. Often, malicious actors use improper certificate validation vulnerabilities as a way to install malware on endpoints.

## **Insecure deserialization**



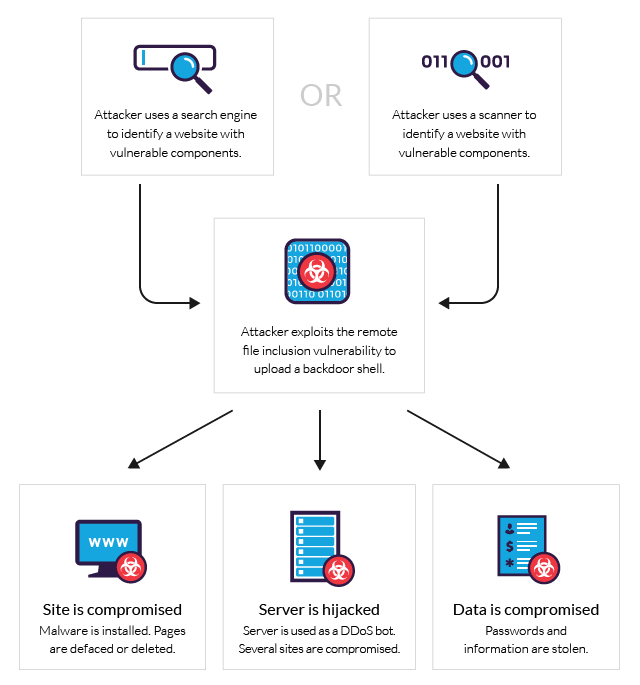
Deserialization is the process of reconstructing the original, expanded data structure. With a deserialization vulnerability, malicious actors can change the application logic or execute code remotely, one of the most serious attack types.

## **Remote code execution (RCE)**



RCE vulnerabilities are coding mistakes in web applications that allow malicious actors to input code regardless of their geographic location. RCEs are a larger category of web application injection vulnerabilities where malicious actors insert their own code into an application that does not verify user inputs so that the server views it as legitimate application code. Generally, attackers will leverage unpatched commonly known vulnerabilities and input their code into the application.

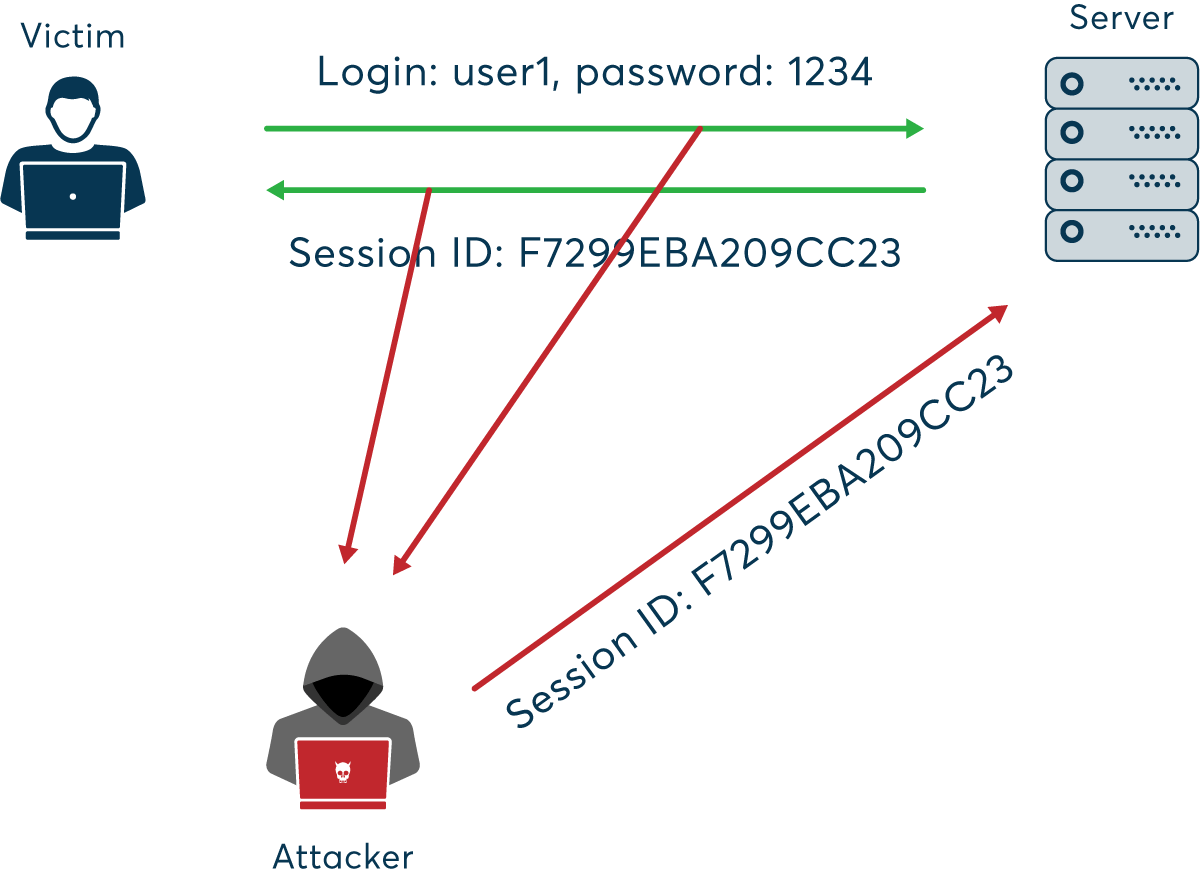
## **Remote file inclusion (RFI)**



Developers use “include” statements in their code to connect common directories to an application. For example, an application might want to pull information from a database. Instead of manually coding it to pull each file, the “include” statement can be used to connect to the entire source directory so that it can use everything stored there.

If a web application has an RFI vulnerability, malicious actors can direct the application to upload malware or other malicious code to the website, server, or database.

## **Session ID leakage**



Session IDs are the unique identifiers that authenticate users and track their activities when they use a web application. Web application vulnerabilities that lead to session leakage include:

Storing the session ID in the query string. By storing the session ID in the part of the URL that asks the application to retrieve information from the database, sharing of that URL allows the recipient to inherit that session without new authentication.

Storing the session ID in HTTP cookies: By storing the session ID in the small data files that let a web server remember a web browser and using the unencrypted HTTP protocol, the application gives the attacker the ability to steal the session ID and impersonate the user.

## **Unvalidated automatic library activation**

Developers use third-party libraries to save time when coding. Often, this allows them to use pre-tested code that speeds up the application development process. However, the use of publicly available, open-source code increases security risks, including:

* Abandoned projects that are no longer updated
* Lack of documented ownership increases the risk of malicious code added
* Monitoring for library updates to fix vulnerabilities

Since many applications involve third-party library dependencies, this vulnerability is becoming more common.

## **Unvalidated redirects and forwards**

Web applications can use redirects or forwards after a user submits a form. For example, if your marketing website has a form so that visitors can download a whitepaper, the page redirects or forwards them to the “thank you” page when they submit the form. However, malicious actors can impersonate these redirected or forwarded page URLs to steal user information.

Examples of this vulnerability include web applications with:

* Large numbers of destination pages
* Fail to store full URLs
* Lack identifiers for these redirects/forwards
* Lack of identifiers used as request parameters
* Failure to filter out untrusted URL inputs

## **Missing function level access control**

Once users authenticate to an application, the function level access controls define the actions they can take within it. For example:

www.insecurewebapp.com/genericusername/read

www.insecurewebapp.com/SuperAd… on this example, Generic Username can read files in this application while Super Adminuser can edit within this application. Because the access rights are included in the URL, no one needs the authentication that protects these actions. Authenticated non-administrative users or unauthenticated users can type in a URL hoping to gain administrative access. For example, the malicious actors might try to type:

www.insecurewebapp.com/SuperAd… missing function level access control means that the malicious actor doesn’t need to authenticate to the system and can now delete data.

## 

Task 5:

**Explain CIS top 20**

**1. Hardware Asset Inventory and Control**

Actively manage (inventory, track, and properly organize) all physical devices connected to the network, ensuring only approved devices gain access, while detecting and restricting unauthorized or unmanaged devices from obtaining access.

**2. Software Asset Inventory and Control**

Proactively manage (inventory, track, and authorize) all network applications to permit only approved software installations and executions, while identifying and blocking unauthorized or unmanaged software from being installed or executed.

**3. Continuous Vulnerability Management**

Constantly obtain, assess, and act upon new information to identify system vulnerabilities, make repairs, and minimize the window of opportunity for potential attackers.

**4. Regulated Use of Administrative Privileges**

Employ techniques and tools to monitor, control, prevent, and rectify the allocation, setup, and usage of administrative rights across computers, networks, and applications.

**5. Secure Configuration of Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**

Establish, implement, and proactively manage (track, report on, rectify) the security configurations for mobile devices, laptops, servers, and workstations using strict configuration management and change control processes to deter attackers from exploiting unsecured services or settings.

**6. Maintenance, Monitoring, and Analysis of Audit Logs**

Compile, maintain, and evaluate audit logs containing events that could aid in the detection, understanding or mitigation of potential cyber-attacks.

**Foundational**

**7. Email and Web Browser Protections**

Minimize attack surfaces by reducing chances for attackers to influence human behavior through their interactions with online browsers and email systems.

**8. Malware Defense Mechanisms**

Regulate the installation distribution, and execution of malicious code at multiple levels within an organization by leveraging automation for prompt updating of defenses as well as data collection and corrective action implementations.

**9. Restriction and Management of Network Ports, Protocols, and Services**

Oversee (track, control, rectify) the ongoing operational usage of network ports, protocols, and services on network devices to eliminate potential vulnerabilities that attackers could exploit.

**10. Data Recovery Capability**

Employ processes and tools necessary to securely back up vital information using a proven methodology for swift data recovery when necessary.

**11. Robust Configuration for Network Devices, including Firewalls, Routers, and Switches**

Develop, implement, and proactively manage (monitor, report on, remediate) the security configuration of network infrastructure devices through rigorous configuration management and change control processes to prevent attackers from exploiting vulnerable services and settings.

**12. Perimeter Defense**

Identify, prevent, and rectify the flow of information across networks with varying trust levels, focusing on data that could compromise security.

**13. Safeguarding Data**

Employ methods and techniques to thwart data exfiltration, minimize the impact of compromised data, and ensure privacy and integrity of sensitive information.

**14. Regulated Access Based on Need-to-Know Principles**

Utilize techniques and tools to track, control, prevent, and correct secure access to vital assets (e.g., information, resources, systems), based on formally determined eligibility of individuals, computers, and programs to access these crucial assets as per established classification.

**15. Wireless Access Management**

Apply techniques and tools to monitor, regulate, prevent, and rectify security aspects of wireless local area networks (WLANs), access points, and wireless client systems.

**16. Account Oversight and Control**

Actively administer the life cycle of system and application accounts – their creation, usage, dormancy, removal – to reduce opportunities for attackers to exploit them.

**Organizational**

**17. Establish a Security Awareness and Training Program**

Identify specific knowledge, skills, and abilities required to defend the organization across all functional roles (prioritizing mission-critical business functions), and implement an integrated plan to assess gaps in understanding; address weaknesses through policies, organizational planning, training programs; ensuring continuous improvement.

**18. Application Software Security**

Oversee the security life cycle of in-house developed and third-party software to address flaws through prevention strategies or timely remediation.

**19. Incident Response and Management**

Safeguard the organization's information, reputation, and assets by constructing and deploying an incident response infrastructure (e.g., detailed plans, designated roles, training, communication protocols, executive support), enabling rapid identification of intrusions and delivering an effective containment of damage and restoration of network and system integrity.

**20. Penetration Testing and Red Team Exercises**

Assess the overall resilience of an organization's defense – encompassing technology, processes, and individuals – by simulating the objectives and actions of potential attackers.

11/09/23

WinCollect and Stand Alone WinCollect

IBM WinCollect: A Comprehensive Solution for Advanced Log Collection and Management

IBM WinCollect serves as a vital component in IBM's extensive security ecosystem, offering robust capabilities for organizations to effectively gather and manage log data from Windows-rooted systems. As an integral element of any Security Information and Event Management (SIEM) approach, WinCollect significantly contributes to strengthening an organization's cybersecurity position. This comprehensive overview will delve into the primary features, functionalities, and advantages of IBM WinCollect.

Essential Features:

Log Collection: WinCollect excels at gathering log information from various Windows-based sources such as servers, workstations, and endpoints. It accommodates a wide array of log types, thus guaranteeing all-encompassing coverage.

Normalization: The assembled logs undergo normalization, a process of converting them into a unified format. This streamlines log administration and examination, ensuring compatibility and effective correlation of data drawn from different sources.

Real-Time Data Ingestion: WinCollect offers real-time data ingestion capabilities enabling organizations to closely monitor critical security events as they transpire. Such immediate data is crucial for rapid incident identification and reaction.

Dependability: IBM WinCollect boasts high reliability, making certain that log data remains intact even amidst network interruptions or system failures. This dependability plays an essential part in sustaining constant visibility into an organization's security stance.

Scalability: Designed with scalability in mind, WinCollect can accommodate organizations of various sizes with differing requirements. From small businesses to expansive enterprises, WinCollect evolves according to your log collection necessities.

Customization: To meet specific security and compliance objectives, organizations have the flexibility to tweak log collection and forwarding regulations. This level of adaptability ensures appropriate data management and accurate dispatch to relevant destinations.

Capacities:

Log Consolidation: Through the consolidation of log data spanning your entire Windows environment, WinCollect establishes a centralized storage location for all security-pertinent information. This unification makes log administration and analysis less complicated.

Security Event Monitoring: WinCollect facilitates real-time evaluation of security events, empowering security teams to detect and confront threats accordingly. The system supports the recognition of irregular or questionable activities that may suggest a potential security compromise.

Compliance Assistance: In an effort to help organizations adhere to regulatory compliance requirements, WinCollect collects and forwards necessary log data, thereby simplifying conformity reporting and audit procedures.

Integration: IBM WinCollect flawlessly integrates with IBM's SIEM platforms, such as QRadar, further extending their capabilities. This seamless integration fosters more sophisticated threat detection and exhaustive security analytics.

**Benefits:**

1. **Enhanced Security Posture:** By collecting and normalizing log data, WinCollect provides a holistic view of an organization's security landscape. This enhanced visibility enables better threat detection and mitigation.
2. **Improved Incident Response:** Real-time data ingestion and alerting capabilities empower security teams to respond swiftly to security incidents. This reduces the dwell time of threats and minimizes potential damage.
3. **Simplified Compliance:** WinCollect streamlines compliance efforts by automating log collection and forwarding. It ensures that organizations have the necessary data on hand for audits and reporting.
4. **Scalable Growth:** Organizations can trust WinCollect to scale as their log collection needs expand. This scalability makes it a versatile solution for businesses of all sizes.

IBM Stand-Alone WinCollect Comprehensive Overview

IBM Stand-Alone WinCollect serves as a formidable and multifaceted log collection and management instrument, specifically engineered to fortify security measures, expedite regulatory compliance, and facilitate the systematic aggregation of log information from Windows-operated endpoints and servers. This sophisticated solution constitutes an indispensable element of the IBM Security QRadar infrastructure and is instrumental in reinforcing an organization's cybersecurity stance. In this comprehensive overview, we shall explore the salient features, advantages, and applications of IBM Stand-Alone WinCollect in detail.

Principal Features:

Log Collection: IBM Stand-Alone WinCollect is meticulously designed to accrue logs from an extensive array of Windows devices such as workstations, servers, and domain controllers. It possesses the capability to gather logs from multiple Windows event channels, application logs, as well as bespoke log sources.

Universal Log Format: This feature facilitates the normalization of log data into a standard format that guarantees seamless analysis and correlation of data from diverse origins within a Security Information and Event Management (SIEM) platform like IBM QRadar.

Event Filtering: WinCollect enables users to devise customized event filtering regulations for the exclusive collection of pertinent data. This optimizes the volume of transferred and stored data while streamlining the focus on crucial security occurrences.

Real-Time Collection: The platform delivers real-time aggregation of log data, ensuring that security-related incidents and events are immediately identified and addressed, thereby diminishing response durations and curtailing potential damages.

Buffering and Load Balancing: WinCollect incorporates buffering functionalities to prevent log depletion during network disruptions. Moreover, it supports load balancing for equitable distribution of log collection tasks among multiple collectors to achieve scalability.

Centralized Management: The logs compiled by WinCollect can be supervised centrally. This empowers administrators with the ability to configure and monitor log sources, rules, and agent health from an all-inclusive console.

TLS/SSL Encryption: WinCollect also encompasses secure log transportation via TLS/SSL encryption, which safeguards sensitive log information during transmission to the SIEM system. This feature elevates data integrity and confidentiality.

Advantages:

Augmented Security: IBM Stand-Alone WinCollect substantially enhances an organization's security posture through the collection and normalization of log data obtained from Windows devices. This information is vital for pinpointing security incidents, identifying anomalies, and executing effective threat response measures.

Preparedness for Compliance: Owing to its capacity for collecting, normalizing, and administering log data, WinCollect assists organizations in fulfilling compliance prerequisites, including those stipulated by regulatory frameworks such as GDPR, HIPAA, and PCI DSS.

Real-Time Alerts: The real-time log collection and forwarding functions of WinCollect equip organizations with instant alerts concerning security events. This enables swift incident resolution and reduces the likelihood of severe consequences.

**Applications:**

1. **Security Incident Detection:** By collecting and normalizing log data, WinCollect assists security teams in detecting and investigating security incidents such as breaches, unauthorized access, and malware infections.
2. **Forensic Analysis:** The solution provides valuable data for forensic analysis, allowing organizations to reconstruct and analyze security incidents to determine their scope and impact.
3. **Compliance Reporting:** WinCollect simplifies compliance reporting by collecting and normalizing the necessary log data, making it easier for organizations to demonstrate compliance with regulatory requirements.
4. **Log Management:** It offers comprehensive log management capabilities, including log collection, storage, and forwarding, ensuring that log data is efficiently managed and readily available for analysis.