Date: 23-08-2023

Task-1

What is Cyber Security?

Cybersecurity, short for "cybersecurity," refers to the practice of protecting computer systems, networks, and digital assets from various forms of cyber threats, attacks, and unauthorized access. It encompasses a wide range of technologies, processes, practices, and measures designed to safeguard information technology (IT) systems and data from potential harm or compromise.

What are the different types of attacks?

The different types of cyber attacks are: Malware, Phishing, Ransomware, Distributed Denial of Service, Man-in-the-Middle, SQL Injection, Zero Day exploitation, Cross site scripting, Drive by download, Fileless Attack, IOT attack, Brute force arrack etc.

Essential terms used in cyber security

Antivirus Software, Firewall, Intrusion detection system, Intrusion prevention system, Security Information and Events management (SIEM), Patching and Patch Management, Access control, two factor authentication, Social Engineering, Penetration testing, Vulnerability, Authentication, Authorization, Encryption, Phishing, Injection etc.

Top 10 Hackers:

1. **Kevin Mitnick:** He hacked and obtained the full control over Pacific bells and he attacked North American Defence Command. He is a **White hat hacker and also grey hat too.**

2. **Anonymous:** in 2008 the group took issue with the Church of Scientology and begin disabling their websites, thus negatively impacting their search rankings in Google and overwhelming its fax machines with all-black images. In March 2008, a group of "Anons" marched passed Scientology centres around the world wearing the now-famous Guy Fawkes mask. As noted by The New Yorker, while the FBI and other law enforcement agencies have tracked down some of the group's more prolific members, the lack of any real hierarchy makes it almost impossible to identify or eliminate Anonymous as a whole. **They are grey hat hackers.**

3. **Adrian Lamo:** he is also called “The home less hacker”. He used an unprotected content management tool at Yahoo, modified reuters article and add a fake quote attribute to former attorney General Hohn Ashcroft. Lamo often hacked systems and then notified both the press and his victims. In some cases, he'd help clean up the mess to improve their security. As Wired points out, however, Lamo took things too far in 2002, when he hacked The New York Times' intranet, added himself to the list of expert sources and began conducting research on high-profile public figures. **He is a grey hat Hacker.**

4. **Albert Gonzalez:** He started himself as the “Trouble pack leader of computer nerds”. He eventually became active on criminal commerce site Shadowcrew.com and was considered one of its best hackers and moderators. At 22, Gonzalez was arrested in New

York for debit card fraud related to stealing data from millions of card accounts. To avoid jail time, he became an informant for the Secret Service, ultimately helping indict dozens of Shadowcrew members.

During his time as a paid informant, Gonzalez continued his in criminal activities. Along with a group of accomplices, Gonzalez stole more than 180 million payment card accounts from companies including OfficeMax, Dave and Buster's and Boston Market. The New York Times Magazine notes that Gonzalez's 2005 attack on US retailer TJX was the first serial data breach of credit information. Using a basic SQL injection, this famous hacker and his team created back doors in several corporate networks, stealing an estimated $256 million from TJX alone. During his sentencing in 2015, the federal prosecutor called Gonzalez's human victimization "unparalleled." **He is a Black hat hacker.**

5. **Mathew Bevan and Richard Pryce:** they are the team of British hacker who hacked into multiple military networks including Griffiss Air Force Base, the Defence Information System Agency and the Korean Atomic Research Institute (KARI). Bevan (Kuji) and Pryce (Data stream Cowboy) have been accused of nearly starting a third world war after they dumped KARI research onto American military systems. Bevan claims he was looking to prove a UFO conspiracy theory, and according to the BBC, his case bears resemblance to that of Gary McKinnon. Malicious intent or not, Bevan and Pryce demonstrated that even military networks are vulnerable. **They are Black hat hackers.**

6. **Jeanson James Ancheta:** Jeanson James Ancheta had no interest in hacking systems for credit card data or crashing networks to deliver social justice. Instead, Ancheta was curious about the use of bots—software-based robots that can infect and ultimately control computer systems. Using a series of large-scale "botnets," he was able to compromise more than 400,000 computers in 2005. According to Ars Technica, he then rented these machines out to advertising companies and was also paid to directly install bots or adware on specific systems. Ancheta was sentenced to 57 months in prison. This was the first time a hacker was sent to jail for the use of botnet technology. **He is a Black hat ethical Hacker.**

7. **Micheal Calce:** Michael Calce, also known as "Mafiaboy," discovered how to take over networks of university computers. He used their combined resources to disrupt the number-one search engine at the time: Yahoo. Within one week, he'd also brought down Dell, eBay, CNN and Amazon using a distributed-denial-of-service (DDoS) attack that overwhelmed corporate servers and caused their websites to crash. Calce's wake-up call was perhaps the most jarring for cybercrime investors and internet proponents. If the biggest websites in the world—valued at over $1 billion—could be so easily sidelined, was any online data truly safe? It's not an exaggeration to say that the development of cybercrime legislation suddenly became a top government priority thanks to Calce's hack. **He is a white hat hacker.**

8. **Kevin Poulsen:** Poulsen, using the alias Dark Dante, hacked into ARPANET, the Pentagon's computer network. Although he was quickly caught, the government decided not to prosecute Poulsen, who was a minor at the time. Instead, he was let off

with a warning.

Poulsen did not heed this warning and continued hacking. In 1988, Poulsen hacked a federal computer and dug into files pertaining to the deposed president of the Philippines, Ferdinand Marcos. When discovered by authorities, Poulsen went underground. While he was on the run, Poulsen kept busy, hacking government files and revealing secrets. Poulsen was soon arrested and barred from using a computer for three years. He has since converted to white hat hacking and journalism, writing about cyber security and web-related socio-political causes for Wired, The Daily Beast and his own blog Threat Level. Paulson also teamed with other leading hackers to work on various projects dedicated to social justice and freedom of information. Perhaps most notably, working with Adam Swartz and Jim Dolan to develop the open-source software SecureDrop, initially known as DeadDrop. Eventually, Poulsen turned over the platform, which enabled secure communication between journalists and sources, to the Freedom of Press Foundation.

9. **Jonathan James:** James attention was his hack into the computers of the United States Department of Defense. Even more impressive was the fact that James was only 15 at the time. In an interview with PC Mag, James admitted that he was partly inspired by the book *The Cuckoo's Egg*, which details the hunt for a computer hacker in the 1980s. His hacking allowed him to access over 3,000 messages from government employees, usernames, passwords, and other sensitive data.

   James was arrested in 2000 and was sentenced to a six months house arrest and banned from recreational computer use. However, a probation violation caused him to serve six months in jail. Jonathan James became the youngest person to be convicted of violating cyber crime laws. In 2007, TJX, a department store, was hacked and many customer's private information were compromised. Despite a lack of evidence, authorities suspect that James may have been involved.

   In 2008, James committed suicide by gunshot. According to the Daily Mail, his suicide note stated, "I have no faith in the 'justice' system. Perhaps my actions today, and this letter, will send a stronger message to the public. Either way, I have lost control over this situation, and this is my only way to regain control."

10. **Astra:** He Hacked into Dassault Group, and he stole cutting edge weapons technology software and data. **He is a White Hat hacker.**

Date: 24/08/23

Task-2

Determining the vulnerabilities of ports in networking:

1. Port 21: FTP (File Transfer Protocol) - Used for transferring files between a client and a server.

   Attacks: FTP Bounce Attack, Brute Force Attack

2. Port 22: SSH (Secure Shell) - Used for secure remote access and command execution on a network device.

   Attacks: Brute force Attack, SSH key theft.

3. Port 23: Telnet - Used for remote terminal access, but it's less secure than SSH.

   Attacks: Password Sniffing, Telnet Brute force.

4. Port 25: SMTP (Simple Mail Transfer Protocol) - Used for sending email messages.

   Attacks: Email Spoofing, SMTP Relay.

5. Port 53: DNS (Domain Name System) - Used for domain name resolution, translating human-readable domain names into IP addresses.

   Attacks: DNS Cache poisoning, DNS Amplification Attack.

6. Port 67-68: DHCP (Dynamic Host Configuration Protocol) - Used for automatic IP address assignment to network devices
   Attacks: DHCP spoofing.

7. Port 69: TFTP (Trivial File Transfer Protocol) - Used for simple file transfers, often in network device configurations.
   Attacks: TFTP Read/Write Abuse

8. Port 80: HTTP (Hypertext Transfer Protocol) - Used for serving web pages and unencrypted web traffic.

   Attacks: SQL Injection, Cross Site Scriping.

9. Port 110: POP3 (Post Office Protocol 3) - Used for retrieving email messages from a mail server.

   Attacks: Brute Force Attacks,

10. Port 123: NTP (Network Time Protocol) – NTP is used to sync the time on computer systems and nerworks. It’s a critical service for ensuring that device have accurate and sync time.

    Attack: NTP Amplification Attack

11. Port 143: IMAP (Internet Message Access Protocol) - Used for accessing and managing email on a mail server.

    Attacks: Brute force Attack, Man in the middle Attack, IMAP Injection, Email Spoofing and Phishing, DOS etc.

12. Port 443: HTTPS (Hypertext Transfer Protocol Secure) - Used for serving secure web pages with encryption.

    Attacks: SSL/TLS Attack.

Task-3:

Date: 25/08/2023

S.no	Name of Vulnerability	CWE Reference
1.	Broken Access Control	CWE 284- Improper Access Control
2.	Cryptographic Failures	CWE 327- Use of a broken or risky cryptographic algorithm
3.	Injection	CWE 91: XML Injection (aka Blind XPath Injection)
4.	Insecure Design	CWE 657 – Violation of Secure Design Principles
5.	Security Misconfiguration	CWE 732- Incorrect permission Assignment for critical resource

1. **CWE: CWE 284- Improper Access Control**
   OWASP Category: A01 2021 Broken Access Control
   Description: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

   Business Impact: In Scenarios the permissions and resources for any services are given access to the authorized users only. If improper access control exists, unauthorized users may gain access to sensitive or confidential information that they should not have access to. This could result in the exposure of sensitive customer data, proprietary business information, financial records, or any other confidential data that the organization handles. This unauthorized access or data exposure can have a several consequences for business including, reputation damage, Legal and regulatory consequences, financial loss, competitive disadvantage, operational disreputation, customer impact.
2. **CWE: CWE 327- Use of a broken or risky cryptographic algorithm**
   OWASP Category: A02 2021 Cryptographic Failure.
   Description: The product uses a risky or broken cryptographic algorithm or protocol.

Business Impact: Using a non-standard or well-known insecure algorithm is dangerous because a determined adversary may be able to break the algorithm and compromise whatever data has been protected. When an organisation uses cryptographic algorithms that are broken or known to be risky, it opens the door to potential security breaches and data loss. Here is how this vulnerability can impact a business like data exposure, loxss of trust, competitive disadvantage etc.

3. **CWE: CWE 91: XML Injection (aka Blind XPath Injection)**
   OWASP A03 2021 Injection
   Description: The product does not properly neutralize special elements that are used in XML, allowing attackers to modify the syntax, content, or commands of the XML before it is processed by an end system.

   Business Impact: Hackers uses XML injection, within XML, special elements could include reserved words or characters like “<", ">", """, and "&", which could then be used to add new data or modify XML syntax. So when an XML injection vulnerability exists in an application, it can have significant repercussions for a business including Data Manipulation, Un authorized Access, Application Disruption, Financial Loss etc.

4. **CWE: CWE 657 – Violation of Secure Design Principles**
   OWASP Category: A04 2021 – Insecure Design
   Description: The product violates the well-established principles for secure design.

   Business Impact: If a company or organisation violates the design principles this will results in a weakness or make it easier for the developers to introduce related weaknesses during implementation. Because the entire security and core part is centred around the design architecture of that application. If a hacker breaches its deign it can be resource intensive to fix design problems. When an application or system violates secure design principles, it can have several adverse effects on a business-like Security vulnerability, Data breaches, Reputation Damage, regulatory nan compliance, Increased development and maintenance costs, loss of competitive advantages. Etc.

5. **CWE: CWE 732- Incorrect permission Assignment for critical resource**
   OWASP Category: A05 2021- Security Misconfigurations
   Description: The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

   Business Impact: When a resource is given a permission setting that provides access to a wider range of actors than required, it could lead to the exposure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution, or sensitive user data. For example, consider a misconfigured storage account for the cloud that can be read or written by a public or anonymous user.

Date: 28/08/2023

Task-4

The different types of web application security risks are:

1. Content security policy bypass
2. insecure file uploads
3. business logic flaws
4. code execution vulnerability
5. frame injection click jacking
6. data tampering
7. captcha bypass
8. cookie security issue
9. Insecure third-party integration
10. URL manipulation
11. DOM clobbering attack
12. forced browsing

1. **Content security policy Bypass:** Content Security Policy or CSP is a built-in browser technology which **helps protect from attacks such as cross-site scripting (XSS)**. It lists and describes paths and sources, from which the browser can safely load resources. The resources may include images, frames, javascript and more. Here is an example of resources being allowed from the local domain (self) to be loaded and executed in-line and allow string code executing functions like eval, setTimeout or setInterval.

   Content Security Policy is implemented via **response headers** or **meta elements of the HTML page**. The browser follows the received policy and actively blocks violations as they are detected.

   CSP bypass occurs when a web application's CSP policy is not configured correctly or when there are security flaws in the website that allows attacker to inject malicious code.

2. **Insecure file uploads:** Insecure file uploads vulnerability refers to a security issue where a web application allows users to upload files without proper validation and controls. This can lead to various types of attacks, such as remote code execution, path traversal, cross-site scripting (XSS), and server-side request forgery (SSRF). Attackers can exploit this vulnerability to upload malicious files, overwrite existing files, execute arbitrary code, or gain unauthorized access to sensitive data. It is important for web applications to implement proper security measures, such as file type validation, file size restrictions, and secure file storage, to mitigate this vulnerability.

3. **Business logic flaws:** Business Logic Flaws (BLFs), also known as application logic flaws or logic vulnerabilities, are security weaknesses that occur when an application's design or logic doesn't adequately enforce the business rules and policies of the application. These vulnerabilities can lead to unauthorized access, data manipulation, financial losses, and other security breaches.

   The impact of the business logic flaws can be severe and wide ranging depending on the specific vulnerability and the applications. Common consequences include unauthorized access to sensitive info, manipulation of financial transactions, bypassing security controls and business rules.

4. **Code Execution Vulnerability:** Code execution vulnerability, often referred to as "code execution flaw" or "remote code execution (RCE) vulnerability," is a serious security issue in software and web applications. It occurs when an attacker can execute arbitrary code or commands on a target system or application, usually with elevated privileges. This can lead to unauthorized access, data theft, system compromise, and other malicious actions.

5. **Frame Injection (click jacking):** Frame Injection, also known as Clickjacking, is a type of web attack where an attacker tricks a user into clicking on something different from what the user perceives, by overlaying or embedding malicious content within a legitimate website. The goal of frame injection is to manipulate user interactions and potentially perform actions on behalf of the user without their knowledge or consent.

   In this attacker creates a malicious web page or identifies a legitimate web page vulnerable to clickjacking. The attacker overlays or embeds the target web page within an iframe on an malicious page. The iframe is typically positioned so that it covers specific elements or buttons on the target page.

   When a user visits the attacker's malicious page and interacts with it (e.g., clicking on a button), they unwittingly trigger actions on the underlying legitimate page, such as making unauthorized transactions, changing account settings, or sharing sensitive information.

   The user is usually unaware that they are interacting with the legitimate page underneath the malicious overlay. They may believe they are performing actions on the attacker's page when, in reality, they are affecting their account on the legitimate site.

6. **Data Tampering:** Data tampering vulnerability, also known as data manipulation vulnerability, refers to a security weakness or flaw in a system or application that allows unauthorized individuals to alter, modify, or manipulate data in a way that compromises the integrity, confidentiality, or availability of that data. This vulnerability can have serious consequences, including data breaches, fraud, and the compromise of critical systems.

   there are different types of data tampering vulnerabilities like Input validation issue, Inadequate authentication and authorization, insecure data storage, lack od integrity checks, and insufficient logging and monitoring.

7. **Captcha bypass:** A CAPTCHA bypass vulnerability refers to a security flaw or weakness in a system's implementation of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) that allows automated scripts or bots to circumvent the CAPTCHA challenge, gaining unauthorized access or privileges on a website or online service. CAPTCHAs are designed to distinguish between human users and automated bots by presenting a challenge that's difficult for computers to solve but relatively easy for humans. A CAPTCHA bypass vulnerability undermines the effectiveness of this protection mechanism.

   Captcha bypass vulnerability occurs when a flaw in the captcha implementation allows automated bots to easily solve or bypass the challenge rendering the captcha inefficient in distinguishing between humans and bots.

8. **Cookie security issue:** Cookie security issues refer to vulnerabilities or weaknesses in the way web cookies are implemented or managed, which can lead to security risks and potential exploitation by malicious actors. Cookies are small pieces of data that are sent by a web server to a user's browser and stored on their device. They are commonly used to track user sessions, store user preferences, and enable various functionalities on websites. However, when not properly secured, cookies can pose significant security risks.

9. **URL Manipulation:** URL manipulation, also known as URL tampering or URL hacking, is a type of cyberattack or manipulation where an attacker modifies or manipulates a URL (Uniform Resource Locator) to gain unauthorized access to a web application, perform unintended actions, or exploit vulnerabilities in a website's functionality. This technique is often used by malicious actors to bypass security measures and access restricted content or perform actions they are not supposed to.

10. **DOM clobbering Attack**: DOM (Document Object Model) clobbering is a security vulnerability that occurs when an attacker manipulates a web page's DOM structure by injecting malicious code or by taking advantage of weakly named variables or properties, potentially leading to unexpected behaviour or security breaches in a web application. This type of attack can be used to alter the behavior of a web application, steal sensitive data, or even execute arbitrary code on the client-side.

    In this Attacker can overwrite properties or methods of DOM objects or globa variables, leading to unexpected behaviour.

Task-5

10 web server attacks:

1. Remote file Inclusion (RFI) or Local file Inclusion
2. Buffer Overflow
3. Zero-day attacks
4. Web server firewall evasion
5. OAuth token hijacking
6. Cookie poisoning
7. HTTP verb tampering
8. Web shell upload
9. LDAP attack
10. Smurf attack

1. Remote file Inclusion: A Web File Inclusion Attack, also known as Local File Inclusion (LFI) or Remote File Inclusion (RFI) attack, is a type of security vulnerability that occurs in web applications. It allows attackers to include files on a web server through the web application. This attack can have serious consequences, including unauthorized access to sensitive files, execution of arbitrary code, and data leakage.

   In this RFI attack, the attacker includes files from the remote servers, whereas in LFI the files are from the same server web applications. This typically occurs when a web application dynamically loads files or content from external sources such as using user-provided URLs for file inclusion. If input validation is weak or non-existent, an attacker can supply a malicious URL pointing to a file on a remote server, which can then be included and executed on the target server.

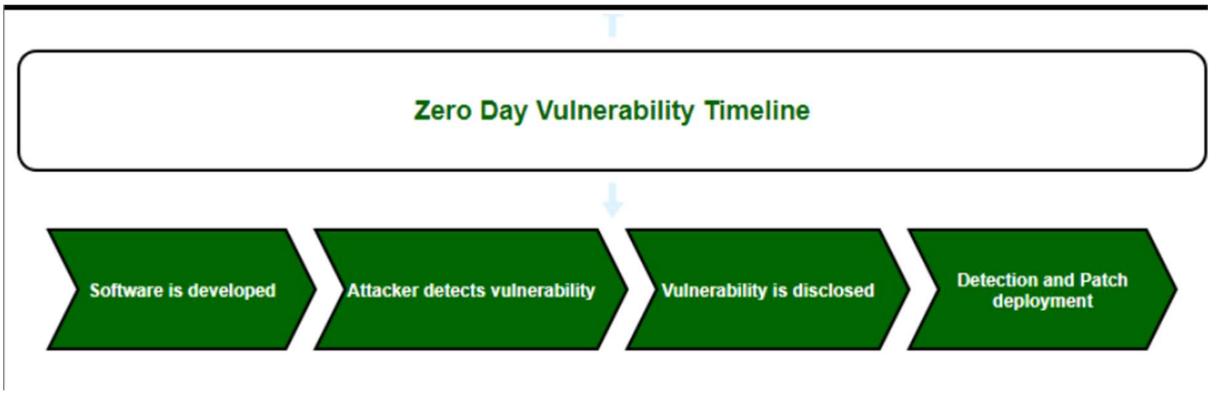
   For example, an attacker could craft a URL like “http://malicious-site.com/malicious-script.php” and inject it into the web application, causing it to fetch and execute the remote script.

2. Buffer Overflow: Buffer overflow is a software coding error or vulnerability that can be exploited by hackers to gain unauthorized access to corporate systems. It is one of the best-known software security vulnerabilities yet remains fairly common. This is partly because buffer overflows can occur in various ways and the techniques used to prevent them are often error-prone.

   A buffer overflow attack takes place when an attacker manipulates the coding error to carry out malicious actions and compromise the affected system. The attacker alters the application’s execution path and overwrites elements of its memory, which amends the program’s execution path to damage existing files or expose data.

3. Zero-day attacks: Zero-day exploit is a type of cyber security attack that occur on the same day the software, hardware or firmware flaw is detected by the manufacturer. As it’s been zero days since the security flaw was last exploit, the attack is termed as zero-day exploit or zero-day attack. This kind of cyber-attacks are considered dangerous because the developer has not had the chance to fix the flaw yet. Zero-day

exploit typically targets large organizations, government departments, firmware, hardware devices, IoT, users having access to valuable business data, etc.


Zero Day Vulnerability Timeline
Software is developed
Attacker detects vulnerability
Vulnerability is disclosed
Detection and Patch deployment

4. Web server firewall evasion: Web server firewall evasion, also known as firewall bypass or firewall evasion techniques, refers to methods used by attackers to circumvent or bypass the security mechanisms of a web application firewall (WAF) or network firewall, allowing malicious traffic to reach the web server or web application behind the firewall. Firewalls are designed to protect web applications from various threats, including SQL injection, Cross-Site Scripting (XSS), and other types of attacks. However, attackers continuously develop new techniques to evade these defences.

5. OAuth token Hijacking: OAuth token hijacking, also known as OAuth token theft or OAuth token interception, is a security threat that occurs when an attacker gains unauthorized access to OAuth tokens used for authentication and authorization in OAuth-based authentication flows. OAuth is a widely-used protocol for delegated authorization, allowing applications to access a user's resources (e.g., data on a third-party service) without exposing their credentials. OAuth tokens are used to grant this access, and if they fall into the wrong hands, they can be misused for various malicious purposes.

6. Cookie poisoning: Cookie poisoning is a type of cyberattack that involves manipulating or tampering with cookies in web applications to compromise the security, privacy, or functionality of a website. Cookies are small pieces of data that a web server sends to a user's browser and are often used for various purposes, including session management, user authentication, and tracking user preferences. When cookies are poisoned, it means that they are altered in a way that serves the attacker's interests rather than the website's intended functionality.

7. HTTP verb hijacking: HTTP verb hijacking, also known as HTTP method smuggling or HTTP verb tampering, is a web security vulnerability that occurs when an attacker manipulates the HTTP request methods (verbs) used in a web application's communication with the server. This attack can lead to various security risks and can potentially bypass security controls and access unauthorized resources. HTTP request

methods, such as GET, POST, PUT, DELETE, and others, are part of the HTTP protocol and are used to indicate the action that should be performed on a resource.

In this an attacker manipulates the HTTP requests in such a way that different parts of the system interpret the requests differently. This can occur because of inconsistent or misconfigurations in how frontend proxies, load balancers and backend servers handle HTTP requests.

8. Web shell upload: A web shell upload vulnerability is a security flaw in a web application that allows an attacker to upload and execute malicious scripts or code on a web server. This type of vulnerability can have serious consequences, as it grants the attacker unauthorized access to the server, allowing them to manipulate files, steal data, or even take control of the entire web server.

   A web shell upload vulnerability occurs when the application's file upload functionality is not properly secured or validated. This may include inadequate input validation, insufficient file type checks, or weak access controls on the uploaded files.

9. LDAP Attack: LDAP (Lightweight Directory Access Protocol) attacks refer to a category of cyberattacks that target LDAP-based directory services and systems. LDAP is a protocol used for accessing and managing directory information, such as user accounts and organizational data, in a network. Attackers exploit LDAP vulnerabilities to gain unauthorized access, extract sensitive information, or manipulate directory data.

   Some of the LDAP attack techniques are LDAP injection, Brute force attack, DOS arrack, Password Spraying, Credential theft, data enumeration, MitM attack, pass the hash attack, unauthorized searches etc.

10. Smurf attack: A Smurf attack is a type of network-based Distributed Denial of Service (DDoS) attack that targets the Internet Control Message Protocol (ICMP). This attack was more prevalent in the past but is now relatively rare due to improved network security practices and the use of anti-smurf measures by Internet Service Providers (ISPs) and network administrators.

    The attacker sends a large number of ICMP Echo Request (ping) packets to an IP broadcast address on a target network. A broadcast address sends the packet to all devices within the specified network segment. The attacker spoofs the source IP address in the ICMP packets to appear as if they are coming from the victim's IP address. This makes it seem like the victim is sending the ping requests. When the ICMP Echo Request packets are broadcast, every device in the target network segment that receives the broadcast responds to the victim's IP address with an ICMP Echo Reply (pong). This results in a flood of responses directed at the victim. The victim's network and system resources become overwhelmed by the sheer volume of ICMP Echo Reply packets, leading to degraded or disrupted network services. In some cases, the victim's network can become entirely inaccessible.

Date: 30/08/2023

Task-6

CIS top 20 critical security controls:

1. **Inventory and Control of Hardware assets:** Identifying and Maintaining an up-to-date inventory of all devices on the organization network. Regularly review and update the inventory.
2. **Inventory and Control of Software assets:** Use software inventory tools to automate all software documentation to ensure unauthorized software is blocked from executing on assets. Implement policies and processes for software installation and approval to prevent unauthorized software from being installed.
3. **Continuous vulnerability management:** Utilize a complaint vulnerability scanning tool to monitor your systems on the network to identify vulnerabilities and keep them up to date.
4. **Controlled use of administrative privileges:** Limit and control access to administrative privileges ensuring that only authorized personals have elevated access. Implement the principle of least privileges (PoLP) to minimize risk.
5. **Secure Configuration for Hardware and Software on Mobile devices laptops workstations and Serves:** Establish and enforce secure configuration settings for all devices and software. This includes applying patches, disabling unnecessary services, and configuring security settings to minimize vulnerabilities.
6. **Maintaining, Monitoring and Analysing of Audit logs**: Ensure that local logging has been enabled and appropriate logs are aggregated to a central log management system for analysis and review. Regularly monitor and analyse logs for suspicious activity and potential security incidents.
7. **Email and web browser protections:** Implement security measures to protect against email and web-based threats, such as phishing attacks, malicious attachments, and web browser vulnerabilities.
8. **Malware Defences:** Utilize centrally managed anti-malware software to monitor and defend each organization's workstations and servers continuously. Deploy antivirus, antimalware, and intrusion detection/prevention systems (IDS/IPS) to detect and block malicious code and activities.
9. **Limitations and Control of network ports, Protocols, and Services:** Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system, and perform automated port scans on a regular basis.
10. **Data Recovery Capabilities:** Implement data backup and recovery procedures to ensure data integrity and availability in the event of data loss or system compromise. It ensures that all systems data and key systems are automatically backed up on a regular basis.
11. **Secure Configuration for network devices such as Firewall, Routers, and switches:** Compare all network device configurations against approved security configurations, and manage all network devices using multi-factor authentication and encrypted sessions.

12. **Boundary defence**: Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges.
13. **Data protection:** Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.
14. **Controllled Access based on the need to know:** Implement strong Access and authentication mechanisms to ensure that users can access only information and resources necessary for their roles.
15. **Wireless Access Control**: Leverage the advanced encryption standard to encrypt wireless data in transit and create a separate wireless network for personal or untrust devices.
16. **Account monitoring and Control:** Continuously monitor user accounts for suspicious or unauthorized activities, and promptly disable or remove accounts that are no longer needed.
17. **Implement a security awareness and training program:** Perform a skills gap analysis and train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.
18. **Application Software Security**: Ensure secure coding practices appropriate to the programming languages and develop environment being used.
19. **Incident response and management**: Establish an incident response plan and team to detect, respond to, and recover from security incidents effectively.
20. **Penetration test and red team exercise**: Establish a program for penetration tests that includes a full scope of common attacks, such as wireless, client-based, and web application attacks.

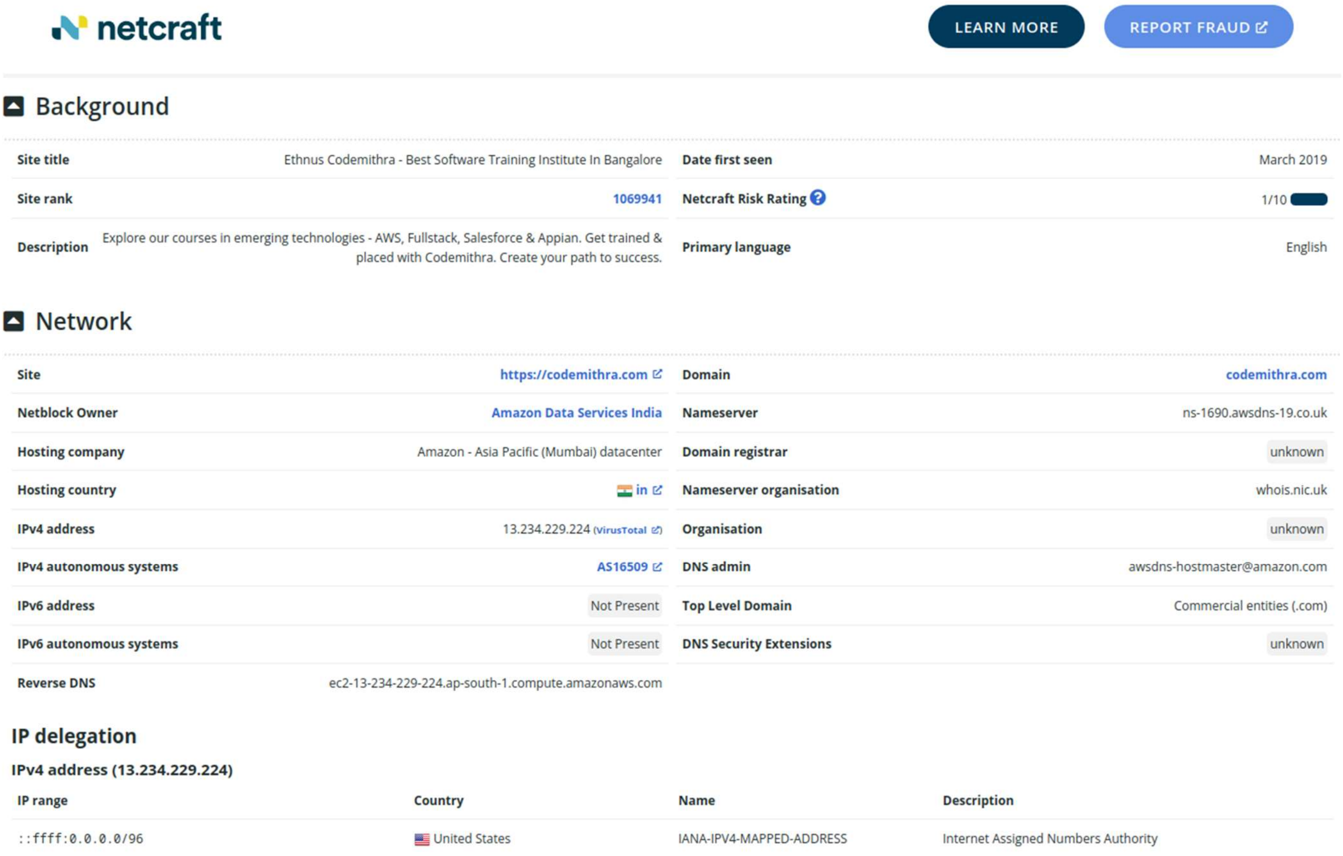
Date: 01/09/2023

Task-7

Select any website and do footprint and reconnaissance on it.

Let us take a website https://codemithra.com/ **and lets do foot printing on that website.**

We can use netcraft tool.



netcraft LEARN MORE REPORT FRAUD

Background

Site title	Ethnus Codemithra - Best Software Training Institute In Bangalore	**Date first seen**	March 2019
Site rank	1069941	**Netcraft Risk Rating**	1/10
Description	Explore our courses in emerging technologies - AWS, Fullstack, Salesforce & Appian. Get trained & placed with Codemithra. Create your path to success.	**Primary language**	English

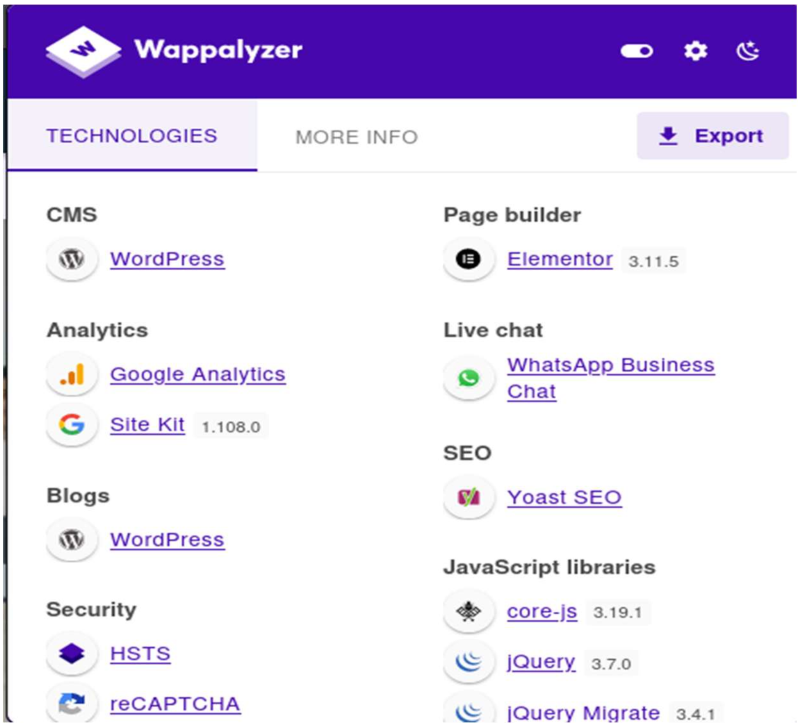
Network

Site	https://codemithra.com	**Domain**	codemithra.com
Netblock Owner	Amazon Data Services India	**Nameserver**	ns-1690.awsdns-19.co.uk
Hosting company	Amazon - Asia Pacific (Mumbai) datacenter	**Domain registrar**	unknown
Hosting country	in	**Nameserver organisation**	whois.nic.uk
IPv4 address	13.234.229.224 (VirusTotal)	**Organisation**	unknown
IPv4 autonomous systems	AS16509	**DNS admin**	awsdns-hostmaster@amazon.com
IPv6 address	Not Present	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	Not Present	**DNS Security Extensions**	unknown
Reverse DNS	ec2-13-234-229-224.ap-south-1.compute.amazonaws.com		

IP delegation

IPv4 address (13.234.229.224)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority



Wappalyzer

TECHNOLOGIES MORE INFO Export

CMS
- WordPress

Analytics
- Google Analytics
- Site Kit 1.108.0

Blogs
- WordPress

Security
- HSTS
- reCAPTCHA

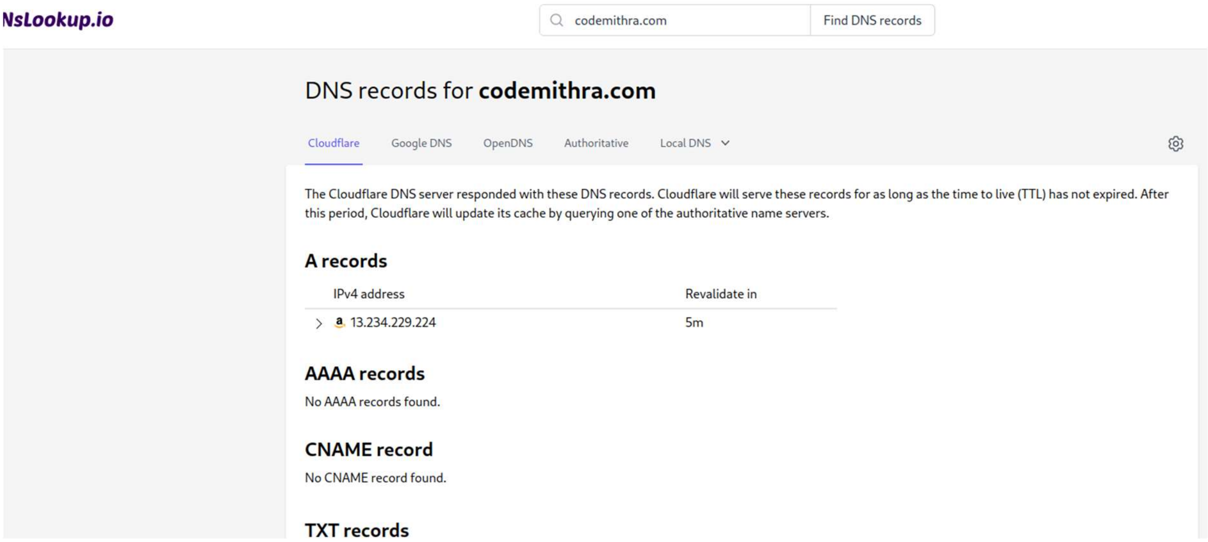
Page builder
- Elementor 3.11.5

Live chat
- WhatsApp Business Chat

SEO
- Yoast SEO

JavaScript libraries
- core-js 3.19.1
- jQuery 3.7.0
- jQuery Migrate 3.4.1

We can use **nslookup** tool for knowing its IP addresses.



DNS records for **codemithra.com**

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
13.234.229.224	5m

AAAA records

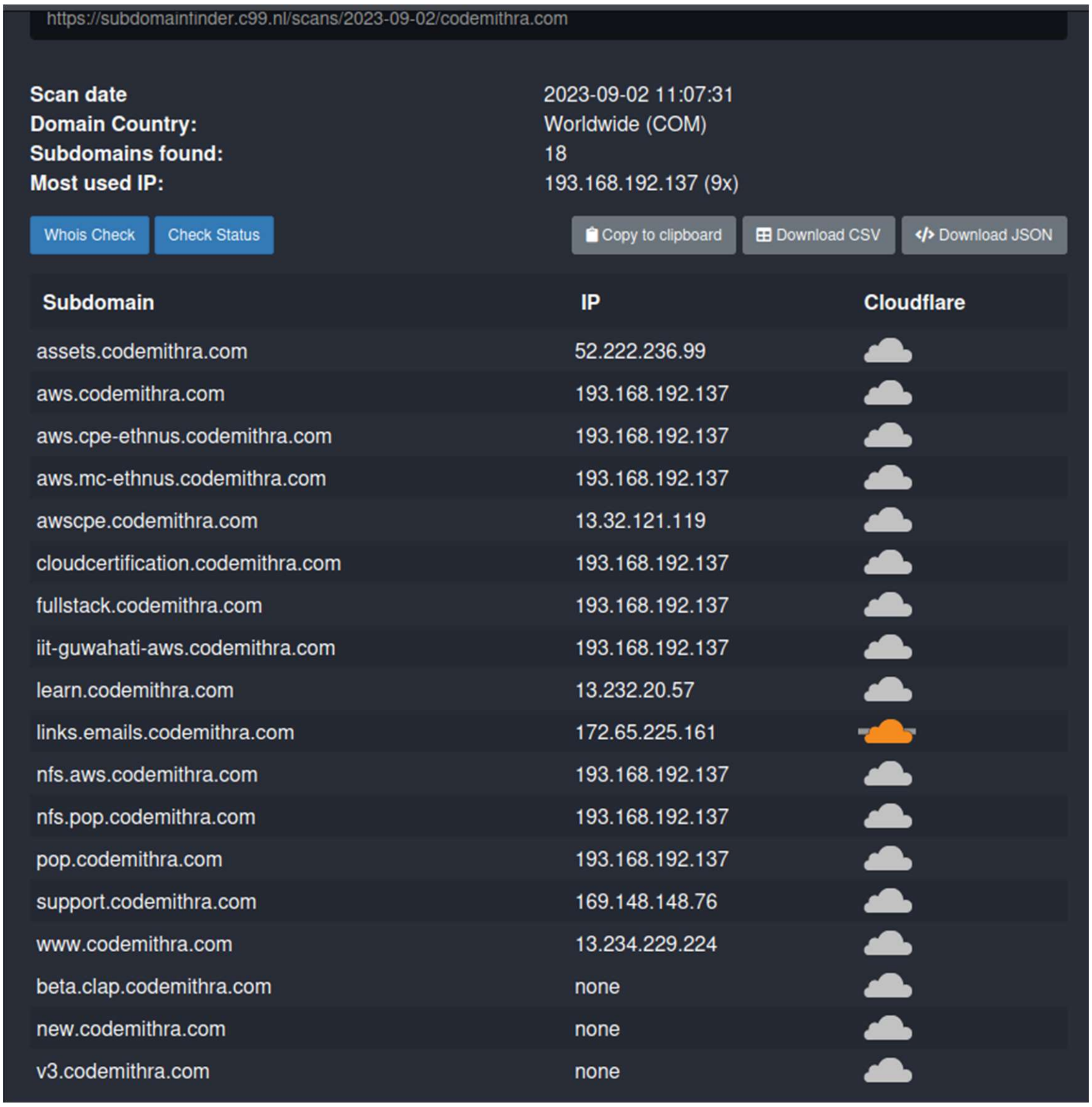
No AAAA records found.

CNAME record

No CNAME record found.

TXT records

For finding its active and passive subdomains we can use **subdomain finder** tool or **sublist3r** tool for that.



https://subdomainfinder.c99.nl/scans/2023-09-02/codemithra.com

Scan date	2023-09-02 11:07:31
Domain Country:	Worldwide (COM)
Subdomains found:	18
Most used IP:	193.168.192.137 (9x)

Subdomain	IP	Cloudflare
assets.codemithra.com	52.222.236.99	☁
aws.codemithra.com	193.168.192.137	☁
aws.cpe-ethnus.codemithra.com	193.168.192.137	☁
aws.mc-ethnus.codemithra.com	193.168.192.137	☁
awscpe.codemithra.com	13.32.121.119	☁
cloudcertification.codemithra.com	193.168.192.137	☁
fullstack.codemithra.com	193.168.192.137	☁
iit-guwahati-aws.codemithra.com	193.168.192.137	☁
learn.codemithra.com	13.232.20.57	☁
links.emails.codemithra.com	172.65.225.161	☁
nfs.aws.codemithra.com	193.168.192.137	☁
nfs.pop.codemithra.com	193.168.192.137	☁
pop.codemithra.com	193.168.192.137	☁
support.codemithra.com	169.148.148.76	☁
www.codemithra.com	13.234.229.224	☁
beta.clap.codemithra.com	none	☁
new.codemithra.com	none	☁
v3.codemithra.com	none	☁

Date: 04/09/2023

Task – 8:

- Download Nessus tool and do a scan on any website and analyse the scan report.

CVSS score tells the severity of the website.
or mitre framework
Nessus essential edition tool.
shodan.io //scans the entire website and gives the open ports

Report Procedure:
vulnerability name
CWE:
OWASP:
Description:
Business Impact:
Affected Url:
POC (Proof of Concept):
Remediation:

Date: 05/09/2023

Task – 9:

Exploring Nmap port scanning tool and exploring the commands in it.

Date: 11/09/2023

Task - 10:

Write a documentation on win collect and Standalone win collect.

Documentation: WinCollect and Standalone WinCollect

Table of Contents

1. Introduction to WinCollect

WinCollect is a powerful log collection agent developed by IBM. It is designed to gather and forward Windows event logs, as well as logs from other Microsoft and non-Microsoft platforms, to a centralized log management system. WinCollect is an integral part of many organizations' security information and event management (SIEM) strategies, providing essential log data for security analysis and compliance monitoring.

2. Standalone WinCollect

Standalone WinCollect refers to a specific configuration of WinCollect that operates independently on Windows-based systems without the need for an additional collector or aggregation server. This mode is particularly useful for small to medium-sized organizations or for collecting logs from isolated environments.

In Standalone WinCollect:

- WinCollect runs as a self-contained agent on each Windows machine.
- It collects logs locally, processes them, and forwards them directly to a designated SIEM or log management system.
- This mode is efficient for situations where centralization of logs isn't a requirement, and logs are sent directly to the SIEM.

3. Key Features and Benefits

a. Universal Log Collection

WinCollect supports the collection of logs from various Windows-based systems, including servers, workstations, and specialized Microsoft applications. It can also collect logs from non-Microsoft platforms, making it versatile in heterogeneous environments.

b. **Event Log Normalization**
WinCollect normalizes event logs into a common format, making it easier for security analysts to correlate and analyze log data across the organization. Normalization ensures that logs are presented consistently, regardless of the source.

c. **Real-time and Scheduled Collection**
It supports both real-time log collection and scheduled collection tasks, allowing organizations to choose the most suitable approach based on their specific log management needs.

Benefits

a. **Improved Security Monitoring**
WinCollect enhances an organization's security posture by providing real-time access to Windows event logs, enabling the rapid detection of security incidents, and supporting incident response activities.

b. **Simplified Compliance Reporting**
For organizations subject to regulatory compliance requirements, WinCollect simplifies the process of collecting and forwarding logs necessary for compliance audits and reporting.

c. **Scalability**
WinCollect can be scaled to accommodate the needs of organizations of various sizes. Whether collecting logs from a handful of machines or thousands, it can efficiently manage log data.

4. Deployment Options

WinCollect offers flexibility in deployment:

- **Standalone Mode**: As previously mentioned, it can operate as a standalone agent on individual Windows machines.
- **Collector Mode**: In larger environments, WinCollect agents can send logs to a centralized collector before forwarding them to the SIEM system. This method reduces the load on individual systems and optimizes network traffic.

## 5. Use Cases

WinCollect is a versatile log collection solution suitable for a wide range of use cases, including:

- **Security Monitoring**: It helps organizations detect and respond to security incidents by collecting and forwarding event logs that contain critical security information.

- **Compliance Reporting**: WinCollect simplifies compliance with regulations such as HIPAA, GDPR, or PCI DSS by efficiently collecting logs required for audit and reporting purposes.
- **Forensics and Investigation**: Security analysts can use WinCollect logs for forensic analysis, investigating security breaches, and understanding the timeline of events leading up to an incident.

## 6. Conclusion

WinCollect, whether used in Standalone or Collector mode, is an essential component of modern log management and security strategies. Its ability to efficiently collect and forward logs from Windows-based systems, along with its event log normalization features, enhances an organization's ability to monitor security, meet compliance requirements, and investigate incidents effectively. By tailoring its deployment to specific needs, organizations can harness the full potential of WinCollect to bolster their cybersecurity defenses.cumentation: WinCollect and Standalone WinCollect

## Table of Contents

1. Introduction to WinCollect

WinCollect is a powerful log collection agent developed by IBM. It is designed to gather and forward Windows event logs, as well as logs from other Microsoft and non-Microsoft platforms, to a centralized log management system. WinCollect is an integral part of many organizations' security information and event management (SIEM) strategies, providing essential log data for security analysis and compliance monitoring.

## 2. Standalone WinCollect

Standalone WinCollect refers to a specific configuration of WinCollect that operates independently on Windows-based systems without the need for an additional collector or aggregation server. This mode is particularly useful for small to medium-sized organizations or for collecting logs from isolated environments.

In Standalone WinCollect:
- WinCollect runs as a self-contained agent on each Windows machine.
- It collects logs locally, processes them, and forwards them directly to a designated SIEM or log management system.

- This mode is efficient for situations where centralization of logs isn't a requirement, and logs are sent directly to the SIEM.

## 3. Key Features and Benefits

### 3.1 Key Features

#### a. Universal Log Collection
WinCollect supports the collection of logs from various Windows-based systems, including servers, workstations, and specialized Microsoft applications. It can also collect logs from non-Microsoft platforms, making it versatile in heterogeneous environments.

#### b. Event Log Normalization
WinCollect normalizes event logs into a common format, making it easier for security analysts to correlate and analyze log data across the organization. Normalization ensures that logs are presented consistently, regardless of the source.

c. Real-time and Scheduled Collection
It supports both real-time log collection and scheduled collection tasks, allowing organizations to choose the most suitable approach based on their specific log management needs.

### 3.2 Benefits

#### a. Improved Security Monitoring
WinCollect enhances an organization's security posture by providing real-time access to Windows event logs, enabling the rapid detection of security incidents, and supporting incident response activities.

#### b. Simplified Compliance Reporting
For organizations subject to regulatory compliance requirements, WinCollect simplifies the process of collecting and forwarding logs necessary for compliance audits and reporting.

#### c. Scalability
WinCollect can be scaled to accommodate the needs of organizations of various sizes. Whether collecting logs from a handful of machines or thousands, it can efficiently manage log data.

4. Deployment Options

WinCollect offers flexibility in deployment:

- **Standalone Mode**: As previously mentioned, it can operate as a standalone agent on individual Windows machines.

- **Collector Mode**: In larger environments, WinCollect agents can send logs to a centralized collector before forwarding them to the SIEM system. This method reduces the load on individual systems and optimizes network traffic.

## 5. Use Cases

WinCollect is a versatile log collection solution suitable for a wide range of use cases, including:

- **Security Monitoring**: It helps organizations detect and respond to security incidents by collecting and forwarding event logs that contain critical security information.
- **Compliance Reporting**: WinCollect simplifies compliance with regulations such as HIPAA, GDPR, or PCI DSS by efficiently collecting logs required for audit and reporting purposes.
- **Forensics and Investigation**: Security analysts can use WinCollect logs for forensic analysis, investigating security breaches, and understanding the timeline of events leading up to an incident.

## 6. Conclusion

WinCollect, whether used in Standalone or Collector mode, is an essential component of modern log management and security strategies. Its ability to efficiently collect and forward logs from Windows-based systems, along with its event log normalization features, enhances an organization's ability to monitor security, meet compliance requirements, and investigate incidents effectively. By tailoring its deployment to specific needs, organizations can harness the full potential of WinCollect to bolster their cybersecurity defenses.