Security Operations Center IDBRT

# Summary

In organizations we need a robust SOC to detect and prevent any security incident.

* We need EDR to detect and prevent malicious activities.
* We need WAF and Firewall to restrict unwanted traffic.
* We need SIEM for meaningful analysis of logs from all sources.
* We need threat intelligence from open and commercial sources to patch any known vulnerability
* We need to perform regular scanning and VAPT on our systems (black/white)
* For detailed analysis and forensics, we can do Threat hunting.
* We need to have all security standards as per industry applicable acts and frameworks

# Stage 1 – List of vulnerabilites

| **Serial Number** | **OWASP Category Name** | **Associated CWE** |
| --- | --- | --- |
| 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-89 (SQL Injection) |
| 4 | Insecure Design | CWE-691 (Insufficient Protection from Relational Database) |
| 5 | Security Misconfiguration | CWE-209 (Information Exposure Through an Error Message) |
| 6 | Vulnerable and Outdated Components | CWE-937 (Improper Control of Filename for Include/Require Statement in PHP Program) |
| 7 | Identification and Authentication Failures | CWE-287 (Improper Authentication) |
| 8 | Software and Data Integrity Failures | CWE-494 (Download of Code Without Integrity Check) |
| 9 | Security Logging and Monitoring Failures | CWE-778 (Insufficient Logging) |
| 10 | Server-Side Request Forgery (SSRF) | CWE-918 (Server-Side Request Forgery (SSRF)) |

1. **Broken Access Control**
   * CWE: CWE-284
   * OWASP Category: A01:2021
   * Description: Broken access control occurs when an application fails to properly enforce access restrictions, allowing unauthorized users to access sensitive functionality or data.
   * Business Impact: The impact can be severe, leading to unauthorized data exposure, privilege escalation, and potential financial losses due to compromised user accounts or sensitive information.
2. **Cryptographic Failures**
   * CWE: CWE-327
   * OWASP Category: A02:2021
   * Description: Cryptographic failures refer to weaknesses in encryption, hashing, or key management. These vulnerabilities can lead to data breaches, unauthorized access, and compromised confidentiality.
   * Business Impact: Organizations may suffer reputational damage, legal consequences, and financial losses if sensitive data is exposed due to cryptographic failures[1](https://owasp.org/Top10/).
3. **Injection**
   * CWE: CWE-89
   * OWASP Category: A03:2021
   * Description: Injection flaws occur when untrusted data is inserted into a command or query, leading to unintended execution. Common examples include SQL injection and OS command injection.
   * Business Impact: Successful injections can result in data manipulation, unauthorized access, and system compromise, affecting both user trust and business operations[1](https://owasp.org/Top10/).
4. **Insecure Design**
   * CWE: CWE-691
   * OWASP Category: A04:2021
   * Description: Insecure design flaws stem from poor architectural decisions. These vulnerabilities may not be fixable through code changes alone and require rethinking the system’s design.
   * Business Impact: Insecure design can lead to long-term security issues, costly rework, and increased maintenance efforts. It undermines the foundation of the application’s security posture.
5. **Security Misconfiguration**
   * CWE: CWE-209
   * OWASP Category: A05:2021
   * Description: Security misconfiguration occurs when an application, server, or component is not properly configured. Default settings, unnecessary features, and exposed sensitive information contribute to this risk.
   * Business Impact: Misconfigurations can lead to unauthorized access, data leaks, and service disruptions. Organizations may face legal penalties and damage to their reputation.
6. **Vulnerable and Outdated Components**

* CWE: CWE-937
* OWASP Category: A06:2021
* Description: Using vulnerable components refers to incorporating outdated or known-to-be-flawed third-party libraries, frameworks, or software components. These components may have unpatched security issues.
* Business Impact: Exploiting vulnerable components can lead to data breaches, system compromise, and regulatory violations. Organizations must actively manage their dependencies to reduce risk

1. **Identification and Authentication Failures**
   * **CWE**: CWE-287
   * **OWASP code -** A07:2021
   * **Description**: Previously known as “Broken Authentication,” this category emphasizes the importance of confirming user identity, proper authentication, and session management. Common issues include weak passwords, missing multi-factor authentication, and session management flaws.
   * **Business Impact**: Authentication weaknesses can lead to unauthorized access, data leaks, and compromised accounts. Implementing strong authentication mechanisms is crucial.
2. **Software and Data Integrity Failures**
   * **CWE**: CWE-494
   * **OWASP Category**: A08:2021
   * **Description**: This new category focuses on assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. Issues include insecure handling of plugins, libraries, and auto-updates. Common Weakness Enumerations (CWEs) include improper code download and insecure deserialization.
   * **Business Impact**: Integrity failures can lead to unauthorized code execution, data corruption, and system compromise. Verifying software and data integrity is essential.
3. **Security Logging and Monitoring Failures**
   * **CWE**: CWE-778
   * **OWASP Code -** A09:2021
   * **Description**: This category emphasizes the importance of detecting, escalating, and responding to active breaches through effective logging and monitoring. Issues include insufficient logging, unclear log messages, and inadequate alerting thresholds.
   * **Business Impact**: Without proper logging and monitoring, breaches can go undetected. Implementing robust logging practices is crucial for incident response and accountability.
4. **Server-Side Request Forgery (SSRF)**
   * **CWE**: CWE-918
   * **OWASP Category**: A10:2021
   * **Description**: SSRF occurs when an attacker manipulates a web application to make unauthorized requests to resources accessible from the server. It allows attackers to bypass firewalls and access internal services. Common Weakness Enumerations (CWEs) include improper URL validation and insecure redirection handling.
   * **Business Impact**: SSRF can lead to data exposure, unauthorized access, and attacks on internal systems. Proper input validation and network segmentation are essential to prevent SSRF.

# Stage 2 - Nessus Scan

Basic Network scan on host - 103.159.84.193

Results:

IP:103.159.84.193

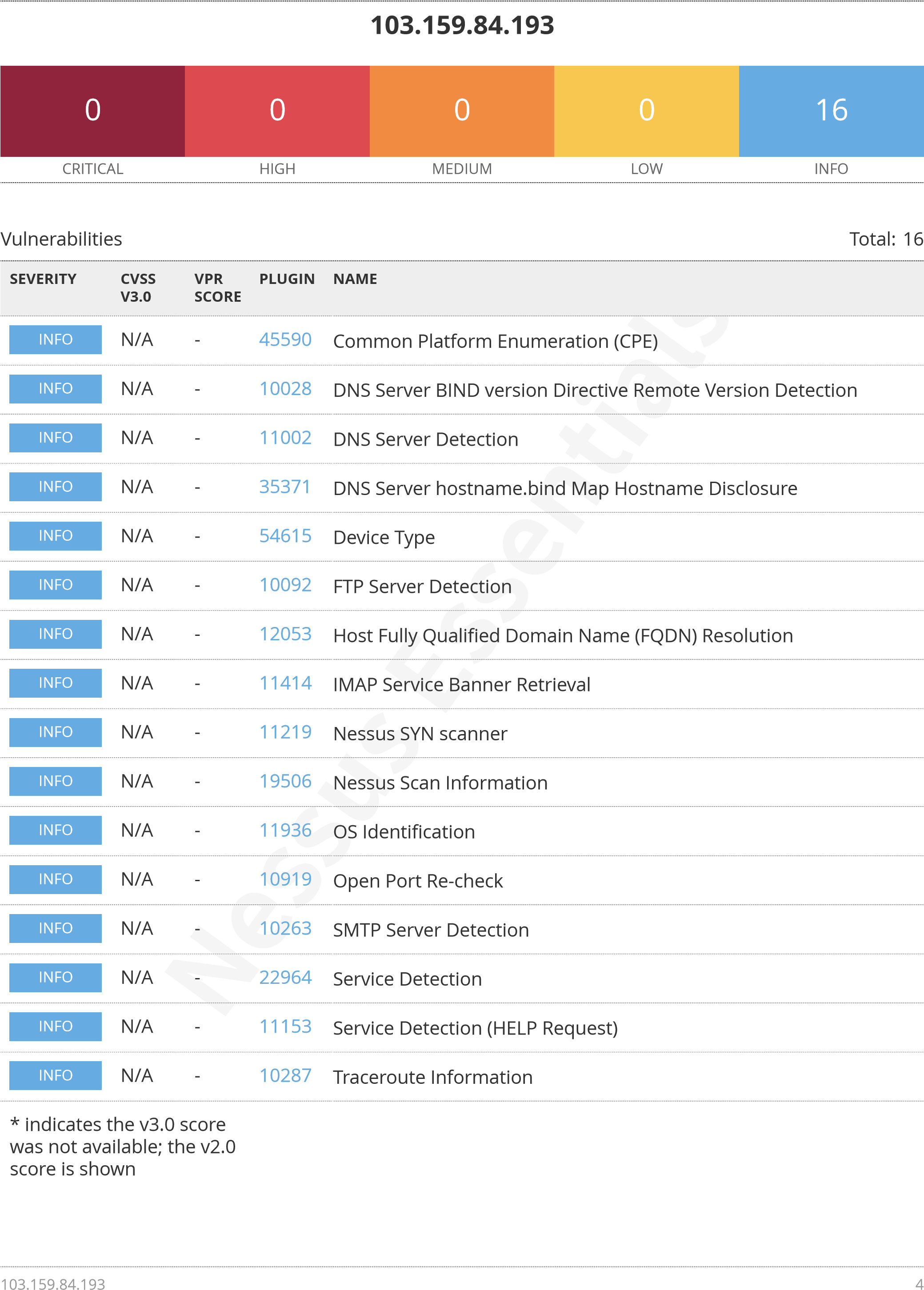
DNS: server75.hostcats.com

OS: Ubuntu 14.04 Linux Kernel 3.13

Start: April 30 at 4:44 PM

End: April 30 at 5:21 PM

Elapsed: 37 minutes



# Stage 3 – SIEM

**Overview** - We have installed Splunk enterprise on our windows device and ingested the Application, System, Security logs from the same.

**About SIEM Tool used –** Splunk

**Logs -**

|  |  |
| --- | --- |
| Time | Event |
| 2024-04-30T12:47:55+0530 | 04/30/2024 12:47:55 PM  LogName=System  EventCode=158  EventType=4  ComputerName=DESKTOP-LU7VRCG  User=NOT\_TRANSLATED  Sid=S-1-5-19  SidType=0  SourceName=Microsoft-Windows-Time-Service  Type=Information  RecordNumber=18820  Keywords=None  TaskCategory=None  OpCode=Info  Message=The time provider 'VMICTimeProvider' has indicated that the current hardware and operating environment is not supported and has stopped. This behavior is expected for VMICTimeProvider on non-HyperV-guest environments.  This may be the expected behavior for the current provider in the current operating environment as well. |
| 2024-04-30T12:40:52+0530 | 04/30/2024 12:40:52 PM  LogName=System  EventCode=10016  EventType=3  ComputerName=DESKTOP-LU7VRCG  User=NOT\_TRANSLATED  Sid=S-1-5-21-1102696979-4129790392-413580853-1001  SidType=0  SourceName=Microsoft-Windows-DistributedCOM  Type=Warning  RecordNumber=18819  Keywords=Classic  TaskCategory=None  OpCode=Info  Message=The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID  {2593F8B9-4EAF-457C-B68A-50F6B8EA6B54} and APPID  {15C20B67-12E7-4BB6-92BB-7AFF07997402}  to the user DESKTOP-LU7VRCG\admin SID (S-1-5-21-1102696979-4129790392-413580853-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool. |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67747  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-21-1102696979-4129790392-413580853-1001  Account Name:admin  Account Domain:DESKTOP-LU7VRCG  Logon ID:0x686C2  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |

|  |  |
| --- | --- |
| Time | Event |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67746  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-21-1102696979-4129790392-413580853-1001  Account Name:admin  Account Domain:DESKTOP-LU7VRCG  Logon ID:0x686C2  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67745  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-21-1102696979-4129790392-413580853-1001  Account Name:admin  Account Domain:DESKTOP-LU7VRCG  Logon ID:0x686C2  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67744  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-21-1102696979-4129790392-413580853-1001  Account Name:admin  Account Domain:DESKTOP-LU7VRCG  Logon ID:0x686C2  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |

|  |  |
| --- | --- |
| Time | Event |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67743  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-21-1102696979-4129790392-413580853-1001  Account Name:admin  Account Domain:DESKTOP-LU7VRCG  Logon ID:0x686C2  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67742  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-21-1102696979-4129790392-413580853-1001  Account Name:admin  Account Domain:DESKTOP-LU7VRCG  Logon ID:0x686C2  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67741  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-18  Account Name:DESKTOP-LU7VRCG$  Account Domain:WORKGROUP  Logon ID:0x3E7  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |

|  |  |
| --- | --- |
| Time | Event |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67740  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-18  Account Name:DESKTOP-LU7VRCG$  Account Domain:WORKGROUP  Logon ID:0x3E7  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67739  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-18  Account Name:DESKTOP-LU7VRCG$  Account Domain:WORKGROUP  Logon ID:0x3E7  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |
| 2024-04-30T12:40:49+0530 | 04/30/2024 12:40:49 PM  LogName=Security  EventCode=5379  EventType=0  ComputerName=DESKTOP-LU7VRCG  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=67738  Keywords=Audit Success  TaskCategory=User Account Management  OpCode=Info  Message=Credential Manager credentials were read.  Subject:  Security ID:S-1-5-18  Account Name:DESKTOP-LU7VRCG$  Account Domain:WORKGROUP  Logon ID:0x3E7  Read Operation:Enumerate Credentials  This event occurs when a user performs a read operation on stored credentials in Credential Manager. |

|  |  |
| --- | --- |
| Time | Event |

# Conclusion -

We have setup and used the basic functionality of -

1. IBM QRadar community edition
2. Splunk Enterprise trial version
3. Nessus Essentials
4. Kali Linux basics
5. BurpSuite
6. Metasploit

Viewed the console of SentinelOne Singularity for EDR working