**PROJECT 2**

**Title: Cat Scan II Big Dog**

***By Titobiloluwa (Tito) Ilori***

**Executive summary**

In this project, I will be providing recommendations on how Big Dog Organizations can develop a monitoring solution within its large network. We want to secure a business that uses a mix of Windows-based servers, Windows 10 Workstations, one Linux system and a Kali Linux system. According to the NIST Cyber Security Framework, the process is first to identify assets “*to focus and prioritize its efforts, consistent with its risk management strategy and business needs*.” NIST Risk Management Framework also recommended preparing and “*Categorising the system and information processed, stored, and transmitted based on an impact analysis*”.

Therefore, I first investigated the version or build available assets, prioritized the assets based on its functions (storage or processes), searched for known vulnerabilities on the NIST National Vulnerability Database, highlighting and prioritizing the risks and vulnerabilities, and thereby making recommendations on how to monitor the network traffic using PAESSLER’s PRTG from the findings. I highly recommend sensors for WMI Microsoft SQL Server 2016, Windows IIS Application, IP on DNS Blacklist, port 445 and port 9200 with a sensitive threshold to alert if it goes off the network baseline.

Kindly Click here to [watch the Video Presentation](https://drive.google.com/open?id=12hd1aJVq7GshCn6PR_IhusSD_EeBsa3E&usp=drive_fs).

**Discussion Section**

a discussion of each of the main systems; make sure you include network infrastructure and a discussion of the network monitoring aspects of the assignment.

First, I would love to provide the network infrastructure for Big Dog Organization. Please see the figure below.

A diagram of a computer network

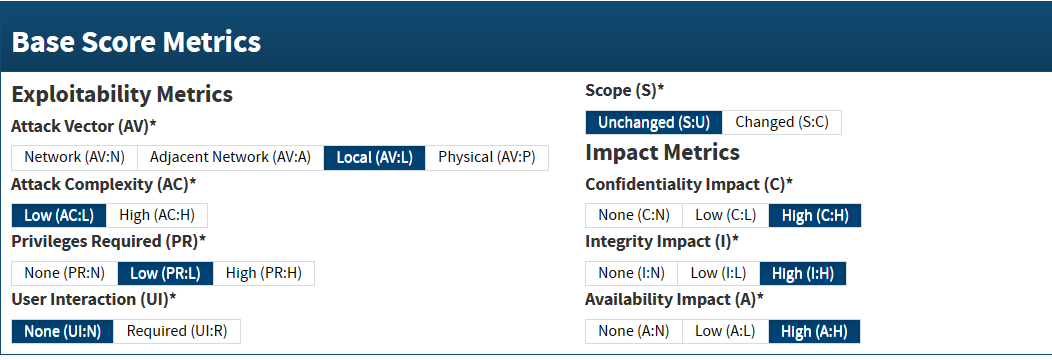
Description automatically generated

*Figure 1: Big Dog Network Infrastructure*

Now, let’s discuss each of the devices or systems within the organization (network infrastructure). Appendix A also gives a tabular description of the findings of known vulnerabilities.

**Windows Server: (172.16.14.53)**

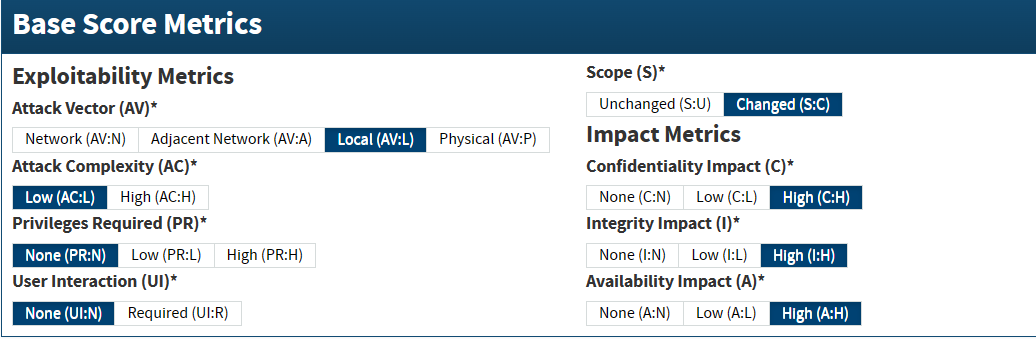
The Server will be responsible for running an SQL database, as well as a website on IIS. This server also has PRTG on it and acts as a file server for the company. This server, therefore, has the highest priority. Based on the version and build of the server, there is a known vulnerability that can exploit Windows Diagnostics Hub for the Elevation of Privilege. If this is performed, then attackers will have administrative rights to the company’s stored intellectual property, web server, and SQL database. This will cause a loss of confidentiality, integrity and eventually, availability. See Table A and Appendix A for more information.



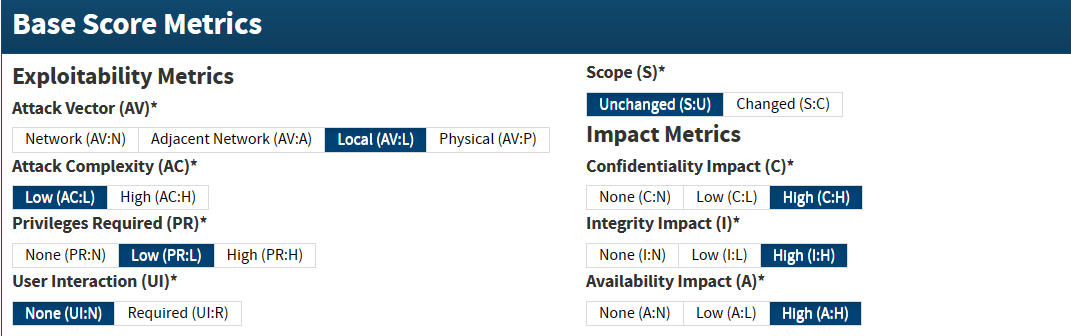
*Figure 2: Showing the Known Vulnerability CVSS Base Score Metrics for CVE-2016-7188 (Score = 7.8 HIGH)*

**Linux system: (172.16.14.52)**

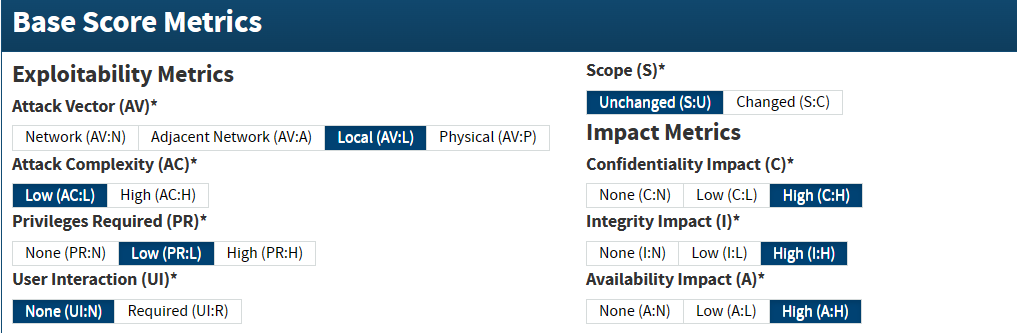
The company has developers that work on this system and these developers create important intellectual property (IP) for the company. This makes this device second in priority rank. It is vital that this system has the least privilege. I discovered 3 vulnerabilities related to the operating system and kernel version of this device, some making sensitive information on the device readable to attackers or insider threats, while the others allowing for privilege escalation. These pose high risks to the organization’s confidentiality, integrity and availability. Therefore, sensors need to be set to monitor any unusual traffic to the port attackers may use (port 9200). It is also important to monitor the network traffic generally using a Packet sniffer PTRG sensor.



*Figure 3: Showing the Known Vulnerability CVSS Base Score Metrics for CVE-2020-15708 (Score = 9.3 CRITICAL) on Linux*

**

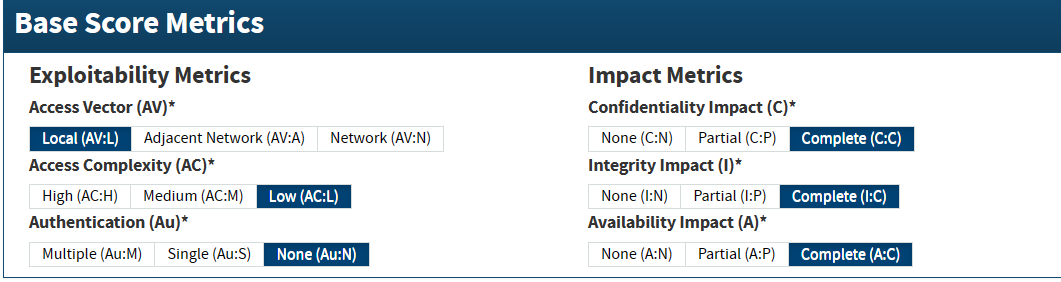
*Figure 4: Showing the Known Vulnerability CVSS Base Score Metrics for CVE-2020-8835 (Score = 7.8 HIGH) on Linux*

**

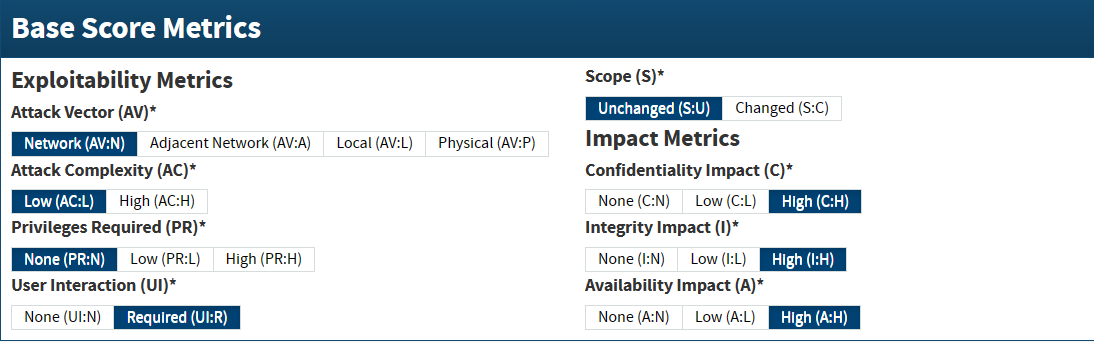
*Figure 5: Showing the Known Vulnerability CVSS Base Score Metrics for CVE-2022-25636 (Score = 7.8 HIGH) on Linux*

**Kali Systems (172.16.14.51)**

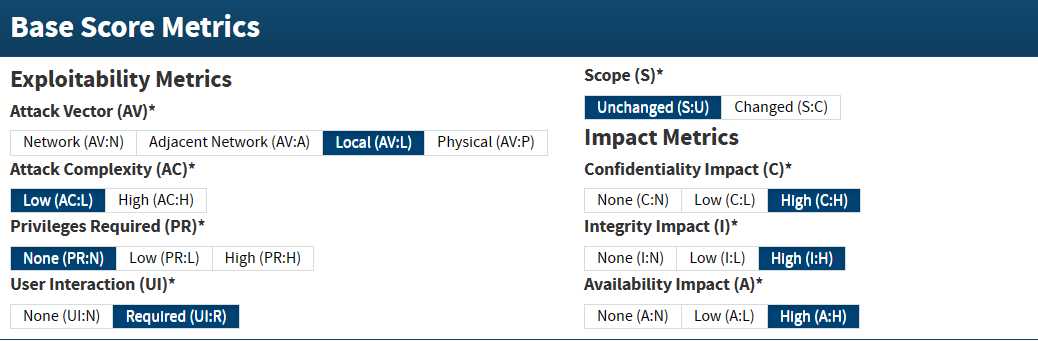
This device will be used to test systems (test environment) and IT systems, and it will be used by the IT department. This device is key for privacy (confidentiality) so that the patent or copyright of the company will not be exposed before its official launch. If this is exposed, the company will experience a financial loss. However, I discovered that there are vulnerabilities in this system as well that put the test environment at risk. Assuming that Big Dog is a company that uses 2D or 3D data software such as Open Design Alliance Drawings SDK before 2023.2, this can expose sensitive data due to a known vulnerability. There is also a web-facing vulnerability on the device given the system has port 9200 opened, this can also cause Cross-Site Request Forgery. It is important to create a sensor for IP on DNS Blacklist. See Table A and Appendix A for more information.



*Figure 6: Showing the Known Vulnerability CVSS Base Score Metrics for CVE-* *2013-2964 (Score = 7.2 HIGH) on Kali*



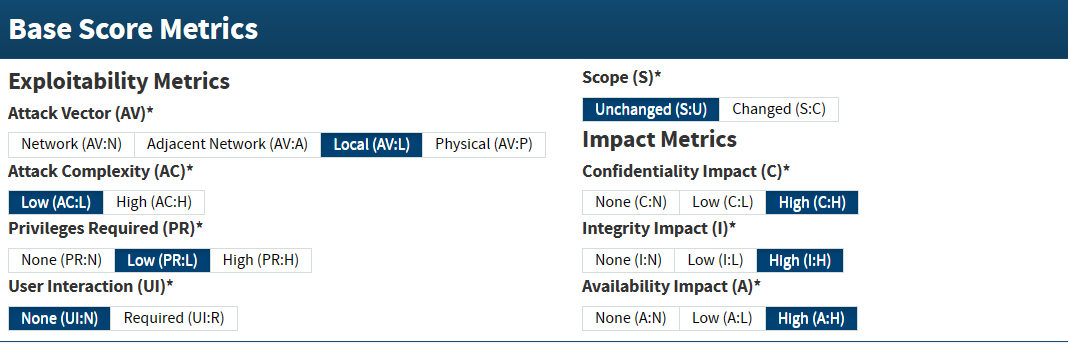
*Figure 7: Showing the Known Vulnerability CVSS Base Score Metrics for CVE-* *2020-36717 (Score = 8.8 HIGH) on Kali*



*Figure 8: Showing the Known Vulnerability CVSS Base Score Metrics for CVE-2022-28807 (Score = 7.8 HIGH) on Kali*

**Windows Workstations (172.16.14.50; 172.16.14.54)**

All sales, marketing, and management functions in the company are performed on these systems/devices. A high score of known vulnerability was also found on these systems. This vulnerability can lead to privilege escalation. Therefore, it is crucial to update patches, monitor network traffic flow and blacklist the installation of this vulnerable software on the workstation. Sensors should also be put on the devices. See more details in Table A and Appendix A.



*Figure 9: Showing the Known Vulnerability CVSS Base Score Metrics for CVE-2020-24557 (Score = 7.8 HIGH) on Windows 10 Pro*

**Table A: Devices and Recommended PTRG Sensors**

| **Devices** | ***Sensors*** | **Threshold** | **SIL** | **IoC** | **Notes** |
| --- | --- | --- | --- | --- | --- |
| **Windows Server** | ***Ping*** |  | Low |  |  |
| ***WMI Microsoft SQL Server 2016*** | Warning 700, 800 Error | High | If service is suffering from a higher-than-normal load | Monitoring the SQL Database. |
| ***FTP*** | Warning 700, 800 Error | High | For expected traffic content | Storage of Intellect Property |
| ***Windows IIS Application*** | Warning 700, 800 Error | High | If web server running as expected | Public facing and PTRG probe |
| ***Port 139*** |  | Moderate |  |  |
| ***Port 445*** |  | High | Monitor unusual network traffic flow to mitigate privilege escalation | Privilege escalation through **CVE-2016-71881** |
| **Linux** | ***Ping*** |  | Low |  |  |
| ***Port 9200 (API calls over HTTP)*** | Warning 700, 800 Error | High | Monitor unusual network traffic flow to mitigate privilege escalation though API | Mitigating **CVE-2022-256369** & **CVE-2020-157084** |
| ***Packet sniffer*** |  | Moderate |  |  |
| **Kali** | ***Ping*** |  | Low |  |  |
| ***Packet sniffer*** |  | Moderate |  |  |
| ***IP on DNS Blacklist*** | Warning 700, 800 Error | High | Alert when vulnerable software/DNS is accessed |  |
| ***FTP*** |  | Moderate |  |  |
| **Windows 1** | ***Ping*** |  | Moderate |  |  |
| ***Packet sniffer*** |  | Moderate |  |  |
| ***IP on DNS Blacklist*** |  | Moderate |  |  |
| **Windows 2** | ***Ping*** |  | Low |  |  |
| ***Packet sniffer*** |  | Moderate |  |  |
| ***IP on DNS Blacklist*** |  | Moderate |  |  |

**Recommendation section**

In the Executive Summary, I recommended sensors for WMI Microsoft SQL Server 2016, Windows IIS Application, IP on DNS Blacklist, port 445 and port 9200 with a sensitive threshold to alert if it goes off the network baseline, I will now present more recommendations. It is best practice that the company operate a Zero-Trust Network Access (Architecture). Big Dog also needs to update patches regularly to mitigate legacy risks/vulnerabilities. There are other sensors that are recommended to be set in the PAESSLER’s PRTG Monitoring; Ping – test devices’ connectivity to the network, packet sniffer – test network traffic flow and communication within the network, and FTP – check network traffic contents. There is also a need to perform Application Isolation and Sandboxing for the test environment. More recommendations specific to each device are available in Appendix A below.

**Appendix A**

| **Items/CVE ID** | **Type** | | Information |
| --- | --- | --- | --- |
| **Windows Server** | **OS Build** | **Windows Server 2016 Standard 1607 (Build 14393.5989)** | |
| **Usage** | | **SQL Database, Web Server (IIS), File server, PRTG probe** |
| **CVE-2016-71881** | **CVSS Base** | | **7.8 HIGH** |
| **Description** | | The Standard Collector Service in Windows Diagnostics Hub in Microsoft Windows 10 Gold, 1511, and 1607 mishandles library loading, which allows local users to gain privileges via a crafted application, aka "Windows Diagnostics Hub Elevation of Privilege Vulnerability." |
| **CWE** | | Permissions, Privileges, and Access Controls |
| **Mitigations** | | Sensors (Port 139 and 445); Security Update for Diagnostics Hub2 |
| **IoCs** | | Network traffic content/flow scan3 |
| **Tactics** | | Reconniassance : Privilege escalation |
| **Techniques** | | Active scanning : Exploitation of Privilege escalation3 |
| **Linux System** | **OS Build** | **Ubuntu 20.04.6 LTS (Kernel: Linux 5.4.0-148-generic)** | |
| **Usage** | | Development: Important intellectual property |
| **CVE-2020-157084** | **CVSS Base** | | **7.8 HIGH** / **9.3 CRITICAL** |
| **Description** | | Ubuntu's packaging of libvirt in 20.04 LTS created a control socket with world read and write permissions. An attacker could use this to overwrite arbitrary files or execute arbitrary code. \*(libvirt library is used to interface with different virtualisation technologies.) |
| **CWE** | | Incorrect Permission Assignment for Critical Resource |
| **Mitigations** | | Packet sniffer PRTG Sensor; Update version5 |
| **IoCs** | |  |
| **Tactics** | | Privilege escalation |
| **Techniques** | | Abuse Elevation Control Mechanism6 |
| **CVE-2020-88357** | **CVSS Base** | | **7.8 HIGH** |
| **Description** | | In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780) |
| **CWE** | | Out-of-bounds Read; Out-of-bounds Write |
| **Mitigations** | | Encrypt Sensitive Information; Multi-factor Authentication8 |
| **IoCs** | | Process Creation, Command Execution8 |
| **Tactics** | | Credential Access |
| **Techniques** | | Network sniffing8 |
| **CVE-2022-256369** | **CVSS Base** | | **7.8 HIGH** |
| **Description** | | net/netfilter/nf\_dup\_netdev.c in the Linux kernel 5.4 through 5.6.10 allows local users to gain privileges because of a heap out-of-bounds write. This is related to nf\_tables\_offload |
| **CWE** | | Improper Privilege Management |
| **Mitigations** | | Packet sniffer PTRG sensor; Antivirus/Antimalware, and this10 |
| **IoCs** | | File Creation, Modification |
| **Tactics** | | Privilege Escalation |
| **Techniques** | | Boot or Logon Autostart Execution11 |
| **Kali System** | **OS Build** | **Kali 2023.2 (6.1.0-kali9-amd64)** | |
| **Usage** | | Test systems and IT systems |
| **CVE-2020-1570812** | **CVSS Base** | | **7.8 HIGH** |
| **Description** | | An issue was discovered in Open Design Alliance Drawings SDK before 2023.2. An Out-of-Bounds Read vulnerability exists when rendering a .dwg file after it's opened in recovery mode. An attacker can leverage this vulnerability to execute code in the context of the current process. \*(A .dwg file is a binary file format used for containing 2D and 3D design data) |
| **CWE** | | Out-of-bounds Read |
| **Mitigations** | | IP on DNS Blacklist PRTG Sensor; Execution Prevention, Network Intrusion Prevention |
| **IoCs** | | Process creation |
| **Tactics** | | Execution |
| **Techniques** | | User Execution13 |
| **CVE-2013-296414** | **CVSS Base** | | **7.2 HIGH (v2.0)** |
| **Description** | | Buffer overflow in dsmtca in IBM Tivoli Storage Manager (TSM) through 5.5.4.0, 6.1.0 through 6.1.5.4, 6.2.0 through 6.2.4.7, and 6.3.0 through 6.3.0.17 on UNIX and Linux allows local users to gain privileges via unspecified vectors. |
| **CWE** | | Improper Restriction of Operations within the Bounds of a Memory Buffer |
| **Mitigations** | | Do not install IBM Tivoli Storage Manager. Sensor = IP on DNS Blacklist |
| **IoCs** | | Network Traffic Content |
| **Tactics** | | Initial Access |
| **Techniques** | | Exploit Public-Facing Application15 |
| **CVE-2020-3671716** | **CVSS Base** | | **8.8 HIGH** |
| **Description** | | The Kali Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.1.1. This is due to incorrect nonce handling throughout the plugin's function. This makes it possible for unauthenticated attackers to access the plugin's administrative functions via forged requests granted they can trick a site administrator into performing an action such as clicking on a link. |
| **CWE** | | Cross-Site Request Forgery (CSRF) |
| **Mitigations** | | Application Isolation and Sandboxing17 |
| **IoCs** | | Network Connection Creation, File Creation |
| **Tactics** | | Initial Access |
| **Techniques** | | Drive-by Compromise 18 |
| **Windows Workstations (2)** | **OS Build** | **Windows 10 Pro Version 10.0 (Build 10240. 16392)** | |
| **Usage** | | All sales, marketing, and management |
| **CVE-2020-2455719** | **CVSS Base** | | **7.8 HIGH** |
| **Description** | | A vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 on Microsoft Windows may allow an attacker to manipulate a particular product folder to disable the security temporarily, abuse a specific Windows function and attain privilege escalation. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected. |
| **CWE** | | N/A |
| **Mitigations** | | Blacklist application site, Update patches. Behaviour Prevention on Endpoint |
| **IoCs** | | Behavior Prevention on Endpoint |
| **Tactics** | | Privilege Escalation |
| **Techniques** | | Process injection20 |

**Citations:**

Framework for Improving Critical Infrastructure Cybersecurity, NIST (April 16, 2018)

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

NIST Risk Management Framework (Updated July 06, 2023)

<https://csrc.nist.gov/Projects/Risk-Management>

Zero Trust Architecture - Rose, S. et al. 2020 NIST (Updated March 23, 2021)

<https://www.nist.gov/publications/zero-trust-architecture>

1. CVE-2016-7188 Detail - NIST NVD (Last Modified: October 12, 2018) <https://nvd.nist.gov/vuln/detail/CVE-2016-7188>
2. Microsoft Security Bulletin MS16-125 – Important (March 1, 2023) <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-125>
3. Active Scanning: Vulnerability Scanning (Last Modified: 13 March 2023) <https://attack.mitre.org/techniques/T1595/002/>
4. CVE-2020-15708 Detail- NIST NVD (November 12, 2020) <https://nvd.nist.gov/vuln/detail/CVE-2020-15708>
5. USN-4452-1: libvirt vulnerability : <https://ubuntu.com/security/notices/USN-4452-1>
6. Process Injection: Dynamic-link Library Injection - Mitre (18 October 2022) <https://attack.mitre.org/techniques/T1055/001/>
7. CVE-2020-8835 Detail – NIST NVD (February 24, 2023) <https://nvd.nist.gov/vuln/detail/CVE-2020-8835>
8. Network Sniffing – MITRE (12 April 2023) <https://attack.mitre.org/techniques/T1040/>
9. CVE-2022-25636 Detail – NIST NVD (February 24, 2023) <https://nvd.nist.gov/vuln/detail/CVE-2022-25636>
10. index : kernel/git/netfilter/nf.git <https://git.kernel.org/pub/scm/linux/kernel/git/netfilter/nf.git/commit/?id=b1a5983f56e371046dcf164f90bfaf704d2b89f6>
11. Boot or Logon Autostart Execution: Kernel Modules and Extensions – MITRE (20 April 2022) <https://attack.mitre.org/techniques/T1547/006/>
12. CVE-2022-28807 Detail – NIST NVD (July 25, /2022) <https://nvd.nist.gov/vuln/detail/CVE-2022-28807>
13. User Execution – MITRE (18 April 2018) <https://attack.mitre.org/techniques/T1204/>
14. CVE-2013-2964 Detail – NIST NVD (August 28, 2017) <https://nvd.nist.gov/vuln/detail/CVE-2013-2964>
15. Exploit Public-Facing Application – MITRE (14 April 2023) <https://attack.mitre.org/techniques/T1190/>
16. CVE-2020-36717 Detail – NIST NVD (June 13, 2023) <https://nvd.nist.gov/vuln/detail/CVE-2020-36717>
17. Application Isolation and Sandboxing – MITRE (31 March 2020 <https://attack.mitre.org/mitigations/M1048>
18. Drive-by Compromise – MITRE (14 April 2023) <https://attack.mitre.org/techniques/T1189/>
19. CVE-2020-24557 Detail – NIST NVD (July 12, 2022) <https://nvd.nist.gov/vuln/detail/CVE-2020-24557>
20. Process Injection – MITRE (30 March 2023) https://attack.mitre.org/techniques/T1055