**Advanced Executive Program in Cybersecurity**

Virtual Internship Project Problem Statement



**Malware Analyst**

**Problem statement:**

You are working as a malware analyst for El Banco Bank, where your primary responsibility is to secure the bank's assets by examining, identifying, and understanding malware, such as viruses, worms, bots, rootkit, ransomware, and Trojan horse. These types of malware can infect systems by exploiting vulnerabilities and cause them to behave in unexpected ways.

**Background of the problem statement:**

El Banco Bank is one of the fastest growing banks in Europe with more than 1200 branches across the country and manages €200 billion in assets.

Handling millions of dollars of banking transactions per day, its customers hugely depend upon the security of their banking data. The recent surge in cyber-attacks and data breaches has become a significant issue for every organization.

According to the latest reports, 51% of cyberattacks are due to various malware, such as viruses, rootkit, trojan horse, and ransomware.

**Expected deliverables:**

**TASK 1:**

As a malware analyst, you have to examine suspicious files or URLs and detect any malware threats. You have been provided a list of files that you need to examine and verify if these files are real and do not contain anything malicious. You can check the digital signatures of the files to verify if it is authentic and hasn’t been tampered with.

For the following applications, determine the Signer Name and the Digest Algorithm used in the digital signatures. If the digital signature is not available, leave the fields blank.

|  |  |  |
| --- | --- | --- |
|  | **Name of Signer** | **Digest Algorithm** |
| **Virtualbox** | Oracle Corporation | sha256 |
| **LibreOffice** |  |  |
| **OWASP ZAP** |  |  |
| **Wireshark** | Wireshark Foundation | Sha256 |

**TASK 2:**

If the digital signature of the files is not available, you can still verify the integrity of the file by comparing the hash values provided for the original files. For those files that cannot be verified using digital signatures, use the following resources to compare the SHA256 values of the files and determine if the given digest and the calculated digest value match.

By comparing the files' hash values, you are able to determine the integrity of the files and be assured that the downloaded files are authentic and haven't been tampered with.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Given Digest value** | **Calculated Digest value** | **Match?** |
| **Virtualbox** |  |  |  |
| **LibreOffice** | f6a3f0794b957e7e95219064639b2a67a315158e614c8cee58a352286b8f38ed | f6a3f0794b957e7e95219064639b2a67a315158e614c8cee58a352286b8f38ed | yes |
| **OWASP ZAP** | 5e1df341b91f65fe0768cb659af41e7671d475074ceab1b332b6520bcedf1dac | 5e1df341b91f65fe0768cb659af41e7671d475074ceab1b332b6520bcedf1dac | yes |
| **Wireshark** |  |  |  |

**Resources for SHA256 values:**

1. <https://raw.githubusercontent.com/zaproxy/zap-admin/master/ZapVersions-2.11.xml>
2. <https://www.virtualbox.org/download/hashes/6.1.30/SHA256SUMS>
3. <https://download.documentfoundation.org/libreoffice/stable/7.2.3/win/x86_64/LibreOffice_7.2.3_Win_x64.msi.mirrorlist>
4. https://www.wireshark.org/download/SIGNATURES-3.6.0.txt

**TASK 3:**

Analyzing files to understand the associated threats is an increasingly important skill for malware analysts. Analyzing malware could be a daunting task. Fortunately, there are many tools and resources at your disposal that could help you make this task a little bit easier.

Your next task is to determine if the files are malicious or not.

**Link to download the malwares:** https://github.com/Simplilearn-Edu/Advanced-Executive-Program-in-Cybersecurity

|  |  |
| --- | --- |
| **File** | **Malware?** |
| 1. **Keylogger** | No |
| 1. **Ransomware** | No |
| 1. **Exeinfope** | No |

**Link for analyzing malicious files:** <https://www.virustotal.com/>

**TASK 4:**

Another important task for a malware analyst is to perform**a vulnerability** assessment to**identify** the most critical**vulnerabilities** for correction. This will reduce the risk of**hackers** exploiting the applications.

Your organization uses GLPI, an open-source IT Asset Management, issue tracking system, and service desk system written on PHP. GLPI uses a barcode plugin used for printing barcodes and QR codes.

|  |  |  |
| --- | --- | --- |
|  | **Version** | **Link** |
| **GLPI** | 9.5.5 | <https://glpi-project.org/> |
| **Barcode GLPI plugin** | 2.6.0 | <https://github.com/pluginsGLPI/barcode> |

Use the NVD database to search for vulnerabilities in GLPI and third-party plugins (minimum 5 vulnerabilities) and suggest a fix or a workaround.

**Link for NVD Database:** <https://nvd.nist.gov/>

|  |  |  |  |
| --- | --- | --- | --- |
| **CVE** | **Description** | **CVSS Severity** | **Remediation** |
| **CVE-2023-35924** | GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.8, GLPI inventory endpoint can be used to drive a SQL injection attack. By default, GLPI inventory endpoint requires no authentication. | 9.8 Critical | Version 10.0.8 has a patch for this issue. As a workaround, one may disable native inventory. |
| **CVE-2023-28849** | GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.7, GLPI inventory endpoint can be used to drive a SQL injection attack. It can also be used to store malicious code that could be used to perform XSS attack. By default, GLPI inventory endpoint requires no authentication. | 10.0 Critical | Version 10.0.7 contains a patch for this issue. As a workaround, disable native inventory. |
| **CVE-2023-23610** | GLPI is a Free Asset and IT Management Software package. Versions prior to 9.5.12 and 10.0.6 are vulnerable to Improper Privilege Management. Any user having access to the standard interface can export data of almost any GLPI item type, even those on which user is not allowed to access (including assets, tickets, users, ...). | 6.5 Medium | This issue is patched in 10.0.6. Upgrade to 10.0.6 |
| **CVE-2021-39210** | GLPI is a free Asset and IT management software package. In versions prior to 9.5.6, the cookie used to store the autologin cookie (when a user uses the "remember me" feature) is accessible by scripts. A malicious plugin that could steal this cookie would be able to use it to autologin. | 6.5 Medium | This issue is fixed in version 9.5.6. As a workaround, one may avoid using the "remember me" feature. |
| **CVE-2021-43778** | Barcode is a GLPI plugin for printing barcodes and QR codes. GLPI instances version 2.x prior to version 2.6.1 with the barcode plugin installed are vulnerable to a path traversal vulnerability. | 9.1 Critical | This issue was patched in version 2.6.1. As a workaround, delete the `front/send.php` file. |