Advanced Executive Program in Cybersecurity

Virtual Internship Project Problem Statement

Get Certified. Get Ahead.

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	Oracal Corporation	Sha1, sha256
LibreOffice	NA	NA
OWASP ZAP	NA	NA
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	65678ac729cd0b545d14703879b601872d285c2934ae8d76452f7c2fb2c62d15	65678ac729cd0b545d14703879b601872d285c2934ae8d76452f7c2fb2c62d15	Yes
OWASP ZAP	3b9862a647b1c5c26d6917f2316113dfaceac06bdb79ad3f2c96e0cbd73861f7	DF49FFBD14CF82CDE5AC06902615E40CBFCE1576F866436366708C0845EB9EC6	NO
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
2. Ransomware	No
3. 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 NA), 9.5.0	https://glpi-project.org/
Barcode GLPI plugin	2.6.0 (No matches found)	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-2023-35940	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to version 10.0.8, an incorrect rights check on a file allows an unauthenticated user to be able to access dashboards data. Version 10.0.8 contains a patch for this issue.	*V3.1:* **7.5 HIGH**	By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites

			https://github.com/glpi-project/glpi/security/advisories/GHSA-qrh8-rg45-45fw https://github.com/glpi-project/glpi/releases/tag/10.0.8
CVE-2023-35939	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to version 10.0.8, an incorrect rights check on a on a file accessible by an authenticated user (or not for certain actions), allows a threat actor to interact, modify, or see Dashboard data. Version 10.0.8 contains a patch for this issue.	*V3.1:* **8.1 HIGH**	By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the

			facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites https://github.com/glpi-project/glpi/security/advisories/GHSA-qrh8-rg45-45fw https://github.com/glpi-project/glpi/releases/tag/10.0.8
CVE-2023-35939	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to versions 9.5.13 and 10.0.7, a user with dashboard administration rights may hack the dashboard form to store malicious code that will be executed when other users will use the related	*V3.1:* **4.8 MEDIUM**	

	dashboard. Versions 9.5.13 and 10.0.7 contain a patch for this issue.		
CVE-2021-21258	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. In GLPI from version 9.5.0 and before version 9.5.4, there is a cross-site scripting injection vulnerability when using ajax/kanban.php. This is fixed in version 9.5.4.	*V3.1:* **5.4 MEDIUM** *V2.0:* **3.5 LOW**	By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may

			be mentioned on these sites https://github.com/glpi-project/glpi/security/advisories/GHSA-qrh8-rg45-45fw https://github.com/glpi-project/glpi/releases/tag/10.0.8
CVE-2020-15217	In GLPI before version 9.5.2, there is a leakage of user information through the public FAQ. The issue was introduced in version 9.5.0 and patched in 9.5.2.	*V3.1:* **5.3 MEDIUM** *V2.0:* **5.0 MEDIUM**	By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse

			the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites https://github.com/glpi-project/glpi/security/advisories/GHSA-qrh8-rg45-45fw https://github.com/glpi-project/glpi/releases/tag/10.0.8
CVE-2020-11031	In GLPI before version 9.5.0, the encryption algorithm used is insecure. The security of the data encrypted relies on the password used, if a user sets a weak/predictable password, an attacker could decrypt data. This is	*V3.1:* **7.5 HIGH** *V2.0:* **5.0 MEDIUM**	By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other

	fixed in version 9.5.0 by using a more secure encryption library. The library chosen is sodium.		sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites https://github.com/glpi-project/glpi/security/advisories/GHSA-qrh8-rg45-45fw https://github.com/glpi-project/glpi/releases/tag/10.0.8