ASAGBA JEREMIAH
Lab Report: Malicious Document Analysis

Objective:

The objective of this lab was to analyze a malicious Microsoft Word document in order to extract relevant information such as the type of exploit it employs, the CVE code associated with the exploit, the name of the malicious software it downloads, the IP address and port it communicates with, and the name of the dropped executable file.

Skills Learned:

Malicious document analysis
Identifying exploits and associated CVE codes
Determining communication channels and malware payloads
Utilizing various analysis tools such as REMnux, rtfdump.py, rtfobj, shell code analyzer, and Gary Kessler's signatures
Virustotal

Tools Used:

REMnux (Linux distribution for malware analysis)
rtfdump.py (RTF file analyzer)
rtfobj (RTF object extractor)
Scdbg (Shell code analyzer)
Gary Kessler's signatures (for signature-based analysis)

Results:

Type of Exploit: rtf.exploit
Exploit CVE Code: CVE-2017-11882
Name of Malicious Software: jan2.exe
IP Address and Port: 185.36.74.48:80
Dropped Executable Name: aro.exe

Steps Taken:

Initial Analysis:

Obtained a suspicious Microsoft Word document.
Fired up REMnux for malware analysis.

RTF Analysis:

Utilized rtfdump.py and rtfobj to extract and analyze RTF objects.
Identified shell code and suspicious patterns using shell code analyzer(scdbg).

CVE Identification:

Cross-referenced identified exploit patterns with known CVEs.
Found a match with CVE-2017-11882.

Malware Download Analysis:
Tracked network activity to identify the IP address and port the document communicated with.
Cross-referenced the IP address with VirusTotal for additional confirmation and context regarding its reputation and associated threats.
Confirmed the IP address as 185.36.74.48 through VirusTotal, which provided insights into its malicious activities and connections to known malware campaigns.
Determined the downloaded file name as jan2.exe, corroborating findings from VirusTotal's analysis.

Dropped Executable Analysis:
Observed the behavior of the malware with SquareX using a disposable text viewer and noted the dropped executable as aro.exe.

Validation:
Verified findings using Gary Kessler's signatures for additional confirmation.

Conclusion
Through the analysis of the malicious Microsoft Word document, various aspects of the attack were uncovered. The exploit used was identified as CVE-2017-11882, leading to the download of jan2.exe from IP address 185.36.74.48 on port 80. The dropped executable after successful execution was determined to be aro.exe. This exercise enhanced skills in malware analysis, exploit identification, and the utilization of various analysis tools and techniques.