Learning Outcome of the Assignment

1. Compare various techniques used in the defense of computer systems against malicious software and software-based attacks. (A4, PLO9)

Instructions:

No marks will be awarded for the entire assignment if any part of it is found to be copied directly from printed materials or from another student. All submissions should be made on or before the due date. Any late submissions after the deadline will not be entertained. **Zero (0)** mark will be awarded for late submission unless extenuating circumstances are upheld.

Questions:

You are required to conduct research individually.

People nowadays are highly dependent on computers and the numbers of people connected to internet showed an increase trend. These two facts have created a new battlefield for attackers to wage war on. Using various methods, techniques and tools of cyber-attacks, an attacker can cripple or demoralize its target without using any military force or weapon and can do so with almost total anonymity. Currently, cybercrime-as-a-service (CaaS) has become more popular to antagonize the victim.

LOLBins = the use of legitimate, built-in system binaries or processes to execute malicious activit

You are required to do research on cybercrime-as-a-service (CaaS) and the focus area is on Living Off the Land Binaries (LOLBins) attack. In your research, you should include the followings:

1. Your research should focus into one of the below areas:
    - POSHSPY – This is a sophisticated PowerShell-based malware that uses PowerShell scripts for persistent backdoor access and data exfiltration. This type of attack is often used by advanced persistent threat (APT) groups for long-term espionage.
    - POWRUNER – use a powershell to run malicious payloads and use BITSadmin to download more malicious code. Thus, it has been used in targeted attacks in order to execute scripts and to have persistence on affected systems.
    - Emotet - new phishing campaigns that use PowerShell for downloading payloads and Regsvr32 for executing DLL files, aiming at spreading other malware like ransomware.
    - Ursnif (Gozi) – This kind of attack uses PowerShell and MSHTA to deliver banking trojans, focusing on stealing financial information from compromised systems.
    - Qbot (Qakbot) - Qbot uses PowerShell for script execution and BITSAdmin for downloading malicious components in its latest email phishing campaigns.
    - TrickBot – based on activities in 2023, this attack involves using WMIC and PowerShell to execute malicious scripts, with a focus on stealing banking credentials and delivering ransomware.

- FIN7 - In 2023, FIN7 has been leveraging PowerShell to execute scripts and integrate MSHTA to run HTML applications in the environment, focusing on the sectors of hospitality and retail and implementing complex intrusion strategies.
- APT29 (Cozy Bear) - Several latest attacks carried out by APT29 in 2023 have involved the use of PowerShell for script-based activities, and BITSAdmin for download management, on targets within the governmental and research sectors.
- Dridex - In 2023, Dridex has remained in operation and has continued to utilize Regsvr32 for the execution of a DLL and also PowerShell for the downloading of further malware; specifically, this has provided itself to deceitful banking phishing messages.
- Netwalker – WMIC and VSSAdmin heve been used to delete volume shadow copies and disable system recovery options and this attack is focusing on healthcare and educational sectors.

2. Research on the vulnerability of the system/device that enables LOLBins attacks. Support your research with Mitre Attack framework or Common Vulnerabilities and Exposures (CVE) database.
3. Discuss on Tactics, Techniques and Procedures used by attackers in performing the LOLBins attacks.
4. As a cyber security expert/consultant provide the following plan for the organization:
    a. Threat modelling
    b. Operational Security (OPSEC)
    c. General and Technical Security

Assesment

This assignment will contribute 30% towards the incoure marks,as mentioned on the Student Assesment &Information sheet

This assignment will be evaluated based on the following criteria.

Assessment Criteria (Marks Breakdown)

Marking Criteria	Weighting	Marks
Section B	100	
System Vulnerabilities and TTP	40	
Operational Security (OPSEC) and Cyber Security (General and Technical Security)	40	
Threat Modelling	20	

Total	100	

Guidelines for the Report:

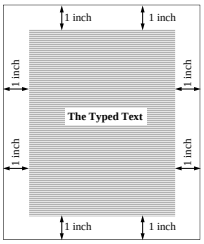
Document the results of your work in a **professional and systematic** manner, in the form of a **computerized report**. **One (1)** softcopy of your documentation is to be submitted.

Your completed documentation should meet the following requirements:

1. Table of contents for every detailed chapter/section.
2. Abstract
3. Introduction
4. Chapters / sections
5. Conclusion
6. Appendices
7. References

Submission requirements

1. Your report must be typed using Microsoft Word with Times New Roman font. You need use to include a word count at the end of the report (excluding title, source code of program & contents pages) Report should be in 1.5 spaces.
2. The report should have a one (1") margin all around the page as illustrated below:



3. Every report must have a *front cover*. The front cover should have the following details:-
   a) Name
   b) Intake code.
   c) Subject.
   d) Project Title.
   e) Date Assigned (the date the report was handed out).
   f) Date Completed (the date the report is due to be handed in).
4. **All** information, figures and diagrams obtained from external sources **must** be referenced using the APA referencing system accordingly.

5. Assignment submission is online submission through Moodle

Marking Scheme Rubrics

Criteria	Fail	Pass	Credit	Distinction
Cyber Vulnerabilities and TTP (40)	All submission requirements were not adhered or poor writing or poor quality of contents. No integration of the tasks given	All requirements are fulfilled but with some missing parts. Research not in detail	All requirements are fulfilled. No missing parts. Acceptable research but research lack of supporting details	All requirements are fulfilled. No missing parts. Outstanding research with good supporting details
	Fail	Pass	Credit	Distinction
Operational Security (OPSEC) and Cyber Security (General and Technical Security) (40)	Poor research and investigation of the operational security. Poor evaluation of the requirement.	Acceptable research and investigation are done. Acceptable evaluation of the operational security with proper reasoning with proper planning and management.	Good analysis and investigation are done. Good evaluation of the operational security with proper reasoning. Good planning and management with detail research	Outstanding analysis and investigation of the problem. Outstanding evaluation of the operational security with proper reasoning. Outstanding planning and management with detail research
	Fail	Pass	Credit	Distinction
Threat Modeling (20)	Poor content of research. Demonstrate dependency on others guidance during presentation. Unable to answer any questions independently.	Acceptable content of research. Demonstrate tendency to dependent on others guidance during presentation. Able to answer question but failed to produce confirmed answers	Good content of research. Demonstrate good understanding and idea in the topic area. Able to answer the questions but answer given lack of supporting details.	Outstanding content of research. Always demonstrate a self-reliant attitude in all situation during presentation. Voice is clear and loud. Able to answer all the questions without referring to notes.
