CSC3064 Practical Assessment *(Lab 5)*

Objective

You have just started a new job as network security analyst at a Security Operations Center (SOC). Your job is to investigate network based cyber-attacks affecting customers of the SOC.

Your manager has asked you to investigate a network packet capture containing malware-related network activity, which was taken from a customer's network a few years ago.

You have been asked to provide an analysis of what you think happened during the packet capture and provide a concise presentation of your findings (according to the requirements on page 2).

The packet capture, called ***CSC3064-Assessment.pcap***, is available to download from Canvas.

This assessment is worth 10% of the available module marks.

You are required to submit a single video file, submitted via the Courses *Assignments*

page. The submission deadline is 07:00 on 23 May 2022.

If you have a question about this assessment email inseclab@uit.edu.vn

Requirements

You are required to produce a **video** report that addresses the following two points:

1. **Basic Summary**

   Must include:

   - Identify the IP addresses of hosts that communicated with each other. Very briefly, discuss any basic insights gained from this information.
   - Identify all protocols in the capture higher than OSI layer 4. For each protocol identified, state the percentage of bytes in the capture belonging to that protocol.

2. **Analysis in Wireshark**

   Must include:

   - A verbal explanation of what you think happened in the network. Identify the name of the malware if you can. Consider a timeline of the communications that took place, supported by evidence displayed in Wireshark.
   - Discuss any successful or unsuccessful operations associated with the malware, and identify any vulnerabilities you believe were successfully exploited via the network.
   - Identify any network-based Indicators of Compromise (IOC) that you think are useful from a network security perspective, and describe how they could be used effectively in the prevention or detection of similar kinds of attack in the future.

   You must justify your findings with evidence, based on the operations observed in the network packet capture.

   In your video report, discuss and display specific individual packets, protocol information, headers, IP addresses, etc. (anything you think is relevant), with commentary about how the information supports your theories or conclusions about what happened in the network.

Examples for guidance:

If you conclude the capture shows a *TCP SYN flood* attack, you might show evidence such as:

- Wireshark statistics that support this conclusion,
- Data showing a very large number of TCP packets with the SYN flag set,
- The IP address of the host that you believe is the target of the attack,
- and so on…

To "justify your findings" you do not need to reference external sources as evidence to explain what SYN floods look like. References are not required.

If you conclude the capture shows *CryptoLocker* ransomware, you should not go into detail about host or software related operations, such as "the malware adds a key to the registry that causes it to run on startup". These are not network-related operations, are not visible in the capture, and are not relevant for this particular security analysis.

About the capture file:

A packet has been removed from the original capture to ensure minimal cyber security risks associated with the content of the capture. This will not affect or hinder your ability to analyse the capture.

The hosts recorded in the file are not believed to pose a current security risk, however it is recommended that you do not visit any hosts that you discover, as this is not necessary for your investigation.

Guidance on Video

As guidance, you should aim for around 5 minutes, but you **must not exceed 6 minutes**. Any videos longer than 6 minutes will be awarded 0 marks for *quality of presentation*.

You may structure your video in whatever way you feel most effectively communicates your findings in a concise, technically detailed, and professional manner. However, the following approach is strongly recommended:

Basic Summary

- Aim for around 1 minute.
- Use a PowerPoint slide to present the required information with a brief and focused discussion.

Analysis in Wireshark

- Aim for around 4 minutes.
- Present your evidence using the Wireshark tool. Discuss your theories and justifications by stepping through any evidence you think supports your findings.
- You may wish to intersperse your discussion with 1 or 2 brief PowerPoint slides to identify key points that you want to emphasise (but don't waste time repeating the same information). For example, you may wish to conclude with a slide to discuss Indicators of Compromise (IOC).
- However, your primary aim is to demonstrate effective practical skills in network security analysis and competent use of Wireshark, so most of your time must be spent working within Wireshark.

Regarding the presentation format and the audience, keep in mind the audience for your presentation is your manager at a Security Operations Center. The information you present must appear professional. It should be informative and convey depth of detail, but be concise.

Assessment Criteria

Your work will be assessed according to the indicative criteria provided as guidance below, and in accordance with the QUB Undergraduate Conceptual Equivalents Scale: https://www.qub.ac.uk/directorates/media/Media,837251,smxx.pdf

	80-100%	70-79%	60-69%	50-59%	40-49%	0-39%
BASIC SUMMARY *Host addresses, insights, protocols, and percentages.* **[15% weighting]**	Correct identification of all requested information. Exceptional insight into identified hosts.	Correct identification of all requested information. Excellent insight into identified hosts.	Correct identification of all requested information. Good insight into identified hosts.	Correct identification of most requested information. Could offer more insight into identified hosts.	Correct identification of most requested information. Lacks insight into identified hosts	Incorrect identification of most of the requested information. No insight into identified hosts.
ANALYSIS IN WIRESHARK *Conclusions, justified findings, evidence, competent use of Wireshark.* **[60% weighting]**	Exemplary critical analysis demonstrating professional capabilities. Outstanding depth of insight across a comprehensive range of evidence. Rigorous justification for findings. Exceptional understanding of communications, operations, and vulnerabilities. Outstanding analysis of IOCs that demonstrate learning beyond module content, with unique insight.	Systematic critical analysis demonstrating very strong capabilities. Excellent insight across a comprehensive range of evidence. Rigorous justification for findings. Excellent understanding of communications, operations, and vulnerabilities. Strong analysis of IOCs that comprehensively addresses prevention and detection, and carefully considers their effectiveness.	Very good analysis demonstrating competent capabilities. Very good insight across multiple pieces of evidence. Well-developed justification for findings. Very clear understanding of communications, operations, and vulnerabilities. Very good analysis of IOCs that addresses prevention or detection. May lack some depth in consideration of their effectiveness	Good analysis demonstrating competent capabilities. Good insight based on identifying a reasonable amount of evidence. Some gaps. Justification for presented findings mostly correct but lacks depth. Minor mistakes in understanding of communications, operations, and vulnerabilities. Good analysis of IOCs that addresses prevention, but with minor gaps.	Adequate analysis demonstrating reasonable competence. Some evidence correctly identified, but with significant omissions, or minor issues misunderstood. Findings lacking and/or not well justified. Gaps in understanding of communications, operations, and vulnerabilities. Reasonable analysis of IOCs, but with gaps or misunderstanding.	Inadequate analysis. Evidence presented shows limited understanding of the main issues. Significant omissions and mistakes in understanding of communications, operations, and vulnerabilities. Weak or missing analysis of IOCs, or significant misunderstanding.
QUALITY OF PRESENTATION *Clarity of reporting, organisation of information, timing, and presentation.* **[25% weighting]**	Highly professional reporting style. Outstanding levels of clarity and organisation of information. Uniquely informative and well presented.	Professional reporting style. Excellent levels of clarity, excellently organised, exceptionally clear, concise throughout, and informative. Excellent balance of time allocated to each point of discussion.	Very clear reporting style. Concise and well organised. Well-balanced time allocated to each point of discussion. Minimal flaws.	Mostly clear reporting style. Could be more concise. Pace of delivery is slightly fast. Could improve balance of time, e.g. too much time on one topic at the expense of others. Minor flaws.	Clarity is acceptable, but with notable flaws. Not all information is presented clearly. Lacks concision. Crams in too much content. Minor audio and/or visual issues.	Lacks clarity. Disorganised or difficult to follow. Problematic flaws in presentation style. Unprofessional approach. Audio edited to increase speed and is distracting. Over 6 minutes.

Guidance on Video Recording and Screen Capture

You may use whichever video and audio capture tools you feel work best for you. However, you must ensure the audio is suitably clear, and any text in Wireshark must be clearly visible.

One possible option is to use PowerPoint, which can capture very good quality screen capture videos with audio. For your information, the links below discuss how to use PowerPoint to capture a video, and use of tools in Windows or macOS for video editing, merging, etc.

- https://support.microsoft.com/en-us/office/record-your-screen-in-powerpoint-0b4c3f65-534c-4cf1-9c59-402b6e9d79d0
- https://www.howtogeek.com/355524/how-to-use-windows-10s-hidden-video-editor/

Save your video as an **mp4** file and upload it via the Canvas 'Assignments' submission page.

Plagiarism and Collusion

This is an independent piece of work and must be completed solely by you. You must not discuss or share your analysis with anyone else. The analysis that you present must be your work, and your work alone.

This is an open-ended investigation. You are encouraged to find and present information that you believe others may have missed.