Case Study: Identify the Attacks

Assignment

2h - 2h20m

Status | Incomplete

Introduction

In this activity, you will create an Incident Disclosure report outlining the details of a Cyber Security attack, including an incident overview, what the attacker discovered and what/how any of this may have been important to the attacker. Incident Disclosure reports are an important part of your work in Cyber Security because they allow an organization to identify and deal with current threats, as well as plan proactively to protect against future threats.

Case Study

In this case study, you will be provided with two PCAP files to investigate using Wireshark.

Gain all the prospect information you can to investigate the events. Focus on collecting IP addresses, Ports, and date/time stamps of events of interest, build a timeline and discover what the attacker discovered. Then complete the Incident Disclosure Report as per the template given in Step 3.

Step 1: Investigate the following artifacts in the order given here; making detailed notes as you investigate each artifact.

1. Incident Information:
    - Using Wireshark, analyse the PCAP files provided here: File 1 and File 2
    - Based on the PCAP files provided, determine which IP addresses and Ports were involved in the incident.
2. Client Note:
    - Incident Notes - Record the approximate time and date of the first attack
    - Give details of how you identified the type(s) of scans that were performed and are seen.

Step 2: Examine the Network.

1. Record observations of systems, applications, services, ports, endpoints, and network traffic.
2. Research any ports discovered and what services they are associated with. Are there any here to be concerned about?
3. Create timeline based on evidence available.

Step 3: Complete the Incident Disclosure Report; including the following information in your report:

- Title of report
- Incident report # 01001
- Date filed
- Date of incident (as reported)
- Incident description (as reported)
- Executive summary
- Description of actual incident
- What was discovered as a result of the scan
- Attacker IP(s)
- Attacker MAC(s)
- Time of attack (first packet of attack)
- Packet number of first packet in attack
- Protocol(s) used in attack
- Suspected Nmap/scan configuration
- List any NVD records that may apply to the attack; describe how they are related
- Screen captures from Wireshark showing attack with explanations (Appendix A)

Step 4: Once the Incident Disclosure Report is completed, post it through Compass. You are also encouraged to submit the report on Discord for any peer feedback.

Case Study Discussion with Peers

You may discuss the findings of *Identify the Attacks* case study with your peers. To discuss with your peers, take the steps given below.

- Review at least two reports posted by your peers on Discord.
- Present highlights of your case study/ report to your peers.
- Share and receieve constructive feedback to support your peers.
- Integrate any feedback to your report and save the updated report to your PKM.

Conclusion

By creating an Incident Disclosure Report, you completed a crucial activity of a Cyber Security professional. You were able to investigate an attack and outline the issues and mitigation strategies that an organization could take to better protect themselves and learn from the attack. Next, you will jump to a reading that that helps your prepare for the project work in this course.

W02D5

Fri Jul 5

- Outline & Notes (1)
- Lectures (1)
- Work (9)

  11 hrs

  - Assessing Scenarios ✓
  - Case Study: Identify the Attacks
  - Develop a Monitoring Solution
  - List of Risks and Vulnerabilities
  - Tools Research and Documentation
  - New Project Open
  - Project: Report on Risks & Vulnerabilities
  - TIs: How to Prepare ✓
  - TIs: Study Guide ✓
- Other (1)

W02D5 Schedule »