AI Cyber Security with (Networking and SOC) Project Details

There Will be Two Major and Two Minor Projects

Major Projects: 2

Project 1: Security Operations Center (SOC) Analyst

Project Background

You have been selected as a Junior SOC Analyst at Nivi Cyber Solu ons, a company that manages IT infrastructure and applications for multiple clients.

The company has recently experienced several suspicious activities, including repeated login failures, unusual network connections, and suspicious processes running on employee computers.

The management has decided to build a Security Operations Center (SOC) monitoring environment to identify and investigate such activities before they become serious security incidents.

As a newly joined SOC Analyst, your first assignment is to build a small SOC lab in your own system and investigate security events generated inside the lab environment.

- Basic lab setup on their own laptop
- Install Wazuh/Splunk
- Generate logs
- Give students scenario-based ques ons
- Students analyse the logs and answer the questions

Lab Setup

Students need to install:

- VirtualBox / VMware
- Windows 10/11 VM
- Kali Linux VM Wazuh or Splunk Sysmon for Windows
- Wireshark — op onal

Student Project Questions

Scenario 1 — Multiple Failed Logins

Scenario: The SOC receives multiple failed authentication events from the same source IP.

Questions

1. What is the source IP address?
2. What is the des na on/target system?
3. Which username is being targeted?
4. How many failed login attempts occurred?
5. What is the first failed login timestamp?
6. What is the last failed login timestamp?
7. Is the activity suspicious? Why?
8. What type of attack could this indicate?
9. Which MITRE ATT&CK technique is associated with this activity?
10. What ac on should a SOC Analyst recommend?

Scenario 2 — Successful Login After Failed Attempts

Scenario: A user account has several failed login attempts followed by a successful login.

Questions

1. Identify the affected username.
2. Identify the source IP.
3. How many failed attempts occurred before the successful login?
4. What time did the successful login occur?
5. Was the successful login from the same source IP?

6. What is the significance of this event?
7. Could this indicate a compromised account?
8. What additional logs would you investigate?
9. What severity would you assign?
10. What immediate action would you recommend?

Scenario 3 — Network Port Scanning

Scenario:

The SOC no ces one internal system connecting to many ports on another machine within a short period.

Questions

1. What is the source IP?
2. What is the des na on IP?
3. Which ports were accessed?
4. How many connections have occurred?
5. What is the me range?
6. Does the activity look like normal traffic?
7. What type of activity could this represent?
8. Which tool could have generated this activity?
9. Which MITRE ATT&CK technique applies?
10. What should the SOC Analyst investigate next?

Final Student Task

After completing all scenarios, students must answer:

SOC Investigation Questions

1. How do you identify a true positive?
2. How do you identify a false positive?
3. What information should be collected from an alert?
4. How do you determine the severity of an alert?
5. What is the difference between an event, alert, and incident?
6. Why is log correlation important?
7. What is the importance of timestamps?

8. Why are sources and does na on IP addresses important?
9. What is the role of Sysmon?
10. What is the role of a SIEM?
11. What is the difference between Wazuh and Splunk?
12. What is MITRE ATT&CK?
13. How does a SOC Analyst perform an initial investigation?
14. When should an alert be escalated?
15. What information should be included in a SOC incident report?

Final Deliverable

Students should submit only:

- Lab setup screenshots
- Wazuh/Splunk dashboard screenshot
- Log analysis screenshots
- Answers to the 3 scenarios
- One final incident report for Scenario 3

Project 2: Find the vulnerabilities on Web Application and write a report.

Ethical Hacking : Web & Network Security Assessment of Nivi Cyber Solutions Corporation

Project Background

You have been hired as a **Junior Ethical Hacker / Security Consultant** by **NiviCyberSolutions**

Nivi Cyber Solutions has recently launched an internal web application and deployed several servers on its corporate network. Before allowing the application to go into production, management wants an independent security assessment.

You have been authorized to perform a **controlled penetration test against the company's lab environment**.

Your objective is to identify security weaknesses, validate them safely, collect evidence, and prepare a professional penetration-testing report.

Reconnaissance

Nivi Cyber Solutions provides you with the following information:

Target Network: Internal lab network
Target: Web application server
Authorization: Testing is permitted only against the assigned lab machines.

Your first task is to understand the target environment without attempting exploitation.

Questions

1. What hosts are active?
2. What IP addresses belong to the target systems?
3. Which ports are open?
4. Which services are running?
5. What versions of services can be identified?
6. Which system appears to host the web application?
7. What information can be gathered without authentication?
8. Which services require further investigation?
9. Which findings should be considered high priority?
10. Prepare a basic network/asset map.

Web Application Enumeration

You discover that Nivi Cyber Solutions has an internal web application.

Your task is to perform application reconnaissance.

Questions

1. What technologies are used by the web application?

2. What web server is running?
3. What directories/endpoints can be discovered?
4. Are there hidden pages or resources?
5. Are directory listings enabled?
6. Are there interesting HTTP response headers?
7. Are there exposed files or backup resources?
8. Are there authentication-related pages?
9. What information is disclosed by the application?
10. Which areas require deeper testing?

Authentication Testing

During testing, you discover the application's login page.

Target: Authorized lab application only.

Your task is to assess whether authentication controls are properly implemented.

Questions

1. Is HTTPS being used?
2. Does the application provide appropriate login controls?
3. Are usernames disclosed through error messages?
4. Are authentication error messages overly informative?
5. Is there account lockout/rate limiting?
6. Are session cookies configured securely?
7. Does logout properly invalidate the session?
8. Can unauthenticated users access protected resources?
9. What authentication weaknesses did you identify?
10. How would you recommend improving authentication security?

Web Input Validation

You notice that several application pages accept user input.
Your task is to test whether the application properly validates and handles input.

Questions

1. Which parameters accept user input?

2. Which parameters should be tested?
3. Does the application properly validate input?
4. Are special characters handled safely?
5. Are SQL-related errors exposed?
6. Are script-related inputs handled safely?
7. Can user input affect application behavior?
8. What evidence should be captured?
9. What is the potential security impact?
10. How should the issue be remediated?

Final Deliverable

Students should submit:

1. **Lab Setup**
   - VM screenshots
   - Network configuration
   - Target application screenshot

2. **Reconnaissance Report**
   - Target IPs
   - Open ports
   - Services
   - Versions

3. **Web Assessment**
   - Discovered endpoints
   - Authentication findings
   - Input-validation findings

4. **Vulnerability Report**

   For every finding:

Finding:

Severity:

Affected Asset:

Description:

Evidence:

Impact:
Remediation:

Reference:

5. Final Penetration Testing Report

The report should contain:

Executive Summary → Scope → Methodology → Findings → Evidence → Risk Rating → Remediation → Conclusion

This keeps the project **practical and beginner-friendly**, while teaching students how a real penetration-testing engagement is structured rather than simply teaching individual hacking tools.

Minor Projects: 2

Project 1: Information Gathering & Scanning to find the loop holes

"Find the Loopholes – Reconnaissance & Security Assessment of a Test Network" Project Story :

You are working as a **Junior Ethical Hacker** for a cybersecurity consulting company.

Your client, **ABC Technologies**, has provided you with a small **authorized test network** containing a web server and a Linux server.

The client does not want you to exploit the systems. Instead, they want you to perform **Information Gathering and Scanning** to identify exposed services, unnecessary ports, outdated software, and other potential security weaknesses.

Your mission is:

"Find the loopholes before an attacker finds them."

All testing must be performed only against the student's own isolated lab/authorized target.

Scenario 1 — Discover the Network

The client gives you only the network range.

"We don't know exactly what devices are currently active. Identify the systems that are responding." Questions

1. How many live hosts did you identify?
2. What are their IP addresses?
3. Which host appears to be the web server?
4. Which host appears to be the Linux server?
5. Are there any unexpected systems?
6. What method/tool did you use to identify live hosts?
7. What information did you collect about each host?
8. Which hosts require further investigation?

Scenario 2 — Find Open Ports

The client says: **"Identify all services that are exposed on our servers."**

Questions

1. Which ports are open on the target?
2. What service is running on each port?
3. Which ports are commonly associated with web services?
4. Is SSH exposed?
5. Are any unnecessary ports open?
6. Which open port represents the highest security concern?

7. What version information can you identify?
8. Which services require further investigation?
9. Are there any unexpected services?
10. What recommendations would you provide to the client?

Scenario 3 — Service Enumeration

The client wants more information about the discovered services.

Questions

1. What web server software is running?
2. What version is identified?
3. What operating system can you identify or infer?
4. What SSH version is running?
5. What technologies are used by the web application?
6. Are there any potentially outdated services?
7. Which information should not normally be publicly exposed?
8. Which service would you prioritize for vulnerability assessment?
9. What additional enumeration would you perform?
10. Document your findings with screenshots.

Scenario 4 — Web Information Gathering

You discover that one of the servers hosts a web application.
The client asks:

“Find out what information an unauthenticated visitor can learn about our application.”

Questions

1. What web technologies are being used?
2. What web server is running?
3. Can you identify the application framework?
4. Are interesting directories or endpoints discoverable?
5. Are backup or temporary files exposed?
6. Is directory listing enabled?

7. Are there unnecessary information-disclosure headers?
8. Are any administrative pages discoverable?
9. What information could help an attacker?
10. Which findings should be reported to the client?

Scenario 5 — Identify Security Loopholes

After completing information gathering and scanning, the client asks:

"You have collected the information. Now tell us where our security weaknesses are."

Questions

1. What unnecessary services did you identify?
2. What potentially outdated software did you identify?
3. What unnecessary ports are exposed?
4. What sensitive information was disclosed?
5. Were any hidden directories or endpoints discovered?
6. Were there any security-related HTTP header issues?
7. Which findings are low risk?
8. Which findings are medium/high risk?
9. Which issue should be fixed first?
10. What is your recommended remediation?

Project Outcome

By completing this minor project, students should understand:

How much information can an attacker learn about a system before exploitation even begins.

Project 2: Penetration testing on System and Stenography

Project Story

You are a **Junior Penetration Tester** at a cybersecurity consulting company.

Your client, **SecureCorp**, has provided an intentionally vulnerable test server and a suspicious image file. Your assignment is to:

1. Identify exposed services on the target.
2. Use **Metasploit Framework** to validate selected vulnerabilities in the authorized lab.
3. Document the security impact.
4. Investigate the suspicious image for hidden information using steganography techniques.

Scope: Kali Linux → intentionally vulnerable lab VM only. No testing of public or third-party systems.

Part A — System Penetration Testing with Metasploit

Scenario 1 — Target Discovery

The client tells you:

"We have provided one vulnerable test server. Identify what services are exposed before attempting any security validation."

Questions

1. What is the target IP address?
2. Which ports are open?
3. Which services are running?

4. What versions are identified?
5. Which services appear vulnerable?
6. Which service would you investigate first?
7. Why did you select that service?
8. What information should be collected before using Metasploit?

Scenario 2 — Vulnerability Identification

After scanning the target, you identify a potentially vulnerable service.

Questions

1. What service is potentially vulnerable?
2. What version is running?
3. What vulnerability is associated with the service?
4. What is the vulnerability's severity?
5. Can you find a corresponding Metasploit module?
6. What is the Metasploit module name?
7. What information does the module require?
8. What precautions should be taken before running the module?

Scenario 3 — Metasploit Module Selection

The security team asks you to validate the vulnerability using Metasploit.

Questions

1. How did you search for the appropriate Metasploit module?
2. What module did you select?
3. What vulnerability does the module target?
4. What target/service does the module affect?
5. What options must be configured?
6. What is the target IP?
7. What payload, if any, is appropriate for the controlled lab?
8. How did you verify that the module was targeting the correct system?
9. What evidence should be captured?

10. What would you do if the module fails?

Scenario 4 — Controlled Exploitation

You have authorization to validate the vulnerability on the lab server.

Objective: Determine whether the identified vulnerability can provide unauthorized access to the intentionally vulnerable target.

Questions

1. Was the vulnerability successfully validated?
2. What evidence confirms successful exploitation?
3. What level of access was obtained?
4. Which user/account context was obtained?
5. What system information can be safely collected after access?
6. What is the potential security impact?
7. Does the result indicate a critical, high, medium, or low-risk issue?
8. What evidence should be included in the report?
9. What remediation should be recommended?
10. How should the test environment be restored after testing?

Scenario 5 — Post-Exploitation Investigation

The vulnerability was successfully validated.

The client asks:

"If an attacker obtained access, what could they potentially learn about the compromised system?"

Questions

1. What operating system is running?
2. Which user context is active?
3. What hostname is assigned?
4. What network interfaces are present?
5. What services are running?
6. What level of privileges does the compromised account have?

7. Is there evidence of sensitive information being accessible?
8. What additional security weaknesses did you observe?
9. What actions should **not** be performed during an authorized assessment?
10. How would you communicate the impact to management?

Part B — Steganography Investigation

Scenario 6 — Suspicious Image

The client provides an image found on the compromised lab system.

"We suspect this image may contain hidden information. Investigate it without modifying the original evidence."

Questions

1. What is the image file type?
2. What is its file size?
3. What metadata is present?
4. Are there unusual metadata values?
5. Are there suspicious strings?
6. Does the file appear to contain embedded data?
7. Which steganography tool would you use?
8. Can hidden information be extracted in the lab?
9. What did you discover?
10. What evidence supports your conclusion?

Final Scenario — Connect the Findings

The client now gives you the complete case:

"Our test server contained a vulnerable service. During your assessment, you successfully validated the vulnerability using Metasploit. You also discovered an image file that may contain hidden information. Determine the overall security risk."

Final Questions

1. What was the vulnerable service?
2. What vulnerability was identified?
3. Which Metasploit module was used?
4. Was exploitation successful?
5. What level of access was obtained?
6. What evidence confirms the compromise?
7. What suspicious file was discovered?
8. Did the image contain hidden information?
9. Could the vulnerability and suspicious file potentially be related?
10. What are the top three security recommendations for SecureCorp?