[F24] Group Project Assignment (30%):

Network and Cyber Security

Project description

In this group project, you will work on the ideas, which should be related to the materials covered in the course as well as the ideas that extend your knowledge, for example towards SecOps, penetration testing, and DevSecOps areas. This is the time when you can apply your cyber security skills

Dividing into groups

Firstly, group your teammates (3-4) people. Then use this link where you fill in the project details. The deadline for project approval is Tuesday **26.11.2024**. Once the project is approved you can start to work on it.

Deliverables:

1. Project Results and Report (20%)

   The report should contain the following sections:

   I. Goal/Tasks of the Project - what are you going to solve and responsibilities for each team member

   II. Execution plan/Methodology - plan for the solution, any graphs, schemes, and description for the planned infrastructure

   III. Development of solution/tests as the PoC - explanation and testing of the solution

   IV. Difficulties faced, new skills acquired during the project

   V. Your conclusion, your contemplations, and your judgment

Be aware to include all important links (with the code, configurations, etc) to an open repository as proof of concept. Long appendixes at the end of the report are okay to use.

2. Demo of the solution (10%)

Provide as the demo all results that were received during the project work (working solution, important configurations, testings, etc). There is no limit in time, but make it concrete, with the logical flow and clear. The demo can be recorded by any team member or all together. We recommend uploading the video on YouTube channel and providing a link in the report and in Moodle.

3. Project Categories Examples

3.1 Application Security

Introduction

You will explore existing software vulnerabilities by creating attack scenarios that exploit them.

Each attack scenario should be placed in a Docker virtual environment, described in the report and demonstrated in the demo.

A list of common category types of software vulnerabilities is provided by the Common Weakness Enumeration (CWE™) community. Choose any vulnerability you would like to explore (but not more than 3) from the category list from CWE and analyze how they can be exploited.

Exploitation scenario

Deploy the necessary environment with Docker for each vulnerability. Use an existing exploit or write your own to attack the deployed system. Describe the steps you performed to attack the system and propose protection mechanisms (how to patch the system). For these purposes use the publicly known cybersecurity vulnerabilities list (CVE list) and exploit database (exploit-db).

Report/Demo

The Report/Demo should contain the following sections:

I. Attack surface and scenarios description

II. Vulnerabilities description [includes CWE and CVSS score]

III. Environment preparation

IV. Exploits steps and defense mechanisms observation

V. Difficulties faced

VI. Conclusion, your contemplations and judgement

Be sure to include links to DockerHub and links to the proof of concept demonstration video.

3.2 Security Operations - SecOps

Introduction

You'll build a Security Operations Center (SOC) using Open-Source tools. All the technology stack should be integrated with the SIEM, which is the core technology of the SOC.

Scenario

Deploy the Open-Source SIEM

Integrate the SIEM with threat intelligence to gather contextual information about the events received.

There should be a ticketing system that can be used by analysts to track incidents.

The SOC should be able to automatically respond to some security incidents, and simulate detection and response of 2 to 3 categories of security incidents using the SOC.

Report/Demo

The Report/Demo should contain the following sections:

I. Environment preparation.

II. Working instances of the selected tools for the SOC.

III. Case management system assigning a case to an analyst.

IV. Simulation of the selected security incidents and automated response by the SIEM.

V. Difficulties faced.

VI. Conclusion, your contemplations, and judgement.

You can add scripts used to your appendix. Be sure to include links to the proof of concept demonstration video.

3.3 Security in SDLC - DevSecOps

Introduction

You'll scan a vulnerable application with automated testing tools such as SAST, SCA, and IAC. Choose and configure at least 2 tools of your choice and send the results to a vulnerability management platform for a centralized view of the security posture of the application.

Scenario

Build or find existing vulnerable applications, and select tools supported by your vulnerability management platform. Integrate the vulnerability management platform with your chosen automated testing tools by writing scripts that upload the results generated by these tools to the orchestration platform. You'll have a centralized location where the results from used tools can be analyzed.

Report/Demo

The Report/Demo should contain the following sections:

I. Environment preparation.

II. Choosing or writing a vulnerable application.

III. Running of selected tools for automated testing.

IV. Writing or use of existing scripts to upload the generated reports to the vulnerability management platform.

V. An alert on the vulnerability management platform from each of the integrated tools.

VI. Difficulties faced.

VII. Conclusion, your contemplations, and judgement.

Be sure to include links to DockerHub, the application repo, and links to the proof of concept demonstration video.

4. Submissions

The report should be uploaded to Moodle by each member of the group.

In addition, you can use open repos such as GitHub, GitLab, Docker hub, etc. for storing scripts, configuration files, docker files/containers, etc. but provide links for that.