Project on Network Security Solutions

As partial fulfillment for the requirements of the “Intrusion Detection” class.
Othman Othman, Ismael Jabr, Ibrahim Amryeh

Introduction

In this project, student groups are expected to showcase their capacity to understand security-related solutions. This involves learning about the solution, applying their knowledge to successfully deploy the solution, and creating scenarios to highlight the significance of this solution. Besides the practical aspects, each group is also required to prepare a report and present their work to the class.

The primary goal of this project is to immerse students in situations that closely resemble real-world work assignments. This approach allows students to gain hands-on experience and a profound understanding of security solutions, equipping them with practical skills and knowledge essential for their future careers.

Project Description

This project is designed for groups of two students. Each group selects one of the security solutions listed in the following section. Each group is responsible for the following requirements:

1. Deployment [deliverable: Report]

   Groups are tasked with deploying their chosen solution using the method they find most suitable. This may involve tasks such as compiling and building, utilizing pre-compiled packages, working with virtual machines, containers, and more. At the completion of this requirement, each group is to submit a comprehensive report detailing all the steps taken. It's important to include proper references in the report.

2. Understanding Solution Capabilities [deliverable:Report]

   Groups must thoroughly study their chosen solution, examining its capabilities, architecture, components, methods, and any other attributes that aid in a detailed understanding of the solution. The capabilities of the solution must be studied in-depth. After fulfilling this requirement, groups are expected to submit a report summarizing their findings. It's important to include proper references in the report.

3. Scenario Design [deliverable: Report]

   This requirement applies the knowledge gained in the previous requirements. Each group is tasked with designing scenarios that demonstrate the solution's capabilities. These scenarios should include all the necessary components such as virtual machines, packet traces, traffic generation software, or attack software. Additionally, the scenarios should outline the required setup and any other prerequisites needed to execute them.

4. Presentation of Work [deliverable: Presentation]

   The final requirement involves a 30-minute presentation to summarize the group's work. Each group will present their findings and experiences to the entire class.

   This project aims to provide students with hands-on experience that simulates real-world tasks in the field of security solutions.

Security Solutions

Required for the project

1. IDS
   1.1. Zeek Cluster

2. SIEM
   2.1. Wazuh
      Installation
   2.2. Elastic
      Installation
   2.3. Alien Vault Ossim
      Installation

   2.4. **Bonus: Integrate the following tool to SIEM**
      2.4.1. TheHive

3. XDR
   3.1. Wazuh
      Installation
   3.2. OSSEC+ (HIDS + XDR)
      Installation
      Installation 2 (probably a better link)
   3.3. CrowdSec
      Docs
      installation

   Other possibility
   3.4. OPEN XDR PLATFORM

4. Digital Forensics and Incident Response (DFIR) [info]
   4.1. Velociraptor
      Docs
      Installation

Evaluation

Evaluation will be conducted by a committee using the following rubric. The evaluation committee will comprise the course instructor, a teaching assistant, and a security industry expert.

Evaluation Rubric

No		Mark	25%	50%	75%	100%
1.1	Deployment	10	Failed to compile, or install packages, or use VMs.	Failed to properly configure basic needs.	Failed to configure a fully functioning solution.	Successfully deployed: with all needed parts in subsequent steps are working correctly
1.2	Deployment **report**	10	Documentation that shows only step-by-step instructions. Without any explanation	Documentation that shows only step-by-step instructions. Without proper explanation.	Exceptional documentation, characterized by thorough explanations and well-documented, step-by-step instructions.	Exceptional documentation, characterized by thorough explanations and well-documented, step-by-step instructions. It adheres to all the conventions of scientific writing practices.
2.1	Understanding Solution Capabilities	10	Copying of the official website, (single source)	Showing only basic understanding of the solution. Showing only the components	Brief explanation of the components, (line or two for each).	A comprehensive and in-depth explanation of the solution.
2.2	Understanding Solution Capabilities **Report**	5	Same as above. Report does **not** adhere to conventions of scientific writing practices.	Same as above. Report **barely** adheres to conventions of scientific writing practices.	Same as above. Report **partially** adheres to conventions of scientific writing practices.	Same as above. Report adheres to **all** conventions of scientific writing practices.
3.1	Scenario Design	30	Simple basic scenario that barely demonstrates the capability.	Comprehensive Scenarios demonstrating at least 1 of solutions capabilities.	Comprehensive Scenarios demonstrating at least 2 of solutions capabilities.	Comprehensive Scenarios demonstrating at least 3 of solutions capabilities.
3.2	Scenario Design's **Report**	20	Documentation that shows only step-by-step instructions. Without **any** explanation	Documentation that shows only step-by-step instructions. Without **proper** explanation.	Exceptional documentation, characterized by thorough explanations and well-documented, step-by-step instructions.	Exceptional documentation, characterized by thorough explanations and well-documented, step-by-step instructions. It adheres to all the conventions of scientific writing practices.
4	Presentation of Work	15	Simple presentation	Good in either presentation, or the presentation skills.	Excellent in either presentation, or the presentation skills. Following all guidelines of presentation making.	Excellent presentation, show, and presentation skills. Following all guidelines of presentation making.
	Total	**100**				

Appendix: Additional Solutions

FYI

SOAR

Shuffler [online with limitations]

Installation [stand alone / local]

Catalyst

Github

HandBook

Packet Capture and Search

Arkime

Install

Network monitoring tools (primarily used for monitoring the health, performance, and availability of various IT infrastructure components, such as servers, networks, services, and applications.)

- Nagios
- Zabbix

IDS

- Falco
- Teler

SIEM

- GRAYLOG Open
- OpenSearch

NSM=NDR / IDS

- ROCK NSM
- EveBox

WAF

- Mod Security

EDR

- Open EDR
- Whids [GitHub]

DFIR = Digital Forensics and Incident Response

- Volatility3 [GitHub]
- PersistenceSniper

UBA

- OpenUBA [GitHub]

Cyber Threat Intelligence

- MISP [GitHub]
- OpenCTI [GitHub]

Email Security

- SpamAssassin
- SORBS

PAM

- Teleport
- JumpServer

Vulnerability Management

- Trivy [GitHub]

Antimalware

- ClamAV [GitHub]

Network Security

- Calico

Continuous Compliance

- Open Policy Agent [GitHub]

IAM / Access Control

- keycloak
- Dexidp
- LinOTP

Visibility and Audit Dashboards

- Prometheus
- Grafana

Threat Emulation and Analysis platform

- VECTR

Malware Analysis Tool

- Cuckoo SandBox

System Monitor

- Ebpf (Linux)
- Sysmon (Windows)

Below is a quick explanation of the differences between XDR and other detection and response technologies:

- **Endpoint detection and response (EDR)**: Monitors end-user devices — desktops, laptops, tablets and phones — for threats that antivirus software can't detect
- **Managed Detection and Response (MDR)**: Essentially EDR purchased as a service.
- **Network Detection and Response (NDR)**: Monitors communications within the network to detect, investigate and respond to threats that might otherwise remain hidden in unmanaged devices across on-premises, cloud and hybrid environments.
- **Identity Threat Detection and Response (ITDR)**: Detects threats to all Service and Privileged accounts on your network and cloud.
- **Extended Detection and Response (XDR)**: Uses EDR capabilities to extend protection beyond endpoints to also monitor data from networks, cloud workloads, servers, email, and more.
- **Managed Extended Detection and Response (MXDR)**: Delivers managed multi-domain protection with 24/7 dedicated support, expertise, and response.

The Fundamentals of Cybersecurity