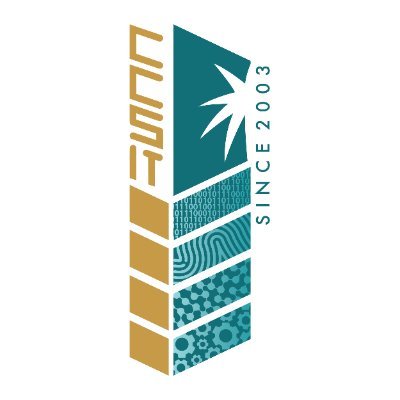
صورة تحتوي على نص

تم إنشاء الوصف تلقائياً

**Kingdom of Saudi Arabia**

**Ministry of Higher Education**

**King Faisal University**

**College of Computer Sciences & Information Technology**

**Feb 2023 , 2 Semester**

CCSIT Networks and Telecommunications

**Network Forensics Project Report**

**Supervised by:**

**Dr. Abdullah Al.Boali**

**CRN: 70**

**Student Names & ID:**

|  |  |
| --- | --- |
| Hamad Adel Al.Khalifah | 219040274 |
| Youssef Hamad Al.Hassan | **219012348** |

**Table of contents**

[**Introduction: 6**](#_Toc86351938)

[**Problem Statement: 6**](#_Toc86351939)

[**Objective of this report. 6**](#_Toc86351941)

**SDAIA** [**Full Archticture : 7**](#_Toc86351942)

[**Evidence : 9**](#_Toc86351943)

[**Objective**](#_Toc86351944) **9**

**Forinsics analysis (Steps taken)** 10

[**Relevant Finding 1**](#_Toc86351946)**0**

[**Conclusion:**](#_Toc86351947) **11**

**Reference table** 12

# Abstract

This project will talk about Network Security and Investigation for SDAIA (Saudi Data & Ai Authority ) , The purpose of this project is to show how the student can deal with the threat that may vulnerable an organization through network security. Also, emphasize our knowledge in cybersecurity objective (CIA Triangle). Furthermore, provided the suitable protection strategy and mechanisms for the system and network.

# Saudi Data and Artificial Intelligence



Figure :SDAIA

SADAIA contributes to achieving the goals of Vision 2030 by offering a set of direct initiatives in the various vision programs, and it also works to empower various government agencies, by providing several services and products, such as: technical services, analytics, data-based scenarios, and artificial intelligence solutions for different use cases. data governance and artificial intelligence; In order to enable safe and orderly technical growth.

# Introduction:

Computer and information technology is by far the world's largest and fastest growing industry. Demand for Network Security and data privacy. Any vulnerability that affects the engaging party in any organization may compromise the confidentiality of their users and ruin their reputations. Computers Networks have become an essential component of many large systems requiring sophisticated control, and hardware placement locations.

# Problem Statement

Scientific organizations place a high value on network design and security since they have a big number of users, therefore network coverage and privacy must be done carefully and properly. It is critical to design the network in a way that is proportional to the size of the buildings and takes into account the number of present and future users and the valuably of data that protective by the organization. Also, it’s important to track and investigate an attack before compromise the system.

# Objective of the project

The goal of this study is to combine our knowledge in Network design and security. Also, seeking to construct the network in a way that is appropriate to exchange data safely from being vulnerable and compromise. Furthermore, exercising the ways of performing security object (CIA triangle). Finally, Assures the security of the systems from the hardware and software that are being used in the organization and instruct the best paths lead to it.

# Full Architecture:

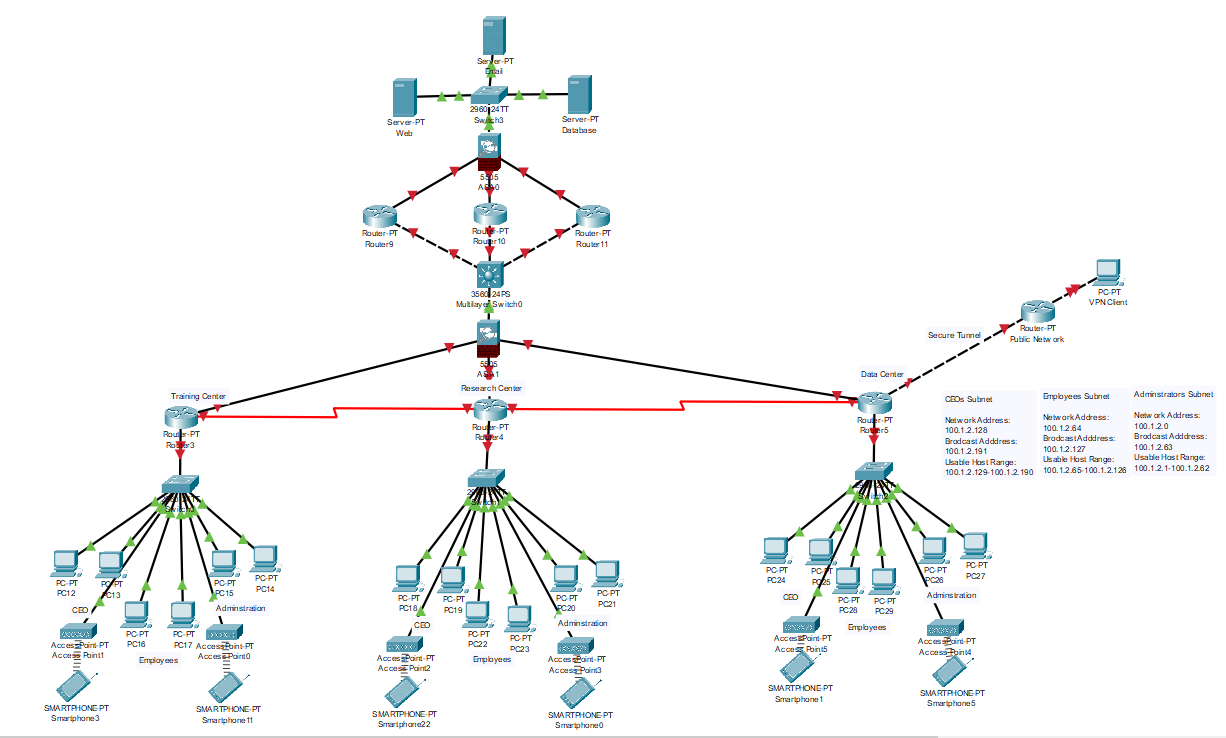


Figure :Full Architecture

We chose to design the network using the Cisco three-layer hierarchical model which consist of Core Layer, Distribution Layer and Access Layer.

Access – controls user and workgroup access to the resources on the network. This layer usually incorporates Layer 2 switches and access points that provide connectivity between workstations and servers. You can manage access control and policy, create separate collision domains, and implement port security at this layer.

Distribution – serves as the communication point between the access layer and the core. Its primary functions are to provide routing, filtering, and WAN access and to determine how packets can access the core. This layer determines the fastest way that network service requests are accessed. This layer usually consists of routers and multilayer switches.

Core – also referred to as the network backbone, this layer is responsible for transporting large amounts of traffic quickly. The core layer provides interconnectivity between distribution layer devices it usually consists of high-speed devices, like high end routers and switches with redundant links.

# Evidence:

In this Criteria we list the finding that may vulnerable the system including the software and hardware. Also, how the attackers was able to compromise the system.

**ARP Spoofing:** is a network attack technique. When the attacker sends fake ARP messages. Firstly, the attacker begins by scanning the IP addresses and mac addresses of the SDAIA network using scanning tools such as (Wireshark, Nmap, Nessus, etc.) Secondly, the attackers send a fake ARP message to the SDAIA computers, pretending to be legal/authorized partner. Thirdly, the attackers were able to steal sensitive data that can be used to compromise the system. Lastly, the attackers now can intercept and modify and block network traffic that passes through attacker’s computers.

**DDoS Attack:** distributed Denial of Service) attack is a type of cyber-attack which compromised multiple computer systems and servers. DDoS Attack are used to flood a targeted website or network with traffic to the point that system is shutdown, then all users can’t log or communicate with the system. Firstly, the Attacker is targeting an authorized user in SDAIA system using fishing attacks and techniques. Secondly, after compromise the authorized user, the attackers seek to gain permissions to manipulate and control the system. After, the gain the permissions they start to create network of bots, known as a botnet, used to launch the DDoS attack, then the attackers target system or network to send a large amount of traffic to the target.

**Phishing Attack**: The attackers target an authorized user inside SDAIA and uses personal information, such as names, job title, or other details to posses’ sensitive data and logs to the system. Also, the attackers send an email that appears to come from a legitimate source to steal their login credentials or other sensitive information. Also, the attackers set up a fake website that looks like a legitimate site, such as a banking or e-commerce to lure the authorize user.

**Password cracking attack**: the attackers target the weak password that doesn’t fulfills regulatory recommendations for security protection. the attackers use dictionary attack in order to not be alerting the server. The attacker will generate a list of hashes and wordlist to match between them using tools such as hashcat. After, the attackers discover the password to log into the system.

**Wi-fi hacking attack:** unauthorized access that compromise the wireless network or the intercept wireless network traffic. Firstly, the attackers scanning the wireless network that are in range. using tools like NetStumbler or Kismet to identify the wireless networks and their details, such as the SSID (network name), channel, and encryption type. Secondly, after identifying encryption type such as (MD4, MD5), the attackers use the dictionary attack “mention earlier”. Thirdly, the attackers set up a fake wireless network that looks like SDAIA Internal network, in order to trick SDAIA users into connecting to it. Lastly, the attackers were able to steal sensitive data and information also, monitoring network traffic and gaining access to network resources.

**Man in the middle attack:** an extinction of wireless attack where the attackers manage to be inside the local network (LAN) then compromise the communication channel. Furthermore, the attackers intercept the communication between two parties and secretly steals and modifying the information being exchanged. MITM attacks can occur in various forms, such as (Email hijacking, DNS Spoofing, ARP Spoofing, Wi-fi hijacking, SSL/TLS hijacking, etc.,)

**Web application Attacks**: are a type of cyber-attack that targets web-based applications, such as websites, online forms, and web-based databases. Firstly, the attacker was able to inject malicious code (XSS) into a DOM (Document object Models) of SDAIA website. Then, the codes were accidentally executed by one of the SDAIA employers. Secondly, the attackers gain access and permission to access the website database to injecting malicious (SQL commands) into web forms or URLs. then, the attackers bypass authentication and access sensitive data and able to compromise the web server by modifying and taking control of the entire database.

# Objective:

This criterion focusses on Incidence response responsibility toward the organization that hire to investigate the attack. There are certain parameters and objectives that should be taken under consideration such as:

1. Valuable the damage of the attack?
2. How many services have been compromised?
3. Did the Attack contain and recovers?
4. How the attack happens external/internal?
5. Did the SDAIA Partners affected by this attack?
6. What is the valuable of data that lost?
7. Did the backup servers compromise?
8. Is ‘it confirmed that SDAIA network is free from any suspicious threats?
9. How long it takes to reconstruct the system into the backup servers?

# Forensic Analysis (Steps Taken)

This criterion discusses the steps taken to mitigate with the attack that affect SDAIA system and network. we need to ensure system security in software and hardware to retrieve system functionality and work environment. Firstly, Isolate the compromised system to prevent the attacker from continuing to access or control the system. The next step is to preserve evidence by creating a forensic image of the system. This image will be used later in the investigation to analyze the attack and identify the attacker. Furthermore, identify the source and nature of the attack. This analysis should include examining system files, system logs, network traffic logs, and any other relevant data. Secondly, for recover the system and securing the resource we create cloud storage and store the data that we able to extract from the damaged server. Also, to reconstruct the system to ensure functionality and work environment. Thirdly, we create a copy from the system that contain sensitive data then store at a safe offsite location to ensure that even if the servers compromise, the system can be reconstructed because we place backup servers in multiple safe location. Fourthly, we need to ensure that the servers from multiple location is communicate together to store the system updates, so we use high advanced technology such as parity RAID 6, Also use mechanism called replication to store the data in all master servers. Lastly, Review and update security policies prevent similar attacks in the future. This may involve implementing additional security measures, such as multi-factor authentication and regular vulnerability assessments, like ensuring that all the SDAIA employer using a strong password that satisfy regulatory recommendations for security protection.

# Relevant Findings

|  |  |
| --- | --- |
| Attack | ID / Mitigation |
| DDOS | https://attack.mitre.org/mitigations/M1037 |
| ARP Spoofing | https://attack.mitre.org/groups/G0003 |
| Web server | https://attack.mitre.org/groups/G0050 |
| MITM | <https://attack.mitre.org/groups/G0094> |
| Password cracking | https://attack.mitre.org/software/S0056 |
| WI-FI Attack | https://attack.mitre.org/mitigations/M0802 |

# Conclusion:

To conclude this is our incidence response analysis report for network forensics we focus in this report how to mitigate an attack that compromise the system. Also, how to conduct a forensics analysis to discover evidence of attack. Also, we discuss our strategy in how restore a compromise system.

# Reference Table:

|  |
| --- |
| https://sdaia.gov.sa/ar/default.aspx |
| Dr. Abdullah Al.Boali KFU Professor |
| https://www.forensicfocus.com/articles/writing-dfir-reports-a-primer/ |
| <https://en.wikipedia.org/wiki/Network_Forensics> |
| https://attack.mitre.org/ |
|  |