1

**CIS 480 Project – Injection 1**

**Injection**

* • Happy Monday Morning! The early bird gets the worm, and it doesn't get much earlier than this huh? I'm your incredibly overbearing CIO and I feel the need to check up on my rockstar security team at all hours of the day and night!
  1. • Please respond to this injection with the following information. o Identify the leader
  2. o Introduce the team and describe the roles and responsibilities of each member during the competition. (*Do not take this seriously and just describe what each is going to do. One paragraph is enough.)*
  3. o Develop a brief security policy of the organization. It can be 10-20 bullets in a half page document. Please do not use ChatGPT for this.
* • Provide your response to this injection at the end of this document.
* • Each team needs to make one submission per injection. The team leader shall make submission on behalf of the team.
* • Follow the naming convention for the submission. Use this format: CIS480Prj-injX-teamY.docx, where X is injection number, and Y is your team number on the team roster.)
* • Each injection is worth 10 points.
* • I rearranged the team numbers. So, your need to make sure your team number. The names in blue are randomly placed by me because of their lack of response.

https://docs.google.com/spreadsheets/d/1JJto2Pm5sn4DEDbf0tkS4x5WZcjHWbeovNVkt8eCPNo/edit#gid=0

* • The injections are posted on BB > Assignments > Project 1 - Red Team Competition > Injections.
* • For inquiries on the injections, Go to Teams > CIS 480 (2023 Fall) > Injection X. Contacting the professor via email is prohibited.

2

* • For submission, Go to BB > Assignments > Project 1 - Red Team Competition > Inj#X.
* • Schedule

|  |  |  |
| --- | --- | --- |
| **Injections** | **Open** | **Close** |
| Injection 1 – Introduce the team | Mon, 13th | Tue, 14th |
| Injection 2 – Scan the network | Tue, 14th | Wed, 15th |
| Injection 3 – Break into the target | Wed, 15th | Fri, 17th |
| Injection 4 – File transfer | Wed, 15th | Fri, 17th |
| Injection 5 – Treasure hunt | Thur, 16th | Sat, 18th |

**Response to Injection 1**

1) Team leader and members.

2) Roles and responsibilities, etc.

3) Develop a brief security policy of the organization.

1. Team Leader: Tristan Rogers

Members: Chip Carter

Eric Lopez-Gutierrez

1. Roles and Responsibilities:

**Security Policy**

**Objectives**

In response to ever growing threat of cyber-attacks we have developed the following guidelines to create safer administrative, technical, and physical safeguards of our data and information. The following safeguards are designed to:

* Safeguard the security and confidentiality of our data and information.
* Deter and shield us from any threats or hazards to the security of our data and information.
* Deter and shield us against any unauthorized access or use of our data and information that could create harm or inconvenience to us.

This Security Policy will:

* Identify and assess risks that could threaten our information and data.
* Develop policies/procedures to mitigate risk.
* Implement and test the validity of created policies plan.
* Adjust accordingly to fit the ever-changing digital environment and its risks.

**Policies**

User Policies

* Permissions are granted based on job roles.
* Review and update access rights regularly
* Enforce strong password requirements.
* Enforce password changes and forbid password sharing.
* Provide security awareness training to employees regularly.
* Educate employees on social engineering tactics.

Network Policies

* Make use of firewalls and intrusion detection/prevention systems.
* Update and patch all network devices regularly.
* Require multi-factor authentication for remote access connections.
* Monitor, log, and review all remote access activities.
* All sensitive data, both in transit and at rest, must be encrypted.
* Encrypt all sensitive data.

Physical Security

* Access to communications equipment rooms and sensitive areas will be restricted.
* Surveillance systems and access logs will be used for physical security monitoring of communication equipment rooms, sensitive areas, and asset storage rooms.

Documentation

* Regularly maintain documentation of security policies.
* Report security incidents immediately to authorities