Detection and Prevention of DDOS using Wireshark and Snort

1. Objectives of RMP

4.1.1. Lists of Threats/Vulnerabilities

Threats/Vulnerabilities	Component
Data Leak/Stolen	Application
Natural disaster	External
DOS Attack	Server/Web application
Human	Social Engineering

1.2. Costs associated with risks

- Confidentiality

Rate	Description	Point
Low	No affect or effect a little	1
Medium	The system can accept the risk	2
High	Seriously affect to the system	3

- Integrity

Rate	Description	Point
Low	No affect or effect a little	1
Medium	The system can accept the risk	2
High	Seriously affect to the system	3

- Availability

Rate	Description	Point
Low	No affect or effect a little	1
Medium	The system can accept the risk	2

High	Seriously affect to the system	3

- Rating Threats/Vulnerabilities:

Threats/Vulnerabilities	Confidentiality	Integrity	Availability	Rate
Data Leak/Stolen	3	2	3	8
Natural disaster	1	3	3	7
DOS Attack	3	3	3	9
Human	3	3	1	7

1.3. List of Recommendations to Reduce the Risks, Cost and Benefit

Threats/Vulnerabilities	Recommendation	Cost	Benefit
Data Leak/Stolen	Ensure the data is encrypted		Data become useless if can't be decrypted by 3rd side/thief
Natural disaster	Ensure the system have backup data/power		Keeping System/Server/Web Application available all time
DOS Attack	Install detection and protection from DOS Attack		Detect and prevent the attack before it happen
Human	Team member training. Ensure the system have multiple layers authenticator for login information		

2. Assigning Responsibilities

Name	Role	Responsibility
Lê Trần Minh Quân	**Team Leader**	Planning and defining the scope of the project for each member in the team. Always keep communication in the team and make the team's keep focus on the main goal. Developing schedules, setting the meetings between the supervisor and the team to discuss the project.
Nguyễn Hoàng Nam	Technical Leader	Researching about technical structure to apply on the project. Assigning tasks and motoring members.
Vũ Tiến Anh	Tester	Responsible for collecting logs, including set-up,attack testing run and error recovery, test results recording.
Nguyễn Tài Đức	Data Analyst	Responsible for analyzing, collecting the data and writing reports.

3. Describing Procedures and Schedules for Accomplishment

The objectives of the risk management plans mostly are to for the most part handle the risks by identifying the risk and provide generally appropriate solutions to minimize risks to the minimum in a major way. Here is the recommendations procedure in a generally big way:

1. **Recommendation** : Hardening System
2. **Proceduce**:
   - Create a backup for server and database.
   - Check update operating system and software
   - Update firewall policies.
   - Create a business continuity plan, recovery plan.

4. Reporting Requirements (yêu cầu của báo cáo)

4.1. Present Recommendations (đề xuất hiện tại)

We separated our recommendations into 2 section :

- Internal recommendation :
  - Cause: Human threats: Users, hackers, etc.
  - Risk :
    - Hacker Attack
    - System out of date (hacker can take advantage)
    - Hardware Error
    - Weak / no firewall or protection
    - System misconfiguration
  - Recommendation:
    - Hardening System
    - Install and configure system firewall and authentication/authorization
    - Update and backup system frequently
- External recommendation
  - Cause : Uncontrolled factor , Human
  - Risk : Social Engineering , Pandemic , Disaster
  - Recommendation :
    - Backup data frequently and have back up server to run system
    - Training team member about security awareness

4.2. Document Management Response to Recommendations

Recommendation	**Accept**	**Postpone/Defer**
Backup data frequently	✔	
Backup server	✔	
Training team member about security awareness	✔	
Hardening System	✔	
Install and configure system firewall and authentication/authorization	✔	

5. Tools and Practices (các công cụ thực hiện)

1. Linux
2. Virtual Machine
3. Windows 8.1
4. Wireshark and Snort