Lab – Assess Risk with DREAD

Objectives

In this lab, you will use the DREAD risk assessment model to assess risk.

Part 1: Using the DREAD Scoring System to Assess Risk

Part 2: Using the DREAD System to Assess the Risk of a Described Vulnerability

Part 3: Reflecting on the Use of the DREAD Scoring System

Background / Scenario

DREAD is risk assessment model used to quantify risk related to security threats and to quantify potential risks. It is not a vulnerability assessment tool, but it is part of the risk assessment. They differ because risks are vulnerabilities that have been evaluated in the context of an organization based on previous attacks. The same vulnerability may present vastly different levels of risk depending on the nature of the organization. There are 5 categories used to compute the result:

- Damage Potential – If the threat is exploited, what is the damage potential?
- Reproducibility – How reproducible is the vulnerability?
- Exploitability – How difficult is it for the vulnerability to be exploited?
- Affected Users – What is the scale of the attack? How many users are affected by this vulnerability?
- Discoverability – How difficult is it to discover the attack?

There are multiple ways to score the DREAD risk assessment model. Microsoft uses a scoring system of 1, 2, or 3 with 3 indicating the high risk for each category (STRIDE). However, for this lab, we will be using the scoring system described by OWASP at the following link:

https://www.owasp.org/index.php/Threat_Risk_Modeling#DREAD

OWASP uses a scoring system of 0, 5, or 10 for each category with 10 indicating a more serious risk, and 0 indicating no risk. Discoverability is the only category that offers an additional option of 9. It is important to refer back to this document when scoring each category for Part 1 of this lab.

Required Resources

- PC or mobile device with Internet access

Part 1: Using the DREAD Scoring System to Assess Risk

For this lab, use any news website or popular and reputable website that reports technology related news.

a. Navigate to the OWASP DREAD link: https://www.owasp.org/index.php/Threat_Risk_Modeling#DREAD

b. Read through the DREAD risk classification system and how to score each of the categories.

How would you score a threat that requires advanced programming and network knowledge to exploit it?

_____

How would you score a threat that if exploited would cause complete system or data destruction?

_____

How would you score a threat that anyone can find the details on how to exploit by using a search engine?

_____

Part 2: Using the DREAD System to Assess the Risk of a Described Vulnerability

Use the following scenario to assess the risk of a threat using the DREAD risk assessment method. Refer back to the OWASP DREAD link as needed for the details of how to score each category.

Jose is a security engineer for XYZ Corporation and has just discovered a threat with an IoT device. XYZ Corp uses IoT devices in their manufacturing facility for monitoring and management of a wide variety of equipment. Jose was searching the Internet for vulnerabilities for one of their IoT devices which indicated a firmware vulnerability. The details of how to exploit this threat were clearly documented and it appears that the exploit could cause the loss of individual user data. The exploit requires a couple of commands for any authorized user who connects to this device. It appears that any web browser could be used to launch the attack but if exploited it wouldn't affect any users directly.

Indicate your score for each of the DREAD categories:

Damage Potential: _____

Reproducibility: _____

Exploitability: _____

Affected Users: _____

Discoverability: _____

What is the Base Score for the vulnerability described above?

_____

Part 3: Reflecting on the Use of the DREAD Scoring System

How should an organization handle a threat with this score?

_____

_____

_____

How could this scoring system be improved?

_____

_____

What are some of the features or advantages of the DREAD system?

_____

_____