Seminar 2 – Student Notes – Zihaad Khan

The industry selected is the ICT and Technology sector. The author is part of a team responsible for several servers that runs on various applications to provide unified communications services to clients. The servers mentioned mostly run-on Linux operating systems. The 3 threat modelling techniques selected are as follows:

1. Abuse Cases
2. STRIDE
3. CVSS (Common Vulnerability Scoring System)

This written piece will attempt to summarize the above techniques as well as provide some mitigating controls in light with the authors experience:

Abuse Cases

Abuse Cases, which is also commonly known as Misuse cases can be described by means of two examples. The first being a cyber-criminal that can use a brute-force technique to obtain root/administrator credentials to a system. The second example is that of malicious staff that currently has access to systems, their motives could include the deletion of sensitive data (Danso, 2021).

Some mitigating techniques for Abuse cases could include:

1. Creating strong password and passwords policies
2. Enabling Multi-factor Authentication
3. Implementing Account Lockout policies

For malicious staff the following would be applicable:

Root/Administrator credentials should only be reserved for system owners. These passwords should be protected by a password management system that maintains elevated privileges as well as session recording activities. An approval process could also be effective i.e., when a user requires to make a change on a production system, approval is granted via the password management system (by the user's manager) for a specified period.

The STRIDE method

The STRIDE method comprises the following (Shevchenko, 2018):

Spoofing - a user pretends to be another (fake identity)
Tampering - cyber attackers modify components or code (data integrity)
Repudiation - threat events are not logged or monitored
Information disclosure - data is leaked or exposed by individuals
Denial of service - services are overloaded with traffic to prevent normal use
Elevation of privilege - additional privileges are granted to gain greater control over a system

The CVSS Method

This Method captures vulnerability scores (ranging from 0-10, with 10 being the worst) and translates them to Low, Medium, High, and Critical areas. This is commonly used in the Authors industry as many servers will undergo vulnerability scans before being added into a production network. Once the results of the scans are obtained, servers will need to be remediated by following the solutions or remediations steps provided by the respective Vendors (FIRST, 2021).

References

Danso, S. (2021) Launching into cyber security [Lecturecast]. LCYS_PCOM7E August 2021 Launching into Cyber Security. University of Essex Online

FIRST - Forum of Incident Response and Security Teams, Inc. (2021). https://www.first.org/cvss/specification-document [Accessed 5 September 2021]

Shevchenko, N., Timothy A C., O'Riordan, P., Patrick S T., Woody, C. (2018). Threat Modelling: A Summary of Available Methods. Available from: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf [Accessed 05 September 2021]