Date: 6 September 2018
To: Romcholo Macatula
From: Cyber Warriors
Subject: Technical Memo 1

1 Summary

Our client, General Dynamics Mission Systems (GDMS) exists as a defense contracting company with a focus to provide innovative solutions to their customers. As cyberspace becomes a more prevalent area, GDMS looks to develop a model to provide cost effective preventative measures. The team shall create an analytic model that identifies the risks of privilege escalation to meet their main objective. Cyber attacks exist as a prevalent threat to private corporations today.

2 Client

The team shall create a deliverable for the client General Dynamics Mission Systems. General Dynamics exists as an American aerospace and defense multinational corporation. John Phillip Holland founded the company in 1899. General Dynamics began as a boat and submarine manufacturer and since expanded to manufacture combat, marine, aerospace, and information systems. General Dynamics evolved over their 119 year life span to support modern defense needs. When air became a new military domain and air superiority became an essential defense need, General Dynamics responded with successful jet fighters and other weapons systems. Today, modern defense involves a new domain, cyberspace. General Dynamics responded to the need for cyberspace defense and incorporated cybersecurity into their information system business segment. This project shall fall under the information system business segment of General Dynamics and contribute to the cybersecurity aspect of that segment [1]. The team shall work with Tim Rabideau, a product development and technical lead at General Dynamics. Rabideau works in the department of Computer and Network Security and he shall mentor the team for the duration of the project.

3 Objective

The objective for this project requires the development of an analytic model that assesses the risk of compromised networks via privilege escalation or lateral movement. The model shall gauge the level of threat an attacker poses if they gain access to a vulnerable area of the network. The team shall create a model with these factors: time privileged account passwords left unchanged, time account active, usage of the account, number of hosts/applications with same credentials, total number of hosts and applications in the network, criticality of the application, and levels of account privilege [2]. To scope the problem, the team shall determine factors to hold constant, such as operating systems and the method of exploitation. If done well, the model shall shift cyberspace defense away from more traditional techniques focused on detection, to more proactive measures that focus on prevention.

4 Problem Importance

Cyber attacks exist as one of the top threats to private corporations today. Privilege misuse exists as the second-most frequent cause of security incidents and the fourth-most common cause of data breaches, in accordance with the 2016 Verizon Data Breach Investigations Report [3]. These data breaches and security incidents cause detrimental effects on a business or corporation. This model shall use analytic techniques to address the risks to an enterprise based on the availability of vulnerable privileged accounts. The economic costs to detect these attacks and respond in an affective matter cost a great amount. General Dynamics Mission Systems focuses on the development of prevention techniques that would reduce cost and lead the way in identification of the best practices for cyberspace defense.

References

[1] *https://www.gd.com/about-gd*, September 2018.

[2] T. Rabideau, *General dynamics: Cybersecurity*, Project Details 2018, (2018).

[3] Verizon, *2016 breach investigations report*, tech. rep., Verizon, 2016.