CONCEPTUAL FRAMEWORK TO IMPROVE CONTROL AND VISIBILITY IN PRIVILEGED ACCESS

Asanka Weerasinghe

A dissertation submitted in partial fulfilment of the requirements for the MSc in Cyber Security and Forensics degree at the University of Westminster.

School of Computing

Informatics Institute of Technology
In Collaboration With
University of Westminster, UK

2022

Abstract

It has become very difficult for organizations to properly defend their crown jewel assets with the increase in targeted and complex security threats by both external attackers and malicious insiders. The defending task of these assets has only grown tougher as infrastructures have become more complicated and extensively spread across geographic locations and in the cloud. The common thing in many high-profile breaches is that they have accomplished by compromising a password. In most cases, attackers have begun by hacking the password through social engineering techniques and then the privilege have been escalated to gain access to more privileged accounts. Attackers always get the advantage from “low level of visibility across privileged access” in organizations to hide under the radar and easily go undetected for weeks or even months, compromise information they seek. With the increase of threats organizations have become much more vulnerable to potential data loss and damage. The risk of protentional compromise have increased due not only lack of understanding of how privileged accounts function, but also not understanding the risk associated with their compromise and misuse.

Unfortunate factor is that majority of organizations not understanding of their current level of security, in order to increase the security level. Even though, there are multiple standards to follow, there is a requirement of single framework to measure their active state with guidance and process to step into next level. With the “Privileged Access security framework”, it allows organization to define the current state of privileged access security and improve their security level to next step according to industry standards. The framework will allow organization to gradually increase their security level and decrease risk level with the step-by-step approach. After defining the current state, the step-by-step approach will help to constrain the adaption according to their budget.

Keywords: Attacks, Privileged Access, Cyber Security, Framework