INVESTIGATION INTO NEW METHODS OF SECURING SERVICES WITH SIEM ALERTING

Author Mark Deegan
Southeast Technological University

Abstract

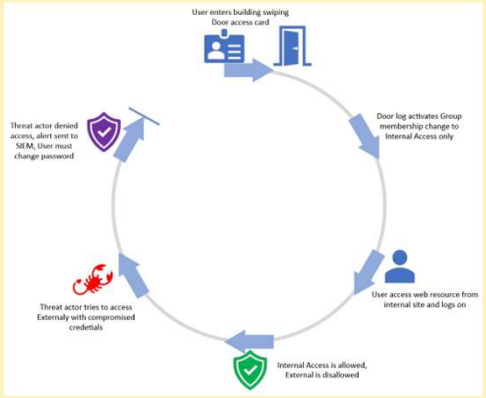
This study is based on the integration of disparate systems to enhance the overall security stance of any given infrastructure. Taking the information that is already collected by the physical access system and utilizing that information to automatically modify a user's group membership within active directory, should allow for faster identification of compromised credentials. This will allow logging and alerting when an invalid user attempts access from a location that the valid user is not within. Ideally this would shorten the time to detection of compromised user's credentials and should further strengthen the zero trust architecture within a system and create a novel transparent third factor authorisation for the access to a web resource.

Introduction

To develop a new authentication system when there are so many out there such as client certificate, multi-factor authentication (MFA), One Time Password (OTP), Remote Authentication Dial-In User Service (RADIUS), is to be competing with a sea of contenders. What seems to be missing from all of these mentioned methods is what happens once you are past the authentication process? What happens when the credentials are compromised, and an intruder is actually utilising them for network access? How would you identify the intruder in your system when the authentication process has completed successfully so no alerts have been triggered? How do you stop this kind of threat actor and intrusion vector? This study will attempt to do with authorisation what is not possible with authentication alone. By utilizing dynamic authorisation for access to resources, it should be possible to block access based on other variables rather than just that the perimeter authentication was successful. The study should identify when an intruder has compromised an accounts login details, block access to sensitive resources, log the event and trigger an alert. It will not be as cut and dry then as the usual pass or fail that is used with traditional login methods but will instead leverage other factors such as the RFID tag used to gain access to a building to verify a location for the user and prevent threat actors from remotely accessing data, or from internal threats, who access a user's account when they are not present within the building. To this end I have broken up the introduction into several parts for ease of digestion. In each section, I will describe the different areas I am addressing with my research study. By the end of the study, I will hope to demonstrate a new area of research using existing infrastructure to prevent unauthorised access to web resources and to report on whose credentials were used in a breach attempt.

Methodology

When approaching this kind of project, it is important to note what would simulate a real-world application of this method. To this end, I used a Raspberry PI to simulate the RFID door entry, a Microsoft Virtual server for the active directory and the Kemp Load Master for Load balancing the target application. Utilizing the raspberry PI, which is doing the card swipe, I was able to read the ID from the card and leverage Python to run a PowerShell script remotely to change group membership of the user in active directory. This changed the user from External only group member to internal only group member. This disabled all external access and only allowed internal access to the web resource. The Load Master was setup with group steering on its Edge Security Pack which examines the group membership of the user before allowing access.

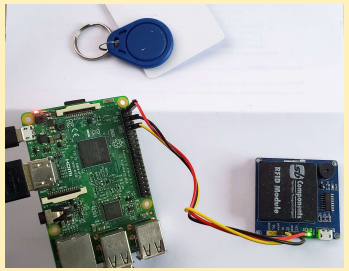


Results

First Test, Internal user, External threat.
In this example we are going to use John Doe as the user that is going to be logging into a web resource. The user in this scenario will be coming into the office during normal working hours and will swipe in the door using his RFID tag. The group membership is then to change and then the user should be allowed normal access to the resource. Meanwhile an external threat actor will attempt to login from outside while the user is at work and should be denied access, have their IP logged together with the compromised identity used in the breach attempt. This should all be logged to the SIEM. This method requires nothing extra for the user to do to secure his identity and will warn the SOC of the intrusion attempt utilising a critical alert. Thus, the timeline for events is as follows,

- User John Doe enters building swiping his access card.
- Transparent to the user this action changes group membership of the user from "External" group to "Internal" group.
- This activity is logged into the SIEM via syslog from the RFID reader.
- When the user gets to his desk he logs in and attempts to access the web resource.
- The DNS points to the Load Master for DNS resolution of the web resource and as it is an internal request the user is sent to the internal virtual service.
- Due to ZTA, the ESP is set up for the web resource forcing all users to login again.
- The Group membership is read by the ESP single sign on system and his connection is directed to the correct web resource.
- This activity is logged in the ESP logs.
- The user goes about his tasks unaware that his group membership has changed or that his location has been logged.
- Now an external threat attempts to access the web resource using John Doe's account. His credentials have been disclosed by another mechanism outside of the scope of this research.
- The DNS points the threat actor to the external Virtual service on the Load Master.
- Using the correct credentials, the external threat actor logs on via the ESP SSO page.
- The group membership is read as internal, but the source is external, this directs the threat actor to a "Server unavailable" page and his source IP is logged, and the identity logged to the SIEM as a critical alert.
- This then prevents further access to the system by the treat actor and the indication presented is that the server is down rather than they have been detected. This is a kind of honey pot feature and allows more in-depth analysis of the threat actors actions.

The results were positive and shows that it was possible for the user to have their group membership modified using the RFID tag and the python script detailed in the design. The user gain access to the web resource without issue and the "threat actor" attempting access with valid credentials was successfully prevented from accessing the web resource and the details of the attempt were forwarded to the SIEM with a critical error message. On a side note, the physical raspberry Pi was sending to the syslog a line with "none" in the message after every one second loop. This can be safely ignored and does not affect the function of the system. A filter could be setup on the syslog server to drop all of these entries or the code changed to not log every loop. For testing purposes on the proof of concept, I will proceed with these log entries.



Conclusion

The study demonstrated that it was possible to prevent threat actors utilizing compromised credentials to gain access to a web resource while improving the security stance of a system by leveraging existing infrastructure in a novel way. That this method can be integrated using many vendors solutions and requires no one manufacturer to deploy the concept to site, means the concept is vendor independent and can be leveraged to a higher or lesser degree by the IT security team as desired.

In successfully demonstrating the denial of intrusion attempts, allowing correctly identified individuals to gain access and having a log of each event clearly identifying the compromised credentials shows a huge benefit to overall system security. The honey pot being particularly useful in differentiating between valid and invalid access attempts with the same credentials.

The focus of the study was proven in our testing, and taken as an additional security practice, can improve the overall security of a system or network. This is worth further study and could be integrated to many more systems and lead to more secure access for the end user. The automation would also reduce the overhead associated with managing a new Multi-factor Authentication system and with the end user not being required to enter yet another token or password means the ease of deployment also is a bonus to implementation.

Additional lines of research identified while undertaking the study showed that there is room to advance this type of integration of security systems with dynamic group membership at its core. Leveraging the authorisation system to be location aware, delivers more secure access for the end user, less administrative effort for the security staff and greater assurance of identity while preventing intrusion attempts.

The heavy lifting of the Identity and Authentication systems in securing access can now be augmented by the Authorisation systems to improve control of access to resources beyond what is traditionally considered or deployed with standard access control methods. At its core it is a concept that could greatly enhance security of any given web service. Variations can be as unique as the network they are deployed into and should integrate whatever system or network an organisation has.

The definitive nature of the Accounting where the critical event supplies the Security Operations Centre with details of the user ID and source IP in the breach attempt and the alerts that can be generated make it very useful to both security teams and in the subsequent threat analysis.