Marshall Eddy

CS332-002

Vincent Skimmer

22 February 2017

Port Scanning

Whenever someone needs to access information on a network drive but do not have the right level of access to read and/or modify the item. This can happen at the most inconvenient time and they would need to get a hold of a system administrator to grant them the right level of privileges. This is rather annoying for all parties involved. There are reasons why there is access control and that is what will be discussed in this paper.

Access control is essentially identifying a person doing a specific job, authenticating them by looking at their identification, then giving that person only the key to the door or computer that they need access to and nothing more. Access control models have four flavors: Mandatory Access Control (MAC), Role Based Access Control (RBAC), Discretionary Access Control (DAC), and Rule Based Access Control (RBAC or RB-RBAC).

The Mandatory Access Control, or MAC, model gives only the owner and custodian management of the access controls. This means the end user has no control over any settings that provide any privileges to anyone. Now, there are two security models associated with MAC: Biba and Bell-LaPadula model is focused on the confidentiality of information. Biba is a setup where a user with low level clearance can read higher level information and a user with high level clearance can write for lower levels of clearance. The Biba model is typically utilized in businesses where employees at lower levels can read higher level information and executives can write to inform the lower level employees. Bell-LaPadula is a setup where a user at a higher level can only write at that level and no lower, but can also read at lower levels. Bell-Lapadula was developed for government and/or military purposes where if one does not have the correct clearance level and does not need to know certain information, they have no business with the information.

The role Based Access Control, or RBAC, model provides access control based on the position an individual fill in an organization. So, instead of assigning Ron permissions as a security manager, the position of security manager already has permissions assigned to it. In essence, Ron would just need access to the security manager profile. RBAC makes life easier for the system administrator of the organization. The big issue with this access control model is that if Ron requires access to other files, there has to be another way to do it since the roles are only associated with the position; otherwise, security managers from other organizations could possibly get access to files they are unauthorized for.

The Discretionary Access Control, or DAC, model is the least restrictive model compared to the most restrictive MAC model. DAC allows an individual complete control over any objects they own along with the programs associated with those objects. This gives DAC two major weaknesses. First, it gives the end user complete control to set security level settings for other users which could result in users having higher privileges than they are supposed to. Second, the permissions that the end user has are inherited into other programs they execute. This means the end user can execute malware without knowing it and the malware could take advantage of the potentially high level privileges the end user possesses.

The last control model is the Rule Based Access control, RBAC or RB-RBAC. Rule Based Access Control will dynamically assign roles to users based on criteria defined by the custodian or system administrator. For example, if someone is only allowed access to files during certain hours of the day, Rule Based Access Control would be the tool of choice. The additional “rules” of Rule Based Access Control requiring implementation may need to be programmed into the network by the custodian or system administrator in the form of code versus checking boxes.

Access Control is a very important part of information security, especially within a business. If someone was given inappropriate access, they might end up bringing the entire system down because they saw a thumb drive in the parking lot, or clicked on a phishing link sent in an email and infected all the computers on the system, potentially taking weeks to recover everything. In my mind, Access Control is essentially to prevent dumb people, or just people who do not know any better, from ruining everything. It is also a way to keep certain confidential files a secret, because most people in a business should not have access to payroll or social security numbers.

References

<http://resources.infosecinstitute.com/access-control-models-and-methods/>