AD Silver Cookbook - Public Comments on Jan 2012 Draft

Objective

The objective of this article is to collect individual comments on the AD Silver Cookbook during the public comment period.

Comments

Comments are presented raw with no editing unless needed to "protect the innocent"...

1. Make it less scary - start out the introduction with a statement that everything doesn't have to be done at once, and with an estimate of the number of FTE involved over some amount of time to get the changes done.
2. Remove "draft" and put a note in at the beginning that says that although no one has been certified using this approach yet, it is a best effort to determine what would need to be done to configure the AD portion of an environment to pass the audit. Once an institution has passed the audit and been certified using this approach, change that wording.
3. Note that this is a starting point, but any institutions wishing to assert Silver should undertake to thoroughly understand the IAP and IAAF documents in relation to their own systems, with a broad understanding of the implications for those systems. The cookbook should not be taken as a manual for achieving Silver.
4. I think the cookbook is laid out very well with strong consideration for the security risks in AD.
5. One suggestion is that there is some mention of the need to change passwords after disabling LM Hashes. As you may already know, disabling LM Hashes in Group Policy only prevents future passwords from being stored this way. Existing passwords/user accounts will not have the LM Hash removed or overwritten until the next password reset. Without being aware of this, new institutions joining the validation program may have a period of 90 days or more (depending on password expiration policy) with remnant LM hashes on their Domain Controllers.
6. Add a change log to the end with dates for each version.
7. The AD Problem Statement in section 4.2.5.1 Resist Replay Attack states that “Kerberos, NTLMv2 and secure LDAP binds or LDAP binds using SSPI/Kerberos do provide resistance to replay attack.” However the mitigation section gives instruction on how to mitigate NTLMv2. Why would NTLMv2 need to be mitigated if it already provides resistance to that attack? Is that supposed to be NTLMv1?
8. Similarly, the AD Problem Statement in section 4.2.5.2 Resist Eavesdropper Attack states “Kerberos, NTLMv2 and secure LDAP binds or LDAP binds using SSPI/Kerberos do provide resistance to eavesdropping or brute force attack.” If we mitigate LM and NTLM1 authentication is that sufficient or do we still need to proceed with one of the two strategies under “All eavesdropper mitigation?”
9. Add a scoping statement that says that this is a theoretical approach and must be carefully applied to the AD environment at your institution, taking into consideration all aspects of the IAPs and IAAF, with regard to the specifics of your environment: A big picture of “this is silver for our campus-wide AD” versus “this is silver for this research specific domain”. I think you are going for the former but it’s good to know where you are coming from in this cookbook.
10. In 4.2.3.4, the discussion of variable salting (and mitigation for the lack of it) relies on the assertion that a well-known salt does not add to the entropy much, because it is predictable. But adding entropy to the individual hash is not the reason for a variable salt. With a static salt, an attacker in possession of the password database and the salt can attack the entire database simultaneously. With a variable salt, the attacker must try to crack each password individually.