It rather required being on the other side of this airtight hatchway: Knowing the domain administrator password

devblogs.microsoft.com/oldnewthing/20231010-00

October 10, 2023

Raymond Chen

A security vulnerability report arrived that went roughly something like this.

> If a system's built-in local administrator account is not a domain administrator, but the local administrator account's password matches that of the built-in domain administrator account, then that local administrator can connect to a domain controller, and it will grant the user domain administrator privileges, even though that user is not actually a domain administrator.

What's happening here is that when you connect to another system on the same domain, Windows will use your userid and password to connect to that system, on the theory that the other system will honor your userid and password, seeing as it's part of the same domain.

The finder argued that this shows that the attacker can gain domain administrator access without knowing the domain administrator password. All they have to do is match their userid and password to those of a domain administrator.

But wait. If the attacker can match the userid and password to those of domain administrator, then this contradicts the claim that the attacker doesn't know the domain administrator password. You need to know the domain administrator password in order to match it! The local account is just a decoy. The attacker doesn't need it. They can just log into the domain controller directly with the userid and password they already know.

This is like saying, "I can open the victim's luggage combination lock without having the code. All I have to do is change the combination lock on *my* luggage to match the victim's. Now I can use *my* luggage lock code to unlock *the victim's* luggage!" Well yeah, but the "change the combination lock on my luggage to match the victim's" step implies that you do know the victim's luggage code. Otherwise, how did you manage to match it?

In this particular case, the userid is "Administrator". The Best Practices for Security Active Directory recommends restricting the built-in administrator account to physical access, so that it cannot be used remotely at all.

Now, if the attacker is someone who was able to take over the account of a local administrator by exploiting some other vulnerability, then it's true that the attacker could use the local administrator account as a stepping-stone to the domain administrator account, but only if the domain administrator is stupid and not only left the domain administrator password enabled for remote access, but also reused their domain administrator password as their local administrator password.

Mind you, even if the passwords didn't match, the attacker might still be able to gain domain administrator access if the local administrator had saved the domain administrator's password in their credential cache. Or the attacker can just sit and wait for the local administrator to enter the domain administrator password in order to do some domain administrative thing, and then take over the session. Once the local administrator account has been breached, the attacker can do anything the local administrator account can do. If you set up the local administrator account so it also has domain administrator access, then you opened a hatchway from one ship to another ship, and you shouldn't be surprised that people who get onto the first ship can use that hatchway to get to the second.