It rather involved being on the other side of this airtight hatchway: Administrator attacking a domain account on the local system

devblogs.microsoft.com/oldnewthing/20230110-00

January 10, 2023

Raymond Chen

A security vulnerability report came in that said that a local administrator can attack the system and sign in on the local system as a domain account without knowing the account's password.

So far, no security boundary has been crossed. The attacker is a local administrator, and a local administrator already has full control over the local system.

While it's true that the administrator has compromised a *domain user* account, this ability to act as the user does not extend outside the local computer. You have control over the domain user account on the local system, but other computer systems will recognize you for the fraud that you are.

In other words, the attacker has gained nothing. They started as a local administrator, which gives them full control over the local system. They then attacked a domain account, which gives them all the powers of that domain user on the local system. But this is a *subset* of the powers they had as an administrator! Nothing was gained.

This compromise of the domain account on the local system does not extend to other systems, so the attacker gained no privileges on other systems.

The finder even acknowledged in their report that the compromised account is not recognized by other computers on the network. I'm not quite sure what vulnerability they were reporting. I mean, maybe they're just saying that they found something interesting, but "interesting" doesn't mean that you have a security vulnerability. Really, all they did was find a way to do something the hard way. The easy way is to just use your existing administrator powers.