Attacking Local Account Passwords

blog.netwrix.com/2022/10/27/attacking-local-account-passwords

Joe Dibley

Learning how attackers target weak domain account passwords is not enough for Active Directory security. Let's look beyond domain accounts and understand the ways adversaries attack local accounts on Windows servers and desktops. For this post, we will focus on the most important local account: Administrator.

The Administrator account is built into every Windows operating system and provides full control over the system, including the ability to compromise domain accounts through Pass the Hash and Pass the Ticket attacks.

Handpicked related content:

Netwrix Webinar | Why Weak Passwords Pose a Serious Threat — and How to Reduce Your Risk

The Administrator account is vulnerable to password attacks for two reasons:

- There is no lockout policy for the Administrator account. Microsoft notes that this makes the account "a prime target for brute-force, password-guessing attacks."
- Administrator accounts often share the same password, so if you can compromise one account, you can often reuse the password across other local accounts in the environment

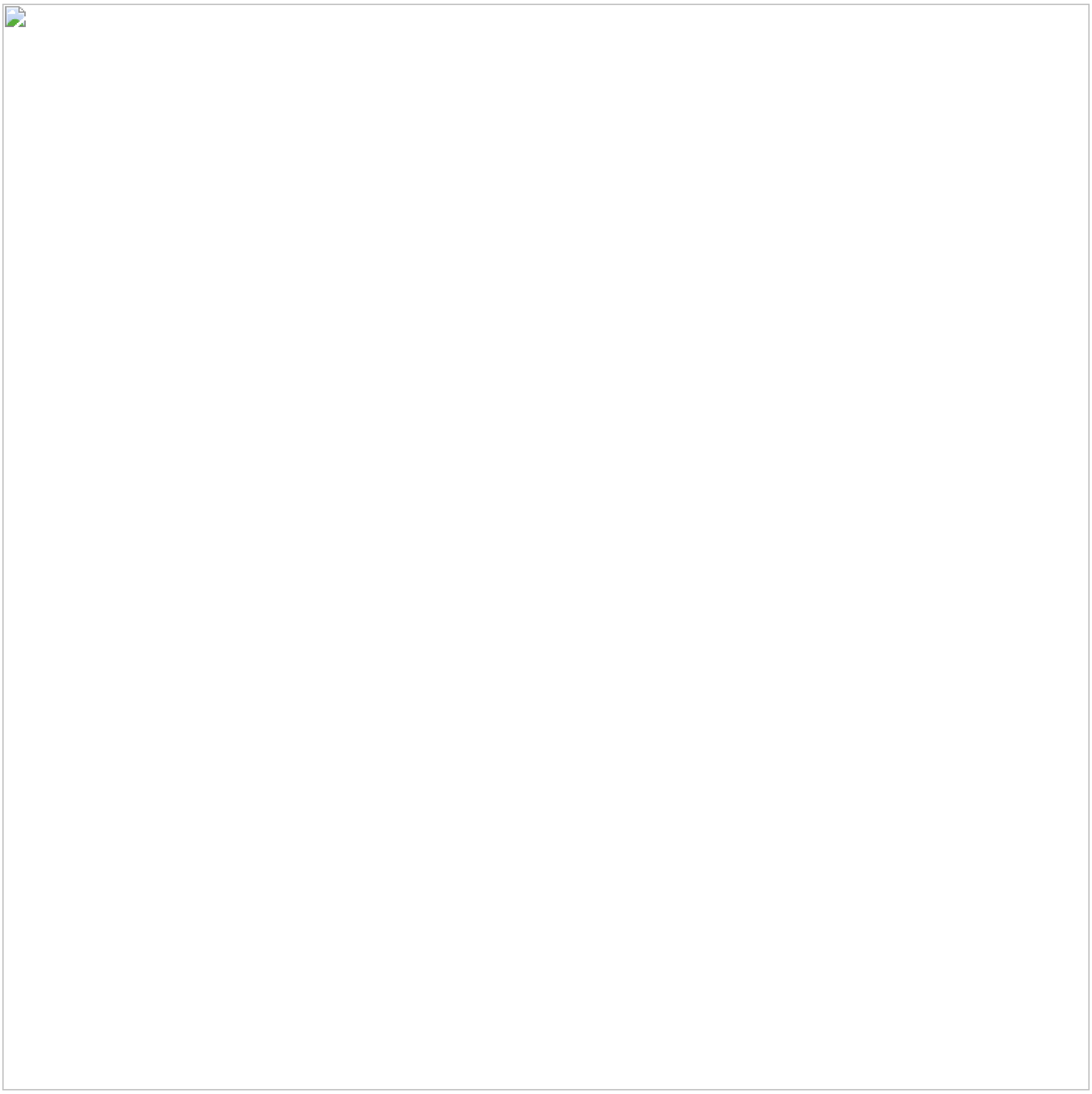
Let's walk through a typical attack against the Administrator account using a popular tool, CrackMapExec.

Step 1. Guess the plaintext password using a brute force attack

Because the Administrator account has no lockout policy, it is possible to make unlimited guesses of the account's password. Using password lists like the SecList collections, an adversary can craft a custom list of well-known passwords to use to try to log on using the Administrator account.

To create a more targeted attack, they can enumerate the password policy on the target systems. This will reveal the minimum password length and password complexity settings, so they can limit their list to viable passwords only. Issuing this command against a member server or workstation will return local policy information.

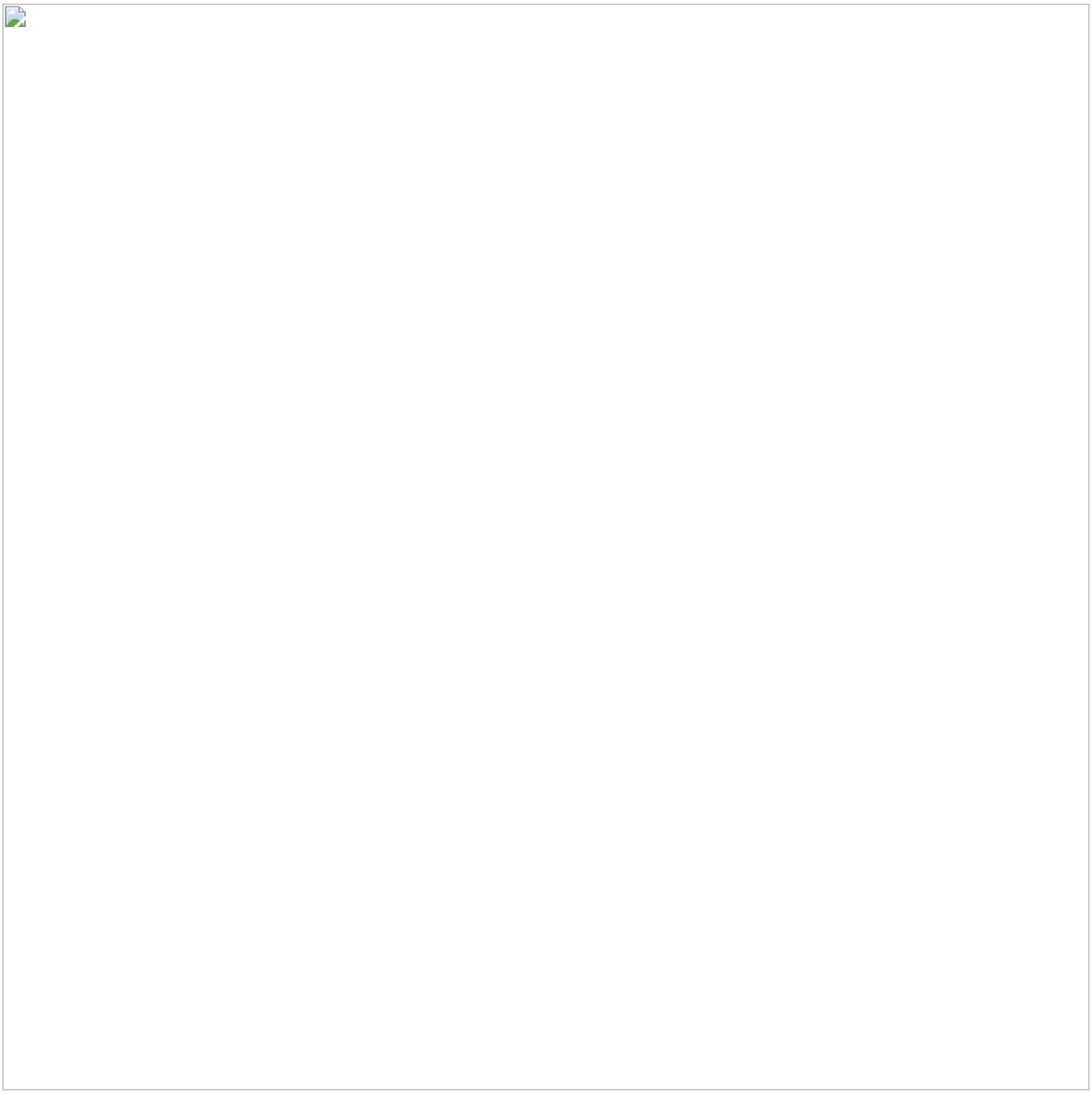
```
cme smb [hostname or list] –u [username] –p [password] –pass-pol
```



Enumerating the local password policy options of a target server with CrackMapExec

Once the adversary has a list of likely passwords, they can use the following command will run a brute-force attack against the local Administrator account, testing each password in turn:

```
cme smb [hostname or list] –u Administrator –d builtin –p [password list]
```



Brute-forcing the Administrator account using CrackMapExec

Here you can see I clearly exceeded the local account lockout policy of 10 bad passwords but was still able to compromise the plaintext password of the Administrator account.

Step 2. Use the password to spread laterally to other systems.

With the password for one Administrator account in hand, adversaries may try using the same password on other systems in the environment. This strategy is often successful because it can be difficult to set and manage different passwords for the Administrator account on each endpoint. Therefore, attackers move laterally from the initial machine to a large number of machines very easily.

Defense strategies

Fortunately, there are several effective ways to protect against password attacks on local Administrator accounts. One option is to disable the account entirely and create a new administrative account in its place.

Another strategy is to use Microsoft’s Local Administrator Password Solution (LAPS) to automatically randomize the Administrator passwords across domain-joined computers and store the secrets centrally in Active Directory. This can guarantee that passwords are long and complex, and not reused across computers, which minimizes the risk of successful attacks.

A third defense is to use Group Policy to deny network logon for all local Administrator accounts. This will help prevent password replay attacks from succeeding.

How Netwrix can help

Secure your Active Directory from end to end with the Netwrix Active Directory Security Solution. It will enable you to:

- Uncover security risks in Active Directory and prioritize your mitigation efforts.
- Harden security configurations across your IT infrastructure.
- Promptly detect and contain even advanced threats, such as DCSync , NTDS.dit extraction and Golden Ticket attacks.
- Respond to known threats instantly with automated response options.
- Minimize business disruptions with fast Active Directory recovery.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.