Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

MANAGING AND CONTROLLING ADMINISTRATIVE PRIVILEGES

JULY 2020

ITSAP.10.094

A user with administrative privileges has more control (to either modify, customize, or erase data) over a computer system, or network than a regular user. Often, organizations assign these elevated privileges to general user accounts. This practice gives outside threat actors (as well as unintentional and malicious insiders) another way to compromise an organization's networks. When your organization better manages and controls its administrative privileges, it can reduce its exposure to common cyber threats.

HIGH-VALUE TARGETS

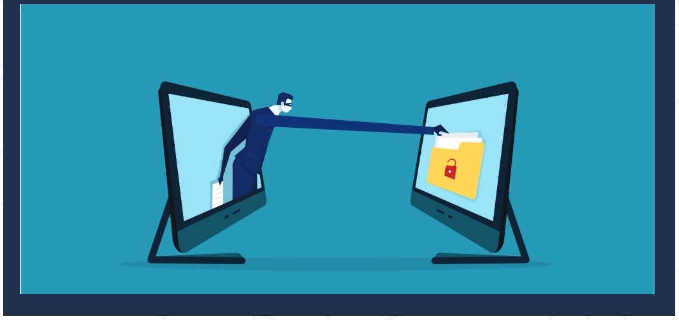
If threat actors gain access to an administrative account they can use the elevated privileges to affect your organization's operating environment, attack your network, and access sensitive information. Attackers can also learn which detection and recovery activities are in place on your systems, helping them avoid discovery and preventing you from stopping further attacks.

TECHNIQUES TO ACCESS ADMINISTRATIVE PRIVILEGES

Cyber threat actors use different techniques to gain entry to networks and systems. Compromises often result from normal user activity, such as opening emails or visiting websites. Threat actors may also take advantage of known vulnerabilities to elevate their privileges, or use stolen credentials to access administrative accounts.

Some common attack methods leading to administrative account compromise include:

- **Malware and phishing:** A threat actor gains access to local or domain administrative accounts when a user (who has administrative privileges or is signed in as an administrator) opens a malicious email attachment or visits a malicious website.
- **Brute force:** A threat actor uses automated tools to randomly guess common password combinations.
- **Privilege escalation:** A threat actor exploits a vulnerability to gain access to an elevated level of privilege in the information system.
- **Pass the hash:** A threat actor exposes a user's hashed authentication credentials (usually a password) on a compromised workstation. These credentials are passed around the network and allow the threat actor to move laterally through a network. When credentials have been hashed they have been changed from readable data into scrambled characters using an algorithm.



AWARENESS SERIES

CONSIDERATIONS FOR SECURING YOUR ORGANIZATION'S ADMINISTRATIVE ACCOUNTS

When assigning administrator accounts or privileged access to users, your organization should take the following measures:

- Apply the principle of least privilege (i.e. giving the minimum amount of access required for a user to complete their tasks)
- Create separate non-administrative accounts for non-administrative functions like checking email
- Use strong authentication methods
  - Use multi-factor authentication for all administrative accounts
  - Use a unique password for each privileged account
  - Change default passwords for applications and devices
  - Authenticate users before they are granted access to applications or devices
- Ensure that unique, identifiable accounts are attributed to individual users
- Log and monitor actions on privileged accounts
- Provide training on expected behaviours for privileged account users
- Delete and remove special access privileges when users no longer requires them

REMEMBER

Threat actors are not only interested in gaining access to administrative accounts; they want to gain access to as many accounts as possible, including regular user accounts.

When your organization manages and controls administrative accounts and privileges, it creates an operating environment that is stable, reliable, and easier to support. Proper access control and account management means that fewer users can make significant changes to the operating environment. In other words, when users only have access to the systems and the information required to perform their job functions, your organization is better protected from not only outside threat actors looking to gain control of privileged accounts and exploit networks, but unintentional and malicious insider threats as well.

ADDITIONAL PUBLICATIONS

The Cyber Centre has additional guidance related to managing and controlling administrative privileges. These publications include:

- ***ITSM.10.189*** *Top 10 IT Security Actions to Protect Internet Connected Networks and Information*
- ***ITSAP.30.032*** *Best Practices for Passphrases and Passwords*
- ***ITSAP.10.003*** *How to Protect Your Organization From Insider Threats*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**